UNITED STATES SENATE

TO RECEIVE TESTIMONY ON UNITED STATES SPECIAL OPERATIONS COMMAND AND UNITED STATES CYBER COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2022 AND THE FUTURE YEARS DEFENSE PROGRAM.

Thursday, March 25, 2021

Washington, D.C.
TO RECEIVE TESTIMONY ON UNITED STATES SPECIAL OPERATIONS
COMMAND AND UNITED STATES CYBER COMMAND IN REVIEW OF THE
DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2022 AND THE
FUTURE YEARS DEFENSE PROGRAM

Thursday, March 25, 2021

U.S. Senate
Committee on Armed Services
Washington, D.C.

The committee met, pursuant to notice, at 9:30 a.m. in
Room SD-G50, Dirksen Senate Office Building, Hon. Jack Reed,
chairman of the committee, presiding.

Committee members present:  Senators Reed [presiding],
Shaheen, Gillibrand, Blumenthal, Kaine, King, Peters,
Manchin, Duckworth, Rosen, Kelly, Inhofe, Wicker, Fischer,
Cotton, Rounds, Ernst, Tillis, Sullivan, Scott, Blackburn,
Hawley, and Tuberville.
OPENING STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE ISLAND

Chairman Reed: Let me call the hearing to order. Just to make everyone aware, we have four votes scheduled to begin at 10:45, so we will have to be, yeah, we will be very flexible.

But let me make my opening remarks, and then recognize Senator Inhofe, and then recognize our panel.

Good morning. Today, the committee meets to receive an update on the readiness and posture of both, the U.S. Special Operations Command and the Cyber Command.

Our witnesses are Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Christopher Maier; Commander of U.S. Special Operations Command, General Richard Clarke; and Commander of U.S. Cyber Command, National Security Agency Director, and Chief of the Central Security Service, General Paul Nakasone.

Both Special Operations Command, or SOCOM, and Cyber Command, are at the forefront of addressing the asymmetric information and technical challenges that transcend the boundaries of the geographic combat commands. I hope our witnesses will convey our appreciation to the men and women you represent and their families, for their dedication and sacrifice in carrying out many of our nation's most difficult and complex missions.
In 1986, when Congress created SOCOM, to ensure the readiness of Special Operations Forces, or SOF, it also established the position of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, or ASD/SOLIC, to be the service-like secretary tasked with day-to-day advocacy and oversight of SOF.

In recent years, Congress has sought to further empower the ASD/SOLIC and optimize the partnership with the commander of SOCOM through the annual National Defense Authorization Act. Unfortunately, the Department has not made sufficient progress in implementing these reforms, particularly with respect to hiring appropriate personnel and establishing a strong role for the ASD/SOLIC and all decisions relating to the organization, training, equipping, and readiness of SOF.

We are pleased Mr. Maier is joining us today as the acting ASD/SOLIC and look forward to receiving a nominee so the Department can have a fully empowered, Senate-confirmed civilian in this important position.

Mr. Maier and General Clarke, I hope you will provide your assessment of how this committee can help to ensure that the SOLIC reforms are both, fully implemented and effective, in their ultimate goal of supporting the SOF enterprise.

In recent years, there have been several incidents and
allegations of misconduct involving special operators that,
as General Clarke has noted, jeopardized the trust placed in
SOF. I applaud SOCOM for taking a hard look in the mirror
by completing a comprehensive review of SOF culture and
ethics last year.

Among other things, the review concluded that SOCOM
disproportionately focused on SOF employment and mission
accomplishment at the expense of training and development of
our force. In some cases, this imbalance has set conditions
for unacceptable conduct to occur due to a lack of
leadership, discipline, and accountability.

General Clarke, I am interested in hearing more about
the specific actions you have taken to address the findings
of the comprehensive review and what more must be done.

Turning to Cyber Command, General Nakasone, you have
been working to mature the cyber force, ensuring their
readiness, and overseeing the development of capabilities to
conduct defensive, offensive, and supporting intelligence
operations. I understand there are positive trends in all
of these areas, but the threat to our cybersecurity may be
advancing at an even faster rate.

Indeed, recent disturbing cyber intrusions and attacks,
likely conducted by Russia and China, will command attention
in today's hearings.

In the SolarWinds incident, hackers conducted a
sophisticated operation that installed a backdoor and a
software update that left approximately 18,000 enterprises
vulnerable to exploitation and attacks, including many
government agencies and companies that provide essential
goods and services. We have recently learned that a Chinese
entity exploited multiple previously unknown vulnerabilities
in the software running Microsoft Exchange email servers and
there are hundreds of thousands of these servers around the
world. After Microsoft announced the breach and issued
methods to protect it, multiple Chinese Government-sponsored
hacking groups rushed to compromise thousands of vulnerable
servers before they could be patched.

A third event that merits attention is the reporting
that China attacked the power grid in India during recent
physical clashes the Himalayan border regions.

General Nakasone, in the first two events, paid actors
exploited vulnerabilities to steal data. While some may
consider this tolerable and expected behavior from a
competitor nation, others view the scope and scale of these
operations as reckless and a different class that merits a
sharp response, and I am interested in your views in this
matter.

In the matter of China's attack on the Indian power
grid, which followed multiple Russian cyberattacks on
Ukraine's power grid, there is a sense of growing
willingness of adversaries who attack critical
infrastructure in any serious confrontation; again, I am
interested in your perceptions on this matter and if we need
to be concerned about our nation's critical infrastructure.

I, again, want to thank the witnesses for their service
and willingness to be here today, and I look forward to your
testimony.

Senator Inhofe, please?
STATEMENT OF HON. JAMES INHOFE, U.S. SENATOR FROM OKLAHOMA

Senator Inhofe: Thank you very much, Mr. Chairman.

Great statement. I appreciate that and for calling this important hearing to examine our posture of the U.S. Operations Command and the U.S. Cyber Command.

I also want to thank our witnesses for being here with us today. They are the right guys for this hearing.

My top priority continues to be ensuring the effective implementation of the National Defense Strategy. We have been talking about that at almost every meeting that we have. It prioritizes competition with China and Russia, while maintaining pressure on the global terrorist groups like ISIS, and I will have some specific questions on that at question time.

As I said on the floor on Tuesday, we need to match the budget with strategy. It takes at least 3 to 5 percent real growth in a defense budget above inflation. It doesn't look like it is going to be easy to get to that point. We are going to have to keep trying.

Military advancements and the expanding global ambitions by China and Russia impose new and increasingly complex challenges to our national security. In addition to growing their conventional military capabilities, China and Russia are expanding their use of irregular warfare tactics,
involving cyber disinformation, proxying their forces, and economic blackmail around the world.

They have proven these tactics are effective in places like Ukraine, in Syria, in the South China Sea, and now they are exporting them to Africa and to the Western Hemisphere.

As we discussed before, this reality makes implementation of the irregular warfare annex to the NDS critically important. It also requires that Special Operations Forces are organized, trained, and equipped to compete in this domain warfare.

At the same time, ISIS and Al Qaeda have proven resilient and still pose a threat. History has shown us without sustained pressure, that threat will grow. I think we all understand that.

I understand that President Biden is reviewing the U.S. counterterrorism policy, and according to media reports, has issued interim guidance, requiring the White House to sign off on operation, military decisions that were previously delegated to the DOD. And let me be clear, I have serious concerns with the decision to return to the Obama era policies that tied the hands of our military commanders and made it harder to keep pressure on ISIS and Al Qaeda. I expect this committee will be consulted often during the administration's review. I have talked to the President about this and I believe that is going to happen.
Another critical component of implementing the NDS is developing robust capabilities to counter growing threats in cyberspace. The 2018 Cyber Strategy provides a roadmap on how we are going to do this. Significant efforts have occurred in recent years across the DOD to implement the strategy and to build the capabilities of Cyber Command and the cyber mission forces.

Today, I look forward to our witnesses' testimony in addressing this critical, these problems that are out there, and we are going to do all that we can to try to solve that. So, I appreciate this hearing and I think we will all benefit from it.

Thank you, Mr. Chairman.

Chairman Reed: Thank you, Senator Inhofe.

Mr. Maier, please?
Mr. Maier: So, good morning, Chairman Reed, Ranking Member Inhofe, and distinguished members of the committee. Thank you for the opportunity to testify on our global posture for America's Special Operations enterprise.

I would also like to thank Congress and especially this committee for its strong support for the SOF community and its mission. I am honored to testify alongside General Clarke and General Nakasone, who have dedicated their careers to safeguarding our nation from complex and unconventional threats.

I would like to begin by acknowledging the service and sacrifice of our Special Operations soldiers, sailors, airmen, Marines, and civilians. Although SOF make up only about 3 percent of the joint force, over the past few years, this community that has bore over half of all U.S. combat casualties. Many more have sustained life-altering injuries and suffer psychological trauma.

As we look forward, Secretary Austin has outlined his three principle priorities for the Department of Defense. Those are: defend the nation, take care of our people, and succeed through teamwork. The SOF community will measure ourselves against these priorities.
Representing just 2 percent of the overall DOD budget, SOF played an essential role within the joint staff in advancing multiple strategic priorities for the Department and the nation. We continue to adapt the unique capabilities and problem-solving expertise of our special operators through the challenge of great power competition with Russia and China, while strengthening the alliances and partnerships that enhance our ability to compete.

As we innovate to compete more effectively below the level of armed conflict, we recognize that our counterterrorism operations, while still critical to protect the Americans from the likes of ISIS and Al Qaeda, must become even more sustainable and focused on the most pressing threats to our citizens and interests.

Enhancing the readiness and resilience of our SOF warriors and their families remains a top priority. Despite the COVID-19 pandemic, SOF have continued to maintain a high level of operational readiness. We remain focused on and are making progress in easing the strain of high rates of overseas deployments.

I look forward to working with you and your staff to collectively continue to build the resiliency and culture of this community that has given so much in protecting us for nearly a generation.

I also remain concerned about incidents of serious
moral and ethical failings within the SOF community, a concern I know General Clarke shares. I commend him and Special Operations Command for leading a comprehensive review of SOF culture and ethics last year.

Civilian-military partnership on all of these issues remains a key priority for me and my team. In response to Secretary Austin's challenge to us, we are also committed to enhancing diversity within the SOF community. As we compete against different and more capable adversaries, a more diverse force empowers us to draw upon broader perspectives, different-lived experiences, and new ideas.

Finally, we recognize the strong interest in Congress in empowering civilian leadership in the Department. We appreciate legislation in the most recent National Defense Authorization Act to codify and strengthen ASD/SOLIC's role. It is our collective duty to ensure these reforms meet your intents and serve the interests of the Department and the men and women of our SOF community.

Mr. Chairman, I would like to conclude by thanking the committee, again, for its strong support for our Special Operations team. Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Mr. Maier follows:]
Chairman Reed: Thank you, Mr. Maier.
General Clarke, please?
STATEMENT OF GENERAL RICHARD D. CLARKE, USA,
COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND

General Clarke: Chairman Reed, Senator Inhofe, and
distinguished members of the committee, thank you for the
opportunity, and I am honored to testify with Mr. Chris
Maier and General Paul Nakasone. Also joining me is Chief
Greg Smith, my command senior enlisted leader. Greg marked
his thirty-first year in uniform this month and I am
thankful for his continued counsel and leadership as he
represents the almost 50,000 enlisted operators in our
force.

USSOCOM, our structure, our authorities, and our
purpose are the direct outcome of Congress and, in
particular, this committee. We strive to honor Congress'
vision by training and employ the world's finest Special
Operations Force, a team that is inclusive and professional,
supremely competent and trusted, and reflective of American
diversity and values, and most of all, committed to our
constitutional oath.

The incredible women and men of this command employ
their unique skills globally, fully integrated with the
joint force, and aligned with national priorities. SOF
continue to detour and disrupt persistent threats by
terrorist and extremist organizations. Twenty years of this
fight have honed our capability and, most importantly, our
resolve.

We remain oriented on these threats with approaches that are both, effective and sustainable, to defend the homeland and our American people; additionally, we are well-postured within the joint force to compete against maligned state influence. SOF provide unique value in this critical endeavor.

Below the level of armed conflict, SOF teams support a wide range of U.S. policy objectives and generate options to counter China, Russia, and other competitors. Often, our activities to counter violent extremist organizations have tangible, derivative value to counter terrorist, extremist organizations.

As SOF forged partnerships and built partner capacity, we gain access, placement, and influence in contested regions. Should future conflicts arise, our modernization priorities will provide interoperable forces that are able to win as part of the joint war-fighting concept.

Your continued support and the vital trust of the American people allow this command to support the nation now and prepare for the challenges of tomorrow. Today, as we sit here, nearly 5,000 special operators stand vigilant in almost 60 countries. Their commitment to American security and prosperity is inspirational, and their enthusiasm to learn, adapt, and serve is infectious.
It is my honor to lead them and I look forward to answering your questions.

[The prepared statement of General Clarke follows:]
Chairman Reed: Thank you very much, General Clarke.

General Nakasone, please?
STATEMENT OF GENERAL PAUL M. NAKASONE, COMMANDER,
UNITED STATES CYBER COMMAND; DIRECTOR, NATIONAL SECURITY
AGENCY; AND CHIEF, CENTRAL SECURITY SERVICE

General Nakasone: Chairman Reed, Ranking Member
Inhofe, and distinguished members of the committee, I am
honored to be here and to testify beside Acting Assistant
Secretary Maier, and my good friend, General Rich Clarke. I
am joined today by CYBERCOM's senior enlisted leader,
Command Sergeant Major Sheryl Lyon.

Entering our Army as an Arab linguist, Command Sergeant
Major Lyon's 30-year career with airborne, special mission,
and intelligence and cyber units makes her uniquely
qualified to serve as USCYBERCOM and NSA's senior enlisted
leader.

Over the past year, I emphasized the importance of
defending the election against foreign interference. With
did this through the Election Security Group, a combined
team from U.S. Cyber Command and the National Security
Agency. We built on the lessons from earlier operations and
honored partnerships with the Federal Bureau of Investigations
and Department of Homeland Security's Cybersecurity and
Infrastructure Security Agency, sharing information with
those who needed it as fast as possible.

We also worked with the National Guard Bureau to create
a mechanism that enabled Guard units to share information
about incidents quickly, easily, and uniformly.

U.S. Cyber Command conducted more than two dozen operations to get ahead of foreign threats before they interfered or influenced our elections in 2020. Three points stand out to me. First, U.S. Cyber Command must be, and is, able, ready, and willing to act. Second, USCYBERCOM's partnership with NSA remains the foundation of our success. And thirdly, we enable our domestic industry allies and partners by providing critical-threat information and insights which improve their ability to act under their unique authorities.

I am proud of the work the Command and the Election Security Group performed as part of a broader government effort to deliver a safe and secure 2020 election.

CYBERCOM is building on a recent guidance from the Department seeking to promote readiness, improve training, and attract and retain high-end talent. Regarding readiness, CYBERCOM is improving its ability to monitor the status of forces provided by the services down to the team, mission element, and even individual levels.

CYBERCOM is expanding, enhancing the training that our personnel receive.

As the trailblazer for the Department of Defense's Cyber Excepted Service, the Command benefits from flexible hiring authorities to recruit civilian talent. Even with
COVID-19 impacts and lengthy security-clearance timelines, that impact to the entire Department, CYBERCOM has offered and was able to attract a number of high-end talent to our force.

Diversity is what makes us better. Extremism can tear us apart. Last week at Cyber Command, we held a Secretary of Defense-directed stand-down day. Extremism has no place in the Armed Services and must not be allowed to affect our cohesion or impact the security of the United States.

At CYBERCOM, I have strived to cultivate an environment where personnel are empowered to report abuses and reject participation in activities that demean or harass their co-workers or neighbors. We owe it to ourselves, our workforce, and our nation to set and be the example.

In closing, the cyberspace environment has changed significantly over the past 10 years. Adversaries are demonstrating a changed-risk calculus. They are undertaking maligned activities in cyberspace at greater scope, scale, and sophistication. They desire to take on the U.S. and cyberspace below the level of armed conflict.

To defend our securities and our interests in this environment, U.S. Cyber Command must continue to adapt, innovate, partner, and succeed against such adversaries. The men and women at Cyber Command are truly grateful for the support this committee and Congress has given to our
command.

Again, thank you for your support, and I look forward to your questions.

[The prepared statement of General Nakasone follows:]
Chairman Reed: Thank you very much, General Nakasone.

Let me make a few points as reminders. Again, at 10:45, we are scheduled to have floor votes and we will continue the hearing as we go back and forth and vote. There is a closed session after this hearing in SVC-217 and we will, as soon as we conclude, go to SVC-217.

This is a hybrid hearing, so the questions will be by seniority, not by arrival time, 5-minute standard questions, and please mute your mics so that we can have no disruption of the questioning.

Mr. Maier, again, what is the status today of the Department's efforts to empower ASD/SOLIC and what additional resources or authorities do you believe we need from the Congress?

Mr. Maier: Thank you, Chairman.

So, the current status is one that is SOLIC, as a standalone organization, both its policy components and its service secretary like our 922 component outside of OSB policy, Secretary Austin and Deputy Secretary Hicks are re-looking that to see if that continues to make sense. I think one of the potential options is to determine a way to better integrate the policy components that were removed from SOLIC towards the end of the last administration, back more integrated into policy, but under no circumstances, am I aware of any COAs that are being discussed that would
remove the service secretary-like responsibility from remaining a principal staff assistant and a directory port up to the Secretary of Defense. So, I think your legislation has been very clear on that point.

As to progress to date, we continue to make progress, I think, on building the capability, in many cases, in the form of expertise and people, on the components in that administrative chain of command. So, the SSO, or Secretariat for Special Operations, that was explicitly directed in the 2021 NDAA is something we built to about 40 people at this point and it includes a cross-section of experts from the budgeting world, the legislative world, the acquisitions world, really, the, if you will, the nascent or core group of people that will perform that service secretary-like function.

But we are not at the point, Chairman, of irreversible momentum at this point and we are not at the point of having something that is probably sufficient to do the roles that have been described in multiple NDAAAs at this point.

The last thing I will say is, I do think the relationship with Special Operations Command is very strong. One of the things that General Clarke and I benefit from of having worked together on multiple occasions in the past, and I think that leadership connection helps to ensure our staffs are proceeding in that direction of collaboration,
Chairman Reed: Thank you very much.

General Clarke, let me, again, commend you from conducting the review of culture and ethics. These are issues that every organization and, particularly, military organizations have to confront. Sixteen recommendations were generated by the panel. Without going into detail on every recommendation, can you highlight the key ones and the overall status of those recommendations, implementation-wise.

General Clarke: Yes, sir, I can, if I can get the mike working. Sir, the primary finding, as you pointed out, was, in fact, that the focus on overemployment and mission accomplishment led to the detriment in leadership accountability and discipline. To that end, with those 16 recommendations and the findings from that, our focus, first, was to the overall employment and how many forces were deployed as we looked at, and we conduct our own zero-baseline review of forces employed. And through that, have reduced the approximate SOF employment by about 20 percent.

But we also, probably most importantly, is reduced the amount of headquarters that were forward that put leadership forward, therefore, you didn't have the leadership that was back during the force generation so that the leadership was not engaged and present.
The other specific aspects that we have looked at is
the training of our forces as they go through the various
pipelines, but also our assessments to improve those. But
at the end of the day, Senator, it's about engaged
leadership to reduce the amount of incidents that SOF has
had in the past.

Chairman Reed: Thank you very much, General.

General Nakasone, SolarWinds, the Microsoft hack, they
don't appear to be the garden-variety type of back-and-forth
that we have seen from nation states.

Are we into a new era in which our adversaries are
conducting more and more aggressive attacks that are
designed to be just short of a redline that would trigger
some type of conventional response? Are we in new terrain?

General Nakasone: Chairman, I think that, as you point
out, what we have seen from both, the SolarWinds and the
Microsoft intrusions, is an increasing level of
sophistication. This is a scope, a scale, a level of
sophistication that we hadn't seen previously. This isn't,
simply, you know, email phishing attempts; this is the use
of supply chain or this is the use of vulnerabilities we
hadn't seen before.

In terms of this changing risk calculus for our
adversaries, their intent, obviously, we continue to
monitor, but for us, I think it is the Clarion call for us
to look at this differently. How do we ensure we have, as a nation, both the resiliency and the ability to act against these types of adversaries?

Chairman Reed: And we have structurally a gap between our civilian authorities and our military authorities that is being exploited by our adversaries?

General Nakasone: Chairman, for both of the intrusions, what we have seen, I think I would point out would be two critical areas that we need to address as a nation. First of all, as you point out, it is not the fact that we can't connect the dots; we can't see all of the dots. So, my authorities and my responsibilities, both as the commander of U.S. Cyber Command and as the director of the National Security Agency, are rightly outside of the country.

But in terms of internal to our nation, our adversaries understand our policies and our laws and the timing to be able to use our infrastructure to achieve access to these companies and have an impact.

Thank you very much, General.

Senator Inhofe?

Senator Inhofe: Thank you, Mr. Chairman.

I am going to go back to a couple of things that I referred to in my opening statement, and I know that, Mr. Maier, in your opening statement, you addressed this. I
would like to have a little more detail and maybe aim this
at both General Clarke and at you.

We all understand what history has taught us, that if
we take our pressure off of the terrorist groups, they are
going to rebuild and threaten and all that, so things have
to be done at the same time. And the two things that I am
concerned with still, and specifically getting into
resources and capabilities, trying to balance the NDS, and
of course we know what we are supposed to be doing there,
the requirements to modernize our forces to compete with
China and Russia, that is on one hand, but against the need
to maintain the pressure on ISIS and Al Qaeda, especially in
places like Africa.

So, do you really think that you have the resources
necessary to accomplish both of these?

And this is a place where you would want to come to,
because if you don't, we need to know about it. Would you
respond to that in some detail.

Mr. Maier: Ranking member, yes, I very much agree with
the idea that we have got to be able to do both and as I
think General Clarke referred to, in some cases, we can do
both with the same forces, but in a lot of cases, we can't.

I mean, in the case of Somalia, there were, as you
know, a lot of changes made over the last few months,
including moving forces out and there is a policy-review
underway now, looking at not only that decision, but how we ultimately posture our forces to ensure we have the right capabilities there and in other places.

And I think one of the benefits of the beginning of a new administration is, there are a number of posture reviews and a lot of assumptions are underway. And one of the key elements of that is just as you described, how do we weigh the need to continue to protect the American public, citizens, our interests against the Al Qaedas, and ISIS, and their affiliates that are still out there, even as we look to, in some cases, change our capabilities or our posture or our focus towards the peer competitors that we face.

So, this is something that I think I would be happy to drill down in more specifics as we go issue by issue or place by place, but I think my take on this is the counterterrorism fight is not over. The NDS says that, and I think that has been reinforced in the early reviews coming out of these policy reviews.

Senator Inhofe: Okay. Now, General Clarke, do you essentially agree with this?

General Clarke: Senator, I --

Senator Inhofe: Okay. Well, I think we have a mike problem there.

But let me go back. You brought up Somalia. Now, this taking some of our resources out of Somalia, going into
Kenya and some other areas, that was actually a policy of the previous administration and I disagreed with it at that time.

Now that we have already done this, Mr. Maier, what is your feeling now, was that the right move or was that not the right move? What kind of results are we getting now?

Mr. Maier: So, Ranking Member, I think we have a review underway right now that is weighing all of this. I think from my perspective, there is probably significant downsides to the pull-out from the perspective of cost and effectiveness, but that is my initial look, and this will have to be an interagency look, but that is something that is being looked at both, from the counterterrorism perspective and the broader, regional objectives we have in the Horn of Africa.

Senator Inhofe: Well, I would like to be in on that because I was pretty outspoken when that decision was made and I would like to see how we are doing on that.

This was brought up already by the chairman, addressing SolarWinds cyberattack, did the Chinese hack into Microsoft, and all that. We know those problems are there.

DOD began building a total of 133 CMF teams in 2012 and reached full operational capacity with over 6,200 cyber personnel in May of 2018.

General Nakasone, SolarWinds and Microsoft Exchange
cyberattacks demonstrate we are vulnerable, we have vulnerabilities out there. What authorities or resources do you need, again, it is kind of the same question I asked Mr. Maier, what resources do you need to accomplish what we have to accomplish, because this is the place you go to for resources.

General Nakasone: Ranking member, thank you very much for the question.

I think, first of all, just taking a step back, we as a nation right now, are taking a very hard look at both of these intrusions. I think there are two gaps that are being addressed right now that have to be addressed and one of them is this idea of information sharing. These attacks took place within the United States, these intrusions, and there are, right now, legal barriers and disincentives for the private sector to share information with the Government.

We have a difficulty, as a government, understanding the totality of the actual intrusion, so that is being worked. And the second piece is, as I mentioned to the chairman, we have an inability to see everything. So, we, as U.S. Cyber Command or the National Security Agency may see what is occurring outside of the United States, but when it comes into the United States, our adversaries are moving very quickly. They understand the laws and the policies that we have within our nation, and so they are utilizing
our own infrastructure, our own internet service providers
to create these intrusions.

The resourcing of U.S. Cyber Command right now to
include the 133 teams has been instrumental in us being able
to have an ability to act. And, certainly, we are looking
as a department, if further growth is necessary, we will
come back to the committee if that is a requirement.

But I would say the first two pieces, being able to
identify and being able to fix those areas, are part of the
resilience of the nation that has to be addressed.

Senator Inhofe: Okay. That is very good.

My time has expired, but we are interested and is it a
work-in-progress right now and you are making headway, I
assume.

Thank you very much, Mr. Chairman.

Chairman Reed: Thank you, Senator Inhofe.

Senator Shaheen, please?

Senator Shaheen: Thank you, Mr. Chairman, and thank
you to each of our witnesses.

General Nakasone, I want to congratulate you on the
work that Cyber Command did on the elections in 2020 and
your also mentioning of the National Guard. The Guard in
New Hampshire were very helpful in securing our election
there.

But as you point out, we still have challenges ahead
and the Defense Intelligence Agency's defense intelligence officer for Cyber, James Sullivan, recently asserted that Russia right now is clearly ahead and the more aggressive and practiced operator in information operations.

So, how should we, do we need more authorities to allow Cyber Command to respond to what is happening in Russia?

You talked about the gaps between the private sector and the public sector. Do we need cyber securities, someone who is going to coordinate the activities on both, the defense side and the private sector side?

What else do we need to do in order to respond to this threat?

General Nakasone: Senator, I think there are two pieces that are really important for us to continue to focus on regarding the threat. First of all, as I mentioned, the resiliency piece. We can have all the capabilities that we want, all the teams that we want, but if there is a hole in the bucket, and we are filling water, and the water is coming out faster than we can fill it in, there is a problem. And that is the analogy I would use in terms of our resiliency right now. We have to be able to see what is happening in terms of the broad depth of our nation.

The other piece is that we should understand what our adversaries are doing. They are no longer just launching their attacks from different parts in the world. They
understand that they can come into the United States, use our infrastructure, and there is a blind spot for us not being able to see them. Those are critical pieces.

The other piece that I would come back, in terms of your information operations question, that is something that both General Clarke and myself have taken on, and I think that you rightly point out that there is work that we have to do here. We have done a tremendous amount in terms of understanding and operating against adversaries to our election, but now we are in the area of great power competition. Is it the ability for multiple combat and commands, not just U.S. Cyber Command, but our geographic commands like European Command and INDOPACOM Command and U.S. Special Operations Command to harness the abilities that we have collectively against adversaries that are using information against us.

Senator Shaheen: So we have had, I remember several years ago we had a discussion in this committee about whether cyberattacks were an act of war and at what point we should consider them an act of war and we never resolved that discussion.

Is that a discussion we should get back to and should we change policy, with respect to cyberattacks on the United States?

General Nakasone: So, that is obviously a policy
question that I would leave to, you know, the policy experts in the Department of Defense and the administration.

In terms of my role in being able to ensure that the nation has capabilities and capacities, what we are focused on is ensuring we understand our adversaries, understand what our adversaries are attempting to do, and having the capabilities and the capacity to be able to get after those adversaries.

Senator Shaheen: Thank you.

I would argue, Mr. Chairman, that we should revisit that discussion in this committee.

General Clarke, there is a lot of debate right now about whether according to the agreement we made in Afghanistan with the Taliban, that we should withdraw our troops by May 1 and I have been an opponent of doing that because I question whether we have the capacity right now within the Afghan forces to be able to respond to the Taliban.

Can you give us an update on where you think the Afghan security forces are in terms of their ability to respond to the threat.

General Clarke: Senator, I was recently in Afghanistan and met with the head of their new, what they have stood up as a joint special operations command. While progress has been made, and I found a very dedicated commander in General
Aziz, I think one of the capabilities that the U.S. provides for the Afghans to be able to combat the Taliban and other threats that reside in Afghanistan are critical to their success.

Senator Shaheen: I find it particularly troubling that violence has increased on the part of the Taliban and in the last couple of months, we have had directed assassinations against civil society leaders in the country in a way that is clearly designed to take out the potential for leadership in the country if western forces withdraw.

Do you think that presents an added risk to Afghanistan?

General Clarke: Senator, it is clear that the Taliban has not upheld what they said they would do and reduce the violence. While, on the positive side, they have not attacked U.S. forces, it is clear that they took a deliberate approach and increased their violence since the peace accords were signed.

Senator Shaheen: Thank you.

Thank you, Mr. Chairman.

Chairman Reed: Thank you, Senator Shaheen.

Now, via Webex, Senator Fischer, please.

Senator Fischer: Thank you, Mr. Chairman, and thank you gentlemen, for being here today.

General Nakasone, I recall the 2015 Rose Garden
announcement with President Obama and President Xi that a common understanding had been reached to halt China's state-sponsored cyber theft of intellectual property. Over 5 years later, how would you assess that commitment and has China's actions matched its words?

General Nakasone: Senator, based upon what I have seen over the past several years that I have been in command of U.S. Cyber Command and as the director of NSA, I have seen the Chinese continue to utilize cyber activities below the level of armed conflict to steal our intellectual property, to steal our personal identification, and at times, attempt to influence our populous.

Senator Fischer: More specifically, did this agreement have any impact on cyberattacks against our defense industrial base?

General Nakasone: Senator, if I might, I would like to take that question for the record just because we are learning things every single day and I want to make sure that it is a fulsome answer.

Senator Fischer: Okay. Thank you.

What lessons have you learned from the experience, especially on how we can reduce this hostile cyber activity that we are seeing in cyberspace?

General Nakasone: So, I think the first lesson is that we should all take this as a wake-up call. That this is not
business as usual, as the chairman had mentioned.

These are adversaries that are operating with increased sophistication, scope, scale, and I mentioned sophistication of what they are doing.

The second piece is that this is about partnerships for us as a nation. How do we drive a better partnership between what the public needs and what the private sector can offer?

That information sharing that I mentioned is really critical for us to have success in the future.

And then the last piece is that we truly need to look at the ability for us to see ourselves and right now it is difficult for us to see ourselves because we have adversaries that are coming into our nation and being able to utilize our infrastructure very timely and very effectively against us.

Senator Fischer: Thank you, General.

General Clarke, your predecessor testified that, quote, our effectiveness over the last 15 years does not necessarily equate to success against near-peer competitors.

We also require urgent investments in capabilities necessary for denied battlefields of the future. This includes submersibles, terrain-following avoidance and all-weather radar, advanced electronic attack capabilities, countermeasures, and precision munitions. We must enhance
our effectiveness in partnership with these services, end quote.

Do you agree with that?

General Clarke: Senator, I do agree with that and I will tell you since General Thomas, my predecessor, made those remarks, SOCOM has been on that path to, in fact, ensure that we are cementing things in place that will allow our force to modernize for both, competition and for future conflict.

Senator Fischer: What progress has SOCOM made in developing these higher-end capabilities?

General Clarke: Senator, both team with both, academia and with industry. We are making sure, first, that we are not procuring capabilities that can't be used in a sustainable extremist fight, but that can also be used in near-peer, and we are focused very highly on next-generation, ISR, mobility, and putting a significant amount of effort into data and our networks to ensure that we have precision strike and effects into the future.

Senator Fischer: In light of the priorities that have been laid out in the NDS, how is SOCOM balancing its investments to operate against those near-peer competitors, like China and Russia, with efforts to fulfill its global counterterrorism requirements?

And I would like to know where, if you could answer
that, and then let me know where you are willing to accept risk.

General Clarke: Senator, first, on the acceptance of risk, intel drive ops, and where we put our focus on are those most virulent threats, you know, that could actually come back to our homeland and the persistent threat against threats like Al Qaeda and ISIS and those networks.

But then as we have looked at those sustainable capabilities against those threats, what else can come back, and that goes with both access and placement in other countries around the globe where counterterrorism can also equate to great power competition in someplace like the Philippines where our access and placement in helping the Filipinos fight ISIS allows us, also, to be involved in great power competition.

Senator Fischer: Thank you, General. Thank you both very much.

Thanks, Mr. Chairman.

Chairman Reed: Thank you, Senator Fischer.

Now, let me recognize Senator Gillibrand via Webex.

Senator Gillibrand: Thank you, Mr. Chairman.

First, for General Clarke, we entrust the special operations community with some of our most important missions and they have truly been the tip of the spear over the last decade. And I wonder if these units are not being
over taxed or undersupervised. In recent years, we have heard troubling stories about SEALs and Marine Raiders, a murder of a Green Beret, and allegations of war crimes by Navy SEALs.

So, first, should we be more concerned about good order and discipline problems in this community and, second, even if these cases are being prosecuted appropriately, are we taxing the operators with too heavy a load?

The chronic stress of these missions lead to post-traumatic stress, anxiety, and other mental health challenges.

And, third, are you adequately resourced to provide the necessary mental health treatment for these servicemembers and their families?

General Clarke: Senator, the items that you bring up are exactly why I directed last year a comprehensive review to look at our forces. And while, yes, I do believe that we are overfocused on employment and mission accomplishment, I do believe that through that comprehensive review, we have taken a hard look at ourselves and are making the corrective steps to ensure, I think most importantly is that we have the engaged leadership present throughout the force at the right time to reduce those incidents from occurring that have been highlighted.

I think one specific area that you mentioned which is
important, is in the resources in our preservation of the
force and family, which Congress allocates to us, today,
more than 40 percent of our manpower that is associated with
that is actually going to the cognitive and, most
importantly, the psychological efforts to ensure that our
special operators and their families are cared for.

Senator Gillibrand: Thank you.

Mr. Maier, as you know, the current special operations
force structure is largely derived from counterterrorism and
foreign internal defense operations in Iraq, in Afghanistan.

Do you think that this structure has created gaps in
Special Operations' capabilities to win against global
rivals like Russia or China?

Mr. Maier: Senator, I think it has and I think that
has been recognized, and I think that is where we are laser-
focused on closing that gap. And whether that gap is, as
General Clarke alluded to, having higher-end capabilities
that is more data-driven, more technology, more cutting-
edge, but also at the same time, as has already been
highlighted, being able to do our counterterrorism mission
in a sustainable fashion and reap some of the benefits of
those partnerships that give us, frankly, an asymmetric
advantage over our peer adversaries, because we do work with
so many countries in so many different ways.

So, this is absolutely something that I think the NDS
has highlighted for us and within the SOF enterprise, continue to be very focused on.

Senator Gillibrand: Thank you.

General Nakasone, I really appreciate your leadership, and it was great to see you last week. I want to talk a little bit about sort of where we are, because in February 2020 when you were at a hearing, you said that you were understanding our adversaries better than our adversaries understand themselves. Well, obviously, we just had the SolarWinds hack. Experts estimate that maybe a thousand software engineers executed that operation.

And so, what did we get wrong? What do we need to do to make sure we don't miss those kinds of assaults in the future, and what do you propose to address long-term concerns?

And, specifically, we talked a lot about cyber workforce, about how to make sure we have the best and the brightest working for us so that we don't have intelligence gaps like this in the future.

General Nakasone: Senator, with regards to our adversaries and understanding them, the comment I was making there was in reference to what we are seeing with their election influence. But I agree with you, we have to understand our adversaries better, particularly, given the recent intrusions that are ongoing.
Part of understanding our adversaries, though, is being able to see our adversaries. And so, again, if we have a problem where we only see our adversaries when they operate outside of their country and we don't see them when they operate inside our country, it is very difficult for us to be able to, as I say, connect those dots.

That is something that the administration and obviously others are addressing right now. In terms of what we are doing at U.S. Cyber Command, we are very much focused on how do we ensure that our capacity, our capability remains the best in the world. And that get back to your point on people what we have learned over the past couple of years is that the services bring in incredible talent for us. We are able to see these young soldiers, sailors, airmen, Marines, Coast Guardsmen come into our force, train them, but then our great challenge is, how do we retain them?

And that is something that certainly I give a lot of attention to every single day, and it is retaining the best of the people that we are able to bring in. Now, we have been able to leverage a number of the authorities that this committee has been able to generate for us, and so that is one of the areas that we are focused on right now, so as we continue to improve being able to see the adversary in its totality, we have the people that are able to apply, obviously, the capacity and the ability to defend the
Senator Gillibrand: I would like to work with the committee on getting you those authorities.

Chairman Reed: Thank you very much, Senator Gillibrand.

Let me recognize Senator Rounds, please.

Senator Rounds: Thank you, Mr. Chairman.

Gentlemen, good morning, and I thank you all for your service to our country. And I would like to thank your families, as well, for their sacrifice, as you continue that service.

General Nakasone, I want to work through this issue a little bit more about whether or not we see our adversaries, and I would like to just have a discussion with you. I understand that you have always made it very clear in all of our discussions that you are not here to tell us how to do public policy, but in order to make the public policy, we really do need your professional advice in terms of what is working and what is not.

You have alluded to it a couple of times today and I would really like to flush this out. Right now, we have provided the ability for Cyber Command to use cyber activities as traditional military activity, and so you can work outside of a war zone, as long as it is not within the United States. And our country has always said that our
Armed Forces are not designed to be utilized within our country; they are designed to be used outside and to defend our country.

And yet now, we face cyberattacks where adversaries, near-peer adversaries, Russia, China, Iraq, North Korea, have figured out that because of the laws that we have in place to protect our personal privacy, that they are using internet connections to literally get into the United States and then to launch attacks probably from systems that are found within the United States.

It seems to me that most Americans would suggest that if we have the ability or we have a design to stop those attacks, we either have to be able to defend forward, to go on out to find them and to literally provide a very active cyber defense outside in an offensive capability, or we have to have the ability, as I think you are suggesting, to be able to see inside of our own country and to find where they are actually launching those attacks at.

And I want to take a few minutes here and just allow you to expand on that and to share with us a little bit so that we have a better understanding of what the public policy challenges are that limit you from the ability to be able to see our adversaries here within the country.

General Nakasone: Senator, thank you.

So, in terms of my authorities as both, the commander
of U.S. Cyber Command and the director of the National Security Agency, I operate outside the United States, our forces do. It is not just a matter of policy; it is also law in terms of we, as a nation, rightly so, have a very, very determined balance between privacy and security. So, the authorities within the United States reside with the Federal Bureau of Investigations and others to do that type of surveillance.

What I am identifying right now, though, is our adversaries understand that they can come into the United States and rapidly utilize an internet service provider, come up and do their activities and take that down before a warrant can be issued, before we can actually have surveillance by a civilian authority here in the United States. That is the challenge that we have right now.

Now, I would, again, would offer that there are probably a number of different ways that we can look at this: whether or not it is greater public and private partnership; whether or not it is, you know, laws in terms of private sector, understanding who their customers are. But these are all areas that I think we, as a nation, have to be able to address.

Senator Rounds: Thank you, General Nakasone.

I just really think it is important that we share with the American public, this is not a case of where we are not
technically adept. This is a case of where we have made laws that we think are correct and that we don't use our resources, our military uses within the United States, but we do expect that our other law enforcement capabilities are able to coordinate and to rapidly assist you so that you can go on out and find and take these folks out before they do it again, so to speak.

Is that a fair way of looking at it?

General Nakasone: Senator, I would offer this is at the heart of our Fourth Amendment, and so being able to obviously look at that in terms of why it is so important that we have that right balance between privacy and security that is maintained, so being able to address that, obviously, is the challenge that we have going forward.

Senator Rounds: Thank you, sir.

Mr. Maier, I just want to bring up an issue that I think is really important. Secretary Mattis implemented a close-combat lethality task force in 2018. This was an organization dedicated to providing resources and policy solutions to the force who have accounted historically for nearly 90 percent of all the casualties, yet constitute only 4 percent of the force, and receive only 1 percent of institutional investments.

This has been and will remain as a very important legislative priority for my office. Nevertheless, despite
its noble goals, this task force has floundered in the
bureaucracy over the last year and I would like to see it
going back on track.

Can you give me your perspective on the need for an
effective cross-functional team such as this task force that
would be focused on our special operations forces, as well
as Army and Marine and infantry units and their enablers.

And I know that I am 30 seconds over my time allotted,
so I am asking the question now, but I would ask if you
would respond for the record to that request.

Mr. Maier: Senator, I would be happy to.

Senator Rounds: Thank you.

Thank you, Mr. Chairman.

Chairman Reed: Thank you, Senator Rounds.

Now, let me recognize Senator Kaine, please.

Senator Kaine: Thank you, Mr. Chair, and Ranking

Member Inhofe.

And it is great to have these great public servants
before us. General Nakasone, I would like to begin with
you. First, just congratulations. I just have been so
impressed with the work of Cyber Command over my time on
this committee both, in the 2018 election cycle and the 2020
election cycle, I think that you have just done a
magnificent job and I just wanted to state that up front.

Here is a concern that I have. I am on the foreign
relations committee and I am the chairman of the
subcommittee that oversees the Western Hemisphere. We had a
hearing yesterday on sort of democracy backsliding in the
Western Hemisphere, and one of the areas of concern is that
the next two years, 2021 and 2022 are kind of, I think one
of the witnesses described it as sort of an avalanche of
elections or a tsunami of elections in Central and South
America in nations where we are partners.

I spoke to the Columbian ambassador to the United
States recently and he talked about increasing cyberattacks
that they are suffering to delegitimize elections, to
promote chaos and division. Most of these cyberattacks seem
to emanate from Venezuela, from probably Cuban or Russian
actors in Venezuela, and other nations in the region that
are aligned with the United States, are seeing the same
thing. The Columbian ambassador to the United States asked
if SOUTHCOM and CYBERCOM could be of assistance in this
significant wave of elections in the next couple of years.

And so, I wanted to ask you, we had our posture hearing
with SOUTHCOM last week, what are you doing or what might
Cyber Command do, together with SOUTHCOM, to try to help our
allies in the region, avoid this escalating trend of
disinformation that destabilizes Democratic elections?

General Nakasone: Senator, let me begin by, first of
all, thanking the committee. What you refer to our
successes in 2018 and 2020 are based upon the work that this committee did in the fiscal year 2019 NDAA to identify cyber as a traditional military activity. That allowed us to operate outside of our networks. It allowed us to do things like hunt-forward operations, of which, we did 11 hunt-forward operations in nine different countries for the security of the 2020 election.

In terms of working with Admiral Faller and SOUTHCOM, both the admiral and I have discussed a series of countries that are coming up. We have worked together to identify teams that can assist these countries to provide advice. We know a lot about what our adversaries are doing in terms of influence and interference when election comes to part. So, we want to make sure that we share that with our allies as well.

Senator Kaine: I think the U.S. has played a good role. EUCOM has played a good role with the NATO and European nations with, you know, cyber defense. It is often centered in Estonia, a great center there of cyber defense, and I hope that we might explore what we can do in the Americas, as well. Thank you for that.

Senator Shaheen asked some questions about war powers that we have to grapple with and I am going to have one question for each, General Nakasone and General Clarke.

In the War Powers Resolution, basically, it requires,
and there is some confusion and some good faith argument about the legality of portions of the 1974 War Powers Resolution, but it requires notice from the administration to Congress when the U.S. military is engaged in hostilities or situations that can lead to hostilities.

And one of the things I have noticed on the committee is over time, even recently, we will get a notice letter from the administration, for example, about the strikes that were carried out in Syria. If my memory is not playing tricks on me, I don't believe we have ever gotten a notice letter about a cyber, an offensive cyber action carried out by Cyber Command.

Am I right about that?

General Nakasone: So, we do have a very strict congressional notification that we do adhere to. I think we had just recently had published a congressional notification for the committee. I will go back and check, though, just to make sure on that, Senator.

Senator Kaine: Okay. It may be that it goes to some on intel or other committees and may not go to all the members of this committee, but I would like to explore that.

And, secondly, to General Clarke, the War Powers Resolution does have a reporting exception for deployments which relate solely to the supply, replacement, repair, or training of forces in a foreign nation. So, if we deploy
forces to do those things, there is not a reporting requirement under the War Powers Resolution and yet sometimes those activities, as in the sad case of the loss of four servicemembers in Niger, I think it was in 2017, they can lead to military action and even loss of U.S. life, and that is something, again, I just think we need to grapple with.

The notion of what hostilities might be quite a bit different than it was in 1974 when Congress drafted the resolution and passed it, and it may require that we sort of get into what is the current nature of hostilities and warfare and grapple with that a bit.

And last, I will just say to you, General Clarke, not a question, but thank you to you and Secretary Maier. The special forces community is a really important and valued portion of our commonwealth and we thank you for the work that you do.

And I will yield back, Mr. Chair.

Chairman Reed: Thank you, Senator Kaine.

I would like to recognize Senator Cotton, please.

Senator Cotton: Thank you, gentlemen, for your testimony.

General Clarke, on January 20, President Biden and his national security advisor, Jake Sullivan, issued a derivative that withdrew authority to conduct certain
military operations outside of Syria, Iraq, and Afghanistan, from our combatant commanders and reserved it to the White House, itself.

Has that affected operations and Special Operations Command, or is that simply affecting our regional geographic combatant commands?

General Clarke: Senator, I am aware of that, as it was reported in the open-source. I would respectfully submit or request that we talk about that in a closed hearing.

Senator Cotton: Okay. It has been confirmed by the National Security Council on the record, but I understand the hesitation.

Maybe I will ask Mr. Maier, do you know the problem that that decision was designed to solve, because it is not apparent to me what problem was raised by having combatant commanders or their subordinate commands make the decision to conduct military operations outside of Afghanistan, Syria, and Iraq. And let's just get down to brass tacks here, we are talking primarily, I think Yemen, Somalia, and the African Sahel.

Mr. Maier: So, Senator, I think it is meant to be an initial review of this administration in the use of a series of different actions that, again, we should probably talk about it in closed session. But I think like a lot of the reviews that are underway, I already alluded to everybody on
the committee certainly knows about Afghanistan, Somalia, the posture hearings and reviews that are underway, those are all part of an overall series of looking at what has been done and whether this administration would continue to proceed with those.

Senator Cotton: Okay. We will discuss it in the closed session. Again, this has been reported and confirmed by the National Security Council.

To make a point, I will relay a story the past President told me. I don't think he will be offended if I share his thoughts. He said early in his administration, he was doing some reading late one night and he got a call from an action officer about approving a strike and his response was, well, what do they expect me to know about it? Don't they have some captain on the ground near this country that has been following this target and knows that this is the bad guy and that we should conduct this strike?

And I agree with that sentiment.

General Clarke, I have the highest confidence in you and in General McKenzie in Central Command and General Townsend in Africa Command to know whether or not we should smoke a bad guy overseas. And that doesn't need to be decided by civilians at the White House.

General Clarke, I want to turn to Special Operations Command and something we discussed in our visit yesterday,
and I just want you to elaborate for us on the record here.

What specific changes in force design and capabilities do you believe are necessary to attain the force that you need to accomplish your mission going forward and what do you believe are the most pressing of those needs?

General Clarke: Senator, in order for us to compete effectively in the future, we have to modernize both, our precision strike and ISR. We particularly have to look at data and data management so that the most specific requirements enabled at the tip of the spear where our operators are, so that they can quickly see and sense the battlefield that they may have to be fighting in, into the time of crisis.

And then we also have to have encrypted and electronic warfare capabilities so that our forces that could be forward in a joint war-fighting capacity, reduce the probability for them to be targeted. So, we are looking at all of these, Senator.

I, personally, changed our modernization priorities and restructured some of our funding to modernize those capabilities.

Senator Cotton: Thank you.

General Nakasone, in the time we have remaining, I want to ask a question that may seem to be a boring bureaucratic matter to some people watching, but it is an important
question that this committee has addressed in the past and
that the intelligence committee has addressed, as well, and
that is the so-called dual-hat. In addition to being the
commander of the Cyber Command, you are also the director of
the National Security Agency; is that right?

General Nakasone: That is correct, Senator.

Senator Cotton: And that is the so-called dual-hat
that you command this military combat command and also that
you run an intelligence agency.

What do you think are the positive things that result
from wearing that dual-hat?

General Nakasone: Senator, over the past 3 years, what
I have learned as being both, the commander of U.S. Cyber
Command and the National Security Agency is that the ability
for myself to operate in both roles provides the nation,
speed, agility, and flexible responses to adversaries that
are increasingly modernizing, getting quicker, and getting
more sophisticated.

We operate in a domain that changes rapidly and this
change is measured in weeks, perhaps months. Being able to
rapidly react to that, as we have been able to prove in such
things as securities of elections in 2018 and 2020, is
empowered by that relationship.

Senator Cotton: Thank you. Thanks, gentlemen. I will
see you in the closed session.
Chairman Reed: Thank you, Senator Cotton.
And let me now recognize Senator King via Webex.
Senator King: Thank you, Mr. Chairman.

General Nakasone, a couple of quick questions about your staffing. Would it help, in terms of recruitment and retention if you had the authority, as part of this process, to forgive student loans, would that be a factor that you think might be effective in helping to retain and bring on the people that you need?

General Nakasone: Senator, certainly, that would.

And the services have that power as they recruit talent for our force. We have utilized it also with our civilian, but that is one mechanism that we get feedback that is very attractive to our workforce.

Senator King: The second specific question, we have had a real backup problem in the past with the security-clearance process. Is that improving or has that been a barrier?

I have heard of people that just get so discouraged they move on even though they have been accepted for a position.

General Nakasone: Senator, it has improved and it has improved significantly over the past couple of years. I applaud the work that has been done by the Department toward that, but even with that said, for those that operate at
U.S. Cyber Command, it does require a full security investigation. So, there are times that there are a fraction of our workforce that takes longer than others.

Senator King: I think that is something we have to continue to work on, because we don't want to lose good people who are making the commitment but can't set their lives aside for a year or more for that process to carry-forward.

You used the term at one point, to change the subject, you used the term "risk calculus." You have used the new authorities very effectively in the elections of 2018 and 2020 in terms of defending forward and engaging with the adversaries in their systems.

Has that had a deterrent effect that you have observed, do you believe that the adversaries are thinking twice about some of the things they may be planning against us because they know of the capacity that you have demonstrated?

General Nakasone: Senator, I continue to see our adversaries operate rapidly in terms of being able to try to operate below the level of armed conflict. We have effectively gone from being a very static to a very active force, as you refer to, to defend for the Department's cyber strategy of 2018 and our instantiation at U.S. Cyber Command of persistent engagement, how do you both, enable your partners and act?
We continue to do that. We are operating in a space where our adversaries are not going to stop. They are going to continue to look for ways to steal our intellectual property, to steal our identification, and to try to influence our populous.

We, at the same time, have to be forward. We have to be operating, and we have to be engaged with our adversaries, and that is what has been my focus over the past couple of years.

Senator King: Well, would you agree that we need to develop a cyber doctrine, if you will, of declared deterrents, because, as you say, they are going to continue to do this until they have a risk calculus that tells them that there will be a price to be paid that they are not willing to undertake.

General Nakasone: So, certainly, Senator, the policymakers continue to look at this type of doctrine and I know that is being worked. From my perspective or my responsibilities, I am very, very focused on operationally, how do we ensure that we can operate against these adversaries that continue to try to operate below the level of armed conflict.

Senator King: I think there is one point that has been discussed repeatedly today that really bears a lot of policy discussion, and that is the gap that you have identified
where you aren't able, either in Cyber Command or NSA, to operate within the United States, but our Vice President Harris have learned that if they can hop and use a server or an ISP in the U.S., they can evade your surveillance, and then we have the FBI, as you mentioned. We are dealing with the fundamental issue of protection of privacy.

But would you agree that this is a serious issue?

SolarWinds is a perfect example where they operated in this country for something like a year, 9 months to a year, and were picked up by the private sector, not by our services.

So, I take it from your prior discussion, this is something we really need to focus upon; isn't that correct?

General Nakasone: I do think we need to focus on it, Senator. The only alteration I would make to it, it is not necessarily that it is U.S. Cyber Command or the National Security Agency that needs to be doing this. I am saying that the nation needs an ability to be able to see what is going on within the United States.

Senator King: I agree. I am not saying that it is your job, necessarily, but what I am saying is this gap is an issue that we have to address and SolarWinds points it out.

I think one other point, and my time is expired, but that needs to be emphasized is the relationship with the
private sector. You have already mentioned that and that is something that we are going to be working on, I hope, in this session of Congress. That is a key part of cyber defense.

Chairman Reed: Thank you very much, Senator King.

Let me now recognize Senator Ernst.

Senator Ernst: Thank you, Mr. Chair.

Gentlemen, thank you very much for being here today and for your command teams and, as well, the men and women within your commands.

General Clarke, certainly, our Special Operations Forces is probably the most capable military element on the face of the planet, and as well, General Nakasone, the men and women within Cyber Command have proven essential to us over the past number of years. So, thank you very much for being here today.

Mr. Maier, I appreciate the opportunity to sit down with you recently and discuss our SOLIC forces. We think it is really important and General Clarke, as well. I will start the questioning with you. I appreciate you sitting down a couple of weeks ago and visiting about our shared commitment to the men and women of SOF, so thank you.

Senator Inhofe and Senator Fischer touched a little upon some of the gray zone activities where our SOF covers down and we know how important that is. As we have seen
counterterrorism actions in the past, and as we move to, you know, the near-peer competition under the guise of our National Defense Strategy, we understand there needs be a little shift, but if you can, just reinforce how important it is that we continue not only to adjust to that near-peer competition with our special operators, but also to continually focus on counterterrorism efforts.

General Clarke: Senator Ernst, as you know, SOCOM has to enable the joint force in both, crisis, competition, and if necessary, conflict. And in this space, there will remain that persistent threat and we have to prioritize towards that persistent threat and that would be groups like Al Qaeda and ISIS.

But there are SOCOM and SOF unique capabilities that can be used in competition that the rest of the joint force doesn't have, and that could be things like undersea, seabed warfare and only we provide, the strategic reconnaissance that our forces are extremely capable of. And so, as we look at that competition area and as we look to modernize our force for the future, those are the specific capabilities that we will continue to work with this committee to move forward on.

Senator Ernst: Thank you, sir.

And just as a reminder to this committee, as we are looking at potentially flat budget for DOD in the future, we
just need to understand the role that SOF plays, that SOCOM has around the globe, and that we do get a lot of bang for our buck when it comes to the men and women within your command.

You know quite well that my heart and soul is behind POTFF and how important it is. And I know, sir, the fifth pillar of your command philosophy is health of the force, but we go back to the SOF truth that humans are more important than hardware. And so, this is something that I have long been involved in.

And if you could, please explain a little bit about what your focusing on in the area of brain health.

General Clarke: Thanks, Senator.

I think it is important that the entire committee understands when we started POTFF, we focused on the physical, our men and women who were physically wounded where you could see the wounds, and in the last couple of years, we have refocused those efforts towards cognitive and the psychological, as we saw suicides go up. But then we looked at the health of our force for 20 years of engaged combat, and now we have put more than 40 percent of our resources and our capability specifically to the brain health and the cognitive domain and the psychological domain to be able to ensure that our operators are both, physically and mentally capable. So, we baseline all of our operators
with their cognitive piece, so if there are reductions in
their capabilities, if they actually have some type of
concussive event, we can then go back later. We are working
with industry academia and even elements like the National
Football League in this space so we can make sure that we
take care of our operators.

Senator Ernst: Right. And I think it is just
important to stress that the investment into these
activities is extremely important for, again, the
preservation of our force. I have had the opportunity to
visit a number of those types of activities in Coronado with
Admiral Green a number of years ago, as we kind of dove into
behavioral health activities, as well as spiritual activity
is very important for our force, but then also the THOR3
facilities that are available for our men and women of the
force and making sure that they are physically strong and
capable of what is expected of them by the American people.

So, again, I will continue advocating on behalf of
SOCOM and I certainly appreciate your wonderful efforts.

Thank you, Mr. Chair. I yield back.

Chairman Reed: Thank you, Senator Ernst.

Let me recognize Senator Blackburn, via Webex. Senator
Blackburn?

Senator Blackburn: Thank you, Mr. Chairman.

And General Clarke, thank you for the time and the
conversation yesterday. We talked about 40 percent of
SOCOM's forces are aligned to support the great power
competition fight. That is a big increase. So, for the
record today, I would like for you to talk about the
resourcing standpoint of what do you need from this
committee in terms of authority; advocacy, what do you need
to engage in near-peer competition from Beijing; and then
let's talk a little bit about the posture that SOCOM has to
counter these nefarious activities from the CCP and where
you are positioned there.

I think you can really do more with a lower dollar
amount than the regular force, so I would love to just get
your comments for the record.

General Clarke: Senator, thank you.

You know, as pointed out, with about 2 percent of the
Department of Defense budget, I think we are a very good
return on our investment, with about 3 percent of the force.

And the continued resourcing, specifically, you know,
for SOCOM so that we can modernize in this area, where we
can provide unique capabilities for our forces is critical.

We have to balance both, operations readiness and
modernization. And the continued support of this committee
remains critical.

As we look at, you specifically asked about our
employment and our capacity at 40 percent. That is exactly
right. We have, in fact, adjusted our forces to a sustainable presence against the persistent terrorist threats, while, at the same time, rebalancing those forces across the globe. Some of our competitors are now global threats and not necessarily specific to Europe or INDOPACOM, and so we continue to look at where our forces are located across the globe so they can counter, you know, those specific threats.

And then the last thing I would hit in this area is the specific authority for our forces to conduct unconventional warfare in this space.

While I can take specific points in closed session, that authority that allows us to work with partner forces to increase both, the resistance and resilience, working in the information space, is absolutely critical.

So, Senator, thank you.

Senator Blackburn: Yes. And we talked a little bit about the term that you and Admiral Davidson use about slowing down China's clock. And I would like for you to hit just quickly on what that means and then what we have, what we can do with operation within that gray zone.

General Clarke: Senator, as you are well aware, we established the joint task force, Indo-Pacific. It is the first task force that went and is actually west of the International Date Line that we developed with INDOPACOM to
ensure that we work with like-minded partners in the Indo-
Pacific. And I think part and parcel of that is that that
element is focused on the information operations so that
China, who works very well in the space of creating false
narratives and not always being up front with the messages
that they send, that we actually are able to tamp down some
of the disinformation that they continuously sew, and that
is an important part to SOCOM and to CYBERCOM, is working in
this information space.

Senator Blackburn: And with the time remaining, we
talked a little bit about OPTEMPO and the changes there and
the comprehensive review from 2019. And where have you seen
holistic improvement across the force and where would you
like to continue to see improvement?

General Clarke: Senator, through our comprehensive
review, we have now ensured that by this year, all of or
forces will be above a 2:1 deployment to dwell ratio. That
will be the first time that that has happened since
September 2001. We continue to strive toward meeting the
3:1 dwell ratio for all of our forces, and some of our
forces already there and we will continue to strive in that.

Senator Blackburn: Thank you, sir.

General Clarke: Thank you.

Senator Blackburn: Thank you, Mr. Chairman.

Chairman Reed: Thank you very much, Senator Blackburn.
Before I recognize Senator Hawley, I will depart for
the vote. Senator Inhofe will preside, and I will return,
and we will switch off.

Senator Hawley, please.

Senator Hawley: Thank you, Mr. Chairman.

Thank you, gentlemen, for being here. It is good to
see you again.

General Nakasone, let me start with you. Many
companies use Chinese hardware like printed circuit boards
in their information systems they provide to the Department
of Defense, including systems that are used to store and to
transmit information. At the same time, DOD and others have
warned that the Chinese Government might be able to tamper
with these Chinese-made products in order to create cyber
vulnerabilities that they can exploit and use against us.

My question is, do you think it is important for the
Department to at least know which systems contain Chinese-
printed circuit boards so that it can address potential
cyber vulnerabilities and contain any exposure or any danger
that is identified?

General Nakasone: Senator, in light of the recent
SolarWinds intrusion, I think this is, as you point out, an
area that we, as a Department, continue to look at very
hard. There are procedures and processes that the
Department utilizes to verify this, but I agree that this is
an area that we have to obviously shine a light on in the future.

Senator Hawley: And do you agree that further steps would be useful in order to identify vulnerabilities here and, as you just said, shine a light on this?

General Nakasone: So, Senator, I am a person that every single day is worried about the vulnerabilities that our adversaries might exploit, so you can well-imagine that this is an area that I have a great deal of, you know, focus on right now.

Senator Hawley: Good. Well, I look forward to working with you on that.

General Clarke, let me come to you. The Baltic nations have spent some years honing their ability to conduct irregular warfare in the event that Moscow attempts to seize a Baltic territory, so it won't be able to hold it. It has become a key part of their deterrent strategy, as you know, in the Baltic region.

What I am asking about this is, do you wonder, do you think that the Baltic model could be applied in Taiwan; in other words, would helping Taiwan improve its irregular warfare capabilities help it deter potential Chinese aggression?

General Clarke: Senator, bottom line, yes.

We have worked closely with the Baltics. I have met
with every Baltic SOF commander personally and we have been engaged in the Baltics for a long time, but we also, and I can talk more specifically in closed hearing, we remain close with capabilities for Taiwan.

Senator Hawley: Do you think that it would be helpful to us and should we be prioritizing helping Taiwan develop its irregular warfare capabilities?

General Clarke: Yes, Senator, I do think we should help them.

Senator Hawley: Let me, still with you, General Clarke, but switching topics. President Obama's former acting special representative for Afghanistan and Pakistan recently wrote that, and I am quoting now, for the long term, the United States will need a counterterrorism capability in that region that doesn't depend on a permanent U.S. military presence in Afghanistan, which I completely agree with.

My question is, what options has SOCOM provided to the secretary to allow us to achieve counterterrorism objectives in Afghanistan without a permanent military presence in the country?

General Clarke: Senator, we will always provide options. As you well know, Al Qaeda and ISIS are not just in Afghanistan, but they are a global threat, and we will always provide the secretary and the Department and the
National Command Authority with options so that if there is a threat, that we can actually detour or actually disrupt or defeat that threat.

Senator Hawley: And, specifically, you are saying, and we can discuss this more in closed session, as appropriate, but just to be clear, you are working on providing options to deal with the counterterrorism threat and with -- for counterterrorism measures that do not rely on a permanent standing military presence in country; is that right?

General Clarke: Senator, there has been no decision made for Afghanistan, so I think it would be, you know, a hypothetical to know what we are going to do at this time, but we will always provide options, you know, for the Department of Defense.

Senator Hawley: Good. Well, I look forward to following up with you more on that.

General Nakasone, I am going to come back to you here in my few remaining seconds. The People's Liberation Army in their writings often refer to cyber capabilities as the strategic commanding heights of future warfare.

I am wondering how the PLA's emphasis on information operations and maintaining the information advantage influences CYBERCOM strategy for detouring China.

General Nakasone: Senator, I think this whole discussion in terms of where our adversaries are going and
in the influence spaces is among the most important areas that we are taking on at Cyber Command, and I know General Clarke is addressing at U.S. Special Operations Command. This is really the competition that we are involved with today where our adversaries are, again, trying to influence ourselves and our people through a number of different means. So, we have work ongoing today, ongoing both, in our commands and with our commands trying to address that, as well.

Senator Hawley: Very good. I will look forward to following up with you on that, as well.

Thank you, gentlemen, for your testimony.

Thank you, Mr. Chairman.

Senator Inhofe: Thank you, Senator Hawley.

Senator Kelly is recognized.

Senator Kelly: Thank you, Senator.

I understand that in January of 2020, nine combatant commanders, including you, General Clarke, sent the letter to the director of National Intelligence requesting more assistance from the intelligence community in being able to publicly illuminate, malign, influence, and coercive activities by China and Russia.

So, to all the witnesses, starting with General Clarke, what, if anything, has been done in response to this request from the nine combatant commanders?
General Clarke: Senator, from that request, SOCOM, with the other combatant commanders, continues to look specifically in the information space and where we can best effect to provide capacity against our adversaries. And I think that specific memo led to some sort of concurrence requirements being lifted for the Department.

Senator Kelly: And in your view, would the illumination of these malign activities help to dissuade or detour China and Russia?

General Clarke: Senator, at this point, I cannot point to specific deterrents or detraction of that. I would tell you we would continue to look, but I think it is most important that we continue to develop the capacity required to work in the information space.

Senator Kelly: General Nakasone?

General Nakasone: Senator, to your second point there, I think that is a really important question. In terms of what our adversaries are doing today, our most effective response is being able to respond to what they are doing. And we have a number of different ways upon which we respond. Sometimes we respond to other means of the power in our government, whether or not it be diplomatic or sanctions or other ways, but I think it begins with the idea that we are competition right now and our adversaries are operating below the level of armed conflict in a matter of
trying to influence us.

Senator Kelly:  But in downgrading the classification of this intelligence, is that helpful in meeting the goal of dissuading more aggressive action from China or Russia?

General Nakasone:  I think we have to think broader than that, Senator.  I think that it is more than just writing to release or perhaps even downgrading.

It is as General Clarke alluded to, there are other means upon which we gather intelligence these days.  How do we take the best tools, the best techniques, not only from our Government, from also from the private sector, to look at what is occurring and being able to shine that spotlight.

I think a lot of times we look and just say, hey, we will simply go ahead and downgrade intelligence and provide that rapidly.  Sometimes the better answer is, okay, where are the other streams of information, how can we use that most effectively with an audience.

Senator Kelly:  Well, thank you, General.

And to Mr. Maier, so, Section 1202 of the fiscal year 2018 NDAA sought to provide a new tool to counter these challenges by authorizing the Secretary of Defense to provide support to regular forces, the regular forces, and individuals supporting U.S. special forces, but that irregular warfare operation part, last year's NDAA raised the annual cap on funding for this authority from ten to $15
So, Mr. Maier, how would you characterize the demand for this authority across the geographic combatant commands?

Mr. Maier: So, Senator, that is a, I think, a very important tool we have that we haven't yet talked about in the great power competition. The demand is high. It takes some time, as you can understand, to build those partnerships to be able to operate in that partnership-driven approach.

We view this very much as the successful 127 Echo or the 1208 program, where there is a crawl, walk, run element to it, and I think that started very small. And as the progress, and in many respects, the high return on investment in terms of dollars and deployments in dwell and impact started to become apparent to the GCCs, and became more and more in demand, we see a similar model for 1202, sir.

Senator Kelly: Thank you.

I yield back.

Senator Inhofe: Thank you, Senator Kelly.

Senator Sullivan?

Senator Sullivan: Thank you, Mr. Chairman.

Gentlemen, good to see you again. Thanks for all your work.

General, let me start with you. General Clarke, how
are you feeling, with regard to the resources that you have for your no-fail mission, you have a lot of no-fail missions, but your Counter-WMD mission that SOCOM was, a couple of years ago, given that mission, as well. It is not like you didn't have a lot of missions on your plate. That is a big one.

A number of us, myself, in particular, were concerned that the Special Operations Command does a lot of things right, really well, but being given the lead on that one was a whole other area that is really, really important, but also needs resources. And are you resourced enough for that mission?

That is a mission that, of course, there is no doubt, you can't fail on.

General Clarke: Senator, the bottom line is we do have sufficient resources to do that. The resources from STRATCOM, you know, that had that coordinating authority for CWMD were moved from STRATCOM over to SOCOM. I will continue to assess if additional resources are required going forward, but as you point out, the WMD threat is something that we must pay continuous attention to, because if we don't, we do it at our own peril.

Senator Sullivan: And as I know you know, and you and I have discussed this, we are reorienting. I think it is the appropriate orientation for our military and national
security to great power competition with China as a rising threat, but the WMD threat continues regardless of great power competition and that could be from violent extremist organizations, which clearly want to get their hands on that. It could be from North Korea, who is a well-known proliferator. Pakistan.

Are there any areas, in particular, that you are focused on, as it relates to the Counter-WMD that is not in the headlines, but we should be sure we are focused on here, as well?

General Clarke: Senator, one thing that we put some strong recommendations for is that is ensuring that our joint forces actually train to work in a contested environment, so that our adversary is well aware that they will be denied the benefit of use of these capabilities. And that deterrent and our principle, I think is critical.

As you and I discussed yesterday, there are those that would like to wish this problem away, but we don't think we can and we have to be prepared for its potential use.

Senator Sullivan: Let me ask another issue, which I think this committee is very focused on.

You know, the SOCOM enterprise, our Special Operations Forces have been very focused, appropriately, Post-9/11 in the Middle East. They have done a great job, a heroic job. Many have lost their lives in their service to their
country.

How are we starting the transition from the focus there, which we still need to do, but we need to also start focusing on China and the Asia Pacific and the INDOPACOM region. Are we doing enough there? Do we have enough experience with special operators?

It is a very different battlefield, as you know. It is probably less kill and capture and more gray zone operations. What is your thinking on that, General?

General Clarke: Senator, this is going back to the future for SOF. Many of our forces were regionally aligned prior to 9/11 that had both, the cultural and language understandings and now as we have actually reduced forces in the places that you have named, some of these forces are going back to where they do have that understanding and those capabilities.

So, we have aligned, in one case, I think important for the employment of our forces, but I think the second and really key aspect from a SOCOM perspective is that we have actually reallocated our budget for the modernization towards the capabilities that are required. So, I have adjusted 14 percent of my budget in modernization towards great power competition for those unique SOF capabilities.

Senator Sullivan: Great. That is good to hear.

General Nakasone, I just want to compliment you, sir.
I think you have been doing a phenomenal job. You probably don't get complimented enough because you can't talk about what you do, but in my own experience here, I am just starting my second term in the Senate, there was a hearing that I really remember in 2015, 2016. It was the Cyber Command. It was some of the others who were, I called us the cyber punching bag of the world. And the witnesses admitted that we don't retaliate when we are attacked from a cyber perspective.

I don't think we are the cyber punching bag of the world anymore and I think it is because of your work. You can't talk about a lot of that work, but can you just let the American people know that whether it is on elections or other cyberattacks, we are not just taking blows; we are going on uh offense, we are preemptive. I think it is really important for people to know that.

That was not the posture 5 years ago. We were just getting pummeled and we wouldn't do anything about it. Can you talk a little bit about that, to the extent that you can, in an unclassified session.

General Nakasone: Senator, I appreciate the question and, importantly, I appreciate the support of this committee, because as I was mentioning, really, 2018 was a watershed year for us, as we had looked at the future to a midterm election and knowing that we did not want to
experience what we had experienced two years previously, the ability for this committee to pass the NDAA that year that allowed us to operate outside of our networks, cyber as a traditional military activity. Moved us from being a static to an active force.

And this idea of persistent engagement, always being involved with your adversaries, whether or not you are enabling our partners or acting against our adversaries is critical in underlying to our support in 2018, 2020, and today.

Senator Sullivan: Thank you, General.

Thank you, Mr. Chairman.

Chairman Reed: Thank you, Senator Sullivan.

Let me now recognize Senator Duckworth via Webex.

Senator Duckworth: Thank you, Mr. Chairman.

And I do join my colleague, the senator from Alaska, in his admiration for the work that we have done, especially under your leadership, General Nakasone.

General Clarke, I appreciate our call yesterday and I wanted to express my support for Special Operations Command's diversity and inclusion strategic plan. As we discussed on our call, bringing more people from diverse backgrounds into the Special Operations community will make it stronger. By infusing teams with different ideas and perspectives and enabling them to engage more effectively
around the world.

I agree with you that greater diversity in the Special Operations community is an operational imperative. That is why I sponsored the ELITE Act in last year's NDAA to identify and remove barriers to underrepresented groups' participation in elite communities of the Armed Forces.

I am glad to see that you have taken on the challenge of increasing diversity and inclusion in Special Operations Command and it is an important first step in strengthening our military, and I really look forward to working together with you on this issue in the future.

My first question, I believe that being able to tap into the full talent of every [inaudible] of our population makes our military stronger. I also believe that in order to build the most capable military possible, we need to capitalize on the natural advantage of our National Guard and Reserve forces, namely, that those servicemembers are highly trained in their civilian jobs, as well as their military jobs.

If we viewed this as a strength, we can benefit from the expertise that our Guardsmen and Reservists bring from civilian life, especially infuse in fields that require advanced technical skills like cyber.

General Nakasone, can you please describe how the National Guard and Reservists like members of the Illinois
National Guard who are currently working the 176th Cyber Protection Team are contributing to your mission at U.S. Cyber Command.

General Nakasone: Senator, thank you, and thank you for the question. The 176th Cyber Protection Team is a team well-known to us at U.S. Cyber Command. They mobilized, came on active-duty, and did a tremendous job in protecting our infrastructure, the actual capabilities, upon which we utilize every single day to engage our adversaries, led by, you know, Major Jaime Marlock, who is the Cyber Protection Team leader.

And, really, it starts at the top with the Illinois National Guard, in general, Brigadier General Neely, who has been instrumental in being out front, being very supportive of our efforts, and I think key to your point, attracting those that leave active-duty service and continue to want to serve. And so, the 176th is a great example of our partnership with the Guard.

Senator Duckworth: Thank you.

And how will increasing National Guard and Reserve components participation in cyber operations improve our national readiness and capacity to combat cyberattacks and how can Congress support this effort to increase the Reserve forces participation in our cyber activities?

General Nakasone: Senator, if I might use just an
example, and I would say it is from the state of Connecticut. As we were operating with the Connecticut National Guard in the early fall of 2020, on the 2nd of September, Connecticut faced a ransomware attack on their public school systems. Operating with the Connecticut National Guard, they provided us information via a capability that we called a Cyber 9-Line. That is utilizing a common ID card, being able to obviously share that and unclassified with us back at U.S. Cyber Command, we could use the power that we have at U.S. Cyber Command at the National Security Agency to look at this malware and to rapidly provide assistance.

But at the end of the day, it was the Connecticut National Guard that did the work and, you know, taking an ability to look at a situation where your school has been shut down because of ransomware and then in a matter of days, being able to bring that back up, I think it shows the power of the Guard and the power of the partnership between the private and the public sector.

Senator Duckworth: Thank you.

And when I think of complex cyber missions, I do think, in particular, about the challenges that U.S. Transportation Command faces in securing its network and safeguarding sensitive information about our troops, our capabilities, and our postures, and movement plans while also working with
numerous commercial partners, whether it is ocean-going or within the aviation community.

General Nakasone, please describe your current work with U.S. Transportation Command and explain why it is important that Congress fully resource and support this and future initiatives like it.

General Nakasone: Transportation Command is really a unique capability for our nation. It provides us global logistics. We are perhaps the only nation that can do that so readily and so well.

And so, under General Lyon's leadership at U.S. Transportation Command, he approached us and said, hey, we operate primarily off of the private sector with unclassified networks. How can you help?

And so, there has been a partnership ongoing for the past year and a half where both, U.S. Transportation Command, U.S. Cyber Command, and the National Security Agency have taken a look at, how do we improve that public-private partnership, how do we ensure the security of the data that is being transmitted, and then, also, how do we look to the future?

Thank you, Senator.

Senator Duckworth: Thank you.

I am out of time.

Thank you, Mr. Chairman.
Chairman Reed: Thank you very much, Senator Duckworth. Let me recognize Senator Tuberville, please.

Senator Tuberville: Thank you, Mr. Chairman.

Thank you, gentlemen. Thanks for being here today.

General Nakasone, Space Force has already taken great steps in advancing U.S. national security in order to provide [inaudible] needed. It is going to continue to need a strong backing from our cyber intelligence community.

What role will the cyber mission force and CYBERCOM play in Space Force?

General Nakasone: Senator, it has been an early and active role already. General Dickinson has been out to U.S. Cyber Command to talk about how do we secure the networks upon which he operates. How do we work, obviously, as we take a look at our overhead constellation, what are the threats that USSPACECOM is going to approach in the future.

And so, we have been actively engaged with him over a period of several months to identify those.

Senator Tuberville: Thank you.

General Clarke, Section 922 of the 2017 NDAA, which was signed into law by President Obama, made clear that the administrative chain of command for the Special Operations community runs from the President to the Secretary of Defense, to ASD/SOLIC, and then to you, the SOCOM commander.

Prior to conducting congressional engagements, do you
obtain approval from ASD/SOLIC?

General Clarke: The secretary, we work very closely with ASD/SOLIC in that administrative chain of command for oversight, particularly for our budget, and acquisition. Mr. Maier and his predecessors provide that oversight. But it also clear that my chain of command, and Secretary Austin made this very clear to me, that my chain of command as a combatant commander runs from the Secretary of Defense to the President.

Senator Tuberville: Thank you.

That is kind of my next question. Do you support the implementation of the law and, specifically, ASD/SOLIC’s absolute control over administrative matters, such as legislative engagements, budgetary resource decisions, acquisitions, public affairs, personnel, legal accountability, and other related authorities held by the traditional military service?

General Clarke: Senator, what I believe is a key role for ASD/SOLIC is actually to be an advocate for SOCOM within the Department. And so, when decisions are made about services and service budgets and service-personnel decisions, I think ASD/SOLIC in the room to be able to be that advocate for us, to me, is the most important aspect that ASD/SOLIC can do for SOCOM.

It goes back to the old adage if you aren't at the
table, you become the lunch, and having ASD/SOLIC in and at
that table, which has occurred, has been very helpful.

Senator Tuberville: Thank you.

Mr. Maier, I noted a moment ago the law mandates that
the administrative chain of command for SOCOM passes from
the President to Secretary of Defense, ASD/SOLIC, SOCOM
commander. And in light of the clear chain of command, have
you met with the secretary of administrative matters related
to SOCOM?

Mr. Maier: Senator, yes, I have, and I participate in
the secretary's regular service secretary meetings. I also
participate, or my staff participate, in the series of
governance meetings that the deputy secretary runs in order
to do, just as was already said by General Clarke, to both
advocate, but for the administrative chain of command.

We are responsible for both, setting direction and
ensuring execution and implementation, consistent with the
law.

Senator Tuberville: How often do you all meet, do you
think?

Mr. Maier: The service secretaries meet at least twice
a month. Obviously, a new administration, so a different
series of meetings, but every day, sir, there are meetings
that I am representing ASD/SOLIC in that service secretary-
like hat with the secretary, deputy secretary, or their
direct reports.

Senator Tuberville: Thank you.

Thank you for your service.

Chairman Reed: Thank you very much, Senator Tuberville.

Senator Peters, please.

Senator Peters: Thank you, Mr. Chairman.

And thanks to each of our witnesses here today.

Mr. Maier, in General Clarke's words, if I may use your words here, General Clarke, they are good words, he says SOF, quote, strengthens alliances and creates diplomatic options.

These strategic effects ultimately, clearly begin with actions undertaken by people in those areas. It is our number-one assets.

So, I would like to hear from you how you are modernizing professional development in a way that really reflects this very unique role of your personnel, how you are basically bridging the gap between direct action and working in an embassy across the span of training and education, a very obviously complex set of skills that are necessary.

So, and, specifically, my question is, how are you broadening mid-level SOF leaders and how much of that focus is on senior-enlisted personnel?
Mr. Maier: Senator, that is a very important part of this pivot, as we described it from being able to still do the counterterrorism missions that we have been involved in for the last, really, generation to be able to do that both, and then be competitive at that level, below armed conflict.

A critical component of that, as we have talked about already, is not only the ability to speak languages and really engage at the right level of cultural awareness, with not only the adversaries, but also those third parties, third countries that those adversaries are attempting to influence.

And a lot of that happens in the information space, social media, as we know. So, a critical component of a professional military education, but even more specifically, the operational imperatives that we have to evolve that force. This is the key part of this.

It was alluded already at the opening statement of General Clarke, that over 50,000 members of Special Operations Command are enlisted members. That is where the rubber meets the road. These individuals, especially in the SOF world, are often called upon to do things well above what their conventional counterparts, whether that is operating embassies, participating on interagency teams, or engaging with partners. So, we see that as really the crux of progress and where we are going to be successful in this
great power fight.

Senator Peters: So, Mr. Maier, does the SOCOM talent management then emphasize regional experience, is that something that you are really seeking out and trying to develop further?

Mr. Maier: Senator, yes, sir. And I think, specifically, evolving to those great power concerns, we often forget at times that a lot of what we have been doing over the last years in the counterterrorism fight was really focused on fairly narrow set of adversaries. And so, I think as we look more broadly and diversely at the adversaries we are going to confront, and in some cases, more importantly, those entities that they are trying to influence, it is important for us to be able to engage in those languages with that cultural awareness.

Senator Peters: Yeah, absolutely. Well, that is good to hear.

General Nakasone, on Tuesday, I asked Admiral Aquilino how he plans to align security assistance in INDOPACOM with the nature of our competition with China and Russia and if he believes that security assistance should include cybersecurity assistance to help our partners protect their critical infrastructure or enhance their resilience against information warfare.

My question to you, sir, is, do you believe that
security assistance to partner nations should include cybersecurity and information warfare measures, first off, and second, do you believe we should pursue these types of relationships outside of the traditional five I nations that we have talked about mostly?

General Nakasone: Senator, I believe that in terms of the theater engagement that you discuss right there, our most effective means is to begin with the discussion with the combatant commander. So, if confirmed, we will look forward to obviously working very closely with Admiral Aquilino.

I do take your point on the idea of a broader partnership. We do need broader partnerships. We have tremendous relationships with our five Is. It is a critical capability that we have as a nation, but we are also looking at how do we expand those partnerships to bring a degree of competitive advantage against our adversaries in the future.

Senator Peters: Great. Thank you.

Thank you, Mr. Chairman.

Chairman Reed: Thank you, Senator Peters.

Senator Blumenthal, please.

Senator Blumenthal: Thank you, Mr. Chairman.

Thank you for your service, all three of our witnesses today.

General Nakasone, I appreciated our discussion before
this hearing about the contributions of the National Guard in Connecticut and you were mentioning them in your testimony. Across the country, the National Guard have really been integral to many of our cyber efforts. Before this last election, the Connecticut National Guard, in particular, was a really invaluable resource to many local officials in preventing cyberattacks and taking action to detour them, and then more recently, as you know and we discussed it, the National Guard was an immense resource to Connecticut in responding to ransomware attacks against Hartford schools and in preparing for responses to particular attacks, but also, again, detouring them.

I am also very expedited about the grant that the University of New Haven received to train more National Guard members on cybersecurity skills under Project Ironclad. Not only will the University of New Haven help us train more cybersecurity talent in New Haven and Connecticut, but it could also help create a national pipeline to recruit and retain the expertise in our country that we so desperately need.

Could you explain how the University of New Haven's Project Ironclad training program fits with our need for more cybersecurity talent.

General Nakasone: Certainly, Senator, but let me take a step back and just talk a little bit about the work of the
Connecticut National Guard, because I think that in my previous statement, I wasn't specific enough on how big a deal this was.

So, if you think about it, a ransomware, and as I indicated, ransomware on the 2nd of September that is impacting the school system, but it is also impacting fire, and police, and emergency medical services. Think about that, if you are losing that from a capability within your community, Connecticut National Guard, 24 hours, working with us at U.S. Cyber Command and National Security Agency, utilizing a capability called the Cyber 9-Line where they are able to leverage our expertise back at Fort Meade, and then being able to deal with the problem.

This is the Connecticut National Guard that is solving the problem. They are just getting a bit of assistance from us. That is a huge deal and I think it is really a great exemplar of how powerful the National Guard can be not only in a situation like this, but also, I want to point out the work that they did during the 2020 election in ensuring its success.

And also, most importantly, and I don't think it is well-known, their work with the Department of Homeland Security in ensuring the security of warp speed, our ability to bring a vaccine for COVID-19 to the American populous. This is the work that the National Guard has done over the
past 9 months and I think it is critical.

In terms of New Haven, this is really a great new story and being able to, again, generate interest, generating context, generating an ability for those that have, you know, a desire, a knowledge, an inkle of what they want to do in the future and bringing them with the capability to train and then being exposed to cyber for the future.

Senator Blumenthal: I think that your points are so well taken. Our National Guard has been such a critical resource in Connecticut in the elections, in countering ransomware, in building the kind of intellectual infrastructure that we need. And as I remarked to you in our conversation, the National Guard draws on the expertise of citizen soldiers who are in civilian jobs involving IT. They are experts in major corporations and they are providing their expertise now to not only our nation's military, through the National Guard, but also to civilian election officials, to local education efforts to deter ransomware, and I think your point about the University of New Haven is so well taken, the ironclad project offers tremendous promise of recruiting, training, and retaining the talent that we need in our military, as well as in our civilian lives for cybersecurity and cybersecurity is our future.

And I thank you for the work that you are doing and
that you are encouraging and promoting by the National Guard. Thank you.

Thank you, Mr. Chairman.

Chairman Reed: Thank you, Senator Blumenthal.

And now via Webex, let me recognize Senator Rosen.

And I thank Senator Kelly for his patience.

Senator Rosen?

Senator Rosen: Thank you, Chairman Reed.

Thank you to our witnesses for your service and, of course, always for being here today.

You know, as a former computer programmer, I am interested in learning how DOD's cyber strategy can really strengthen our nation's ability to withstand and respond to cyberattacks.

And I would also like to recognize today, the role that Nellis Air Force Base plays in supporting SOCOM mission in the battlefield. It is really, really important and I am proud of our men and women there at Nellis Air Force Base.

But I want to talk about information warfare. Despite an unprecedented level of foreign influence campaigns, we know they are targeting the United States and other democracies. We lack a clear strategy to combat information warfare.

As the National Security Strategy makes clear, our autocratic adversaries are using aggressive, aggressive
information warfare tactics to interfere in our democratic
elections around the world, exploit the pandemic, and erode
trust in the rules-based international order.

So, General Nakasone, and then General Clarke, what is
the appropriate role for the military to play in this
environment of heightened information warfare?

General Nakasone: Senator, I think the appropriate
role is the role that we have begun playing since 2018,
which is the perspective of how do we defend for the idea of
operating outside of the United States, being able to both,
enable our partners with information and act when
authorized.

This is an active approach to our adversaries. It has
been most effective, as we have seen, with the 2018 and 2020
elections with adversaries attempting to influence us,
attempting to interfere, but not being able to do that.
That is based upon the strategy of defend forward and the
instantiation of persistent engagement. That is the start
of it.

As I mentioned earlier today, I also think there is a
broader piece that is being worked right now by the
administration in terms of how do we improve the further
resilience of the United States as we look at adversaries
continuing to avoid our laws and policies and try to use our
own infrastructure in their own attempts.
This is a continual effort that we have to be at. This is not going to be episodic. This is something that U.S. Cyber Command and the other combatant commands need to continue to work in.

Senator Rosen: So, perhaps, General Clarke, you can speak to this. I want to add one more thing to this question now that you talk about defend forward.

How do we detour our adversaries' cyber aggression by changing their cost-benefit analysis? How do we make it not worth their while to attack us and what policies are we doing there? When you speak about defend forward, isn't that part of this equation, too?

General Clarke: Senator, you raised a great point. Number one, I think we have to work closely with our Department of State and other agencies in this space. Number two is that while General Nakasone talks about forces forward, which I agree with, we also have SOCOM forces for it that are absolutely the meso professionals that work closely with the embassies and with foreign partners, and that ties this ecosystem of forward all the way back to the capabilities and capacities that exist in the U.S.

And I think by working closely with those partners to ensure that our adversaries or competitors are not getting that free pass and to recognize what is truth from fiction and continue to highlight that through using our intel
1 communities is critical.

General Nakasone: And, Senator, if I might add on to
2 that, to your point with regards to imposing costs, this is
3 not just the Department of Defense. As General Clarke
4 rightly points out, this is a Whole-of-Government effort.
5 This is what the power of Treasury brings to it, the Federal
6 Bureau of Investigations, Justice, Department of Homeland
7 Security. This is the lesson that we have learned is that
8 we have to operate together, because the partnership is
9 where the power is.

10 Senator Rosen: Well, that is great.
11 I want to continue on that. We do have a Cyber
12 Strategy. We have had a lot of cyber espionage.
13 How often should our cyber strategy be updated to
14 reflect current threats and the current challenges? How
15 often do you envision that we need to do that in order to
16 stay relevant?
17 If it is 2 years old, 3 years old, it is not being
18 responsive, and so I was wondering what you think would be
19 appropriate for these kinds of cyber strategy reports to be
20 updated.

21 General Nakasone: So, we have an interim National
22 Security Strategy guidance that is out, that the
23 administration has put out, that has been very effective for
24 us to start our guideline with it. It talks about
cybersecurity as a key enabler in that. That is an important piece of what our nation needs to do.

Senator Rosen: Yeah, but actual threats, how do we let people stay up to date on actual threats?

General Nakasone: Obviously, that is through the continuing dialogue in terms of what our intelligence community is talking about, obviously, what our Government is talking about, and also, really importantly, what the private sector is talking about, because they are seeing so many of these threats, Senator.

Senator Rosen: Thank you. I believe my time has expired, Mr. Chair.

Chairman Reed: Thank you very much, Senator Rosen. Gentlemen, thank you for your service to the nation and thank you for your testimony today.

This will conclude the open portion of the hearing. We will reconvene in SCV-217 as quickly as possible.

Thank you very much, again. The open hearing is adjourned.

[Whereupon, at 11:39 a.m., the hearing was adjourned.]