[H.A.S.C. No. 118–5]

THE FUTURE OF WAR: IS THE PENTAGON PREPARED TO DETER AND DEFEAT AMERICA'S ADVERSARIES?

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

HEARING HELD
FEBRUARY 9, 2023

U.S. GOVERNMENT PUBLISHING OFFICE
52–380 WASHINGTON : 2023

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

MIKE GALLAGHER, Wisconsin, *Chairman*

MATT GAETZ, Florida
LISA C. McCLAIN, Michigan
PAT FALLON, Texas
DALE W. STRONG, Alabama
MORGAN LUTTRELL, Texas
JENNIFER A. KIGGANS, Virginia
NICK LaLOTA, New York
RICHARD McCORMICK, Georgia

RO KHANNA, California
SETH MOULTON, Massachusetts
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
ELISSA SLOTKIN, Michigan
JARED F. GOLDEN, Maine
PATRICK RYAN, New York
CHRISTOPHER R. DELUZIO, Pennsylvania

Sarah Moxley, *Professional Staff Member*
Michael Hermann, *Professional Staff Member*
Payson Ruhl, *Research Assistant*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

PREPARED STATEMENTS:

DOCUMENTS SUBMITTED FOR THE RECORD:

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:

[There were no Questions submitted post hearing.]

THE FUTURE OF WAR: IS THE PENTAGON PREPARED TO DETER AND DEFEAT AMERICA'S ADVERSARIES?

House of Representatives,
Committee on Armed Services,
Subcommittee on Cyber, Information
Technologies, and Innovation,
Washington, DC, Thursday, February 9, 2023.

The subcommittee met, pursuant to call, at 8:30 a.m., in room 2118, Rayburn House Office Building, Hon. Mike Gallagher (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MIKE GALLAGHER, A REPRESENTATIVE FROM WISCONSIN, CHAIRMAN, SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

Mr. Gallagher. The subcommittee will come to order. Welcome to the first hearing of the Cyber, Information Technology, and Innovation [CITI] Subcommittee in the 118th Congress. I am thrilled to lead this subcommittee with my friend and colleague, Representative Ro Khanna, who is going to be joining us in about 30 minutes. I believe it is his wife's birthday. That is more important. But I have worked very productively with Ro for 6 years, and I would like to enter into the record an op-ed that Representative Khanna and I wrote together as freshmen Members of Congress.

The piece focuses on congressional reform, not defense, but it demonstrates that we have long been willing to work across party lines to modernize this institution. And while Ro is a progressive, and I am a conservative, we both like to think for ourselves. And we both believe that the Department of Defense can do better when it comes to innovation.

In my opinion, the only way to truly win World War III is to prevent it. And if we accept the slow bureaucratic status quo, deterrence will fail again, as it failed in Ukraine. And on this subcommittee, I would like us to dedicate ourselves to the question of how we deter war. There are three questions in particular I think we need to answer.

First, is the Pentagon prepared for an invasion of Taiwan that has already begun in cyberspace? Second, what technologies are most important for winning a future war, and what are the barriers to the Department rapidly adopting such technologies, particularly commercial technologies. And third, are the services and the Pentagon sensibly structured and resourced to recruit, train, and maintain and equip cyber warriors?

As we work to deter war, time is not on our side. It has taken me 6 years to get this gavel, and I intend to wield it against the forces of darkness that waste our time, which is our most precious resource. So behind me, you see a picture of the clock at Lambeau Field, which is always set 15 minutes early to reflect—15 minutes fast to reflect Vince Lombardi's wisdom that if you are on time, you are 15 minutes late. This committee will operate with the Lombardi time principle in mind.

To this end, I have developed the three CITI commandments, which you will see on the other side here, on this sign behind me.

First, we will start on time. We passed our first test. Thank you to Representative Moulton for being here on time. And since I have to be here the whole time anyways, I may just yield my initial question time to punctual members like Mrs. McClain who was here on double Lombardi time, 30 minutes early.

Second, 5 minutes shall be 5 minutes. I have gained a profound respect for former chairman, now Ranking Member Adam Smith's ability to enforce the 5-minute timeline. That being said, if you stick around until the end, I am always more than happy to entertain a second round of questions.

And third, to the extent possible, let's not use acronyms or jargon. The Pentagon suffers from a disease called acro-nymphomania, a fetishistic use of acronyms that clouds clear thinking. And on this subcommittee, let's please try to communicate in simple and direct language that normal Americans can understand.

So in the spirit of these three commandments, and in the hope this is the longest speech I will ever give on this subcommittee, I will stop talking and yield to Representative Moulton, who did phenomenal work chairing the Future of Defense Task Force and has long been a leading voice for innovation in the defense enterprise.

Mr. Moulton.

[The prepared statement of Mr. Gallagher can be found in the Appendix on page 45.]

STATEMENT OF HON. SETH MOULTON, A REPRESENTATIVE FROM MASSACHUSETTS, SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

Mr. MOULTON. Thank you, Mike.

General C.Q. Brown, Chief of Staff of the Air Force, has written and said many times over the last several years: accelerate, change, or lose. And that really is what is at stake here. If we do not change more quickly to modernize our ability to conduct warfare, we will lose. By many measures, we are losing to our adversaries already who are modernizing much more quickly than we are. So, we have a lot of work to do to catch up, so that the ultimate goal, as Mr. Gallagher so well articulated, is achieved, which is preventing war, deterring war, showing our adversaries that we will beat them if they try. So we have a lot of work to do, and it is an honor to be back on this subcommittee. We have some excellent witnesses here today, some of the best of the best.

So let me turn it over to all of you.

And Mr. Gallagher, thank you very much and congratulations on making it here after 6 years.

Mr. GALLAGHER. Thank you. As Representative Moulton said, we have a phenomenal panel of witnesses joining us today. We have Mr. Christian Brose, Chris Brose, who is the chief strategy officer of Anduril Industries, and author of an incredible book called, “Kill Chain: Defending America in the Future of High-Tech Warfare,” which I recommend to all of you. Prior to his current role, Mr. Brose served as senior policy advisor to Senator John McCain and later staff director of the Senate Armed Services Committee.

We also have Admiral Mark Montgomery, who is the senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. He served in the U.S. Navy for 32 years, holding posts as director for operations at U.S. Pacific Command and commander of Carrier Strike Group 5. Admiral Montgomery served as the executive director of the Cyberspace Solarium Commission, which I co-chaired with Senator Angus King, and it was a pleasure to work with him.

And we also have Mr. Peter Singer, who is currently a strategist at New America, and founder and managing partner at Useful Fiction, LLC. He served as a consultant for the U.S. military and intelligence community, was coordinator for the Obama campaign’s defense policy task force, and is a prolific writer on futuristic national security issues, including having written one of my favorite books of all time, “Ghost Fleet.” “Burn-In” is also exceptional. I am waiting for movie versions of these books, Mr. Singer, and I believe has more books on professional reading lists than any other author alive—military professional reading lists than any other author alive or dead.

So with that, I will turn it over to Mr. Brose for his testimony.

STATEMENT OF CHRISTIAN BROSE, CHIEF STRATEGY OFFICER OF ANDURIL INDUSTRIES; AUTHOR; FORMER SENIOR POLICY ADVISOR TO SENATOR JOHN MCCAIN; AND FORMER STAFF DIRECTOR, SENATE ARMED SERVICES COMMITTEE

Mr. BROSE. Thank you, Mr. Chairman, members of the subcommittee, it is an honor to have the opportunity to testify before you today on the future of warfare.

Often when this topic is discussed in U.S. defense circles, it is treated as a future problem. Something coming in the 2030s or 40s, something we have time to get ready for. This, I would contend, is dangerously wrong. The future of warfare is here, and America is largely being ambushed by it. The U.S. military and our way of war are being disrupted. Our idea of national defense is largely based on the ability to project military power across the globe using small numbers of large, expensive, exquisite, heavily manned, and hard-to-replace ships, aircraft, and other platforms. The Chinese Communist Party knows this, and has been working diligently and with regrettable competence to be able to not just degrade and destroy America’s small number of large expensive military things, but to render U.S. forces deaf, dumb, and blind, and unable to fight.

At the same time, our defense enterprise is also being disrupted by new technologies, such as artificial intelligence, autonomous systems, robotics, ubiquitous sensors, and low-cost access to space. Technologies such as these are changing the character of war, and this, too, is happening now. In the recent Nagorno-Karabakh conflict and the continued fighting in the Middle East, and in the ongoing war in Ukraine, we are seeing how low-cost robotic vehicles, AI-enabled loitering munitions, digital targeting systems, cyber weapons, persistent communications and surveillance satellites, and other advanced capabilities, especially when paired with large volumes of more traditional weapons, are transforming warfare.

Some lessons are emerging from this recent experience. On the current and future battlefield, moving and communicating is highly contested. Hiding is nearly impossible. And once detected, surviving is just as difficult. This means that a correctly armed and ready defender can make life hell for militaries that have optimized for long-distance power projection and offensive operations, militaries such as our own. These dual disruptions of threat and technology have been underway for years, but for many reasons having largely to do with our own politics and bureaucracy, the United States has been too slow to respond.

As a result, we are entering what the chairman has called the window of maximum danger, a period over the coming years when the Chinese Communist Party, feeling undeterred by the U.S. military, may seek to remake the status quo in the Asia-Pacific region through force, for instance by invading Taiwan. None of us wants that to happen, nor can we predict whether it will. All we can do is ensure that we are ready if, God forbid, deterrence fails and U.S. forces are called to maintain the peace.

This responsibility falls most heavily to you and your colleagues in the 118th Congress. Nothing you do in this Congress will make larger numbers of traditional ships, aircraft, and other platforms materialize over the next several years. It is possible, however, to generate an arsenal of alternative military capabilities that could be delivered to U.S. forces in large enough quantities within the next few years to make a decisive difference. Those decisions could all be taken by this Congress.

The goal would be to rapidly field what I have referred to as a money-ball military, one that is achievable, affordable, and capable of winning. Such a military would be composed not of small quantities of large, exquisite, expensive things, but rather by large quantities of smaller, lower cost, more autonomous, consumable things, and most importantly, the digital means of integrating them.

These kinds of alternative capabilities exist now or could be rapidly matured and fielded in massive quantities within the window of maximum danger. You could set this in motion in the next 2 years. The goal would be more about defense than offense, more about countering power projection than projecting power ourselves. It would be to demonstrate that the United States, together with our allies and partners, could do to a Chinese invasion or a Chinese offensive what the Ukrainians with our support have thus far been able to do to their Russian invaders: degrade and deny the ability of a great power to accomplish its objectives through violence, and in so doing, to prevent that future war from ever happening. After all, this is all about deterrence.

All of this is possible. We have sufficient money, technology, authorities, and we still have an enough time, if we are serious. If we make better decisions now, we can push this looming period of vulnerability further into the future, and this will mostly be up to you, for if these decisions are left even to the next Congress, they may be too late.

Thank you very much.

[The prepared statement of Mr. Brose can be found in the Appendix on page 49.]

Mr. GALLAGHER. Well within the 5 minutes. Thank you, Mr. Brose.

Admiral Montgomery.

STATEMENT OF RADM MARK MONTGOMERY, USN (RET.), SENIOR DIRECTOR, CENTER ON CYBER TECHNOLOGY AND INNOVATION, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Admiral MONTGOMERY. Chairman Gallagher, Ranking Member Moulton, other members of this subcommittee, thanks for inviting me here today. I mean, to answer the basic question, are we ready, I am afraid that like Chris, I believe that unless we make substantive changes to how we develop and procure weapons and how we embrace emerging technologies, the United States will not be ready to deter and defeat China in the demanding technological environment we are going to face in the next 5 years.

The U.S. relies heavily on precision-guided munitions, the ability to conduct large-scale mobility and sustainment ops [operations], and extensive intelligence collection capabilities to deter and defeat adversaries. But the Chinese have spent the last 25 years working this problem, investing in asymmetric weapons and sensor systems, using emerging technologies to neutralize America's operational superiority, and they have reduced the ability of U.S. forces to rapidly detect, track, and kill the adversary.

The Chinese now have a military force designed to place U.S. air and naval forces at risk within the first island chain, and the Chinese may soon have the same impact on U.S. forces within the second island chain. While U.S. military leaders have talked about China as the pacing threat, the Chinese have procured weapons as if the United States was their pacing threat. So, not surprisingly, Chinese action has outperformed American rhetoric.

But despite these challenges the U.S. can flip the script, and if we make the right investments to retain our military technological advantage, we can overcome Chinese asymmetric advantages. I would just say, outside of CITI's jurisdiction but inside HASC [House Armed Services Committee], there is a few things we could do right away. We could increase procurement of long-range weapons to strike Chinese ships. We could develop and deploy cruise, ballistic, and hypersonic defense capabilities throughout the Pacific. We could pre-position munitions in Taiwan for Taiwan's use in a contingency because we are not going to be able to resupply them like we do Ukraine. And we could actually train and exercise with the Taiwan air and maritime forces in theater as we do with every ever other ally and partner.

All of these actions will increase deterrence, and if a war comes, improve the chances of U.S. victory and drive down U.S. casualties, and we can do this only using a fraction of the current defense budget. Within the CITI Subcommittee, there are equally important steps that could be taken to ensure U.S. forces are ready. First, we can improve the cyber resilience of the military and the Nation. In the conflict with China, our forces need to be able maintain our ability to detect and track the adversaries, to communicate among units, and mobilize and sustain forces in the field.

To ensure this connectivity, the U.S. military needs to invest in better resilience and redundancy across every node and operational link. And I think this effort has to extend into our national critical infrastructure. The resilience of the transportation, electrical power, water, financial systems that enable the mobilization and resupply of U.S. forces has to improve.

The second thing this subcommittee can do is assess and strengthen the readiness and structure of U.S. cyber forces. U.S. cyber forces are really inconsistent in their organization, readiness, and training across the various military services. And the size of each military service's contribution to the cyber mission has not changed appreciably since the original agreements in 2010, despite significant changes in the threat from China and Russia. Really, this subcommittee has got to figure out if the current design of the cyber mission force is what we need for the 21st century, or should we be considering an independent cyber force, as was recently done with the Space Force.

The third thing this subcommittee ought to be pushing is an environment to innovate. The U.S. has learned some really important lessons from the conflict in Ukraine. For example, the Ukrainians needed anti-ship cruise missiles to limit Russian naval operations in the Black Sea, but there was no program of record available for a land-based Harpoon missile launching system. So the Ukrainians worked with Boeing, the Danish Army, and the U.S. Navy to "MacGyver" together a launcher system, and they did this in 2 months.

But Taiwan was approved for a similar land-based Harpoon system in 2020, and they have been told delivery of the new design system will be 2027 or 2028. Clearly, we could do a similar "MacGyver" approach, and we should do that with Boeing and the Navy to ensure that our key partner, Taiwan, has the weapon systems it needs to deter Chinese action sooner than 7 or 8 years after they ordered it.

Finally, this committee could ensure that the U.S. works with our allies to maintain interoperability with U.S. forces. You know, we have a problem when we modernize software and technology systems. We often create gaps that lead to challenges conducting coalition operations. I think we have to be particularly aware of this as we develop and field the—and I will use an acronym here—JADC2 [Joint All-Domain Command and Control] architecture.

So in conclusion, what I would say is that the U.S. may not be on the right track today for a conflict with China, but we can make some smart investments now to get back on track, and this subcommittee can help make that so.

[The prepared statement of Admiral Montgomery can be found in the Appendix on page 58.]

Mr. GALLAGHER. Thank you. You can use an acronym. You have to spell it out first. Joint All-Domain Command and Control. But thank you.

Mr. Singer.

STATEMENT OF PETER W. SINGER, STRATEGIST, NEW AMERICA, AND MANAGING PARTNER, USEFUL FICTION LLC

Mr. SINGER. Thank you, Mr. Chairman and members, for the opportunity to speak to this important hearing. As with the other witnesses, my testimony today represents my personal opinion, not the official position of any organization I have worked with.

You asked us whether the Pentagon is prepared to deter and defeat America's adversaries. A valuable approach to answering your question is to ask a question in turn. What would a "yes" look like in the future? We can then work backward and explore both the elements of such a potential future successful history and how we can build towards them today.

One methodology for this cross of strategy and scenario is the deliberate blend of nonfiction research and analysis with narrative. Known as FICINT or useful fiction, the goal is to share the facts of new trends and technologies, but in a scenario format that the science of the brain shows is more likely to lead to both understanding and action. I have entered into the record such a scenario crafted for this committee entitled "What Would Winning Look Like?" Told from the perspective of an imagined PLA [People's Liberation Army] officer in the future, it envisions a positive outcome for the hearing's question and the central problem for U.S. defense planning, a future world in which the United States has successfully deterred the PLA from attacking Taiwan.

While I hope you take the time to engage with and even enjoy the narrative, today I would like to share with you some of the policy findings of it.

The key elements of a winning outcome for the U.S. military in the future of war would include that we, one, enact regular open-ended war games designed to truly test and learn.

Two, avoid letting political and bureaucratic inertia and the mentality of sunk cost drive acquisitions.

Three, foster a dynamic defense marketplace where the military can engage with and easily purchase from both big and small firms.

Four, scale innovation hubs and experimental task forces such that every command has access to rapid means of learning and implementation. And we should also replicate the current "Shark Tank" contests in some portions of the force across it to award bottom-up proposals and fixes from junior troops.

Five, acquire a new generation of unmanned systems across all domains but avoid unmanned systems that simply replicate the expensive manned systems that they are replacing.

Six, develop new doctrines to take advantage of robotics' unique attributes, allowing swarming and cheap, high-risk uses.

Seven, prepare for certain adversary use with counter-drone systems of kinetic, EW [electronic warfare], and directed energy.

Eight, invest in AI [artificial intelligence] and quantum technology to match its growing civilian importance.

Nine, reform U.S. military networks to create a federated model of mesh data to take advantage of the benefits of AI.

Ten, ensure that the U.S. military is able to retain its professionalism while evolving to reflect the new America that it both draws upon and protects.

Eleven, scale new U.S. military units able to operate across multidomains, rapidly deploying networks of small teams, each able to operate independently yet generate disproportionate kinetic and non-kinetic effects against major systems.

Twelve, transform special operations forces into blended teams of technical experts and elite soldiers, able to provide a more comprehensive full continuum of uses.

Thirteen, create redundancies in scale and space through fleets of micro-sats [microsatellites] and cheap launch systems.

Fourteen, bake security into the emerging Internet of Things through requirements and regulation so as to limit physical damage from digital threats.

Fifteen, utilize cyber and diplomatic means to repeatedly out covert campaigns designed to undermine democracies.

Sixteen, engage in persistent competition on the info [information], economic, political, and cyber fronts to create greater friction for the PLA and CCP [Chinese Communist Party].

Seventeen, provide Taiwan distributed anti-air weapons and unmanned systems to take away adversary quantitative advantage, and most especially cheap rapidly deployable smart mines to block essential seaways.

Eighteen, aid efforts to create a Taiwanese society prepared for resistance, especially in urban settings and by mirroring its digital systems outside the country.

Nineteen, bolster multilateral ties between states that have worsening bilateral ties with China.

And finally, twentieth, secure Russia's defeat in Ukraine, both to weaken it and its allies, as well as provide a model of success for other democracies under threat.

In closing, I hope you find both the lessons and the approach useful as a means to stoke healthy discussion about the future of war through envisioning a successful outcome of the committee's work.

[The prepared statement of Mr. Singer can be found in the Appendix on page 72.]

Mr. GALLAGHER. Thank you.

Before we go to questions, I ask unanimous consent to enter Ranking Member Khanna's opening statement and our joint op-ed into the record.

I think it just happens like that. Look at that. Without objection, so ordered. Okay. Hey, I am learning. With great power comes great responsibility.

[The prepared statement of Mr. Khanna can be found in the Appendix on page 47.]

[The op-ed referred to can be found in the Appendix on page 93.]

Mr. GALLAGHER. I know Mrs. McClain has to go to another hearing and was here earlier than anyone else, so I will recognize her for 5 minutes of questions.

Mrs. MCCLAIN. Thank you, Mr. Chairman. And thank you all for being here today. I really appreciate it.

I come from the business sector. So this is new to me, but I try and apply a lot of the same concepts and principles that work in private sector. And I realize government isn't the same as the private sector, but it doesn't mean that we necessarily shouldn't adopt some of the same concepts.

So with that said, obviously for the past several years we have seen that the United States has had significant shortcomings in cyber defense. From January 2020 to February 2022, Russian state-sponsored actors hacked numerous defense contractors. May 2021, the Colonial Pipeline was the victim of ransomware. In June 2022, the FBI [Federal Bureau of Investigation], National Security Agency, and CISA [Cybersecurity and Infrastructure Security Agency] announced that Chinese state-sponsored hackers targeted and breached major telecommunication companies, et cetera, et cetera. We could go on and on, right?

Mr. Singer, you asked a very prudent question in your testimony when you talked about what would winning look like. I would like you to expand on that. And then the second thing is, you gave us 20 ideas, which are wonderful, but in all reality, if we can do one, that would probably be an accomplishment. So let's talk a minute about in your opinion, what would winning look like?

Mr. SINGER. Thank you for the question.

I think to break it down in particular on the area that you are interested in, in terms of business practices in cybersecurity, let's imagine a future Internet of Things, because we have a core change happening from using the internet for communication to operating our systems. What would we like it to look like to be both—deliver what we need, but also secure. And a big problem right now is that we are repeating the mistakes that we made in the original design and lack of regulation for the internet. That is——

Mrs. MCCLAIN. And I don't mean to keep interrupting, but I only have like 2 minutes, or 3 minutes, and the chairman is going to hold me to it.

Mr. SINGER. Yeah. Go for it. What winning would look like would be a secure——

Mrs. MCCLAIN. So it is regulation?

Mr. SINGER. It would be in part regulation towards greater design security for Internet of Things systems, much like the approach that has been taken within the defense economy. We have parts of regulation of other aspects of critical infrastructure, but it is very spotty. So for example, banking cybersecurity is great right now. Energy, water systems, not.

Mrs. MCCLAIN. So what is interesting to me is from the private sector, and I am going to tie the two together, is you know, we have to have a cyber defense officer. And if a business owner gets hacked, we pay a consequence. We are held accountable, right, to our own dime at our own expense.

Can you speak to the lack of accountability or consequence? Do you think that plays a role?

Mr. SINGER. Very much so, yes. We have unclear accountability, and the result is for the most part, the costs fall upon the victim.

Mrs. MCCLAIN. What would you say the accountability is? Because from my situation as an outsider looking in and from a lot of my constituents, it seems like the answer to that accountability is just throw more money at the problem. And until we get to the root cause of what these issues are, we can—it is like throwing mud at the wall.

What, in your opinion, are the root causes of all of these failures? There might be 20 of them, but give me the one that if we could fix this one, it would give us the biggest bang for our buck?

Mr. SINGER. I think I would agree with, actually, my colleague, Mr. Brose. If we could get most bang for the buck right now in terms of future of war, it would be greater numbers of small unmanned systems and smart mines that would be able to deliver a greater defense to allies under threat like Taiwan.

Mrs. MCCLAIN. And in your opinion, why don't we do that? Meaning, is it a priority? Is it a lack of funds? Is it accountability? Is it talent? Why don't we do it?

Mr. SINGER. I think it is a combination of the sunk-cost mentality. They aren't old programs. They would require new programs.

Secondly, many of these systems, the profit margins aren't great unless you buy them in scale, and, bluntly, the defense economy right now doesn't trust the military to buy small cheap systems in scale.

Finally, many of them are not, bluntly, sexy. Sea mines is on one hand been most lethal to U.S. Navy ships, but they are not the kind that you get great promotions from.

Mrs. MCCLAIN. Thank you.

Mr. GALLAGHER. The gentlelady's time has expired.

Mr. Moulton.

Mr. MOULTON. Thank you, Mr. Chairman. When we co-chaired, Mr. Banks and I, the Future of Defense Task Force, a couple of the interesting conclusions we came to is that essential to deterring and winning future conflicts, not just modernizing our military, that is pretty obvious. But also developing a next generation or a new generation of alliances and arms control. And I would like to focus on those for a second.

We have seen how important the NATO [North Atlantic Treaty Organization] alliance has been for decades of deterrence in Europe, and now winning the war in Ukraine. But we don't have a NATO alliance or a NATO-like alliance in the Pacific, which is of great concern as we look at the rise of China. Likewise, arms control has been effective at both deterring and putting us in a position to win future conflicts.

The deterrence piece is probably pretty obvious. If you have well-balanced deterrents on both sides, a comparable number of nuclear capabilities between the United States and Russia, for example, you are less likely to get into a conflict. And obviously, by reducing arms overall, we try to reduce the likelihood of conflict to begin with.

But we don't often think about the role that smart arms control can also play in setting us up to win a future conflict. If we limit the number of nuclear warheads that either side has, but ours are much more accurate, then we are giving ourselves an advantage.

Can you speak for a minute to the role of arms control in preparing us to better deter and win a fight with AI-enabled systems? Because we have a lot of nuclear arms control. We haven't even discussed arms control when it comes to AI.

Mr. Brose, perhaps I will start with you.

Mr. BROSE. So I think the problem is less about arms control at the moment. I think it is more about actual arms generation. I think the reason——

Mr. MOULTON. I understand that. But I would just like to focus on the arms control piece. Because here is my concern: If there are no rules for the use of AI, we are going to still constrain ourselves by our values but our adversaries may not, which gives them an inherent advantage. So how do we counter that?

Mr. BROSE. I think it really comes down to developing these types of capabilities with our values at the core of them. And I think a lot of times in the past where we have developed technologies, remotely piloted aircraft, we have made the mistake of being overly secretive about how we are thinking about them, how we are building them, how we are using them.

I actually think in the development of these technologies being more transparent about the challenges, the brittleness, the ways in which we are building these and developing and fielding these technologies with our values at the core of them will provide us the moral high ground. It will give us greater leverage and greater kind of public standing to make demands of others, primarily countries that don't share our values.

I guess the thing that I would just underscore is, even if we do all of that, I am not terribly confident that they are going to follow suit. I think at the end of the day, this becomes something where we have to have the capability such that there is even something to be able to discuss. I think you have already agreed with that.

Mr. MOULTON. Yeah. Of course.

Admiral Montgomery, do you have any comments on this?

Admiral MONTGOMERY. So I think where we are looking at this closest now is what kind of agreement—what kind of way—how do we proceed with man-in-the-loop, man-on-the-loop, and man-out-of-the-loop as you bring AI technology into our unmanned craft, and how do we talk to the Russians and Chinese about it. I think it is fine to talk to them. In cybersecurity, we looked at this and we found that there was just no way to verify, and therefore it became very hard to trust our discussions with the Russians that we had on this.

And what I would say is, we operate with man-in-the-loop. We design systems to man-on-the-loop. We probably need to design systems to man-out-of-the-loop, have that capability and capacity. So that if we understand that our adversaries are operating man-out-of-the-loop, we are able the to do it. Because the OOTL [out-of-the-loop] loop—not to use another acronym—but the decision-making cycle for man-out-of-the-loop is so much faster than on-the-loop and in-the-loop, that if we have not developed those weapon systems and sensor systems, we will not succeed.

Mr. MOULTON. Mr. Singer—we are running out of time, but I would appreciate your comments for the record on this. I want to get to another question quickly.

[The information referred to can be found in the Appendix on page 99.]

Mr. MOULTON. Admiral Montgomery brought up the idea of having an independent cyber command.

Mr. Brose, do you think that that is a good idea?

Mr. BROSE. An independent cyber service, I think is definitely something that needs to be looked at. I think that the reasons that the Congress led the creation of the Space Force are just as prevalent, if not more, inside of the cyber capabilities and the cyber services. It is definitely something that needs to be seriously considered.

Mr. MOULTON. Thank you, Mr. Chairman. I yield back.

Mr. GALLAGHER. Thank you. And before I recognize one of our members for a question, I want to recognize that the ranking member, Mr. Khanna, has showed up. I know it was his wife's birthday. So I have gotten her a birthday present for you to open. I am sure it is exactly what she wanted. And feel free to open it as we ask questions.

Mr. KHANNA. I thought I was in trouble, Mr. Chair, for being non-punctual, but you had advance notice.

Mr. GALLAGHER. No. You worked with us, and Mr. Moulton covered you very well. So, thank you, Mr. Moulton.

Now, I am going to recognize one of our new members, Congressman LaLota from Long Island, who is a U.S. Naval Academy grad, a surface warfare officer [SWO] who has deployed to 20 countries, and most importantly, his brother is a Marine sniper; is that correct?

Mr. LALOTA. Yes, Mr. Chairman.

Mr. GALLAGHER. Great. Well, we are very excited to have your wealth of experience on the committee. I now recognize you for 5 minutes.

Mr. LALOTA. Thanks, Chairman, and thanks for hosting this very important meeting on this topic. And to you gentlemen, we appreciate your insight, your expertise, but more than anything else, your dedication in this very important warfare area to help defeat and deter our Nation's adversaries. Very much appreciate that insight.

Admiral, appreciate your service. I read that you were a SWO as well, and Mr. DeLuzio on the other side who is going to return to us as well, has our common background too; so it'd be nice to have a chat with you.

But specifically to you, Admiral, in looking at the readiness of the cyber mission force, how far back does this issue go? Has it improved since the cyber mission forces marked full operational capability in 2018, Admiral?

Admiral MONTGOMERY. Thanks. That is a great question because really to the best of my knowledge, readiness has been and remains a problem for the cyber mission force. You know, before reaching FOC, full operational capability, we kind of all had a widespread belief that once they reached—the CMF got there, they would then burn down the readiness problem over the years. They would only get better. Well, that has not happened. We reached FOC almost 5 years ago, and we know that assumption didn't pan out.

Readiness today is relatively the same as it was and then, so now, people come to us and say, well, look it is really about metrics. If you just understood—you know, it is hard to do metrics in cyberspace. The metrics are wrong. I don't agree with that. I think Cyber Command under Admiral Rogers and then General

Nakasone has absolutely laid out some good cyber metrics. And the truth is, the services aren't meeting them.

It is not always a priority. It is sometimes a priority, not always a priority. And when you don't prioritize cyber—the train, maintain, equip functions—it won't function. And really, it is unreasonable to believe that pursuing the same course of action for a sixth year in a row is going to get us healthier.

Mr. LALOTA. I appreciate that, Admiral.

My second and last question is for Mr. Brose. Sir, in hearing your testimony, it reminds me of the wise words of our Chief of Naval Operations, Admiral Gilday: "Get Real, Get Better." I especially appreciate your money-ball analogy. You also mention in your testimony how technologies are changing the characters of war, the technologies such as AI, our autonomous systems, and robotics.

My question is: How would you suggest that we best integrate these new technologies with our current and traditional weapons, and if you have enough time, would you recommend prioritizing these new technologies over traditional weapon systems?

Mr. BROSE. Yeah. Thank you for the question.

I think when it comes to the integration, much of that is going to be a software problem. This a solvable problem. Modern software is more than capable of figuring out how to pass information to and receive information from military systems.

In terms of integrating from more of an operational and organizational perspective, I don't think we have even begun to scratch the surface of that, and I think the problem is because we don't actually have enough of these capabilities to even begin to wrestle with the kind of question that you are posing.

So I guess my contention would be, first and foremost, we have to start fielding these types of systems that are absolutely available now. We are not talking about, you know, photon torpedos and cloaking devices. The challenge is, I think in the government we tend to make the easy problems so hard that we never actually get to the hard problems, which are the ones that you are asking, which is how are we actually going to organize ourselves and fight with these different kinds of capabilities, primarily autonomous systems.

Admiral MONTGOMERY. Can I jump in on that for 1 second?

Mr. LALOTA. Absolutely.

Admiral MONTGOMERY. I have to tell you, one of the issues is that the services do not procure munitions in the right levels. So as we develop a new system—I will give you one good example—something called the long-range antiship cruise missile. Every war game I play—I play about a dozen a year—as the Blue Force commander—we need about 1,200—let's say 1,000 or 1,200, these are unclassified war games. The Navy and Air Force have 240 right now.

We're building—the Defense Department's input every year has been 38 to 50. Congress has bumped it up to 75. If you do the math on that, the Department won't get us there until 2045. So this is the most critical weapon in the warfight with China, and we buy it at absolutely minimum production rates at the factory.

And the reason we do that is we cut munitions production—every service puts in a hundred percent of the munitions they need at the beginning of the budget cycle, and it is the bill payer every budget cycle. With China, it is the long-range antiship cruise missile and the SM–6 [Standard Missile 6] missile, and a few others. With Russia and Ukraine, we saw it was the Javelin and Stinger. We burned through 8 years of Javelin production in 9 months of combat. That is unacceptable at munitions production rates.

Mr. LALOTA. Thank you. I yield back.

Mr. GALLAGHER. Thank you. I want to recognize my first boss in the Marine Corps, Bert Steele, is in the audience. I just did a double-take. So if you need any kompromat about a young precocious Second Lieutenant Gallagher. He is right there. How are you, sir?

I am now thrilled to recognize another new member of the committee with an incredible background, another New Yorker, Pat Ryan, who is a West Point grad, a Georgetown grad, two tours in Iraq, worked at Palantir, a wealth of experience.

You are recognized for 5 minutes, Mr. Ryan.

Mr. RYAN. Thank you, Mr. Chair, and it is an honor to be on the committee with all of you all. And really, really appreciate you taking the time and your insights.

One question, and ask you to really try to push on this, to your money-ball approach, which I love, Mr. Brose, what should we get rid of? We always talk about what we should add. To push you all a little bit, can you think of one or two maybe legacy programs or anything that comes to your mind? I know it is a controversial question, but we never ask it. What—even a smaller thing that we could get rid of to help free up dollars and energy and resources for the good recommendations you are making.

Mr. Brose, start with you.

Mr. BROSE. I think there is plenty of opportunities to take a look at. I think there is force structure we need to consider in terms of the number of people, how large the services are going to need to be, because at the end of the day, people tend to be the most expensive investment in the Department.

I think there are a lot of legacy systems in terms of surface combatants in the Navy, sort of infantry fighting vehicles in the Army, fourth-generation fighter aircraft that don't have the legs or the signature to be able to do the kinds of things that we would have to do in a high-end fight.

But here too, I think the challenge is—I would focus more on the things that we need to start to get into the hands of our operators, because unless you start to give people new tools, I would not be in favor of taking the tools that they have away from them.

And I think that tends to be the challenge here, which is we focus on the things we need to cut, which is totally something we need to do. The problem is that the future never shows up. The new things never show up, so people can be forgiven for wanting to hold onto the things that they have.

Admiral MONTGOMERY. I do agree with Chris Brose that we have to look at troop levels. I think the Army has settled out around 450,000. We ought to keep them there. There was a Future of the Army study in 2016 where the Army said they needed to be

450,000. They don't like to discuss that in public, but that is the history of it.

The second thing I would do is adopt what Commandant Berger said when he first took over the Marine Corps, which is reduce large amphibious ships from 31 down to 21, and add in light amphibious warfare ships, LAWs. He has since been dragged off of that by former retired—by retired Marine Corps generals and shipbuilding interests. But the reality is amphibious ships are not a priority in a conflict in China.

I wrote our war plans for 4 years. I wrote our war plans for Europe for 2 years. They are not a priority there. They are a priority for Korea. Korea is not our number one priority. So if you are going to have to de-prioritize something, I would take that down. And I would do everything else Commandant Berger said in his re-imagining of the Marine Corps because it was fantastic.

As a Navy officer, I would say I wouldn't do anything to the Air Force. Honestly, the Air Force is the critical element in the conflict with China right now, and they are underresourced for the mission they have.

Mr. RYAN. Mr. Singer, anything to add?

Mr. SINGER. I would just add I think the focus shouldn't be simply on which systems, but rather the design, the organizational structure, the wire diagram. Basically, we have unit designs that primarily date from between the 1940s to the 1980s, and a Pentagon and command and control structure that reflects military reforms in Prussia in the 1800s.

So if you updated those, you would actually get a lot of the personnel gains that would save the money that you want and it [would] more reflect 21st century needs.

Mr. RYAN. Thank you. And I appreciate the nuance of understanding that we'd have things to add that would be more thoughtful. And thank you for that point, Mr. Brose.

Second question—I know we are running low on time—but the idea of talent, mindset, and what we need to do, sort of, as a whole of Nation, particularly looking at cyber forces, but in general, new ways of thinking and talent, any specific—I know that is a broad question, but any specific thoughts, recommendations there?

My district, proudly home to West Point. What can we be doing at our military academies, in our—even just our schools and community colleges to get at the cyber talent and other talent issues; with 27 seconds. Sorry.

Mr. BROSE. Just very briefly, I think the key talent challenge is going to be having the sufficient amount of technical talent in the government, in the Department of Defense or advising them, to be able to make informed and intelligent decisions about what is going to become—what is already becoming a highly technical force in terms of these types of emerging and advanced technologies in particular.

You know, if you are looking at it, and you can't sort of call balls and strikes and differentiate what is good from what is not, the government is going to make a lot of bad decisions. So having technical people in the room who are capable of helping the government make those decisions or make those decisions themselves I think is key.

Mr. GALLAGHER. The gentleman's time has expired. We will have to come back to the question of talent in the second round.

Next up, a Texan, a "Domer" [Notre Dame alumnus], a national champion, a man who has ran seven marathons on seven continents in 7 days; is that right?

Mr. FALLON. When I did that, I was as skinny as Mr. Gaetz.

Mr. GALLAGHER. An Air Force officer, Mr. Fallon.

Mr. FALLON. Thank you, Mr. Chairman. And thank you to the witnesses.

Mr. Brose, in my opinion, the future of warfare is going to be defined by innovative capabilities that we possess and how they compete against potential adversaries' capabilities, of course. Under the auspices of the Under Secretary of Defense for Research and Engineering, there is no less than seven different entities generally defined that are responsible for innovation within the DOD [Department of Defense].

With these entities like the defense advanced research agencies, there is some, you know, renowned breakthroughs. But still, there is a considerable amount of wasted time and effort and taxpayer dollars, et cetera, through the notoriously bureaucratic system. You know it seems like every time that the "good idea fairy" visits the Pentagon, you know, a new office is born, and a colonel gets his wings.

What can we do about the duplicative offices that are packed with bureaucrats for everything? It comes as no surprise to me that we struggle to bridge the "valley of death" in system designed like this. So through your experience, how do you think the Department can best streamline the efforts to capture innovation in timely manner moving forward?

Mr. BROSE. Thank you for the question.

And I think you are spot on. I would actually turn it back to this subcommittee to say, I think from my experience in government and out of government, there is a crying need for greater oversight, exactly to your point. You know, we are spending billions of dollars on research and development, new types of technologies, some of which are duplicative, some of which the commercial industry is already 10 years ahead on. Some year, some have, you know, no path to making an operational difference.

I think the first place that I would start is sitting down and actually going into real detail over, what are we spending, what are we actually working to develop, and using the powers that this committee and this Congress has, beginning to make some of the hard choices that, you know, perhaps the Department is not positioned or incentivized to make. And I think, you know, in so doing, you know, you can begin to start to create patterns of behavior on the executive branch where they may begin doing more of this themselves. But there is a desperate need to rationalize what we are spending and what we are doing on advanced technology and start really focusing on what are going to be the priorities that we need to get fielded fast.

Admiral MONTGOMERY. Can I jump on that?

Mr. FALLON. Yeah. Please.

Admiral MONTGOMERY. First, I would bottle up whatever the Marine Corps has going on, because—I will give you two systems, and they are acronyms, I apologize because I don't know them. The first is MRIC [Medium-Range Intercept Capability], where they took an Iron Dome system, their G/ATOR [Ground/Air Task-Oriented Radar] radar, and the existing all-domain command and control, and created a short-range air defense system that has eluded the U.S. Army for over a decade.

And then the second is they took a naval Standard Missile, paired it on top of a HIMARS [High Mobility Artillery Rocket System] launcher, and got themselves an anti-ship cruise missile system that can deploy all around the first island chain. Both of those were innovations that started down at the major/lieutenant colonel level and worked their way up through the system and succeeded. I mentioned earlier the Harpoon system, where the Ukrainians adapted that in 2 months.

They also ran out of SA–6 missiles for their Buk launchers, and grabbed our RIM–7 Sidewinders [missiles] and installed them in 1 week and began shooting down Russian cruise missiles.

Again, the Army has been working for 10 years on a system called IFPC, Indirect Fire Protection Capability. And it seems to me that we need to take this innovation that starts at the ground level and move that up because that is where you save money, and that is where you get real capability.

Mr. FALLON. Go ahead.

Mr. SINGER. Two specific ways that you could accomplish that. And really what you are after is that you don't want to scale innovation initiatives within the Pentagon. You want to scale them out at the edge.

And two very specific ways the committee could support this. The first is one of the most successful organizational efforts of this is Task Force 59, which is a naval task force out in the Middle East that is actually working and testing with unmanned systems in cooperations with the private sector and allies. It has been a great success in the Middle East. Scale it across the regions. Scale it across the services.

The second type of organizational structure to get after this is some units have—they are basically copies of the Shark Tank model, where it is you are taking bottom-up ideas from junior troops and rewarding them. The 18th Airborne Corps has one. Replicate those across the force. That is where you want scale.

Admiral MONTGOMERY. I can give you one other one, sir.

Mr. FALLON. Sure.

Admiral MONTGOMERY. We had the Strategic Capabilities Office—or Special Capabilities Office run by Will Roper, where he basically was read into all the SAP programs, the Special Access Programs, for every service, and all the normal programs. And he was able to marry up systems, take peanut butter and chocolate and make a Reese's Cup that we couldn't do with all those nine standard research and development organizations you mentioned. So continuing to support that is critical.

Mr. FALLON. Thank you, Mr. Chairman. I yield back.

Mr. GALLAGHER. The gentleman's time has expired.

Next up, the man from Massachusetts 9, whose district includes Martha's Vineyard, Nantucket, and Cape Cod, correct?

Mr. KEATING. Yes.

Mr. GALLAGHER. Not quite Green Bay, Wisconsin, but nice nonetheless.

You are recognized for 5 minutes.

Mr. KEATING. Thank you. It also includes Joint Base Cape Cod and Woods Hole Oceanographic Institute, UMass [University of Massachusetts] in Dartmouth that has contracts with the Navy Undersea [Naval Undersea Warfare Center], and a lot of things we are talking about, the research is going on right in my district. Thank you for being here.

Just looking in the mirror first before we just look at you, I would like at your own fear of answering the question, Congress, continuing resolutions, our inability to deal with the regular order, appropriations, even when we do it in House side, it goes nowhere in the Senate. I mean, these are stumbling blocks too in our own [inaudible].

Can you comment on how they are harmful? Our inability to do this, I mean, with the continuing resolutions for everyone else listening here, it locks us into what we are doing yesterday, and we can't go forward. And this has been going on for a long time. Can you comment on how that is one more barrier that we face?

Mr. BROSE. Thank you, sir. And you are spot on. Continuing resolutions and appropriations not passed on time are absolutely devastating for national defense. They are devastating for any company that is trying to actually plan and forecast what it is going to do. It is devastating for program offices that are trying to rationally spend money in efficient ways. But I would argue that they are absolutely worst of all for the kinds of nontraditional, emerging technology, the builders and providers of those systems, because they don't have an enormous amount of programs of record to fall back on. All of their things are new.

So if you are locked in the past, past requirements, the past budget, you are de facto not moving these types of things forward. So while it is harmful to everyone, it is most harmful to exactly the kinds of technologies and capabilities and the people building them that I think this subcommittee is focused on and this hearing is focused on.

Mr. KEATING. Thank you for re-enforcing that from your perspective too. I think it is a direct impediment to what we are talking about trying to achieve here in this morning's hearing.

Mr. BROSE. And if I could say just very briefly, I am highly confident that the Chinese military is getting its money on time.

Mr. KEATING. That might be one great thing of—that is about maybe the only thing good about their system perhaps.

We talked about Russia and Ukraine, examples of the learning going on. And one of them, you know, within days of the invasion, SpaceX provided Starlink dishes to augment the country's, you know, battered internet system that was in place. And then right after that, the Russians tried to jam the system. But Starlink's response was swift and efficient, even I think one of the DOD directors said the response was eye watering.

Again, is that an example of what we are talking about this morning, that our ability—our need to really be more agile, make determinations in the defense arena the way we often see in the private arena?

Admiral MONTGOMERY. I agree.

The important thing to look at there is what happened beforehand, which was the Russian—you know, people seem to think Russia didn't do anything effective in cyber. They had a fairly successful first night. They took down Viasat. They took down, as you said, the internet, but more importantly the command and control system for the Ukrainian army. If Starlink had not been put in there, they would have really struggled in that first week when you saw that lumbering line of tanks heading towards Kyiv without that command and control, so that is critical.

But you are absolutely right. The agility in the Starlink system says a lot about where we need to go. And I think you will have the opportunity to really—to advocate for a thick belt of low altitude—a LEO [low Earth orbit] constellation that provides—that can provide that kind of persistent communication support to our forces in the same way that Starlink has to the Ukrainian forces. And I do think it is critical that we talk to our allies and partners about having those contracts ahead of time, with whichever private sector company, so they are ready to switch to a redundant reliable system after an attack.

Mr. KEATING. And I think, as we look forward to the threats from China and Taiwan, the lessons there that are learned are going to be extremely important. So thank you for this hearing. Thank you, Mr. Chairman, for having this hearing. Thank the ranking member for having this hearing.

And I yield back.

Mr. GALLAGHER. The gentleman yields.

Next up, another new member of the committee with a wealth of experience. A Marine pilot, helicopter pilot, a Navy commander, emergency physician, and most importantly the proud custodian of my pullup bar, which is now in your office, Mr. McCormick—Dr. McCormick. Excuse me.

Dr. MCCORMICK. Thank you, sir. And we are enjoying that pullup bar which frames my desk right now. Great picture taking availability in my office if you want to stop by some time.

You know, I had all these great questions and the Rear Admiral Montgomery threw me off when he said the Air Force is the key, hurting my heart as a Marine and hearing that from a fellow naval force person. I am curious, though, when we were in Command and Staff [College of Naval Command and Staff], we always said the same thing right after World War II, that the Air Force was the key.

When we are talking about this particular theater in the Chinese/Taiwan Straits and so forth, I would hope that most of us understand if we go to a full-scale war, of course, the Air Force is going to be central to our strategy and tactics. The problem is we are probably not going to be—I hope to God we are not a full scale war, so I don't think the Air Force will be as strategic—or, tactically important as maybe you are indicating because they won't be engaged directly.

In other words, we will be relying on Taiwan deploying their own forces that we have hopefully pre-positioned, which gets back to my main point. Without disclosing any classified information, how much do we have pre-positioned in Taiwan?

How much capability do we have out there already ready to deploy? I love the ideas of using the low-tech or I guess somewhat low-tech smart mines. I think it is brilliant.

Once again, Command and Staff talked about that, using these low-tech things to take out high-tech targets. What other kind of opportunities do we have out there as far as weapon systems that we can use at a reduced cost to take out higher cost weapon systems that take a lot more time to produce, if you would comment on that.

Admiral MONTGOMERY. So first—to answer your first question, we don't have weapons stowed in Taiwan. In the last National Defense Authorization Act [NDAA], you approved—you authorized up to $300 million a year to be appropriated for Taiwan specific munitions. The appropriators, which happened about 7 days later, appropriated $0. In fact, almost all of the Taiwan Enhanced Resilience Act, which you all pushed through the NDAA, ended up not being appropriated in the Consolidated Appropriations Act that passed 8 days later.

So the answer to the question is we have none there. We do have significant munitions in Guam, Japan, and elsewhere in the AOR [area of responsibility]. But we don't have them in Taiwan. I think we need to. We have been pushing for something similar to what we have war reserve supply Israel, where we store munitions jointly with the Israelis in Israel for a future conflict. And we are, in fact, drawing on them for Ukraine right now. We should be doing the same thing in Taiwan.

Dr. MCCORMICK. How much easier would it be for us to deploy that when something goes down, it doesn't seem like it would be—I am not optimistic we would be able to deploy things from Guam and Israel and other places to get to Taiwan once the Chinese get engaged.

Admiral MONTGOMERY. One hundred percent I agree with you, even in a blockade—which as you mentioned is probably more of a naval than an Air Force thing—but in a blockade or invasion scenario, the United States is not going to be able to resupply Taiwan. So Taiwan has to have the munitions they need. And if we are somehow able to get the 12th Marine Regiment over there from Okinawa, which is a great new initiative from the Commandant [of the Marine Corps], they are going to need to have—the Naval Strike Missiles will already need to be stowed there because we are not going to be able to resupply those Marines.

Dr. MCCORMICK. I will say you redeemed yourself, sir, with the 2004, 2005 Marine comment of being ingenuitive, and ahead of the Army, which I agree on also.

We talked about—it is interesting Elon Musk always talks about I have a million ideas, it is what can be executed that matters. And you mentioned Starlite [Starlink]. What about the integration of the high-tech and the low-tech stuff? What is achievable as far as something, the most bang for the buck when we talk about our technologies. Not things that take years to develop, than when we have something that may happen within a year, maybe within 5 years, it is almost inevitable in this case in my opinion. I am worried about how fast we can deploy something, how fast we can ramp up when we start to gear up for that sort of thing.

What is the best bang for the buck?

Mr. SINGER. Rapidly, first, counter-drones systems. We are not talking about a photon. In fact, China is working on them as well right now. I have an article out today on it. That would provide great defense for both our allies and for U.S. forces. Second, the naval smart mine aspect, really cheap, very easy to create.

I just want to answer real quickly your prior question. The key issue for the committee to explore given the dilemma that we talked about is logistics supply in contested areas. We have redesigned the Marine Corps to deploy into these areas. We haven't figured out the logistics for it, same thing for Taiwan. So the more that you can invest in contested logistics, which is another area that doesn't require high-end solutions.

Dr. MCCORMICK. Thank you.

Mr. GALLAGHER. The gentlemen's time has expired.

Next up, from New Jersey, a Rhodes Scholar with experience at USAID [U.S. Agency for International Development], the Pentagon, [Department of] State, and a member of the Select Committee on the Chinese Communist Party, Mr. Kim.

Mr. KIM. Thank you, Mr. Chair.

Thank you to the three of you for joining us.

Mr. Singer, I want to start with you. I found your testimony, your written testimony, very interesting. I also like to kind of think through scenarios and try to understand and parse that through.

And, I guess, when I am thinking about what is a potential lead-up to another conflict, I am often thinking about what is the will of the American people to be able to engage in this, what are the needs for our own protection, and how would this potential lead-up to a conflict or this very intense deterrence situation affect our own security and our own protection.

And so cyber is one of the places that kind of keeps me up at night, because it feels like it is one of those places where, when you work through the scenarios, you can see how this is a place where you could see some kind of blowback towards our homeland or towards the American people.

So I think about that in terms of the scenario you were raising, talking about the challenges that were incurred upon—on the Chinese government, the CCP, but I worry about using cyber as some sort of attack to be able to create conditions for the American people that would be difficult, whether that is coming after our grid or coming after GPS [Global Positioning System] or other things like that.

So I guess my question to you is, to what extent does this need to be sort of an equal part of this strategy, not just in terms of thinking through how this is something that we do, whether for the defense of Taiwan or some other aspect, but hardening it here at home?

And I was kind of intrigued, because one of your points, if I remember correctly, was about creating digital literacy programs, for instance, that seemed like it was kind of getting at this point of, like, how do we raise that foundation of awareness for the American people about this. But it feels like there is more there that we need to do on top of that. So if you can expand on that some more.

Mr. SINGER. Thank you. It is a great question.

Rapidly, two answers for you.

The first is, in terms of traditional cyber attacks, much of the focus has been on critical infrastructure in the power grid area, not enough in the other parts of critical infrastructure, for example, water systems and the like.

And as I wrote about and spoke about in the testimony, in particular, Internet of Things systems that we are currently not baking security in; that is, the ability to cause physical damage through digital means. And the more that we can do on that, the more secure we will make our Nation.

Second, I was part of a project working with Northern Command where their experts identified top scenarios that concerned them in homeland threats in terms of everything from nuclear, bio threats, extremism, great power conflict.

And what was interesting, in each and every scenario, it was not merely the nuclear threat; every single time, their experts and the team that we put with them identified information operations as making it worse.

And, unfortunately, in the United States right now, we are not doing a great job of defending ourselves against information operations. And one of the keys that our Baltic allies have learned is what are known as cyber citizenship programs, digital literacy programs, where it is not censorship, it is training youth and members of the military to deal with the other part of the cyber threat that targets them every single day.

Mr. KIM. Yeah. No, that is a really important part, and I think that is something that can bring out a little bit more holistic approach in the way we think about it, not just in terms of our own DODIN [Department of Defense Information Network] systems, and things like that.

But this question of—deterrence requires not just capabilities, but it requires resolve. And I worry about just sort of the resolve of the American people. If we start to feel squeezed, if we start to feel some of this here at home, what does that mean for our resolve abroad?

One last point I want to raise is you kind of mentioned how other countries have moved forward with other types of programs of this. You also mentioned, as part of your statement, about trying to make sure that we can align U.S. cyber rules and regulations with other major allies.

I wanted to get a sense, does that include this idea of privacy-enhanced tech and AI? It is sort of another angle of how we look after the American people as we start to scale up.

Mr. SINGER. Yes. And I think it points to a larger mentality, which is that, just as much as we seek to aid other democracies, we should be learning from their best practices and trying to implement them here so that we can have cohesion.

And that is an example of one area, the digital literacy, learning from what the Baltics have done successfully, et cetera, and then trying to replicate them across our allies like in a Taiwan or whatnot.

Mr. KIM. Okay. Great. Thank you.

I yield back.

Mr. GALLAGHER. The gentleman yields.

Next up, from Florida's First Congressional District, a humble country lawyer who represents the Blue Angels, Mr. Gaetz.

Mr. GAETZ. Thank you, Mr. Chairman.

One of the frustrations that we have had on the Armed Services Committee has been the gestation period from R&D [research and development] to actually getting these cyber capabilities to our cyber warriors. And one of the things that has been presented to us as a way to bridge that long gestation period is the Defense Innovation Unit, the DIU.

I was wondering if any of you had a perspective on how we ought to think about resourcing that and whether or not that is a way to get capabilities into the hands of cyber warriors faster.

Mr. BROSE. Thank you, sir.

I do have a lot of experience with the DIU, both in government and out of government, and I think that it does a terrific job for what it was established to do. And there are many other organizations focused on, similarly, kind of reducing the barriers to entry to get these kinds of more mature, kind of commercially developed advanced capabilities into the Department of Defense.

I am all in favor of that, and I think anything that you can do to encourage that is good.

What I would contend is that the bigger challenge that I would recommend the committee focus on is what happens after that.

So when you reduce these barriers and you bring in small companies doing small things on small contracts for small amounts of money, and you have hundreds of them, that is good.

Now we need to go through and sort of systematically determine, what is the best 10 percent that needs to get large-scale production contracts to really make the kind of impact at scale that you are talking about.

That apparatus or process does not exist in the Department, and it is something that I would say is ripe for congressional oversight.

Mr. GAETZ. I also—go ahead, Admiral Montgomery, if you had a perspective.

Admiral MONTGOMERY. No, I agree. And I am disappointed that Mike Brown left leadership of the DIU. I think his personal leadership had a lot to do with its success.

So we will have to see what happens over time with that. Sometimes these small organizations can be very personality-driven.

Mr. GAETZ. That is good feedback.

Another concern I have in the cyber sphere is the threat presented by these DJI drones. I have seen report after report from the Department of Homeland Security about the capabilities of these drones to be able to collect intelligence, to transmit intelligence, and ultimately to impair our cyber defense infrastructure.

How do you think we ought to think about these DJI drones?

Admiral MONTGOMERY. I will step in there. And I will tell you, I was sorely disappointed that the American Security Drone Act dropped out of the last National Defense Authorization Act.

It makes no sense that the Department of Defense has recognized that these drones are unacceptable in our system and removed them and replaced them at some cost, yet other Federal agencies, intelligence agencies and law enforcement agencies, are not being compelled to follow suit.

We know that these systems can communicate back to the servers of their host company in China, and we know that those companies can be compelled by the Chinese intelligence agencies to provide information.

If you had asked me as the J3 [Director of Operations] at PACOM [U.S. Indo-Pacific Command] what would be my dream scenario when I woke up in the morning, it would be that U.S. drones were flying up and down all Chinese critical infrastructure every night and sending photos and information back to my team so that I could easily target.

Well, U.S. critical infrastructure companies are buying DJI and other Chinese drones at about 80 percent of market share, and they are flying up and down our pipelines, our electrical power grids, our water systems, and they have the opportunity to transmit that information, and the Chinese intelligence has the opportunity to request it.

Mr. GAETZ. And oftentimes are these DJI drones not provided to our local and State law enforcement agencies at incredibly low cost?

Admiral MONTGOMERY. They are. And in both Florida, as I am sure you have experienced, and Texas, we have seen that, and in Norfolk and San Diego. And I can't imagine what a Chinese drone would detect flying in the San Diego and Norfolk areas on a daily basis while doing legitimate law enforcement work, but also grabbing a good picture of everyone who is at every pier.

Mr. GAETZ. Yeah. It is deeply frustrating to think that our own law enforcement agencies are almost being utilized, essentially being utilized by the Chinese Communist Party to engage in this activity.

So, Mr. Chairman, I know you have got a lot of hats you wear on this subcommittee and also working to chair the Select Committee on China, and I would suggest that the National Defense Authorization Act would be a wonderful place to nestle some drone doctrine for defense against this Chinese capability.

Appreciate the testimony.

And I am still waiting to see who in Washington is defending these drones. I don't know why that legislation dropped out of the NDAA. Maybe they will perk up at some time.

Mr. GALLAGHER. Well, they actually used—they had a pretty robust lobbying effort that used law enforcement officials, if memory serves, to go into Members' office and say——

Mr. GAETZ. Now we know better.

Mr. GALLAGHER. Yeah.

Mr. GAETZ. Thank you. I yield back.

Mr. GALLAGHER. I share your desire to pass the DJI ban in the next NDAA.

I now recognize the—I already said a bunch of nice things about you when you weren't here, Ro.

Mr. KHANNA. I heard. You don't have to redo it.

Mr. GALLAGHER. I drew attention to our op-ed when we were freshmen Members of Congress together.

But the ranking member of the subcommittee, Mr. Khanna.

Mr. KHANNA. Thank you, Mr. Chair. And let me just say the respect that I have for you, both as a leading thinker on how to make the Department of Defense more innovative and how to make sure we have a modern national security strategy, but also the way you have conducted this committee, reaching out to the wealth of knowledge we have on both sides.

We have a really stacked committee with some of the most experienced and thoughtful people on both sides, and you have really run it in a very bipartisan way, in an idea-focused way. So I respect how you are doing it, and I am excited to work with you in these next 2 years.

Mr. Brose, I couldn't have agreed more with one of the things you said, which was that we are not going to need more traditional ships, aircraft, and other platforms as much, because spending ever more money on multibillion-dollar capabilities that China can overwhelm with multimillion-dollar weapons is a losing game. And the money-ball military idea was certainly an interesting one to me.

And this question is for all three of you. What can we do to overcome this valley of death? I mean, Michael Brown has talked about how now most of the innovation on the critical technologies is happening in the commercial space, not in the military space, a sort of reversal of the creation of the internet and GPS, where it was the Department of Defense innovating and then proliferating out. Now we need it adopted.

The problem isn't the startups. It is often that the DOD doesn't have the budget, then, to acquire it, adopt it, actually use the technology.

And in some cases—I was talking to Pat Gelsinger and others—the semiconductors, even though we are leading in it, China actually is adopting it faster in terms of some of the technologies.

And so my question for you, all three of you, is do you think we need a different position under the acquisition and system DAS [Deputy Assistant Secretary]? What can we do to get the budgets and adoption faster?

Mr. BROSE. Thank you very much for the question, sir.

I have thought a lot about this, worked on this in government and out of government, and I guess what I would tell you is the conclusion that I have come to is that we are wildly overthinking this problem.

I think that the answer basically comes down to we need to buy more of the things that we say are important and that we say are priorities. And that is the thing that doesn't happen. It is not necessarily the fault of the acquisition system. It is the entirety of the system that is not incentivized or prepared to really kind of incentivize disruption.

Mr. KHANNA. Just to push you a little bit on that. The Pentagon budget is sort of 5 years in advance, right, or 4 or 5 years in advance, and a lot of these technologies are 1 to 2 years. How do we sort of structurally overcome this?

Mr. BROSE. So I would say in the next month, it seems, you will see a budget request from the Pentagon that, yes, was put into concrete somewhere between 5 and 18 months ago.

Congress has the budget authority to determine what is actually going to be bought, what are actually going to be the funded priorities of the Department of Defense. You have the ability to readjust that consistent with laws and other things that, obviously, you need to abide by.

I would say that the technology is there. The authorities exist. They don't need to be recreated or built anew. We are spending over $800 billion a year on defense, and billions of that is being reprogrammed with congressional approval in the year of execution.

I think many of the capabilities that I talk about in my testimony, that we are talking about here today, don't actually cost a lot of money in the broader scheme of things. They do need to cost more money than we are currently spending on them. But they are also quite mature technologies that are ready to be bought at scale.

And if we start buying them at scale they are going to get better faster. You are going to see the kinds of companies that are building them become more capable. You are going to see others rush in and investment behind it to do more and encourage more of this activity.

My basic contention, I guess, sir, is our system, unfortunately, looks too much like China at its worst and not enough like America at its best in terms of really getting capitalism and market creation into this part of the Department where it actually can exist.

You are not going to have markets for aircraft carriers. You can absolutely have them for AI-enabled weapons, ubiquitous sensors, and distributed space constellations.

Mr. KHANNA. Mr. Montgomery, did you have—I know my time is——

Admiral MONTGOMERY. Yeah. A quick thought is, I agree completely with the oversight comment. I will give you one quick example.

The Air Force innovated and figured out, Hey, we need to put this LRASM [Long Range Anti-Ship Missile] on the B–52. It is a quick software change. Congress authorized it 4 years ago, and it hasn't taken hold.

I don't think Congress comes back enough to the services and says, Hey, we innovated something. We innovated something together. We approved it. We paid for it—we began to pay for it. And we haven't seen it come out.

And that is because it competed against what the Air Force really cared about, an engine remodel, an engine upgrade of the B–52.

Mr. GALLAGHER. The gentleman's time has expired.

On your comment, Mr. Brose, Bill Greenwalt has persuasively written about how DOD looks too communist at times in its system.

Next up, another great new member of the committee from Alabama. Am I sort of contractually obligated to say "Roll Tide" whenever I say that, or how does that work?

Mr. STRONG. I have got two children at Auburn University.

Mr. GALLAGHER. Oh, there you go.

Mr. STRONG. So you better stay away. But we have got two great universities there, no doubt.

Mr. GALLAGHER. Mr. Strong, you are recognized for 5 minutes.

Mr. STRONG. Thank you, Mr. Chairman.

And, first of all, Members, I am honored to serve on this committee with each of you. I believe each of us offer a skill set that is going to be very beneficial in the days ahead, just from the geographic regions that we come from.

We have heard many times about the valley of death, drawn-out procurement processes and contract protest that often delays critical technologies from getting in the hands of the U.S. warfighter.

My question is, how do you believe the Department of Defense and military services should balance RDT&E [research, development, test, and evaluation] funding versus procurement?

Mr. BROSE. Thank you, sir.

I would say that there is a time and a place for each. I think that a lot of the types of capabilities that we are talking about today can be shifted to procurement. It is possible to have the Department buy more of these kinds of capabilities and actually push the burden for research and development more onto private industry so that they can develop these technologies at the pace that they are actually capable of being developed at.

RDT&E, I think, is more useful when we are talking about technologies that are further out, where there is not kind of commercial drive to really kind of put that investment in and develop those technologies.

Those are the kinds of things that I would contend RDT&E really needs to be focused on. I would say that many of the things that we are talking about here we need to think about through a production and procurement lens, not a research and development or science and technology lens. Because if they are thought of that way, they will forever stay science projects, they will forever stay in the laboratory, they won't transition, they won't get fielded, they won't make an operational impact.

Mr. STRONG. Yes, sir.

Mr. Singer.

Mr. SINGER. To build on that, and actually to answer Representative Khanna's question as well, the only way that you get change is not merely through bureaucratic reform. It is through successful use cases. And you get either successful use cases of the new in wars, like what we are learning out of Ukraine—that is how you push past inertia, but you don't want to have that experience—or you get them through your own war games, experiments, task forces, and field uses.

And one of the most important things that a committee like this can do is to be very blunt and direct. Every year in the budget cycle the Pentagon comes in with a request and then, after the fact, Congress jams in a couple more procurement of some single system that is not going to win or lose a war.

That same amount that you spend on that additional beyond Pentagon request single system, if it was spent on wargaming, task forces, some of the things that we have talked about here to get successful use cases, that would actually help potentially win a war.

Mr. STRONG. Thank you.

My home is Huntsville, Alabama, also known as Rocket City, USA. It is a hub of innovation. You think about it—satellites, drones, missiles, counterintelligence—we have got a little bit of all of it.

What are the biggest challenges you see facing new companies and startups when trying to work with the Department of Defense?

And what I mean by that is these new companies have some of the brightest ideas, the up-and-comers, very unique employees that may be directly out of college. And what I am trying to do is, how can we work that better with the Department of Defense?

Admiral MONTGOMERY. I will give you one quick one then turn it to Chris.

One of the biggest problems they face when a startup company comes to this is that their runway for getting a—beginning to get investment from a customer is 18 to 24 months. And the Department of Defense's runway for their laborious plane to take off is about 4 years.

And somewhere in that point, from 18 to 24 months to 4 years, they have to sell their intellectual property to a prime, which then begins to reimagine it into something they already have. And to me that destroys a lot of the innovative intellectual thought and entrepreneurial thought that goes on in our small companies. So figuring out how to shorten that runway to that first procurement being at 18 to 24 months.

Mr. BROSE. I would go back to many of the things that I have said about the need to buy at scale faster, the capabilities that are best and that are working. But I will give you one sort of very concrete example.

A challenge for a lot of these companies that are brand new is they don't even have access to the problem because it is classified.

And you say: Well, how am I going to be able to get access to the problem?

Well, you need a classified contract.

Well, how am I going to get a classified contract?

Well, you need security clearances.

Well, how do I get security clearances?

Well, I need a classified contract.

It is a catch-22. So when I—my last day as the staff director of the Senate Armed Services Committee I was a TS/SCI [Top Secret/Sensitive Compartmented Information]/Q SAP super user. The day I left I was essentially a new émigré from Beijing.

We have thousands of people who are leaving military, government, intelligence service every year who could be helping these kinds of companies understand the problem and create better synergies with the government, and we are just, like, leaving all of that value on the table.

Mr. STRONG. Thank you.

Thank you all for coming before us today.

Mr. GALLAGHER. The gentleman's time has expired.

I now recognize myself for 5 minutes.

All of you in one way or another today have made a compelling case that certain new technologies are changing the character of war, though the nature of war endures.

What are some lessons from wars past that we would do well to remember, that might caution us against what I would call magical third offset thinking about technology, just basic lessons about the past of war that are still relevant today?

Starting with Mr. Brose.

Mr. BROSE. Indulging my inner historian.

I think there is an interesting experience that you can look at from sort of the middle of the 19th century to the onset of World War I, World War II. The types of technologies that showed up on the battlefields in 1914 were visible as far back, in some form or another, as the American Civil War, the Wars of German Unification, the Boer War, all of these conflicts of the second half of the 19th century. It is that people weren't paying attention to how they were actually changing the character of war, to your point, which is why the beginning of 1914 the war was so bloody, was because we were using new technologies with old doctrine.

That completely changed over the 4 years of that conflict. It changed the nature of defense and offense, where the ability to kill in large numbers had grown considerably, but people, troops, were still walking across the battlefield the way the Roman legions did. So there was a sense that defense was now preponderant.

The onset of the internal combustion engine 10 years later completely changed that.

So I guess it is a lesson to say the things that we think are in the future are happening now, but the lessons that we derive from what is happening now can change very quickly with new technologies or the utilization of new technologies that we might not be able to see but are coming.

So it is just to say learn the lessons of today so that we can be ready for tomorrow, but be ready for surprise because it is coming.

Mr. GALLAGHER. Mr. Montgomery. Keep in mind I only have 2 minutes and 54 seconds.

Admiral MONTGOMERY. Yep, and I will keep this to 1 minute then.

So you tend to think of World War II and the U.S. Navy that, well, we failed to understand the emergence of the carrier. And that is certainly an important element in our concentration on the battleship, that was inappropriate and cost us a year's worth of production, cost us 1942 in the war in the Pacific.

But I also remember the most important thing we did was at the Naval War College we executed Plan Orange and Plan Black wargaming for 8 years straight, with Commander King and Captain Nimitz and Admiral Leahy, our future leaders, executing different various war plans till we understood what was likely to succeed in an expansive campaign with Japan in the Pacific.

That kind of wargaming is critical. I think it is important for the military to do it. And I would also recommend that congressional committees get involved more in wargaming, go observe these events, so they get a better understanding of what the risks and consequences are of decisions they are making in their budgets and their NDAA authorizations.

Mr. GALLAGHER. Thank you.

We used to have, it is my understanding, organic wargaming capability in Congress that was housed at NDU [National Defense University], but was subject to us.

Mr. Singer.

Mr. SINGER. Rapidly, three lessons from history,. First, as the blitzkrieg—and I think all of these are parallels from the 1920s and 1930s.

One, as the blitzkrieg showed, it is not how many of the new technology you have, even how good it is. It is actually your doctrine for bringing it all together.

The Germans didn't have the most tanks. They arguably didn't have the best tanks. But they had the best doctrine for bringing it all together.

I don't think we have talked about or thought about enough of the new doctrines for the U.S. military using these technologies.

Second, there is no such thing as truly first mover advantage. Very parallel to us, the British, they invent the aircraft carrier, they invent the tank, but they lock into the early designs of it, they lock into the first uses of it. We as an innovative military need to be very, very careful not to lock in.

And then, third, those war games that the U.S. Navy was doing in the 1930s and 1940s, the successes during the Pacific, all comes out of personnel reforms during the 1910s. And so, again, Trent Hone's book "Learning War" is a great example of that.

So for all the discussion of changing technology, it is also about your human talent management. If you are not making any changes there, you are not going to win.

Mr. GALLAGHER. Thank you.

I am almost out of time, but I am the chairman, and so I am going to entertain a second round of questions, if you all are interested in a second round of questions. And so I am going to recognize myself for 5 more minutes. It is nice.

Mr. Brose, in your testimony in response to various questions—I think you see everyone is interested in this valley of death problem. We have been talking about it endlessly. For some reason, we can't kill the valley of death. You said we are overthinking it. We just need to buy—the Pentagon needs to buy more of the things it needs, right?

In just like the simplest terms possible, if we, as you say in your testimony, have given the Pentagon all the authority they need, all sorts of OTAs [other transaction authorities] and this and that, what then is the problem? Is it just a lack of SECDEF—maybe that is sort of an acronym—Secretary of Defense prioritization of certain things?

What is standing in the way of us buying more LRASMs or take your pick of preferred weapon system?

Mr. BROSE. I think it is a failure of imagination. I think what we are talking about is disruption, and disruption is a cognitively challenging experience.

When you have an organization that has been set up for a very long time in terms of the ideas at its core, the conception of military power that it has, the types of programs that it is fielding, obviously, all of the kind of outside apparatus, industrial and otherwise, that is geared to produce it, it is very hard to get disruption.

When you look at disruption in the commercial sector, most of those stories don't end well. They end with the incumbent going out of business and the disrupter getting to scale and becoming successful.

I think in the defense sector innovation and disruption doesn't just happen, because it is not rewarded, because there aren't incentives for it. I think those incentives need to be created in a way that haven't been created.

It is going to be challenging, but I think we have to be capable, first and foremost, of imagining—and I think this is your point—what are the kinds of ways in which we are going to have to fight, and what are the kinds of capabilities that are going to enable us to do so, not in the distant future, but potentially in this decade? What are the things that we can have?

I think we need to make this problem much clearer. So often innovation gets talked about in this very kind of ephemeral way, and we need to get brutally precise about the kinds of innovations we actually need to move the needle on deterrence.

And I think the war in Ukraine is providing a lot of opportunity to both see what those disruptions look like, because they are literally on the battlefield now, and I think there is creating a sense of urgency about the things we need to do to really kind of buy that at scale.

Mr. GALLAGHER. But to your point—and forgive me for being obtuse—if the Secretary of Defense wants to stockpile a bunch of Switchblades, a bunch of LRASMs, a bunch of Harpoons, and surge them west of the International Date Line, he could do it, right?

Mr. BROSE. He has the authority to do it. He has plenty of money. In the annual reprogramming process—so put aside the budget—I believe the Secretary of Defense is authorized to reprogram upwards of 3 or 4 percent of the defense budget, which it doesn't sound like a lot, but 3 percent of $800 billion is quite a lot. It can buy a lot of loitering munitions or LRASMs or what have you.

I think the challenge is you actually have to start doing that. As I think we have seen in the war in Ukraine, even things like tactical weapons don't just materialize overnight. You need to get the industrial base moving. You need to get facilitization and investment happening so that you are on a war footing from an industrial base perspective, both in terms of things that you are going to need that you have already, as well as things from loitering munitions or autonomous systems in every domain, small satellites and the like, that are absolutely possible to have in large numbers in the next few years if we make the investment.

The Secretary has the authority. He certainly has the money. Congress does as well. It is a question of——

Mr. GALLAGHER. The technology exists.

Mr. BROSE. Yeah. Again, we are not talking cloaking devices here. We are talking about things that are literally being used on the battlefield in Ukraine or things that could be rapidly matured to meet different operational needs on a quick timeline.

I think we need to get—and Admiral Montgomery kind of hit this well—we need to dispense with the idea that the kinds of things that we are talking about take 15 years to get through the development process.

Again, we are not talking about a nuclear submarine here. We are talking about things that should be viewed as, essentially, consumable items. We are going to buy them in large numbers. We are going to use them or consume them in a period of 18 to 24 months. And then we are going to buy new, better versions of them.

And I would say that a crazy thing happens in a capitalist society when you buy new things often: More people want to build them, technology gets better.

Mr. GALLAGHER. I guess what this is making me think is maybe we don't have a structural problem or an authorities problem. We have a sort of a cultural problem in DOD in the acquisition sort of workforce.

We will have to come back to that because I am out of time, and I have to abide by my own commandments.

Mr. Ryan is recognized for 5 minutes.

Mr. RYAN. Thank you, Mr. Chair. Appreciate the bonus round here.

And thank you, again, to our witnesses.

I want to build, Mr. Singer, on something you said in your last answer about personnel reform. And going back, I would kind of ask us to think about the cyber force.

Specifically broadening beyond just sort of our kind of conventional sense of talent development, how do we look across the country more creatively, looking at earlier STEM [science, technology, engineering, and mathematics] education and ideas like that? Are there any lessons, again, from history that you have seen with other, in other conflicts that we could apply to think about really broadening that base of cyber talent across the country?

Mr. SINGER. Thank you.

I think a couple of tangible things that we could do beyond the obvious issues that America has within STEM education.

The first is we could create a version of a cyber Reserve or a cyber auxiliary where there is a gap between what the private sector is able to provide and what the formal National Guard and Reserve is.

What we are talking about here is something modeled roughly after the Civil Air Patrol or the Coast Guard Auxiliary, successful models in the air domain and in the maritime domain. We don't have a version of that for the cyber domain, where it is both able to aid in education, draw kids in, but also serve as an auxiliary at points of crisis.

We did a report at New America about this, and its rough cost would be approximately $25 million for something that one major cyber incident, if it stops, would pay for itself.

The second within the military is that we still have a problem of basically drawing people into cyber forces and actually hit some of the things that the Admiral spoke about.

When you go to the academies, their top talent, including people with incredible digital expertise, and then you ask them, "What are you going to go into?" it is very rarely, "Oh, I am going to go into 10th Fleet," or, "I am going to go into Cyber National Mission Force," et cetera, even though that is arguably the most active part of the U.S. military right now in its day-to-day contestation with our foes.

So there is kind of an issue of and a longer conversation of how to get the best talent within the military to want to join cyber organizations.

Admiral MONTGOMERY. Can I jump in on that?

Mr. RYAN. Please, yes.

Admiral MONTGOMERY. I will jump in on that, and I will differentiate one thing.

At West Point, the Army Cyber Institute actually is leading in their—I go up there every year. They have between 21 and 42, depending on what the Army numbers are that year, of graduates from the course going in. And they really are the smartest kids there on cyber and computer science engineering.

The other services aren't near as strong. The Navy is—the Naval Academy is abysmal in this, historically taking about four students into it from the class, and, obviously, they need to adjust to be more—the Naval Academy needs to adjust to be more like West Point in this regard.

I will give you one other one. The Scholarship for Service Program inside the government—nonhumbly, I will say I created it 23 years ago—it has about 500 graduates a year right now going into Federal service. It is at 82—or 92 universities and colleges.

We need to expand that to about a thousand graduates a year. It is modeled on ROTC [Reserve Officers' Training Corps], the way I was commissioned, and it pays for room, board, and tuition. So I would definitely continue to fund that.

And there is a DOD version of it called Cybersecurity Scholarship Program that uniquely gives 100 students a year to the Department of Defense, and I would expand that as I look forward to these things.

Mr. RYAN. Thank you.

I want to just—I apologize, Mr. Brose—I just want to bring up one other quick point. And hearing West Point beating Navy just warms my heart. So thank you for saying that on the record.

Mr. Singer, I know we don't have time, but can you point me towards the direction of any writing or thinking on sort of your idea of fictional—fiction intel around ChatGPT specifically and some of the newer—I know I sound like a Luddite—but, I mean, seeing it myself now is just really almost paralyzing to think about the implications.

Anything that you have written or others that you could point us towards on that?

Mr. SINGER. There is one scenario that we did looking at potential Chinese use of it. Happy to engage with you further.

But, more broadly, that is the only one that I am aware of, and it points to a larger agenda, that if we think this is a key new technology area, let's game out, let's envision what is both our potential use of it, but also adversary potential use of it, so it doesn't hit what both Mr. Brose, but also the 9/11 Commission, described as a failure of imagination. It is easy to solve that failure of imagination.

Mr. RYAN. Thank you. I yield back.

Mr. GALLAGHER. The gentleman's time has expired.

Mr. Khanna.

Mr. KHANNA. Thank you, Mr. Chair.

I have two questions, one following up on the Chair's point about how we overcome this adoption issue.

Other than imagination and talking to the Secretary of Defense and trying to change the culture, what specifically can the committee do? I mean, are there any legislative recommendations? I mean, hard to change the culture. I mean, the committee can talk to people. But what specifically legislatively can we do.

And then the second question is, do you think there is any value in having the DOD have its own venture fund, like In-Q-Tel, where they are actually taking a stake in the company?

And maybe just start with Mr. Singer, and as much time as we have, if you could keep your remarks about a minute.

Mr. SINGER. So if we look at successful cases where an innovation has made it across the valley of death, like, for example, the Predator drone, it doesn't happen merely because of top down. It happens because you create demand within the system. You give members of the services a taste of it, an experience with it, and then they say: We want more of this.

So the more that you can fund—not merely creating the system, go out and buy it—the more you can fund programs designed to draw those technologies in.

I earlier referenced, for example, we have a task force in the Middle East for naval drones. Why is it not across multiple different services, across multiple different commands?

Same thing, we have got a couple of fleet problem exercise type models, but not replicated. The more that you can replicate that across the system, give people experience at it, then you are going to create that demand force within the military culture.

Admiral MONTGOMERY. I will give you two quick ideas.

You have three posture hearings coming up next with Department of Defense officials. I would put them on the record to come back to you with ideas for how they can push specific initiatives that they have or are willing to do over the next 2 years.

The embarrassment of coming back the next year with an empty folder should be enough to drive some of that change.

And to answer your other question, I do think the Department should have a venture capital kitty fund. Chris Brose and I—Chris worked on that hard when he was on the Senate Armed Services Committee. We didn't get it across the finish line. And I am a little worried. What I saw them announce so far sounds like a venture capital fund without capital, and that worries me a little bit.

Mr. BROSE. Very briefly. I would actually say, the many powers that Congress has, I would sort of put legislation to the side and I would say oversight and funding are the most important.

So the Predator drone is an illustrative example. It began as a congressional earmark. If left to its own devices, the United States Air Force still would not be flying remotely piloted aircraft. The Congress had to force them to adopt a capability that was disruptive and contrary to the culture of the service.

I am not saying that you guys should go wild with earmarks. I am saying that the power of actually funding different kinds of military capabilities is the power of this committee. It is the power of the Congress.

That is something that I think can be exercised. And I think with that is the oversight to say: Why aren't you buying these kinds of capabilities? Why aren't you scaling these things that work? Getting down into those details where you can call balls and strikes I think is wildly important.

Final piece on the capital. I would argue that DOD should not become a venture capital arm. There is plenty of money in private capital markets to fund worthwhile companies doing worthwhile defense work.

The thing that the DOD uniquely has that it doesn't use is its sole power for demanding and buying disruptive capability. That is how it sends a signal to the market in terms of what it values. If it does that more and it does that at larger scale, that is how it is identifying what winning looks like, what right looks like, the kinds of things that it wants more of.

I would argue capital will flow into the companies and the places that are providing those capabilities if the Department in this monopsonistic world of national defense does what it needs to do, which is demand and buy it in the first place.

Mr. GALLAGHER. Great.

I am now going to move to a third round of questions and recognize myself for 5 minutes.

One thing your question, Mr. Khanna, makes me think is whether—and Mr. Montgomery's answer—is whether we need to think through like a periodic—in my head I think of it as like other transaction authority thunderdome, where we put the services on the record in terms of how and why they have or have not used the authorities that we have given them.

Quickly, I want to amend slightly something I said earlier when Mr. Brose and I were talking.

It seems, based on your testimony, that we don't lack authorities, we don't lack money, we lack leadership willing to take intelligent risks when it comes to buying certain things. Is that accurate?

Mr. BROSE. I think it is partly accurate. I think part of the challenge is integration doesn't just happen at the Department of Defense.

Mr. GALLAGHER. Yeah.

Mr. BROSE. We have this incredibly fragmented accountability, from requirements definition, programming and budgeting, acquiring. That integration sort of resides at the senior leadership level.

I think the challenge is not simply that those people are unwilling to take risk. I actually think they are incredibly willing to take risk. And in my conversations with all of you and other Members of the Congress I think there is an enormous appetite to take risk.

The challenge is: How do we identify the right risks to take? How is timely information being surfaced such that, whether it is the Secretary of Defense or a Member of Congress, can say: I will bear the risk and be accountable for doing something that, if left to its own devices, the bureaucracy is not incentivized to do and deems too riskworthy.

That I think is the real challenge here, which is the ability to gain kind of an appropriate signal or information of what is working, what innovations are promising, what capabilities are there, companies that are doing good work, and pull those up to real scale with the authority that the Congress and the senior leadership of the Department have.

Mr. GALLAGHER. And, Admiral Montgomery, so let's say the Secretary of Defense comes to you and says: You have persuaded me on this LRASM issue, Long Range Anti-Ship Missile. I violated commandment number three. I am sorry. How do you fix it?

Admiral MONTGOMERY. Well, the good news is the very first step was taken by the Congress in the last National Defense Authorization Act. You added in extra money to specific targeted defense industrial base companies to increase their ability to produce more weapons. In other words, what had happened with LRASM was——

Mr. GALLAGHER. But was it appropriated?

Admiral MONTGOMERY. Yes, it was appropriated. That is one of the only things that you did in this area that was appropriated.

And so what we now have to do is increase—the companies have to put in their money too. So what we need to do is get, like, the maximum production capability of LRASM, to use the acronym, up to about 250 a year, so we can have this problem solved within 5 years.

You will then have to ramp up production there. So you will have to put money into the procurement of it. And as I mentioned, you need to then kick the Air Force and the Navy in the backside to get the B–52 and the P–8 ready to launch the weapons. Because once you have more of these weapons, you need to have more launch vehicles for them.

So that is a three-step process. The Congress took the first step. We will see on March 9 whether the Department took the second step and increased actual LRASM production.

Mr. GALLAGHER. Mr. Brose, maybe you can answer this. I know you want to say something.

What about, I mean, the stuff in the weapon, energetics? Do we have an opportunity—I mean, we are using technology that was made in 1941. The Chinese are using our technology that was made in 1984, CL–20 [China Lake-20], which has like 30 percent more penetrating power, longer range.

Can we leverage that to take a quantum leap in certain weapon systems?

Mr. BROSE. Yeah, I think everything that we are saying about the Long Range Anti-Ship Missile is true of many of our other critical munitions, all of which we are going to need more of, to say nothing of future things we could develop.

The only thing I would add is we have to do this as a function of time. It is not enough to buy more in 1 year, because the signal to industry is that, if you are not going to continue to do this, the maker of that particular weapon doesn't feel the incentive to put a bunch of capital at risk to build more facilities, hire more workers, if the fear is that next year the government is going to change its mind.

So I know there is a debate about multiyear procurement for weapons and other strategic capabilities. I think that is exactly the right kind of direction for the Congress to go.

So you start signaling the incentive that you are going to do this over time. Industry will respond in terms of capacity, but also the kinds of innovations you are talking about.

Admiral MONTGOMERY. The good news is you also authorized that for—you were doing it already—DOD asked you to do it for Russia— for Russia-based Javelins and Stingers. The Congress actually added in LRASM, SM–6, and others into the last National Defense Authorization Act, so it is authorized. We will see if the Department takes advantage of it in the fiscal year 2024 budget.

Mr. GALLAGHER. There is no debate that we need multiyear authority for procuring munitions. It is just there are certain people that don't like that.

Mr. Khanna, I am really sorry. I have to ask one more question.

Mr. KHANNA. Please.

Mr. GALLAGHER. So I am going to entertain a fourth round.

Mr. KHANNA. You can have my fourth and third round time.

Mr. GALLAGHER. You are a good man, good man.

You can open the present while I am asking if you like. Your wife is going to like it.

Mr. KHANNA. It is for my wife.

Mr. GALLAGHER. That is true. We should have invited her. I am sure this is exactly how she wants to spend her birthday, right.

Mr. Singer, I really enjoyed your testimony and the way in which you tease this out through a fictional futuristic scenario. That is told from the perspective of a PLA general, right?

In doing that and going through that thought process, how would you describe the PLA's critical vulnerability? What do you think its true weak points are?

Because one of the big questions we have is: Can they fight? I mean, they look tough on paper, but until you actually fight, it is hard to know whether you can fight. And they haven't fought a war in a long time.

So I am just curious what you learned in doing this exercise.

Mr. SINGER. Thank you.

And this actually reflects not just that exercise, but I help run a series that may be of benefit to you in this committee and the other called "The China Intelligence," which pulls open source intelligence on Chinese military technology and personnel issues.

So a couple of issues that they have problems with, and they know that they have problems with.

One is, as we have talked about, is the personnel issue. They have a particular issue at recruiting from their highly educated and retaining. And it is not just at the NCO [noncommissioned officer] corps part, which they lack, but it is also at the officer side.

A second issue that they have is, by the very nature of their political system, highly centralized. And it is not yet clear whether that is the best model for AI and utilizing it across networks. And we can have a longer discussion. That is what I was talking about.

And one of the things that you can help push forward bureaucratically is a federated data—it is called a data mesh model—for the Pentagon, which is what the CDAO [Chief Digital and Artificial Intelligence Officer] is working on. They probably could not do that within their system because it relies on trusting different parts to act.

Another key problem for them is politicization of their military. It is not a national military. It is a party military. And so that has created different kind of tribes, so to speak, within their system of who is beholden to which political leader and the like. That is also why they have had sort of a recent set of purges, corruption purges.

So those are some of the vulnerabilities.

I think to flip your question is to ask: What are advantages, unique advantages that we have, and how can we bolster those? And so what is it that a PLA officer would say: Gosh, I wish I could have in my system, but I can't implement the way that the Americans can.

Mr. GALLAGHER. Would sort of decentralized commands, mission tactics, be one of our unique advantages?

Mr. SINGER. Yes, yes. And that applies to both the human side, but also if you are thinking about with autonomy, that side too.

Mr. GALLAGHER. Mr. Montgomery, less than 2 minutes, maybe comment on that, as well as what we need to know about the cyber aspects of a fight over Taiwan.

Admiral MONTGOMERY. So thanks.

First, on that last question, I agree completely with Mr. Singer's comments.

And I would just say at PACOM, when I went to sleep at night, the thing I dreamed about was a weapon that would damage Chinese C2 [command and control] in war, whether it was cyber, space, or kinetic.

We have got to optimize those weapons, because if we can take down their command and control system, I think when it comes down to our empowered pilots, ship commanders, noncommissioned officers versus their not empowered pilots, ship drivers, and noncommissioned officers, we would have a big advantage.

When I think about Taiwan, I don't think we are ready—in a scenario with China and Taiwan, I don't think we are ready in cyber. And, really, the biggest blind spot for us is the cyber resilience of our national critical infrastructure, as I said earlier, the transport, electrical power, water, financial services.

I think it is highly likely, that the beginning of a crisis or contingency, the Chinese will begin to conduct cyber malicious activity around the ports of Oakland, the port around Long Beach and Los Angeles, with the train systems that go into them, to send us a strong signal that you are not going to be able to mobilize and sustain the forces like you think you can.

I think that they could easily—they have malware already—we admit they have malware in our electric power systems, our water systems, our transport systems, our nuclear power generation systems. All those areas are susceptible.

We really have to figure out how to prioritize our most systemically important critical infrastructure and how we work with those SICI assets in order to ensure that we have the right level of cybersecurity for a crisis or contingency with China.

Mr. GALLAGHER. Thank you.

I am out of time. I want to thank all of our witnesses for their time, for their testimony. This was a really thoughtful conversation and we hope to follow up with you on a variety of fronts and hope we can continue to leverage your work as we try and solve some of the problems we identified over the next 2 years in a bipartisan fashion.

So what do I say at the end of one of these? Do I, like, bang the gavel again?

The hearing is adjourned.

[Whereupon, at 10:20 a.m., the subcommittee was adjourned.]

APPENDIX

FEBRUARY 9, 2023

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 9, 2023

Statement of Chairman Mike Gallagher
Subcommittee on Cyber, Information Technologies, and Innovation

"The Future of War: Is the Pentagon Prepared to Deter and Defeat America's Adversaries?"

February 9, 2023

The subcommittee will come to order. Welcome to the first hearing of the Cyber, Information Technology, and Innovation Subcommittee in the 118th Congress.

I am thrilled to lead this subcommittee with my friend and colleague, Representative Ro Khanna, with whom I have worked productively for six years. I would like to enter into the record an op-ed that Representative Khanna and I wrote together as freshman members of Congress. While this piece focused on Congressional Reform rather than Defense, it demonstrates that we have long been willing to work across party lines to modernize this institution. While Ro is a progressive and I am a conservative, we both like to think for ourselves and we both believe DoD can do better when it comes to innovation.

The only way to truly win World War 3 is to prevent it. If we accept the slow, bureaucratic status quo, deterrence will fail again, as it failed in Ukraine. On this subcommittee, we will dedicate ourselves to deterring war. There are three questions we must answer:

First, is the Pentagon prepared for an invasion of Taiwan that has already begun in cyberspace?;

Second, what technologies are most important for winning a future war and what are the barriers to the Department rapidly adopting such technologies?; and

Third, are the Services and the Pentagon sensibly structured and resourced to recruit, train, maintain, and equip cyber warriors?

As we work to deter World War 3, time is not on our side. It has taken me six years to get this gavel, and I intend to wield it like Thor's hammer against the forces of darkness that waste our time, our most precious resource. Behind me you'll see a picture of the clock at Lambeau Field. It is always set 15 minutes fast, to reflect Vince Lombardi's wisdom that if you're on time, you're 15 minutes late. This committee will operate with Lombardi Time in mind. To this end, I have developed the three CITI commandments that you will see on this sign behind me.

First, we shall start on time: hearings will begin at their designated time. And since I have to be here the whole time anyway, I'll often yield my initial question time to punctual members.

Second, five minutes shall be five minutes: opening statements, and questions and answers will be strictly limited to the allotted time. That being said, if you stick around to the end, I will always entertain a second round of questions.

Third, thou shalt not use acronyms nor jargon. The Pentagon suffers from a disease called "acronymphomania"—a fetishistic use of acronyms that kills clear thinking. On this subcommittee we will strive for simple and direct language normal Americans can understand.

In the spirit of the three commandments, and in the hope that this is the longest speech I will ever give on the subcommittee, I will stop talking and yield to Ranking Member Ro Khanna.

Ranking Member Ro Khanna
Cyber, Information Technologies, and Innovation Subcommittee

The Future of War: Is the Pentagon Prepared to Deter and Defeat America's Adversaries?

February 9, 2023

Thank you, Mr. Chairman, for holding this hearing, and I am excited about the hard work ahead of us for the 118th Congress. To you and to all the Members of the subcommittee, I look forward to continuing the incredible bipartisan history of this subcommittee with each of you.

And thank you to our witnesses for appearing before us today and joining our first subcommittee event for the year.

The rapid proliferation of new technologies continues to radically change characteristics of warfare. The ongoing Russia-Ukraine war has shown us a set of potential paths for conflict to evolve, but there is a clear expectation that not all of the lessons learned may hold true in a contest involving the United States and a near-peer competitor.

Still, there are clear insights to be gained. The expanded role of unmanned systems, particularly at the tactical edge; the utility of loitering and precision munitions; the integrated use of information operations, including electronic warfare, cyber, and military information support operations; all have been illuminated in significant ways. But in other dimensions, we've seen the war devolve into trench warfare and artillery battles reminiscent of the First World War. All within the same conflict in less than a year.

How, then, to ensure that the United States is prepared to compete effectively in the coming decades in such a dynamic environment?

We can see some imperatives - most particularly rapid adoption of new technologies, including the integration of commercially available capabilities. But technology alone is not enough, and it doesn't happen in isolation. Research and development means the development of a pipeline of dedicated professionals in sometimes highly specialized fields, and a commitment to training and retention. It means a test and evaluation enterprise able to rapidly evolve with the software-driven and highly adaptable systems of the future, while still evolving to support high-end capabilities such as hypersonics, electronic warfare, and next-generation platforms. It takes labs with modernized infrastructure, capable of supporting and enabling cutting-edge research at a variety of maturity levels. It takes close partnerships with the defense industry and the commercial sector. And, it needs the bureaucratic and organizational tools to succeed, especially when it comes to creating the operational "pull" from the warfighters that is essential to successfully crossing the valley of death. Then, it will require the training, personnel, modernization, and sustainment that make it a credible capability for our men and women in uniform to use to deter our adversaries. Every link in the chain must succeed.

As far as the cyber domain, global networking is now one of the fundamental building blocks of our society. Defense, health, energy, finance, and more all depend on reliable and secure communications. We expect our military to be able to secure, fight, and win in cyberspace in order to defend our national interests. But what will it take to get to and remain in a position to do that? Our operators must be able to detect and track adversaries, secure communications, and create effects. Our workforce must be supported and engaged, with the right number of people in the right jobs with the right tools. Our systems must be defensible and resilient. This subcommittee has a history of being an engaged partner in the growth of the DoD's cyber mission and cyber forces, including in last year's creation of an Assistant Secretary of Defense for Cyber, and it is crucial that we maintain that momentum in this and future years. I look forward to hearing from our witnesses as to what next steps may be necessary to fully enable our men and women who operate in defense of our interests in cyberspace every day.

I hope that we can talk frankly today not just about the challenges we face, but also the organizational and systemic adjustments that might be necessary in order to meet those challenges and ensure that our men and women in uniform never have to enter a fair fight, and ideally, through deterrence, never have to enter a fight at all. Mr. Chairman, thank you for convening this hearing, and I look forward to a robust discussion.

Testimony of Christian Brose
To the House Armed Services Committee
Subcommittee on Cyber, Information Technologies, and Innovation
The Future of War: Is the Pentagon Prepared to Deter and Defeat America's Adversaries

Chairman Gallagher, Ranking Member Khanna, Members of the Subcommittee: It is an honor to have the opportunity to testify before you today on the future of warfare.

Often, when this topic is discussed in U.S. defense circles, it is treated as a future problem, something coming in the 2030s or 2040s, something we have time to get ready for. This is wrong, dangerously wrong. If you take nothing else from my testimony today, let it be this: the future of warfare is here. It is a present problem. And America is largely being ambushed by it.

The U.S. military and our entire way of war are being disrupted, and this has been happening for the past 25 years. Our idea of national defense is largely based on the ability to project military power across the globe using small numbers of large, expensive, exquisite, heavily manned, and hard to replace vehicles, aircraft, ships, and other platforms—all of which depend for their effectiveness upon access to forward land and sea bases, logistics, communications, intelligence, space, the electromagnetic spectrum, and other critical enabling capabilities that we have largely assumed would operate safely, in sanctuary, beyond the operational reach of any adversary.

The Chinese Communist Party knows this. And it has been working diligently since the end of the Cold War to field massive arsenals of modern military capabilities to disrupt our ways and means of war—primarily long-range precision strike weapons and advanced sensors to target them. This is all focused on executing what Chinese doctrine refers to as "systems destruction warfare"—the ability not just to degrade and destroy America's small numbers of large, expensive military things, but to render U.S. forces deaf, dumb, and blind and unable to fight.

At the same time, our defense enterprise is also being disrupted by new technologies, such as artificial intelligence, autonomous systems, robotics, ubiquitous sensors, and low-cost access to space. Technologies such as these are changing the character of war. This, too, is happening now. In the recent Nagorno-Karabakh conflict, in the continued fighting in the Middle East, and in the ongoing war in Ukraine, we are seeing how low-cost robotic vehicles, AI-enabled loitering munitions, digital targeting systems, cyber weapons, persistent communications and surveillance satellites, and other advanced capabilities—especially when paired with large volumes of more traditional weapons—are transforming the modern battlefield. Dare I say, what China recently demonstrated it can do with thousands of dollars of plastic and helium is another example of how low-cost, commercially available technologies are altering the character of military competition.

Some lessons are emerging from these recent experiences: On the current and future battlefield, moving and communicating is highly contested. Hiding is nearly impossible. And once detected, surviving is just as difficult. This means that a correctly armed and ready defender can make life hell for an opponent seeking to project power and conduct offensive operations. This is bad news for more traditional militaries that have been optimized for decades, and at great cost, for long-distance power projection and a largely offensive way of war—militaries such as our own.

These dual disruptions of threat and technology have been underway for years, but for many reasons having largely to do with our own politics and bureaucracy, the United States has been too slow to respond. As a result, we are entering what the Chairman has called the "window of maximum danger," a period over the coming years when the Chinese Communist Party, feeling undeterred by the United States military, may seek to fundamentally remake the status quo in the Asia-Pacific region through the unilateral use of military force, for instance by invading Taiwan. None of us wants that to happen, nor can we predict whether it will. All we can do is ensure that we are ready if, God forbid, deterrence fails and U.S. forces are called to maintain the peace.

This responsibility falls most heavily on you and your colleagues in the 118th Congress. In recent years, some positive steps have been taken to better prepare U.S. forces for the future of war, but many of them will not meaningfully materialize, if they ever do, until the next decade, which may be too late. At the same time, the plethora of new initiatives and organizations started in the past several years to advance defense "innovation" have largely become theater: They appear real, but they are not delivering the large-scale production of disruptive military capabilities. As a result, if U.S. forces were called to fight a major war in the coming years, they would largely do so with the same traditional systems they have had for decades. This is a recipe for disaster.

It does not have to be this way. Nothing you do in this Congress will make larger numbers of traditional ships, aircraft, and other platforms materialize over the next several years. And even if you could, it would not be the right answer: Spending ever more money on multibillion-dollar capabilities that China can overwhelm with multimillion-dollar weapons is a losing game.

It is possible, however, to generate an arsenal of alternative military capabilities that could be delivered to U.S. forces in large enough quantities within the next few years to make a decisive difference. Those decisions could all be taken by this Congress. The goal would be to rapidly field what I have referred to as a Moneyball Military—one that is achievable, affordable, and capable of winning. Such a military would be composed not of small quantities of large, exquisite, expensive things, but rather large quantities of smaller, lower-cost, more autonomous, and consumable things and, most importantly, the digital means of integrating them.

These kinds of alternative capabilities exist now or could be rapidly matured and fielded, in massive quantities, within the window of maximum danger. You could set this motion in the next two years. The goal would be more about defense than offense, more about countering power projection than projecting it ourselves. It would be to demonstrate that the United States, together with our allies and partners in the Asia-Pacific region, could do to a Chinese offensive what the Ukrainians, with our support, have thus far been able to do to their Russian invaders: Degrade and deny the ability of a great power to accomplish its objectives through the unilateral exercise of violence. This is all about deterrence, for the best way to prevent war is by demonstrating to our adversaries that they would be unlikely to achieve their goals through war.

Our current and future challenges are not beyond our ability to influence. If we make better decisions now, we can push this looming period of vulnerability further into the future. This will mostly be up to you. If these decisions are left even to the next Congress, they may be too late.

Let no one tell you this is impossible. We have the money: Low-cost alternative military capabilities could be purchased in large numbers for less than one percent of our annual defense budget. We also have the technology: We are not talking about photon torpedoes and cloaking devices here, but rather the large-scale fielding of existing capabilities, many of which have already been proven in combat. Nor do we need yet another round of "reform": Thanks to the good work that Congress has done in recent years, the Department of Defense has the authority it needs to buy and field capabilities that can restore deterrence. The question is whether it will use those authorities to do different things, and whether Congress will demand it.

Ultimately, this comes down to one thing and one thing only—whether or not we are serious. For too long, I would submit that we have not been serious. We have said many of the right things but failed to do them. We have watched threats gather but been too slow to respond. We have watched as new technologies have demonstrated their potential to transform how militaries could be built and wars could be fought, but we have been unwilling to truly embrace them. Now the bill has come due. Our margin for error is gone. It is time to get serious. And if we do, we can be confident that, while the choices we make now and in the years to come will have an outsized impact on America's security and prosperity, they will not be in vain, for we still have every opportunity and ability to prepare for the future of war, and in so doing, to prevent it.

Christian Brose

Christian Brose is a Visiting Fellow at the Hoover Institution, where he focuses on the intersection of national security, emerging technologies, and international affairs. He is also the Chief Strategy Officer of Anduril Industries, a venture-backed defense technology company; a member of the Aspen Strategy Group; and the author of The Kill Chain: Defending America in the Future of High-Tech Warfare (Hachette 2020).

From 2015-18, he served as Staff Director of the Senate Armed Services Committee, supporting the majority members of the Committee in overseeing all national defense spending, programs, and policies across the Department of Defense and Department of Energy. He managed the production, negotiation, and final passage of four National Defense Authorization Acts (Fiscal Years 2016-19), which enacted major reforms to defense acquisition and technology policy, strategic planning, management and organization, military retirement and health, and security assistance. From 2009-15, he was senior policy advisor to Senator John McCain, supporting the Senator during his membership on the Committees on Armed Services, Intelligence, and Foreign Relations as his principal advisor on national security, foreign policy, intelligence, and trade. He conducted official travel to more than 70 countries during his service in the Senate.

Brose began his career in government as a speechwriter to Secretary of State Colin Powell. From 2005-08, he was chief speechwriter to Secretary of State Condoleezza Rice and a member of the Secretary's Policy Planning Staff at the U.S. State Department. He has degrees in political science from Kenyon College and international economics from the Johns Hopkins University's School of Advanced International Studies.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 118th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: 9 February 2023

Hearing Subject:

The Future of War: Is the Pentagon Prepared to Deter and Defeat America's Adversaries?

Witness name: Christian Brose

Position/Title: Author, The Kill Chain

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

<u>Federal Contract or Grant Information</u>: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2022

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2022

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
Anduril Industries	Chief Strategy Officer

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2023

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment

2022

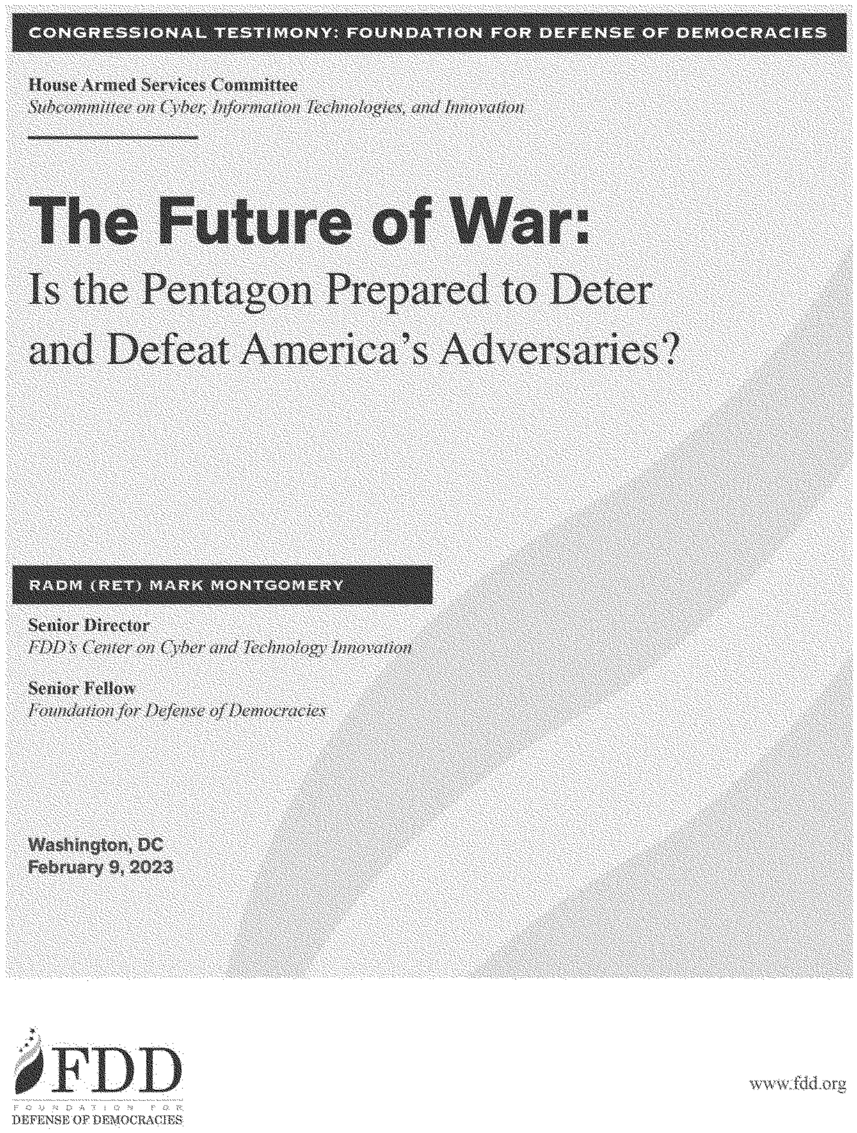
Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment



CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Armed Services Committee
Subcommittee on Cyber, Information Technologies, and Innovation

The Future of War:
Is the Pentagon Prepared to Deter and Defeat America's Adversaries?

RADM (RET) MARK MONTGOMERY

Senior Director
FDD's Center on Cyber and Technology Innovation

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
February 9, 2023

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chairman Gallagher, Ranking Member Khanna, and other members of the subcommittee, thank you for inviting me here today.

The United States Department of Defense (DOD), with the support of both Congress and the U.S. defense industrial base, has built the most powerful military force in the world. The United States has unmatched power projection capability, the ability to establish air and maritime dominance far from our shores, the resources to execute large scale ground maneuver operations, and the ability to conduct brigade-level amphibious operations. But despite all this, the United States will not be ready to deter and defeat America's most capable adversary — China — in the demanding technological environment we will face in the next five years.

This testimony will first discuss the People's Republic of China's build-up and the advantages it has in a Taiwan conflict, mainly geographic. Next, the testimony will address the five key steps the DOD/U.S. military as a whole must take to restore the balance of power. Third, the testimony will highlight four steps this subcommittee can take within its jurisdiction to facilitate the DOD-wide effort.

The Chinese Challenge

The United States has relied heavily on precision-guided munitions at range, large-scale military mobility and sustainment capacity, trained and empowered non-commissioned officers, and expansive intelligence collection and analysis capabilities to deter and, if needed, defeat adversaries. But our adversaries, particularly the Chinese, are investing in similar weapons and sensor systems, using emerging technologies to attempt to neutralize America's operational superiority and reduce the ability of U.S. forces to rapidly detect, track, and kill the adversary.

The Chinese military's capability and capacity growth has been meteoric. The Chinese Communist Party (CCP) was embarrassed by the military's relative impotence during the Third Taiwan Straits crisis of 1995-1996, when two U.S. carrier strike groups operated with impunity in the waters immediately off China's coast. The CCP has spent the past 25 years addressing that problem — building a military force designed specifically to place U.S. air and maritime operations at risk within the first island chains and soon will have the same impact within the second island chain. These Chinese investments in advanced technologies targeted observed U.S. weaknesses, such as the missile defense of ships and airfields, looking to create asymmetric advantages for Chinese forces. The Chinese also spent aggressively on technology that would marginalize existing U.S. advantages, such as military mobility and precision targeting. While the United States labeled China as the "pacing threat," the Chinese acted to develop and procure weapons as if the United States was actually *their* "pacing threat." Not surprisingly Chinese actions outperformed American rhetoric.

It is likely that current Chinese war plans will include a comprehensive pressure campaign that uses these emerging technologies to try and blind U.S. intelligence networks and silence our ability to communicate with forward forces, employ malicious cyber activity to weaken our critical infrastructure in order to both paralyze our military mobility and logistics enterprises and bring America's economy to a standstill, and conduct a disinformation campaign to try and freeze national security decision making. The Chinese objective would be to deliver a strong signal to U.S. leaders about the vulnerabilities in our systems, ensuring the United States does not come to the support of its allies and partners.

This emerging technology challenge is complicated by a number of issues this committee cannot directly solve. The first is geography. The United States is trying to deter conflict in Taiwan and in the East or South China Seas, areas within 100 miles of Chinese ports and airfields but 8,000 miles from the U.S. West Coast. Second, China is also likely to have a "first mover" advantage — as an authoritarian regime with rapacious designs, they are much more likely to strike the first blow in a conflict. Finally, China maintains a strong advantage in the "gray zone," able to conduct operations that push the bounds of international law, lack transparency, and slowly, sometimes imperceptibly, establish advantage. While we cannot fix these problems directly, we need to acknowledge them.

Despite all these challenges, the United States can retain its military-technological superiority and, in the process, overcome China's asymmetric advancements, thus maintaining America's ability to project power and impose cost and ensuring the United States supports its allies and partners and the stability of the region. This effort will require targeted investments in multiple areas where the United States can develop and deploy new capabilities in ways that China will struggle to match.

Challenges and Recommendations for the HASC

There is a great deal that Congress and the Armed Services Committees can do to address the challenges posed by China. My colleague at FDD, Bradley Bowman, and I have written that recent war games have made clear that we need to: (1) increase procurement of long-range weapons to strike Chinese ships;[1] (2) develop and deploy cruise, ballistic, and hypersonic defense capabilities throughout U.S. basing in the Pacific; (3) pre-position munitions in Taiwan for their use in a contingency as we will not be able to resupply easily in a crisis (as we have in Ukraine); (4) resource and position Deployable Air Base Systems, so air assets can rapidly move around the theater;[2] and (5) train and exercise with Taiwan air and maritime forces. All of these actions — which need to be executed by other subcommittees of the HASC — will increase deterrence and, if a war comes, improve chances for success and reduce U.S. casualties — all at a fraction of the current defense budget.

Procuring Long Range Anti-Ship Missiles. In most unclassified wargames I have played, the U.S. forces required 1,000-1,200 of these weapons to allow U.S. airmen to stay at a relatively safe range and destroy the Chinese Navy. Unfortunately, the current U.S. inventory contains less than 250 of these missiles, and the Department of Defense has been comfortable procuring

[1] Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "America's arsenal is in need of life support," *Defense News*, October 12, 2022. (https://www.defensenews.com/opinion/commentary/2022/10/12/americas-arsenal-is-in-need-of-life-support)

[2] Rear Admiral Mark Montgomery (ret.) and Bradley Bowman, "Washington is waking up on weapons for Taiwan," *Defense News*, December 19, 2022. (https://www.defensenews.com/thought-leadership/2022/12/19/washington-is-waking-up-on-taiwan)

between 38 and 88 of these a year for the past five years. At this rate the department would reach 1,200 missiles by 2035-2050, which is a bit late for comfort.[3] Additionally, these weapons are currently only launched from Air Force B-1s, which have poor readiness, and Navy F-18s, which are tied to aircraft carrier presence. The Air Force has been very slow in working to make the B-52 capable of launching these missiles. Sinking ships in a Taiwan Strait contingency must be a priority for the U.S. Air Force.[4] The Navy is also considering placing these missiles on P-8 surveillance aircraft. The HASC should continue its efforts to maximize missile production while strongly encouraging the services to expedite installation of missile launch compatibility on B-52s and P-8s.

Developing and Deploying Cruise, Ballistic, and Hypersonic Missile Defenses. One of the most salient lessons from the invasion of Ukraine is the impact of Russian cruise and ballistic missiles on Ukrainian critical infrastructure and the significant air defense capacity required to deter them. While the United States has both sea based and land based ballistic missile defense capabilities and has sufficient sea-based cruise missile defense capabilities, U.S. forces have significant gaps in protecting against cruise missiles attacking land-based targets and against all forms of hypersonic missiles.

In defending against cruise missiles targeting U.S. airfields, prepositioned equipment, ports, and logistics systems, the U.S. Army has failed to develop a follow-on mid-range air defense system to replace the Hawk systems, which were retired nearly 30 years ago. The Army has struggled to deliver the Indirect Fire Protection Capability (IFPC) system, which is now years late, and the Army refuses to consider procuring the National Advanced Surface to Air Missile System (NASAMS) that we have provided to Ukraine for the same mission and the National Guard deploys to protect you here in the National Capital Region. As a result, our airfields and logistics sites in the Pacific are left insufficiently protected against cruise missile threats.

The development of U.S. offensive hypersonic capabilities is starting to pace those of China and Russia. However, the development of U.S. hypersonic defensive countermeasures lags Beijing and Moscow's offensive efforts. The Missile Defense Agency (MDA) is still in the early stages of developing hypersonic defense systems — probably leveraging the Glide Phase Interceptor work — and the MDA will need to be both aggressive and lucky to pace Chinese offensive capability development. It would be especially worrisome and destabilizing if a "first mover" authoritarian state were to develop significant offensive hypersonic capacities before the United States and its allies had hypersonic defense capabilities.

There are also several revamped technologies that need to be brought into the air defense fight. Upgrading the outdated E-3 Sentry Airborne Early Warning and Control System (AWACS) aircraft to the new E-7 Wedgetail is a much-needed step. The department should also consider medium- and high-altitude persistent aerostats (dirigibles and balloons) with installed air defense

[3] Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "America's arsenal is in need of life support," *Defense News*, October 12, 2022. (https://www.defensenews.com/opinion/commentary/2022/10/12/americas-arsenal-is-in-need-of-life-support)

[4] Bradley Bowman and Lt. Gen. Michael A. Loh, "Guarding Contested Skies," *Foreign Podicy*, January 27, 2023. (https://www.fdd.org/podcasts/2023/01/27/guarding-contested-skies); Bradley Bowman and Lt. Gen. Richard G. Moore, "Building the Air Force the U.S. Needs," *Foreign Podicy*, October 11, 2022. (https://www.fdd.org/podcasts/2022/10/10/building-the-air-force-the-us-needs)

radars for the defense of both Guam and the homeland. These are technologies the United States has excelled at but has been slow to exploit.[5]

Pre-positioning Munitions in Taiwan for Taiwan. Another important lesson from recent wargaming is the difficulty in re-arming Taiwan during a conflict. This is in stark contrast to Ukraine, where land borders with Poland, Slovakia, and Romania have facilitated re-arming and re-supply. In the case of a Chinese blockade or invasion of Taiwan, it will be nearly impossible to resupply Taiwan. Instead, this will require pre-positioning key munitions in Taiwan that the United States might want to transfer to Taiwan in a crisis, such as anti-armor missiles, air defense missiles, anti-ship missiles, and mines. Just such an effort was authorized in the FY 2023 National Defense Authorization Act, but no funding was appropriated to execute this task. Pre-positioning of munitions in Taiwan should be prioritized for appropriation in FY 2024 budgets.

Resourcing and Positioning Deployable Air Base Systems (DABS). The USAF Agile Combat Employment (ACE) operational concept is a key element in building resilience into regional U.S. air power capabilities. The concept relies on utilizing numerous airfields distributed throughout the theater — in Japan, Australia, the Marianas, the Compact States, and possibly the Philippines — in order to complicate Chinese targeting opportunities, from both military and political perspectives. To support this concept, the Air Force needs to expedite the procurement of thirty or more DABS for the Pacific theater — each system includes maintenance, runway repair, munitions handling, and air traffic control equipment. Despite Congress identifying this issue as early as 2018, the Air Force has struggled to procure sufficient Pacific positioned DABS units.

Training and Exercising with Taiwan Forces. The United States has not exercised with the Taiwan air and naval forces in theater in nearly 40 years. This failure to train together has left U.S. and Taiwan forces at the lowest level of operational partnership — "deconflicted" — which basically means your forces stay over there and our forces will stay located over here. To effectively counter Chinese military moves, the United States and Taiwan need to raise their level of operational partnership to "coordinated" or even "integrated." This will take significant operational exercises, table-top drills, and wargaming — all of which were authorized and directed in the FY 2023 NDAA after years of "sense of Congress" statements that such work was needed. Given the previous Department of Defense reluctance to conduct such bilateral exercises, Congress will have to carefully oversee and manage the department's efforts.[6]

[5] Bradley Bowman, Maj. Lauren Harrison, and Ryan Brobst, "Between E-3 And Eyes In Space, The Air Force Needs A Bridge, Now," *Breaking Defense*, October 5, 2021. (https://breakingdefense.com/2021/10/between-e-3-and-eyes-in-space-the-air-force-needs-a-bridge-now); Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "Time To Wedge The E-7A Wedgetail Into The US Air Force Fleet," *Breaking Defense*, October 25, 2021. (https://breakingdefense.com/2021/10/time-to-wedge-the-e-7a-wedgetail-into-the-us-air-force-fleet); Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "If The Air Force Buys The E-7A Wedgetail, What's Next?," *Breaking Defense*, October 26, 2021. (https://breakingdefense.com/2021/10/if-the-air-force-buys-the-e-7a-wedgetail-whats-next); Bradley Bowman and Maj. Brian Leitzke, "Let the Air Force let go of the E-3 'Sentry'," *Breaking Defense*, July 29, 2022. (https://breakingdefense.com/2022/07/let-the-air-force-let-go-of-the-e-3-sentry)

[6] Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "Standing With the Free People of Taiwan," *Foundation for Defense of Democracies*, December 15, 2020. (https://www.fdd.org/analysis/2020/12/15/defending-forward-standing-with-the-free-people-of-taiwan)

Specific Challenges and Recommendations for the CITI Subcommittee

In this Cyber, Information Technologies, and Innovation (CITI) subcommittee, there are equally important steps that need to be taken to ensure U.S. forces are ready to deter and defeat America's adversaries in the demanding technological environment we will face in the next five years. At a minimum, this subcommittee should work to: (1) improve the cyber and information resilience of the military and the nation; (2) assess and strengthen the readiness and structure of U.S. Cyber Forces; (3) enable an environment where innovation is encouraged and risk is accepted; and (4) help allies and partners maintain interoperability with U.S. forces as they modernize.

Improve our Cyber and Information Resilience. In a contingency or conflict with China, U.S forces must maintain their ability to detect and track adversaries, communicate among forces, and mobilize and sustain forces. China's opening moves in any crisis or conflict, either to deter U.S. action or to defeat U.S. efforts, will be aimed at limiting or eliminating: the U.S. military's ability to sustain its operations logistically; the U.S. ability to see, track, and locate Chinese forces; and the capability of U.S. military leaders to command and control forces. Unable to communicate, deploy, or resupply, U.S. forces will be paralyzed. To avoid this situation, the U.S. military needs to build resilience, including through redundancies, across every link and node of its operations — from sensors to attack platforms, in information architecture and networks, across command-and-control systems, and at a pace commensurate with the threat. In addition to this cyber hardening, the United States will need to acquire large numbers of low-cost and expendable platforms that would support surveillance, communications, logistics, and strike — especially during the opening days of a campaign. This subcommittee can and should have a significant say in investments that protect the resilience of the military cyber and information enterprise.

This resilience will have to extend into our national critical infrastructure — the transportation systems, electrical power systems, water systems, financial systems, and other sectors that enable the mobilization and resupply of U.S. forces. Building such a resilience is a more burdensome process as it requires the development of a public-private collaboration that has not succeeded despite 20 years of government efforts. It is estimated that 85 percent of the national critical infrastructure is owned and operated by private sector or state and local utilities, not the federal government. This creates a defense challenge that is much more complex than traditional warfare areas, such as anti-submarine warfare or air defense, where all the assets are owned and operated by the U.S. military. The responsibility for this collaboration extends across multiple federal agencies and congressional committees, but this subcommittee can ensure that key elements of the public-private partnership are being addressed, such as establishing a cyber threat information collaboration environment (CTICE). This CTICE would consist of technical tools for information analytics and a portal through which relevant government and industry parties can submit and access cyber threat information from different sources across the federal government, including the intelligence community, with the requisite clearances and permissions. This subcommittee's former chairman, Rep Jim Langevin, attempted to champion just such legislation last year.

Assess and Strengthen U.S. Cyber Forces Readiness and Structure. Over the past decade, this subcommittee has provided extensive guidance and oversight to the development and employment of U.S. cyber forces. Despite this attention and inspired leadership from the U.S. Cyber Command, U.S. cyber forces are inconsistent in organization, readiness, and training across the military services. Additionally, the size of each service contribution to the cyber mission forces has not changed appreciably since the original agreements in 2012, despite significant changes in the cyber threat. As a result, the United States is not optimized for conflict with a Chinese adversary, which created a single military component in its Cyber Support Force back in 2016. This Chinese effort is improving in capability and already has a significantly (up to 10 times) larger capacity.

This subcommittee should address the challenges to U.S. cyber force posture across three issues: force readiness, structure, and operations. In the cyber force readiness area, the subcommittee should assess the inconsistent readiness of service cyber forces in light of the recently delivered cyber force structure review. The subcommittee should also evaluate the utilization and performance of the Pentagon's special hiring authorities for cyber professionals.

In the force structure area, the subcommittee should assess if the force design of Cyber Mission Force, conceived more then 10 years ago, can effectively produce forces for 21st century warfare, or if more dramatic solutions, such as an independent Cyber Force, should be considered, as was recently done with the Space Force. The committee should also look at the structure and responsibilities of the newly created Assistant Secretary of Defense for Cyber Policy and determine from what additional authorities the office would benefit.

In cyber force operations, the subcommittee should ensure that the principles laid out by the Congress in Section 1632 of the FY 2019 NDAA — supporting "defend forward" operations and increasing the level of U.S. efforts to impose costs on adversaries in cyberspace — are being adhered to. Additionally, the subcommittee should assess and encourage the development of both the offensive and defensive cyber capabilities of certain allies and partners, including Taiwan.

Enable an Environment to Innovate. The United States has learned some important lessons from the conflict in Ukraine, and the Department of Defense should be working to apply these same lessons in dealing with the defense industrial base. For example, the Ukrainians needed anti-ship cruise missiles to limit Russian Navy operations in the Black Sea. With no program of record available for a land-based Harpoon missile launching system, the Ukrainians had to work with Boeing, the Danish Army, and the U.S. Navy to "MacGyver" a cobbled together launcher system. Taiwan has asked for a similar land-based Harpoon system and was approved for purchase in 2020, but delivery of a "new design" system is not expected until 2027 or later. Clearly a similar "MacGyver" approach can and should be taken by Boeing and the U.S. Navy to ensure that a key partner has the weapon systems needed to deter Chinese action sooner than seven years after they ordered it.[7]

[7] Rear Admiral Mark Montgomery (ret.) and Bradley Bowman, "How 'MacGyver' magic can get Taiwan its Harpoon defenses faster," *Defense News*, December 7, 2022. (https://www.defensenews.com/opinion/commentary/2022/12/07/how-macgyver-magic-can-get-taiwan-its-harpoon-defenses-faster)

Similarly, Ukraine is desperately seeking air defense solutions for the Russian cruise missile challenge. As the Ukrainians ran out of Soviet-era missiles for their BUK-M1 launchers, they again worked to pull together a non-standard solution. The United States provided RIM-7 Sea Sparrow missiles that the Ukrainians rapidly integrated with their radar and fire control systems. This is especially impressive given the U.S. Army's 10-year-long unsuccessful struggle to build a similar medium-range air defense system from the ground up. The subcommittee should work to encourage a little more "MacGyver" and a little less "Valley of Death."

Help Allies and Partners Develop and Maintain Interoperability with U.S. Forces. The United States often modernizes its forces, including investments in software and command, control, and communications systems without sufficient consideration for the gap it creates in capabilities with our allies and partners which eventually lead to challenges conducting coalition operations. A number of issues can inflame this gap, including insufficient defense spending by partners and U.S. security (classification) concerns. The United States must address these challenges if it is to capitalize on one of its most enduring asymmetries against China — its network of alliances and partnerships. This is particularly true as the United States begins developing and fielding the Joint All Domain Command and Control (JADC2) architecture. This JADC2 system will clearly need a multilateral capability for key partners to participate in, including Japan, Australia, and eventually Taiwan, and in doing so, the U.S. will need to accept far greater risks in information sharing and transfer of technologies.

Conclusion

The United States and its allies and partners may not be on the right track to be ready for a conflict with China in the next five years, but they certainly can be, and this committee can help make that so. Targeted investments by the whole committee in anti-ship munitions, missile defense capabilities, prepositioned gear in Taiwan, air asset deployment capabilities, and exercising with Taiwan forces, will restore the U.S. ability to maneuver forward and reduce U.S. casualties — and all at a fraction of the current defense budget. This subcommittee can work to improve the cyber resilience of the military and the nation; bolster the capacity of the U.S. cyber forces; enable an environment where innovation is encouraged; and keep our allies and partners on step with us. All of these efforts will restore our ability to deter malicious Chinese efforts in the Western Pacific and — if deterrence fails — defeat Chinese aggression.

RADM (Ret.) Mark Montgomery
Senior Director, FDD's Center on Cyber and Technology Innovation
Senior Fellow, Foundation for Defense of Democracies

Mark Montgomery serves as senior director of the Center on Cyber and Technology Innovation, where he leads FDD's efforts to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish them. Mark also directs CSC 2.0, an initiative that works to implement the recommendations of the congressionally mandated Cyberspace Solarium Commission, where he served as executive director. Previously, Mark served as policy director for the Senate Armed Services Committee under the leadership of Senator John S. McCain, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy.

Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017. His flag officer assignments included director of operations (J3) at U.S. Pacific Command; commander of Carrier Strike Group 5, embarked on the USS George Washington, stationed in Japan; and deputy director for plans, policy and strategy (J5) at U. S. European Command. He was assigned to the National Security Council from 1998 to 2000, serving as director for transnational threats. Mark has graduate degrees from the University of Pennsylvania and the University of Oxford and completed the U.S. Navy's nuclear power training program.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 118th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: 9 February 2023

Hearing Subject:

“The Future of War: Is the Pentagon Prepared to Deter and Defeat America’s Adversaries?”

Witness name: Rear Admiral Mark Montgomery, U.S. Navy (Ret)

Position/Title: Senior Director, Center on Cyber and Technology Innovation

Capacity in which appearing: (check one)

○ Individual ● Representative

If appearing in a representative capacity, name of the organization or entity represented:

Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NONE			

2022

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NONE			

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NONE			

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NONE			

<u>Foreign Government Contract, Grant, or Payment Information</u>: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NONE			

2022

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NONE			

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NONE			

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NONE			

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
NONE	

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2023

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NONE			

2022

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NONE			

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NONE			

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NONE			

What Would Winning Look Like? A Scenario From The Future

Testimony Submitted for the House Committee on Armed Services Subcommittee on Cyber, Innovative Technologies
Hearing on
"The Future of War: Is the Pentagon Prepared to Deter and Defeat America's Adversaries?"
Thursday, February 9, 2023

By Peter W. Singer

Whether the Pentagon is prepared to deter and defeat America's adversaries in the future turns on not merely our own plans and capabilities. It is actually determined by what our adversaries think of those plans and capabilities compared to their own.

Thus, a valuable approach in such discussions of strategy is to ask "What would winning look like?" not just for us, but to our foes, who fear such an outcome. We can then work backward and explore what are the potential elements of such a successful future history and how can we build towards them today?

A methodology for this cross of strategy and scenario is the deliberate blend of nonfiction with narrative communication techniques. Known as FICINT for "Fictional Intelligence" or "Useful Fiction," the goal is not to replace the traditional white paper, article, or memo, but to achieve a greater impact of research and analysis through sharing insights through the oldest communication technology of all: Story. The narrative is designed to allow a reader to visualize new trends, technologies, or threats, not just from altered perspectives, but in a format that the science of the brain shows is more likely to lead to both understanding and action. As such, the approach has been used by organizations that range from the U.S. and NATO militaries to Fortune 500 companies.

The following is such a scenario designed to visualize various elements of "What Would Winning Look Like?" in a successful future, where the Pentagon proved able to deter and defeat America's adversaries. It envisions a positive outcome in the central dilemma in current U.S. defense planning and congressional concern: how to successfully deter the PLA from attacking Taiwan over the long term, especially as the PLA advances its strength and confidence.

The narrative, which is set an unspecified number of years in the future, is told from the perspective of an imagined PLA officer in the wake of a leadership purge after the regime failed to bring Taiwan under Communist rule, despite decades of military buildup. It thus explores various conditions that might lead China to "blink" in its long-running threat against Taiwan, as well as how US policy might create such conditions through:

- Keeping pace with ongoing changes in technology and warfare
- Training and equipping US and allied military personnel to have needed skills cutting across the kinetic as well as cyber/info space
- Building greater resilience, both in the US and in Taiwan
- Learning lessons from recent conflicts in Ukraine and elsewhere
- Creating "imperial overstretch" and readiness challenges for our foes
- Bolstering regional capability and will to resist China

That is, the scenario blends fact-based research with story, to share purposeful lessons with application across a wider set of issues for the future of war.

To clarify, while every trend, technology, and policy recommendation woven into the narrative is real, the narrative is not "prediction." Rather, it is meant to stoke healthy discussion and debate about the future of war and deterrence, by envisioning elements of a successful outcome of the Subcommittee's work.

OPENING STATEMENT BY PRISONER R-45 TO THE PEOPLE'S COMMITTEE FOR REVOLUTIONARY RENEWAL

I offer my gratitude to the People's Committee for Revolutionary Renewal for deigning to accept my opening statement. I come to you humbled and reflective, based on the welcome time that the new leaders of the Party have provided me to contemplate my extensive errors.

While I can only speak to my own past role as a general officer in the People's Liberation Army strategy cell, it is my duty to accept personal responsibility for our collective humiliation at the failure to complete our historic mission. We did not live up to the great trust placed on us, for which the Party struggled and the people sacrificed, literally for decades.

Solving the Taiwan question and realizing the complete reunification of the Motherland was the unswerving historical task of the Party from its founding. It has been the common aspiration of all our sons and daughters, and a requirement for realizing the great rejuvenation of the Chinese nation. As we now enter the second century of the Party's great rule, rejuvenated in leadership by the recent Revolutionary Renewal, I must apologize for our failures.

The Party had a theory of victory in this mission, which we who led the PLA at the time did not deliver upon. With reflection, I can now see how the pride and arrogance of a few led to such a heavy weight upon the shoulders of many, which was not recompensed with success. We missed the window of opportunity to unify China that was offered to us by the Party and by history. And for that, I am ashamed.

Just as each of us have rightly been asked to enumerate our crimes against the Party, so too shall I specify the areas where we failed in accomplishing reunification.

To begin, we seemingly grew in power and reach over the period of my service, yet the PLA's mission readiness, particularly within our naval forces, fell with each year that we looked farther and farther from home. It was much lower than reported because we military leaders lacked the courage to speak the truth. We avoided open-ended wargames and fleet problems, designed to test and learn, instead choosing scripted exercises that hid our flaws out of fear of the consequences.

It was not merely an issue of our own performance. At the same time, our foes made steady improvements that didn't just reflect lessons from their own experience of two decades of conflict, but grappled with the enormous changes occurring in technology and warfare itself.

They didn't fall prey to political and bureaucratic inertia and the heavy weight of so-called "sunk cost" major platforms to keep them on the same path. Rather, their military instituted a wave of new initiatives and reforms. They altered everything from what systems they bought to how they bought them. While we depended upon a plan of "civil-military fusion," with a few state-supported corporate titans, they cultivated a more dynamic defense industrial marketplace, where their military could engage with and purchase from both big and small firms.

Even how they learned about innovation showed innovation. They didn't just create singular innovation hubs and experimental task forces in only a few locations, but scaled them across their force, such that every command had access to a more rapid means of learning and implementation. The Americans also scaled out contests that rewarded "bottom-up" proposals and fixes from the most junior of troops. These were hard to even contemplate in our force, but proved of great value to theirs. Indeed, I know the committee might think me a fiction writer, but the American military even created copies of the "Shark Tank" program that you may be familiar with from Shenzhen TV as "Dragon's Den," creating successful versions in their Airborne corps and then replicating them across every other unit.

We saw the effect of this mass culture of innovation, for instance, in how American military culture and industry alike overcame decades of doubt about unmanned systems. They soon deployed these "drones" across every domain, and, most importantly, in manners and designs that didn't just simply replicate the expensive manned systems they were replacing. They took advantage of robotics' unique attributes, allowing swarming and cheap, high-risk uses in the air, ground, and sea domains, especially under the waves. They also stayed one step ahead of the back and forth of arms races. Projecting our own planned use, they made sure to simultaneously develop and actually deploy counter-drone systems of kinetic, EW, and directed energy types.

America's new hardware, though, wasn't perhaps the most important part of the story of their military acquisitions. It was how their hardware was integrated and advanced with the latest in the ongoing revolution in artificial intelligence. We sought to be the dominant power in intelligentization, but they made sufficient investments to keep pace with the civilian embrace of AI, and even push it forward toward new frontiers like in quantum technology.

It is striking to say, but here the American government bureaucracy proved as important as their software. While we built a centralized data model, reflecting our government and industry model, their Pentagon chose the path of a federated model of meshed data systems, which reflected their own democratic culture and the growing economy of microservices. It allowed simultaneous data ownership and a universal interoperability layer to foster communication between distributed data across different locations. Thus, their systems were not just smarter out on the edge of their use in the field, but also less vulnerable to the cyber attacks we had planned to transform the strength of their networks into vulnerabilities.

Unfortunately, the very same building of resilience happened across the new domains that we hoped to take away from them. In outer space, the American space forces eschewed their old approach of billion dollar platforms and single points of failure. Our threats of orbital warfare rank empty after they created redundancies and scale in their networks through fleets of micro-sats and cheap launch systems. In cyberspace, we similarly saw great opportunity in how the Americans seemed to be recreating all their same mistakes in the new "Internet of Things" that had made the original form of the Internet so vulnerable. Unfortunately, after a few episodes made evident what could be done to military networks, power systems, gas pipelines, and even hospitals, the Americans learned their lessons. With the higher stakes of digital attacks on physical systems becoming obvious, they finally created the needed requirements and regulations to bake cybersecurity in, while also aligning their standards with their allies.

Yet, the Americans didn't just create deterrence by denial, through making our attacks less likely to succeed. They pushed back and dared to engage us in persistent competition and even harassment on the information, economic, political, and cyber fronts. Most of these incidents are still difficult to attribute, which is by design, as they were often carried out by US and allied cyber and special operations forces in a deniable manner. Yet, as we sought more and more influence and presence in the world, it instead felt like we were constantly pushing against more than just normal operational friction. Our morale and confidence were repeatedly undermined, inefficiencies compounded, and local parties alienated.

Our arrogance prevented us from understanding the significance of what could be accomplished by such a long-running, strategic campaign put in place by Americans. Their aim was not merely to provide direct support to the illegal regime in Taiwan; they thought more broadly about both renewing their strength and eroding our global military, political, and economic effectiveness.

To us, our growing military presence and Belt and Road Initiative projects represented the means to gaining back the rightful power that our nation has historically wielded well beyond its borders. We failed to see that to them, this greater activity presented an opportunity to cause for us the very same kind of imperial overstretch that has long troubled great powers.

We were not able to overcome what turned out to be an array of initiatives meant to create resistance against the justness of our cause. For instance, our information and cyber campaigns, supplemented by military, diplomatic, and economic lines of efforts, sought to reproduce in Taiwan what we accomplished in Hong Kong, as both had been unjustly ripped away from us by foreign powers. We believed that, over time, we could simply use our growing power to awe into submission both the local population and, perhaps even more importantly, the government and business leaders of the wider world. They would be led to think that our victory was inevitable, so why fight it?

Alas, it was our alternative that became unthinkable. Taiwan's civilian and military populations alike were well not just physically, but cognitively prepared to resist. Our covert campaigns were not able to maintain their secrecy, in large part due to their combined cyber and diplomatic efforts. This drained the poison we sought to inject into their corrupt system, while efforts to distract and divide our global foes met with counters in each domain.

With peaceful reunification unlikely, that left us only with the option of an assault. It was the scenario that had driven decades of our military planning and reform, upon which the Party and the people had invested literally hundreds of billions in yuan. It was to be the culmination of all our careers.

Yet when it came time to truly contemplate such action, we shamed ourselves and those who trusted us. For all our gains in hardware that we generals proudly paraded in front of you each year through the streets of Beijing, Taiwan's ability to repel an amphibious and airborne assault increased even more dramatically. It seems that they distracted us with all the talk of purchasing expensive new fighters and easy-to-target warships, when what they really built was an agile defense and a resilient society. With American aid, they gained widely distributed anti-air weapons and new swarming drone systems to take away our quantitative advantage in ships, tanks, and planes, and cheap, smart mines able to rapidly block the very seaways that we needed to cross.

This all transformed a once vulnerable target into the equivalent of a "porcupine," that ugly rodent native to America, which even the most powerful predator avoids. It was not just that even a successful invasion across the straits would have meant countless of our families without their only sons. It was that somehow digesting that barbed animal would prove ever more costly. We never figured out how our forces would be able to control a society prepared for resistance without great losses, especially in the urban terrain in and around Taipei, Kaohsiung, and Taichung.

For much of this, we can blame our pathetic "partners" to the north. They did not just drain our own resources; they also guided the world's democracies toward successful resistance models through the lessons learned from how their folly-filled invasion of their own break-away province was defeated.

The barbs of this porcupine also extended into new realms in creative ways that we failed to grapple with. As an example, for all our vaunted cyber capabilities, Taiwan's illegal government mirrored its digital systems outside the country in friendly nations, here again creating resilience through redundancy.

My discussion of all this high technology, however, must not miss our human mistakes. As we rolled out new missile after missile, assuming bombardment from afar might create the equivalent of a blockade of falling projectiles, new American units were formed to be able to operate within the very same areas to which we sought to deny access. Their forces developed the competency to operate across multi-domains and units became rapidly deploying networks of small teams, each able to operate in cohesion or independently, yet generate disproportionate kinetic and non-kinetic effects against our major systems. In turn, their special operations forces moved beyond the mentality of direct action honed during their wars against terrorists, which we mimicked with our own “Wolf Warrior” videos and mindset. Instead, they transformed, fielding innovative blended teams of technical experts and elite soldiers, able to provide a more comprehensive “full continuum” of uses, utilities, and identities. Underscoring these efforts was the building networks of personal and professional ties with their peers across the region.

Most of all, the Americans proved able to succeed at the most essential human part of any military: recruiting and retaining the best of their society. We had hoped that their domestic political divisions, amplified by our and Russian information operations, would be replicated in their military, tearing it apart from the inside. Instead, they created digital literacy programs like in their Baltic allies, to better equip their youth for a world of new online challenges and threats, while the US military proved able to retain its professionalism while evolving to reflect the new America that it both drew upon and protected.

This attention to the human element in warfare stands in contrast to our failure, especially to build up a truly professional NCO corps. You are well aware of our struggles to recruit and retain talent from our educated youth, especially amidst a population shrinkage and the greater lures of the competing civilian economy.

The human side of politics and war also became a factor in regional developments that further limited our options. Through both inducements and threats, we built a network of political, economic, and military cooperation agreements across Asia and beyond. It was bolstered by a strategy of growing other nations' reliance upon our infrastructure and financing, provided at below-market rates. We supplemented this with extensive efforts to create similar dependence by their major corporations and even most wealthy individuals, such that they would dare not to cross us and even self-censor even the most mild critique. This was all as much about our own power as the tacit message that, during any crisis, it would be best for them to stand aside or face dire consequences for their own operations and bank accounts. We thought that this network of pressure could create wedges between Taiwan, the US, and its allies, denying them everything from global and domestic political support to needed military basing to crucial elements in their supply chain.

We failed to realize that there was another side to this coin: what we invested could also be held hostage. They turned the tables on us, leaving us the ones isolated, and with a vulnerable supply chain and far-flung infrastructure investments that we struggle to defend from afar. Here again, the hand of America was at play. They identified and shored up dependencies, offering more palatable and profitable alternatives. They worked with regional partners in a manner that respected local priorities rather than only Washington's, building local confidence and capability to stand against us. In each bilateral tension, they saw multilateral opportunity. Our weaker neighbors now all align in opposition, in an arc running from India to Vietnam to the Philippines to Japan. Whatever historic grievances existed gradually became less important than their unity against what they grew to perceive as a greater threat.

These American allies proved as valuable to them as the feckless ones we put faith in failed us. Russia imagines itself a great power, but showed itself to be an ineffective junior partner. For all that we sensibly took advantage of Moscow's moment of need through rewriting deal terms and growing their dependence, Russia's loss in Ukraine was a strategic loss to us. Its defeat, ensured by NATO aid, didn't just hollow out one of our only allies' capability and confidence; it also signaled to the world that democracies could indeed resist aggression. So too did the mercurial potentates in the Persian Gulf disappoint us as much as they had the Americans. We must now admit that we made the very same mistake that they had for decades, confusing contracts for actual alliances.

In closing, I offer these lessons learned too late, in the pathetic hope that they might somehow prove of value to your own efforts to lead China into the second century of the Party's great vision. I fully understand that none of it excuses my own failings and those of my generation's leaders. For that, I can only beg for your forgiveness and mercy.

==

Key Elements For A Successful US Policy In The "What Would Winning Look Like?" Scenario:

1. Engage in open-ended wargames and fleet problems, designed to truly test and learn

2. Avoid letting political and bureaucratic inertia and the heavy weight of"sunk costs" drive acquisition decisions

3. Create a more dynamic defense marketplace, where the military can engage with and easily purchase from both big and small firms

4. Scale innovation hubs and experimental task forces across the force, such that every command has access to a rapid means of learning and implementation.

5. Replicate more widely the current "Shark Tank" contests that reward "bottom-up" proposals and fixes from the most junior of troops

6. Invest in a new generation of unmanned systems, across *all* domains

7. Avoid "drones" that simply replicate the expensive manned systems they are replacing

8. Implement new doctrines and acquisitions that take advantage of robotics' unique attributes, allowing swarming and cheap, high-risk uses

9. Develop and deploy counter-drone systems of kinetic, EW, and directed energy types

10. Invest in AI to match its growing importance in the civilian sector

11. Reform US military data networks to take advantage of AI and reflect commercial best practices, through creating a federated model of meshed data, that allows simultaneous data ownership and a universal interoperability layer to foster communication between distributed data across different locations

12. Create redundancies and scale in space networks through fleets of micro-sats and cheap launch systems

13. Create requirements and regulations to bake security into emerging Internet of Things systems, so as to limit physical damage from digital threats

14. Align US cyber rules and regulations with major allies

15. Engage in persistent competition on the information, economic, political, and cyber fronts, designed to create greater friction for PLA and CCP, compound its operational inefficiencies, and worsen its relations with local parties

16. Build a strategy designed to foster "imperial overstretch" challenges for major foes and invert the perceived value of their Belt and Road investments

17. Utilize cyber and diplomatic means to repeatedly out covert campaigns by adversaries to undermine democracies

18. Provide Taiwan distributed anti-air weapons and unmanned systems to take away adversary quantitative advantage, and cheap, smart mines to block seaways

19. Aid in Taiwanese efforts to create a society prepared for resistance, especially in urban settings

20. Mirror Taiwanese and other allied digital systems outside the countries, creating resilience through redundancy.

21. Scale new US military units able to operate across multi-domains, rapidly deploying networks of small teams, each able to operate independently yet generate disproportionate kinetic and non-kinetic effects against major systems

22. Transform Special Operations Forces into blended teams of technical experts and elite soldiers, able to provide a more comprehensive "full continuum" of uses, utilities, and identities,

23. Build networks of personal and professional ties between US officers and their peers across the INDOPACOM region

24. Create digital literacy programs modeled after successful allied efforts, to better equip American society for new online challenges and threats

25. Ensure that the US military is able to retain its professionalism while evolving to reflect the new America that it both draws upon and protects

26. Work with regional partners in a manner that respects local priorities rather than only Washington’s

27. Seek to bolster multilateral ties between key states that each have worsening bilateral ties with China

28. Do not confuse contracts for shared values or actual alliances that will deliver in crisis

29. Raise costs for China’s aid to Russia in the Ukraine war, worsening ties between the two

30. Ensure Russia’s defeat in Ukraine, both to weaken it and its allies, as well as provide a model of success and inspiration for other democracies under threat

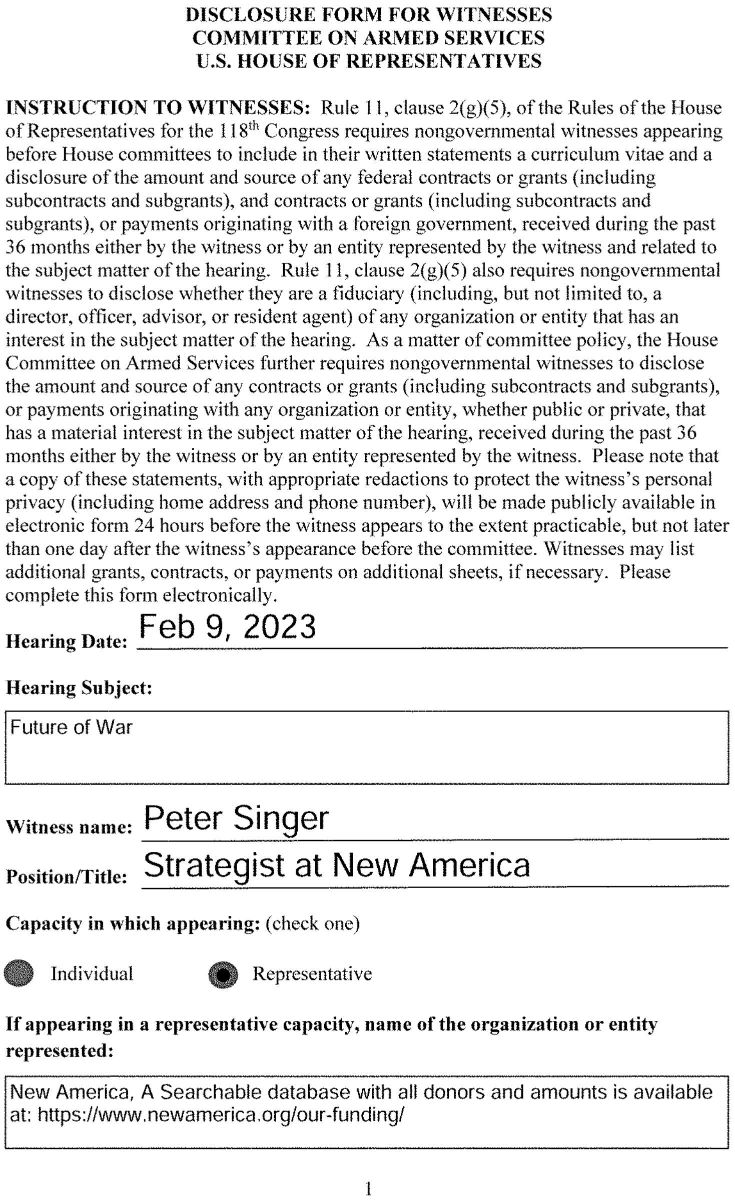
Biography:
Peter Warren Singer is Strategist at New America, a Professor of Practice in Global Security at Arizona State University, and a founder and managing partner at Useful Fiction. He has served as a consultant for the US military and intelligence community and previously worked at Harvard University, The Brookings Institution, and the Office of the Secretary of Defense. A best-selling author of both fiction and non-fiction, he has had more books on the US military professional reading lists than any other author, living or dead.
More at https://www.pwsinger.com

The scenario essay was developed in partnership with the author and futurist August Cole. Bio at https://www.augustcole.com/

Peter Warren Singer

Peter Warren Singer is Strategist at New America, a Professor of Practice at Arizona State University, and Founder & Managing Partner at Useful Fiction LLC.

A *New York Times* Bestselling author, described in the *Wall Street Journal* as "the premier futurist in the national-security environment" and "all-around smart guy" in the *Washington Post,* he has been named by the Smithsonian as one of the nation's 100 leading innovators, by *Defense News* as one of the 100 most influential people in defense issues, by *Foreign Policy* to their Top 100 Global Thinkers List, and as an official "Mad Scientist" for the U.S. Army's Training and Doctrine Command. No author, living or dead, has more books on the professional US military reading lists. His non-fiction books include *Corporate Warriors: The Rise of the Privatized Military Industry, Children at War, Wired for War: The Robotics Revolution and Conflict in the 21st Century; Cybersecurity and Cyberwar: What Everyone Needs to Know* and most recently *LikeWar,* which explores how social media has changed war and politics. It was named an *Amazon* and *Foreign Affairs* book of the year and reviewed by *Booklist* as "LikeWar should be required reading for everyone living in a democracy and all who aspire to." He is also the co-author of a new type of novel, using the format of a technothriller to communicate nonfiction research. *Ghost Fleet: A Novel of the Next World War* was both a top summer read and led to briefings everywhere from the White House to the Pentagon. His latest is *Burn-In: A Novel of the Real Robotic Revolution*. It has been described by the creator *of Lost* and *Watchmen* as "A visionary new form of storytelling—a rollercoaster ride of science fiction blended with science fact," and by the head of Army Cyber Command as "I loved Burn-In so much that I've already read it twice."



DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 118th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: Feb 9, 2023

Hearing Subject:

Future of War

Witness name: Peter Singer

Position/Title: Strategist at New America

Capacity in which appearing: (check one)

○ Individual ● Representative

If appearing in a representative capacity, name of the organization or entity represented:

New America, A Searchable database with all donors and amounts is available at: https://www.newamerica.org/our-funding/

<u>Federal Contract or Grant Information</u>: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
	State	400000	Ranking Digital Rights
	Army War College	25000	Army FEF Fellowship

2022

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
	State	400000	Ranking Digital Rights
	State	437500	Blockchain Accelerator
	Army War College	25000	Army FEF Fellowship

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
	State	400000	Ranking Digital Rights
	State	584731	Blockchain Accelerator
	Army War College	25000	Army FEF Fellowship

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
	State	584731	Blockchain Accelerator
	Army War College	25000	Army FEF Fellowship

<u>Foreign Government Contract, Grant, or Payment Information</u>: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2022

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
	Australia	330,046	New America Digital Impact and Governance Initiative
	Japan	17500	New America International Security Program

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2023

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment

2022

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
	Northrop	75,000	New America, International Security Program
	Lockheed	10,000	New America International Security Program
	Bluepath	2,500	New America General Operating Fund

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
	Northrop	75,000	International Security Program

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
	Northrop	75,000	International Security proram

DOCUMENTS SUBMITTED FOR THE RECORD

FEBRUARY 9, 2023

USA TODAY

OPINION *This piece expresses the views of its author(s), separate from those of this publication.*

U.S. Congress Add Topic

Two congressmen offer a bipartisan plan to 'drain the swamp'

Congress should seek common ground across party lines to end gridlock and corruption.

Mike Gallagher and Ro Khanna
Published 9:15 a.m. ET June 1, 2017

You'd be hard-pressed to find two congressmen more dissimilar than us. We come from different parties, and we represent very different districts. One of us taught economics in the technology hub of Silicon Valley; the other is a Marine veteran from the dairy farming capital of the country. One of us campaigned against the Iraq War; the other served in it. Though we may not agree on everything, we do agree wholeheartedly on a key takeaway from our first few months as members of the U.S. House of Representatives: Congress is in critical need of reform to reduce corruption and diminish the power of special interests.

While the phrase "structural reform of Congress" often gets pushed aside to seemingly more urgent debates about domestic and foreign policy, we ignore this issue at our peril. The comedic newspaper *The Onion* ran an article in 2010 with the satirical headline "American People Hire High-Powered Lobbyist To Push Interests In Congress." We aren't sure if people would even recognize that as satire anymore.

Whether in Cupertino or Green Bay, we have heard loud and clear that our constituents want a fairer system of government, less money in politics, more bipartisanship and fewer lobbyists in Washington. Each of us have core values on which we will never compromise, and our voting records reflect that. However, 83% of Americans believe that Congress should find common ground on issues in order to get things done.

If voters want us to work together to solve problems, then why the years of gridlock? Put simply, because the system supports the status quo and resists real change.

We are at a historic opportunity to change that and institute reforms that will reduce corruption in our government and the influence of money in politics. The new administration, whatever your views on it, came to power pledging to drain the swamp. Bernie Sanders, whose populist message inspired millions, agrees with that goal, if not the method. The current freshman class of House of Representatives, which includes 27 Democrats and 28 Republicans, is more receptive to these ideas than any before.

As two of those 55 new voices in the House, we are proposing a series of reforms that will diminish the influence of special interests in politics, as well as encourage new voices to embark on the path we have taken to public service.

> Nonpartisan redistricting is essential to ensure politicians aren't allowed to gerrymander their districts and choose their own voters. The less competitive a district becomes, the more general elections become formalities. This practice is already at work in Arizona, California, and Iowa and having independent, nonpartisan commissions commonplace across the country will ensure our congressional districts are drawn by the people, not politicians.
>
> Congress should not be a career. The longer people stay in Congress, the more adept they become at making the system work for them and not their constituents. That is why we and a number of our fellow freshmen support legislation that would set term limits of 12 years for Representatives and Senators.
>
> People should also run for Congress to serve, not to profit. That is why we call for a five-year ban on lobbying after a member of Congress leaves office. We hope that our colleagues all have successful careers after they turn in their voting cards; however, that success should not come from the "revolving door" between the Capitol Hill and K Street.

This is just a modest start. We hope to talk to many of our constituents and colleagues from both sides of the aisle in the weeks and months ahead to gather more proposals to encourage a culture of reform in Washington. We want to challenge the administration to live up to its campaign promise about "draining the swamp." We also want to challenge ourselves and our colleagues to put self-interest aside and start putting forth reforms that reduce the power of special interests.

And, most importantly, we want to challenge voters to demand that their elected representatives support these efforts, or else find others who will.

Draining the swamp is not enough. Unless you structurally change how the swamp is fed, it will fill right back up. So let's start on that structural reform and lay a pathway for tomorrow's leaders to unite the country and confront the problems of the 21st century in the only manner we have a chance at solving them: together.

Republican Rep. Mike Gallagher represents the 8th congressional district of Wisconsin, which includes Green Bay. Democratic Rep. Ro Khanna represents the 17th congressional district of California in Silicon Valley.

You can read diverse opinions from our Board of Contributors and other writers on the Opinion front page, on Twitter @USATOpinion and in our daily Opinion newsletter. To submit a letter, comment or column, check our submission guidelines.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

FEBRUARY 9, 2023

RESPONSE TO QUESTION SUBMITTED BY MR. MOULTON

Mr. SINGER. Thank you for the question.

Almost every new tech in war, whether the battleship to nuclear weapons, has created new questions of their use and abuse, often leading to arms control discussions. So we should not be surprised to see this happen with AI and robotics.

Yet, this new wave of intelligent automation is different in that it is more than just another new tool. It is ever-improving and ever more autonomous, one that decides and acts more and more on its own, with its very value being that it is increasingly a so-called "black box" that processes and acts in manners we humans can't understand. Thus, there are basically are of two new types of ethical/legal issues that result:

1) Machine permissibility ("What should our ever more intelligent and capable machines be allowed to do, including on their own?") and

2) Machine and human accountability ("Who should be in control of them and how? What should we do if things go awry?").

What is notable is that these issues will play out everywhere from the battlefield to our highways to our businesses. This also shows how AI/Robotics present an added challenge compared to most weapons in the past, in that their creators, users, and uses don't just lie in the military realm.

Specific to arm control, AI could be a positive tool, such as helping us detect and track arms control treaty violations or illegal arms trade networks, as well as help unearth war crimes.

But it also could potentially be utilized in manners that lead to war crimes, such as through more lethal or tailored weapons that go after civilian targets or even individuals. It could raise the risks of accidents and algorithmic bias problems that lead to the wrong results, such as what has played out in driverless car firms, killing at least three people on our streets already. It could lead to overconfidence or miscalculation that raises the risks of war, such as how misunderstanding on whether new technologies would help or hinder the offense led the European Powers to each try to mobilize first during a crisis, fueling the start of World War I. And, of course, there is the longterm/science fiction fear of AI somehow getting out of control.

As with nuclear weapons, arms control of AI/robotics could happen via formal treaties, norms that steer behavior, and/or "epistemic communities" that shape understanding.

Currently, the U.S. government has pushed two tracks in effect on arms control related to AI. One is creating its own guidelines and principles for use by the U.S. military. The other is efforts at the UN and by the State Department at global conferences to try to shape emerging international discussion on the topic. For example, the State Department sought to urge nations to keep humans in the loop of any nuclear weapons related use at a recent international conference in the Netherlands.

The challenge for these laudable efforts at the international level are threefold 1) Other nations like Russia and China might not agree or even respect such agreements and principles, even if they sign them, seeking to use such limits as a way to advance their own relative strengths in the AI field and military use 2) Most of our principles/efforts give us leeway to step around them in some manner if need be, and thus other nations might see our stance as more rhetorical than firm, ironclad commitments. 3) Our efforts are not in full alignment with even our closest allies. As an example, the U.S. military has five principles for the future use of AI and the British government has five principles . . . But they are not the same five. [See page 11.]

○