Julian Barnes (00:05):

Welcome, everyone. I'm Julian Barnes from the New York Times. I am going to introduce our speakers here as I ask them questions. But I want to remind you all that I can get questions from you right here on this lovely little iPad if you would submit them via the app or put them on Twitter with the #RNDF. So thank you for coming. I'm going to jump right into this and I'm going to start with Gen. Paul Nakasone, the Director of the National Security Agency, the Head of U.S. Cyber Command.

Julian Barnes (00:49):

Gen. Nakasone, you've spoken a lot about the changing strategic environment that we face here. And at this conference, we've already been talking a lot about China and China's been a cyber challenge, cyber threat for a long time. Want you to talk a little bit it about how that strategic environment has changed in your time as in command and talk to us a little bit about the challenge of China.

Gen. Paul M. Nakasone (01:17):

I think we'd all agree, it's nice to be back at Reagan and in-person. 2019 was the last time I think all of us were there, in fact, many of us were on a panel. And so to come back here, I think not only is it striking to be back in the presence of all of you, but the other piece of it is think about how much the world has changed in two years. And nowhere has that world changed more than in cyberspace. Think about what we've seen as a nation over the past 11 months. We've seen SolarWinds, Colonial Pipeline, Microsoft Exchange, KBS... I mean, JBS, Kaseya.

Gen. Paul M. Nakasone (01:49):

We've seen ransomware, we've seen implants, we have seen proxy forces. This is in 11 months. But to your question, Julian, what I would say is that what I've seen over three years is really three things. First of all, is the realization that we have to compete in cyber space. That we can't stay and be passive, we have to compete because our adversaries are competing. Secondly, is the role of influence. We began the influence piece in 2018 with Russia Small Group and a focus on a safe and secure election.

Gen. Paul M. Nakasone (02:25):

Our adversaries have moved on from elections to other topics upon which they're trying to create influence operations. And truly, the last piece is I think that what we've learned is that it's all about partnerships. We succeed through partnerships. Our partnerships internal to us begin with the National Security Agency in U.S. Cyber Command, tight partnership. But it's broader than that's, it's working with private and history like Alex in terms of what we can be able to do. It's working with obviously the services, the interagency. This is the piece that makes us successful. It's also the same piece that's going to make us successful against China.

Julian Barnes (03:02):

I'm now going to turn to Adm. Michael Gilday, the Chief of Naval Operations. Earlier in your career, you were the head of the Navy's cyber operations, the 10th Fleet. As you prepare the Navy for the future, linking all your vessels together, how are you thinking about the cyber domain and both for defending those ships and those networks, and fighting in the cyber domain in the future?

Adm. Michael M. Gilday (03:31):

Cyber's inextricably linked to everything. It might be a bit heretical to say this, but is its own domain when it is so interconnected with everything and everybody. And so with respect to the Navy, we have to be able to connect things at long distances. And we have to be able to be connected to a joint force, so maintain that synergy, that we're known for and that we succeed because of. And so, one of the biggest efforts that we have undergoing right now and my number two priority is a task force called Overmatch.

Adm. Michael M. Gilday (04:10):

The focus of overmatch is to provide a software-defined systems of systems, networks of networks that allows us to transmit any data over any path. And to get it to microprocesing applications at the far end for one big reason, decision advantage. The ability to decide and act faster than the other guy. And so, whether it's the Chinese, the Russians or anybody else that effort is making great strides, number one, mostly due to the capabilities that exist right now in the private sector. And leveraging the good work that's going on in industry, particularly small companies that have allowed us to harness that technology to turn it quickly to experiment, fail fast, regroup and to double down.

Adm. Michael M. Gilday (05:03):

And so I do think, to your point with your question, that has to may that has to be a central concern of not just the Navy, but the joint force going forward. That we're able to use each other's data in a way to put us in a position of advantage against any adversary.

Julian Barnes (05:23):

Dr. Alex Karp is the co-founder of Palantir and the Chief Executive. Dr. Karp, how can the private sector better help to counter the cyber threat, better work with NSA, better work with the military? What do we need to do to make these partnerships more robust?

Dr. Alex Karp (05:46):

Well, thank you. I'm hugely honored to be here on stage in front of people who serve our nation. And Palantir, most of our customers are commercial, most of our revenue doesn't come from intel and defense and we're pretty global. I think, first, part of our history was both being born in Silicon Valley, and then leaving Silicon Valley. I think the first thing industry needs to do is affirm that if it's going to work with adversaries, it should always supply at least as good a technology to our services and the people who are defending our nation, which in the past has not been the case, always.

Dr. Alex Karp (06:25):

America, one of the things that we forget because it's so obvious to us, to the rest of the world, but often not to us is in software, America is the number and one nation in the world, far none. There is really no number two. Number two is Israel because there has to be a number two, but we are number one. I spent a lot of my life abroad, I did my dissertation in Germany and I get people baffled all over the world asking me how can it be that America is so much better at this than we are?

Dr. Alex Karp (06:58):

Take Germany has a lot of smart people, but the delta between what America delivers in software and what everyone else delivers is very wide. And so the key question for me is, how do we make sure that people doing the most important work in the world like people on the stage have access to the resource

we already have? Some of that is educational, people who are in industry and leadership positions must tell their employees, "If you are developing software in this country, you are going to give it to the people on the stage and people in this room, and explain why."

Dr. Alex Karp (07:37):

That I think is actually the most important thing. There's a lot of interest as you see from the opening remarks of leveraging industry and hardware and software. The U.S. government has moved from a government that bought software in a way that was hard for people who built software to supply namely off PowerPoints, to being the leader in the world and buying software that actually works. This is an enormous shift and no other government in the world that I work with and we work...

Dr. Alex Karp (08:07):

We don't work obviously in certain countries, but in the Western world, we're almost in every country has made this shift. So that if you want to supply software to the U.S. government, you will show it working in the real world. Which means that we're in an iterative cycle in a way that no other country is. And then there's the cultural, why is America so good at software? Well, we actually play fair in teams. We have highly technical people, we're goal-oriented. And we are willing to admit we're wrong and not be stained by failure when we screw up.

Dr. Alex Karp (08:43):

So I think what we need to do is continue on this trend. I think U.S. government officials should really say loudly to people they want to work with who are developing software, that they must supply the best software in the world to them. I think we in industry... By the way, it's often framed as you framed it, but I would say from my vantage point, there are certain technical issues like how do you do AI at the edge? How do you actually create an all-encompass environment, which is what we're doing with a lot of industry in the Western world, but where the data is segmented.

Dr. Alex Karp (09:20):

So if you have a global industry, you're not going to be able to hit the data store in France, Korea, America, because of regulatory issues. These are challenges that the U.S. government understands very well and has made great efforts to solve that industry doesn't understand yet. That industry is not yet even actually aware of its existence of. And a lot of our reason we've done well is we've understood these things early. So I think the kind of interaction is working. It could work a lot better, but there is also a lot of responsibility on U.S. industry to step up and do more.

Julian Barnes (09:54):

We'll get into some of those issues in more depth in a little bit. I want to turn the floor to Mike Gallagher, who is the U.S. representative, a U.S. representative from Wisconsin. Don't want to shrink to state, is the-

Rep. Mike Gallagher (10:07):

Really the U.S. representative.

Julian Barnes (10:10):

And the co-chair of the Cyberspace Solarium Commission. Mike, you've been talking about the cyber threat from China, specifically some alarms about Taiwan. And I'm wondering, could a conflict over Taiwan begin with a cyber operation? Talk about what you're thinking there.

Rep. Mike Gallagher (10:34):

Short answer is yes, but I'd like to start with something that Dr. Karp said a few weeks ago, that I found very refreshing. Which is that American companies that seek to do business with China should be forced to disclose and defend their position. Forgive me if I paraphrase that inelegantly. I think that's absolutely correct, particularly in light of the recent changes that the CCP has made to exert near total control over the data that foreign firms have if they're operating in China. And in light of the fact that the risk of a confrontation over Taiwan is increasing, or at least the Navy continues to tell us that it is likely.

Rep. Mike Gallagher (11:17):

Adm. Davidson before he left said, "Within the next six years, it could happen." At one point in a hearing, the CNO agreed as well as the comment on the Marine Corps agreed. And I think the private sector is underestimating the extent of pain that would be involved for all Americans in general, but them in particular if that really comes to a head within the decade. And increasingly I'm convinced that corporate America is going to be forced to choose at a time when too many American tech companies are like resurrecting IBM's 1930s justification for doing business with Nazi Germany under the banner of World Peace Through Trade. That has to stop.

Rep. Mike Gallagher (11:54):

And until that stops, I think we're going to be behind the curve, because in such a confrontation, and I'll get to your point, Las Vegas rules would not apply. What happens in the Taiwan Straits would not be confined there. Not just because of the financial and economic escalation, but because I do believe that there would be an attempt to target our critical infrastructure here domestically in the United States. And I think we, and I include Congress in this have done a poor job messaging to the American people how much at risk we are to a devastating cyber attack if we confront the PLA over Taiwan.

Rep. Mike Gallagher (12:31):

Both in an effort to is economic pain on us, they could target our electricity grid, water systems, et cetera, et cetera. But also our entire ability to surge humans and weapons and other material to a fight, which we would have to do because we don't have the necessary forward forces right now, depends upon key logistics and transportation nodes that are owned in large part by the private sector. So our aerial ports of demarcation, our seaports of demarcation would be a target.

Rep. Mike Gallagher (13:01):

Look how much chaos was caused by the Ever Given blocking Suez. Imagine something like that in the Panama Canal. So I just fear we're not attacking this with a sense of urgency. I fear we're sleepwalking into a disaster that could define the course of the 21st century. And I feel like, unless we change course that we're going to lose. We're going to lose World War III before it begins, either through preemptive surrender or battlefield defeat.

Rep. Mike Gallagher (13:28):

And so I think we have to ask some hard questions, are we wargaming the financial and economic escalation? Are we wargaming the risk posed to the Homeland from a cyber attack for JADC2? And I salute the way in which the CNO's prioritized over match. But when is that going to be operationally capable? If it's not before 2025, that may be too late. And for other things, I just think the ultimate choice that a lot of American companies are going to have to make is between whether they want to do business with the U.S. government and the defense industry in particular.

Rep. Mike Gallagher (14:06):

Or whether they want to do business with a genocidal communist regime that as a mere matter of fiduciary responsibility is a massive, massive risk for them. Other than that, I'm an optimist.

Julian Barnes (14:18):

Okay. I actually want all three of our other panelists to react to Rep. Gallagher here. Gen. Nakasone, talk a little bit about some of these issues here. Is American critical infrastructure at risk in an initial conflict over Taiwan? Should we have... You've had hunt forward, defend forward teams in a variety of allied countries. Is this something that we should have in Taiwan now?

Gen. Paul M. Nakasone (14:53):

I agree with Rep. Gallagher's point about warfare in the 21st century. I think that borders mean less as we look at our adversaries. And whatever a adversary that is, I think we should begin with the idea that our critical infrastructure will be targeting. And I think that's why it's so important that we work that he led in the Solarium Commission to start looking at that very seriously. One of the things I would say a bit differently though, is the fact that I think we have made a very, very strong shift to starting to address this.

Gen. Paul M. Nakasone (15:23):

I see the changes that are taking place, and I've watched this now for over a decade. The fact that we have an executive order, the fact that all services are now starting to talk about, "How do I secure my weapons platform?" The fact that we're taking very, very seriously the partnership opportunities with the private sector in not only things like election security, but how do we look at the future? There's more to be done, I agree, but it's different, again, coming back to my point than it was in 2019.

Gen. Paul M. Nakasone (15:51):

There was no one that was really talking about the seriousness of what I hear talked about today, and more importantly, starting to address some of those issues.

Julian Barnes (16:01):

Adm. Gilday.

Adm. Michael M. Gilday (16:02):

In the opening forum this morning, there was a slide that was up. I thought it was quite illuminating that 70% of Americans now view China with strategic concern. And I think we need to leverage that. Certainly, the discussions on capital he'll reflect that concern. I think that we're seeing that in the National Security Strategy, we have an interim strategy now that's being developed or a more finalized

strategy that's being developed. The next National Defense Strategy, I think will double down on that. And I think we need, need to leverage that.

Adm. Michael M. Gilday (16:33):

The successes that Gen. Nakasone talked about would also include the interagency work that went on in support of our 2018 elections, in support of our 2020 elections. Not only as a joint force, our ability to intertwine cyber, his work into our conventional warfare areas, but also even perhaps even more importantly with respect to defending the country, is that cooperation within the interagency. Some of that you saw the grease of those wheels, I think were some of the authorities that we saw that were given to Gen. Nakasone, his teams in 2019.

Adm. Michael M. Gilday (17:13):

I would be more of an optimist than a pessimist about the direction that we're heading in. I do think, to Rep. Gallagher's points, we do need to be concerned and take it seriously. I don't talk to anybody that's not concerned about China and the parts that we have to take. I think for us, rolling into the new year and a new defense strategy, a budget that we presented, another one that's close to being delivered to this administration.

Adm. Michael M. Gilday (17:39):

I really do think that that forces us to focus on what we invest in, both in the here and now and for the future so that if anything, this bipartisan agreement about China being a concern helps us laser-focus on what's prioritized in terms of what we invest in to defend the country.

Julian Barnes (17:58):

Dr. Karp, after your CNBC interview a couple weeks ago, where you said, "American high tech companies shouldn't do work with China." What was the reaction? And are you moderating that a little bit by saying like, "At least do the work with the United States," or do you feel like a Google, a Microsoft shouldn't be working with the Chinese government?

Dr. Alex Karp (18:30):

Well, first of all, we're in our little myopic perch in the Valley, so I'll just... The background in the Valley is we've been fighting the Valley aggressively pretty much since we started our company in 2004. And we've been battling the Valley on two issues. One, it is my deep belief and the belief of my company that it's pretty odd to be able to sell your product abroad under very fair terms. Essentially because our allies are willing to go along with your pricing because they're being protected by people here, and then not ship your software to them, A.

Dr. Alex Karp (19:10):

B, I'm in very in favor of free speech. If people disagree with working with the U.S. military, great, they should be able to voice that. But you, as a leader should explain to them, I would hope what the history is of, especially the U.S. military. Not that I have to lecture anyone here, but surprising how many people I have to lecture in the Valley about the positive effects and what the world would look like without the efforts of people in the U.S. military.

Dr. Alex Karp (19:37):

But be that as it may, while they protest at my house every day and put barbed wire around our cafeteria. We at Palantir here, not just me, but engineers who are 22 fought through that to be able to do something that is more important than just working with the many companies we work with. And so we're already on the unpopular side. And by the way, we say in public what we say in private in this context, which we're also not supposed to do according to Valley rules.

Dr. Alex Karp (20:08):

So we're a little used to being unpopular. I actually had very minimal standard, which is lower... In the interview, I tell people in the Valley, "If you want to do something, that's your right. This is America by the way, fought for by people on the stage, but be that as it may. But you do have a responsibility to articulate what is it you're doing and why are you doing something with an adversary you're not dealing with U.S. government? That is your responsibility to this country and to everybody in the Valley for which I'm a prior," whatever. And that's what I believe.

Dr. Alex Karp (20:44):

I think there should be a most favored nation status i.e. America, and you should have to... And I also believe there's something wrong with not explaining to people what the backdrop is of the way in which the world works, but any case. But the key point for me is, why does it matter so much? It matters so much because the core differentiator in technology now for America is software. It's not just that we're not delivering candy toys. We are delivering the thing that we are the best at in the world, and the difference is not linear.

Dr. Alex Karp (21:27):

So it's not like we have a slightly better can opener than other countries. No, we have the can opener. And for whatever reason, it's very hard for other countries to do what we do. And that is our central advantage. I know from the way we built Palantir that we are constantly... Like in the commercial context, we constantly try to get the most complex IT projects in the world and put them in our platform. Why? Because that's our central advantage. We're bad at sales, but we're great at product.

Dr. Alex Karp (21:59):

So we want everyone to... If your central advantage is X, you cannot give that up, and we should not let people give it up. And if they want to give it up, they don't want to deliver, great stand on stage, go on TV. They all like being on TV more than I do. Explain why you're not going to give this to the army, the Navy, the NSA. Great, explain it. But you can't then not explain it.

Julian Barnes (22:25):

I want to call up a slide. This is another question from the Reagan Institute panel... Sorry, Reagan Institute poll that came up and talks a little bit about military capabilities. This is from the Reagan Institute's Annual Poll of Americans, and it's the perception of military capabilities. And it's not up here yet, but there are... I'm going to talk about it a little bit while we wait for it to appear. The-

Adm. Michael M. Gilday (22:59):

There it is.

Julian Barnes (23:00):

Excellent. Okay, good. I just needed to filibuster a little longer. As you're looking at this, I want to draw attention to a couple of the columns here. We have, when it comes to conventional weaponry, 45% of Americans saying, "The United States is the best in the world." Dropping to 39% when we're talking about high tech. And then 27% for cyber capabilities. And so, I want the panel to react to a couple things here. One, is the public perception accurate? Are we really just one of the best in the world?

Julian Barnes (23:48):

And if that is true, does that matter? Is it good enough to be one of the best or do you need to be the best? And I'm going to start with Gen. Nakasone.

Gen. Paul M. Nakasone (23:59):

We have to be the best, there's no doubt. When I look at this, my first thought is that I've got to do a better job of obviously communicating to the American public, I don't agree with that. I look at it right now and both as a director of The National Security Agency and the U.S. Cyber Command, there's no doubt in my mind. No doubt in mind to, Dr. Karp's point, One, and then two is a long ways off.

Gen. Paul M. Nakasone (24:22):

That's not to say that our adversaries have shrunk some of that military offset. But when you take a look at our capabilities across the world whether or not it's in foreign intelligence or whether or not it's effects, that's not what I would point it as.

Julian Barnes (24:38):

Adm. Gilday.

Adm. Michael M. Gilday (24:40):

The first thing that I'd say as I take a look at this slide is, don't bet against America. This is about capabilities. This is about the science of war and somebody's missiles that are a longer range than our missiles, so it's game over. End of war game, pencils down. That is not the case. It's as much about what we fight with as how we fight. How devilishly fiendish we can be in areas like cyber that give us an asymmetric advantage. Our people are the best in the world. And our job is to make sure that we not only harvest or attract and recruit the absolute best that our nation has to offer, but that we also retain them.

Adm. Michael M. Gilday (25:25):

I spoke earlier about the work that Gen. Nakasone led in 2018, and he led in 2020. It was phenomenal work, not just done with exquisite capabilities, but by incredibly well trained people.

Julian Barnes (25:40):

Rep. Gallagher, what do you think?

Rep. Mike Gallagher (25:41):

Well, I think this is the poll... Well, the poll accurately reflects the perception of the American people. But I think an accurate statement would be that we are the best in the world in terms of our offensive capabilities, but we have unique defensive problems given the nature of our open society and the prominent role that the private sector plays in controlling 80% of the critical infrastructure in cyber. So

the reality is a bit more nuanced than that. However, this makes sense. We've had a string of high profile cyber attacks from SolarWinds, Microsoft Exchange, Colonial Pipeline, an explosion of ransomware.

Rep. Mike Gallagher (26:18):

And I think just given the nature of cyber, your average American interacts with it in a way they may not interact with conventional weaponry and high-tech weaponry. It's more pervasive in Americans' daily life, so I understand it. But as you compare this poll, I think to the 2018 data, what you actually see is it's gone in the right direction. It's gone from 15% who thought we were the best in the world to 27%. I'll abandon my pessimism and my optimistic story would be that because of the work that Gen. Nakasone and his team have done, learning lessons from the 2016 election, applying that to 2018-2020, everything that CNO talked about, we're headed in the right direction.

Rep. Mike Gallagher (26:56):

We have a long way to go, but we're headed in the right direction. What concerns me, however, both Adm. Gilday and Gen. Nakasone referenced the fact that I think the single best thing we've done in cyber in the last five years has been to loosen the rules of engagement in order to speed up the decision-making process for cyber. And that was a joint collaboration between the legislative branch and the executive branch. That has been a great thing. We've unshackled Gen. Nakasone and his team to do what they need to do to defend us.

Rep. Mike Gallagher (27:31):

I know there are discussions underway right now to revise that process and make it more onerous and inject more people into the decision-making process for offensive cyber. I hope I'm wrong about that, but that would be a massive, massive mistake. Because if anything, we need to be looking at how we can build upon that success and further unshackle Gen. Nakasone and his team to do things. For example, you've talked publicly about how we need to get into the ransomware game. We've successfully recovered ransomware payments.

Rep. Mike Gallagher (28:04):

We should be publicizing that. Why not? It's not a covert operation, it's not escalatory. Why are we not publicizing that work to bolster our deterrent posture in Cyberspace? We should be doing that as frequently as humanly possible. And above all, we should do nothing to slow down the decision-making process. We don't want to go back to a world in which it's more difficult to get approval for an offensive cyber operation than it is to get approval for a lethal drone strike somewhere. And that was the case in many cases a few years ago.

Julian Barnes (28:39):

Excuse me, in-opportune cough. Gen. Nakasone, will you react to that? Do you feel that you are... Two things, one, the 2018 shift to push down more authority, did that make you more nimble? And is there any fear that that will be adjusted, ratcheted back?

Gen. Paul M. Nakasone (29:01):

I think Adm. Gilday hit on a really important point as he talked about the evolution of the policy process here. And really, it's the idea that it's more than just what the Department of Defense is going to do.

We're one aspect of it. It was, how do you bring along the interagency? And now I think to the point of when I think about going forward in the future is, how do you make sure the private sector is tightly woven into this? Because to Rep. Gallagher's point, our challenge with a broad attack surface on the defenses, how do we ensure all those 16 sectors of critical infrastructure? The bar is as high as it can be against our adversaries.

Julian Barnes (29:41):

Dr. Karp, I want your thoughts, but there's a question from the audience for you that I'm going to read off here. "You mentioned that the United States is number one in the world in software. How do you assess China's capability and rate of progress in that area?"

Dr. Alex Karp (30:00):

Well, there's in some ways linked. We have worthy adversaries. I have this long PhD in totally arcane topic that should have left me without a job. But one of the most useful things about the training was, to not turn the person you're critical of, author critical of into a caricature, and then render the caricature irrelevant. It's like, our adversaries, really all of them are super intricate, deep cultures with enormous technical and intellectual capabilities.

Dr. Alex Karp (30:53):

However, it happens in this one area that... And it's a long... There's a debate about who developed the computer and some people, but I think the real answer is, it was even the early developments of the computer with Von Neumann in the Manhattan Project. A lot of our capabilities go back to our ability to both work, bring highly intricate, some people would say batch-it-crazy people together under a roof to deliver excellence for not primarily monetary return in the near term. Of course later you could turn to a business and do well, but.

Dr. Alex Karp (31:32):

And that capability in this one area that looked like it would be one of many technical areas is the dominant area. And our issue as America is to simultaneously be aware of the adversaries, but also realize that to make this work, you have to focus on how do we raise our game to the best game we are? So when I look at that, I'm like, "Yeah, I know there are things," like projects we've worked on, just Project Maven as an example. I never know how much one's allowed to say, but there are insights in that project that are very unique and very much done in a way that is not understood and not done as well by others, including adversaries.

Dr. Alex Karp (32:17):

But we should be so dominant that nobody can even imagine we're not number one. As with the Manhattan Project, which I think should be our standard. We took a small group of people, interestingly, actually very few from Ivy Leagues. Almost everyone who worked on the project went to like a school in the Midwest and a bunch of people who are highly eccentric and developed something that was transformational. And de facto what we're doing in AI is equally as transformational.

Dr. Alex Karp (32:53):

And you need this combination between people that know the material, that's the people on stage, and people who can extend what they're doing. And also people, in my case, I'm really good at managing

really complicated, difficult people. And so that's what I do for a living. And then you get this thing where nobody can... And of course, there are these enormous... Where no one can imagine they're not number one, and that should be our standard.

Dr. Alex Karp (33:21):

And if that's the standard, and then most of the issues we have in America are not actually because of adversaries, it's because of internal divisions and not being able to agree on certain things. This is why the shift here agreement, America having consensus on anything is very powerful. And we haven't had that for lots of reasons you can debate. But we do have it now.

Julian Barnes (33:45):

Adm. Gilday, when we last gathered here at the Reagan Library, you talked about this constant cyber activity in the gray zone. The example you gave at the time was Russia, and I'm wondering, are we in a constant gray zone cyber battle with China at this time? And what's the nature of that?

Adm. Michael M. Gilday (34:12):

I think the gray space really are the global commons, and I think a day-to-day basis, I'm mostly involved in the maritime. But I see the Chinese and the physical looking towards the sea, Belt and Road, would be an example, what they've done to reefs, they've militarized reefs in the South China Sea. And so that happens and takes advantage of gaps and seems perhaps in international law or places where law doesn't exist, and they may gain slowly but surely going forward. I see Cyberspace as another global common that they also are involved in this same type of activity below the level of arm conflict.

Adm. Michael M. Gilday (34:55):

But certainly, flagrantly disregarding international norms, which really have been in place since Bretton Woods in 1944 and have really raised the tide of billions with respect to prosperity, with respect to literacy rates. With respect to immigration that not just the transfer of commerce, which I would argue floats on seawater, but also ideas. And so that's the contest in gray space, it's a global commons. And what we try to do in the Navy is operate forward, not just to be there with the Chinese, but to be in the way.

Adm. Michael M. Gilday (35:39):

And I think you need to be in the way, and I don't say that provocatively. I say that just as a matter of fact, because the coin of the realm in grace-based operations is attribution. We have to be able to attribute those actions that disregard are those international norms to them. And we have to do the same thing, obviously in Cyberspace that Gen. Nakasone can speak to much more eloquently than I.

Adm. Michael M. Gilday (36:04):

But I think it's reality, we have to be out there, we have to be taking advantage of allies and partners that are like minded for all the reasons that I spoke to earlier about international norms. And I think that the Chinese are isolating themselves through their behavior. People are not running towards them to be their friends. We are gaining trust with allies and partners, they're buying it. There's a big difference.

Julian Barnes (36:31):

Gen. Nakasone, I wonder if you could react to that a little bit. And maybe as you talk about it a little bit about what this cyberspace gray zone competition with China looks like now, how are you at cyber command working with the Indo-Pacific Command to make sure that the real world operations and the cyberspace operations are meshed?

Gen. Paul M. Nakasone (36:59):

Coming back to this idea of what's changed over the past three years. 2018 was a pivotal year for us in the sense that our department published a concept called Defend Forward. Same idea that Adm. Gilday, expressed, but the idea that we would operate in cyberspace outside the United States against our adversaries before they could do harm to us. At U.S. Cyber Command, we call that persistent engagement. The idea of both informing our partners and acting. And it's to Adm. Gilday's point, I like this idea of getting in the way, it's exactly about that.

Gen. Paul M. Nakasone (37:35):

That we operate in a domain where deterrence is about imposing costs, and imposing costs means that every single day you're operating against an adversary. Identifying what they're doing, attributing it, being able to send, as Rep. Gallagher, talked about hunt forward teams to different countries to be able to expose our operations. This is all part of it, and I think, what we have seen is things like, "Hey, let's publish the top 25 different pieces of malware that the Chinese have produced at an unclassified level. Let's share it with the broad public, just so they understand that, 'Hey, we know all about this.'"

Gen. Paul M. Nakasone (38:13):

And by the way, we'll sign our name to it as the National Security Agency, U.S. Cyber Command, CSA will sign up and the FBI will sign up to it. And then we have a series of partners that do that as well. And this brings the idea of you're getting in the way, to quote the Admiral's point. This is what it looks like today in terms of being able to ensure that our adversaries have a very, very difficult time to operate.

Julian Barnes (38:36):

Rep. Gallagher.

Rep. Mike Gallagher (38:38):

I quite like this idea of getting in the way, but it sounds very similar to the concept of deterrence by denial, which was the intellectual cornerstone of the 2018 National Defense Strategy. Which I thought was a great piece of work. But now what concerns me is that we are moving away from that intellectual framework towards what I presume the Secretary of Defense will talk about in a few minutes, which is this new concept of integrated deterrence. Which I fear is a buzzword that will justify cutting conventional hard power.

Rep. Mike Gallagher (39:12):

And what you need in the way primarily in INDOPACOM is conventional hard power in order for that denial to work. That's one concern. I agree with what the CNO said about China not making friends. I think in many ways, the Wolf Warrior diplomacy has backfired, although they're playing primarily to a domestic audience or an audience, Xi Jinping. However, I don't think we've made any friends with our recent moves in Afghanistan. I think a lot of our friends are questioning our resolve.

Rep. Mike Gallagher (39:43):

And what's interesting is they may not need friends to be successful in a Taiwan scenario, particularly, if they creatively leverage disinformation. You could imagine a disinformation campaign aimed primarily at Taiwan itself, the Taiwan... the military. You could imagine a flood of fake or synthetic reports designed to confuse and disorient. Fake chat over military communications. Think of the ways in which they could leverage new technology, deep fake technology. Could imagine a video of President Tsai surrendering before it even happened.

Rep. Mike Gallagher (40:19):

And for the international community or the non-aligned fence sitters in the region, if that was amplified by a disinformation campaign online or on American social media companies, pushing the narratives that this was all because of a provocation by Taiwan or PLA forces are being hailed as liberators. Well, they could confuse us long enough to be successful in a fait accompli. All they need is a little bit of a fig leaf to justify not getting involved.

Rep. Mike Gallagher (40:45):

And in that way, the CCP could drive various wedges through our united front in a Taiwan scenario. So, there are ways that they could be successful even if they don't have many friends in the region.

Julian Barnes (40:58):

Gen. Nakasone, there's a question from the audience, which touches on some of Dr. Karp's points, which are, how can the United States effectively deter in cyberspace, given that we're generally secretive about our country's offensive and defensive cyber capabilities?

Gen. Paul M. Nakasone (41:14):

I think the first point is that we have to look at it differently than we looked at nuclear deterrence. This isn't a binary yes or no. This is a domain that our adversaries, given the ability to move into this domain so quickly, are going to operate every single day. So we have to operate every single day. We have to have a spectrum of capabilities, everything from the defense to the offense, as you say. And certainly we have to be engaged with that. And I think that at the end of the day, this is how we have success. That we are going to impose costs in a number of different ways, and with the interagency and with the private sector.

Adm. Michael M. Gilday (41:51):

If I could just make one comment about that just to perhaps reinforce Gen. Nakasone's points, I don't think you have to take credit for everything. And I think that there's a certain advantage, whether if a U.S. team creates a certain effect against a certain adversary to lead that adversary guessing on who actually did that effect. Let them burn the resources to try and figure it out. And perhaps in the back of their mind, they're thinking, "Yeah, it could have been the Americans. It also could have been some rogue who thinks, who agrees with America. Or it could be another nation state, another like-minded nation state that took the action."

Adm. Michael M. Gilday (42:34):

I think as Gen. Nakasone, the point I'm trying to reinforce is the fact that it's not exactly like thinking about deterrence as years ago. And I think that there are ways that you can leverage information and powerful ways that we haven't fully explored yet.

Julian Barnes (42:51):

Rep. Gallagher, do we talk enough or too much about our cyber military capabilities?

Rep. Mike Gallagher (42:59):

Well, earlier I made the case that we don't talk enough. I guess I would respond by saying, I don't think the criminal groups are guessing after we launch attack against them, who carried it out in certain cases. It's obviously a mix, it obviously depends on the operation, but I think the big mistake we make, and I agree cyber deterrence is not perfectly analogous to strategic nuclear deterrence during the Cold War. In fact, we tease that out in the final report of the Cyberspace Solarium Commission.

Rep. Mike Gallagher (43:33):

But at the end of the day, we're trying to deter certain people and states from doing things. It's not like cyber deterrence exists in its own little world. We're trying to deter China, we're trying to deter Russia, we're trying to deter North Korea, and we're trying to deter Iran largely from doing bad things. It's a bit harder when you talk about criminal groups with opaque connections to state entities, but we are trying to deter decision-makers in those countries from doing stupid things that jeopardize our interests.

Rep. Mike Gallagher (44:08):

And so we can't talk about cyber deterrence as unconnected from other forms of deterrence or operating under its own unique rule-set. I think that the tenets of basic deterrence still apply. And as for an earlier strand of conversation, I was primarily talking about deterrence by denial. It's my observation that since we made a commitment to that in 2018, we have not implemented that commitment in any meaningful way. At least in our primary most important theater INDOPACOM, where I think we have a long way to go in terms of reestablishing deterrence before it's too late.

Julian Barnes (44:48):

The topic of the panel is also the future of warfare. And as I was thinking about this, I was wondering, in the future, does the special operations team that gets deployed to overseas, is it going to have a software engineer as a part of it? Is it going to have a couple people from Cyber Command with it? Or is it simply that those will be separate, but they will be as important to be equally nimble and forward deployed in the future? And I'm wondering, Gen. Nakasone... I'm going to ask all the panel this question as we wrap up. Gen. Nakasone, what are your thoughts?

Gen. Paul M. Nakasone (45:35):

Presence matters and we will be there. We're ready there. What have we learned over the past 20 years that we have our developers with our operators. We have them understanding what the issues are. We have our best operators with our elite forces and they have a number of different capabilities. This is not the future, this is now, and we're practicing it today.

Julian Barnes (45:56):

Dr. Karp, what do you think?

Dr. Alex Karp (45:57):

A wholeheartedly, it's like if you're talking about the symbiotic relationship between industry and government, then that has to have a micro component. And the micro component will be that you will have operators that are both technical and operators that are more kinetic and a spectrum. And I think the units will be small and very effective. And I agree, I couldn't say it any better.

Julian Barnes (46:24):

Adm. Gilday, any final thoughts from you?

Adm. Michael M. Gilday (46:26):

It's got to be a Swiss army knife. To reinforce the points that have already been made, it's got to be interoperable, it's got to be integrated. And it has to be generate effects that are technically feasible and operationally relevant. And you're not going to be able to do that quickly against a high-end adversary like China unless you're better integrated. So I think small teams going forward in the future are going to be tailored to different types of operations with exquisite capabilities and ways that I think we're completely open to and are doing it now, experimenting with how we get the biggest bang for the buck.

Rep. Mike Gallagher (47:04):

I agree with what Gen. Nakasone said about presence matters. I would argue that is enduring lesson from the old school of Cold War deterrence, so we can apply to the present day. And I think having spent a couple years on this commission, attempting to think about cyber issues, ultimately, I think it's still fundamentally human problem. Both our biggest failures are human failures and our success will ultimately be a function of whether we can convince the best and the brightest to work with our defense leaders to solve some very difficult issues.

Rep. Mike Gallagher (47:40):

And as Brad Smith alluded to in the first panel today, we're not where we need to be. But ultimately I still believe that we have out of very talented, smart patriots in this country that want us to win. That believe deep down that we're still the good guys. And that's absolutely true.

Julian Barnes (47:57):

I hope you'll join me in thanking our panelists.