[H.A.S.C. No. 117–71]

DEFENSE INTELLIGENCE POSTURE TO SUPPORT THE WARFIGHTERS AND POLICY MAKERS

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

HEARING HELD
MARCH 17, 2022

U.S. GOVERNMENT PUBLISHING OFFICE
48–627 WASHINGTON : 2023

SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

RUBEN GALLEGO, Arizona, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
WILLIAM R. KEATING, Massachusetts
FILEMON VELA, Texas
MIKIE SHERRILL, New Jersey
JIMMY PANETTA, California
STEPHANIE N. MURPHY, Florida, *Vice Chair*

TRENT KELLY, Mississippi
DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia
SAM GRAVES, Missouri
DON BACON, Nebraska
LIZ CHENEY, Wyoming
C. SCOTT FRANKLIN, Florida

Shannon Green, *Professional Staff Member*
Patrick Nevins, *Professional Staff Member*
Will Braden, *Clerk*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

Prepared Statements:

Documents Submitted for the Record:

[There were no Documents submitted.]

Witness Responses to Questions Asked During the Hearing:

[There were no Questions submitted during the hearing.]

Questions Submitted by Members Post Hearing:

DEFENSE INTELLIGENCE POSTURE TO SUPPORT THE WARFIGHTERS AND POLICY MAKERS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS,
Washington, DC, Thursday, March 17, 2022.

The subcommittee met, pursuant to call, at 4:33 p.m., in room 2118, Rayburn House Office Building, Hon. Ruben Gallego (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. RUBEN GALLEGO, A REPRESENTATIVE FROM ARIZONA, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

Mr. GALLEGO. Good afternoon. I call to order the hearing of the Intelligence and Special Operations Subcommittee of the House Armed Services Committee. I need to do some formalities first.

Members who are joining remotely must be visible on screen for the purposes of identity verification, to establish and maintain a quorum, participating in the proceeding and voting. Those members must continue to use the software platform's video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera.

If a member experiences technical difficulties, they should contact committee staff for assistance. Video of members' participation will be broadcast in the room and via the television and internet feeds. Members participating remotely must seek recognition verbally and they are asked to mute their microphones when they are not speaking. Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding.

Members may leave and rejoin the proceeding. If members depart for a short while for reasons other than joining a different proceeding, they should leave their video function on. If members will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely and then rejoin it if they return. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I have designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceedings.

Thank you.

I would like now to welcome today's witnesses. Mr. Ronald Moultrie, Under Secretary of Defense for Intelligence and Security; General Paul Nakasone, Director of the National Security Agency, Chief of the Central Security Service, and Commander of USCYBERCOM [U.S. Cyber Command]; and Lieutenant General Scott Berrier, Director of the Defense Intelligence Agency.

I am pleased to see each of you today. This hearing takes place during a very perilous time. Russia's invasion of Ukraine just shows how crucial it is to maintain strong democratic alliances and partnerships. It also reinforces the importance of the work being done by the defense intelligence enterprise from exposing Russia's destructive disinformation to working with our allies and partners to share critical intelligence and ensuring our intelligence apparatus is agile so we can respond to the needs of each combatant commander.

Russia's unprovoked assault on Ukraine's sovereignty threatens the world order and presents a dangerous level of aggression. As the situation in Europe unfolds, I am also concerned about China's threatening posture toward Taiwan, the threats we face from Iran and its proxies, and North Korea's persistent testing of ballistic missiles.

We also continue to face threats from extremist groups who would, given the opportunity, strike us on our own homeland. We can only effectively combat these challenges with close collaboration with allies and partners, especially through our intelligence partnerships.

I am interested in hearing today how the defense intelligence enterprise is implementing reforms that this subcommittee [included in] the FY22 NDAA [fiscal year 2022 National Defense Authorization Act] to ensure that we are better postured to quickly provide releasable intelligence to combatant commanders to combat malign disinformation and support DOD [Department of Defense] messaging and influence operations.

In the interest of time, I ask the witnesses to keep their opening remarks brief so that we will have more time for the closed session.

With that, I will now turn this over to Ranking Member Kelly for any opening remarks. In the meantime, I will try to get——

[The prepared statement of Mr. Gallego can be found in the Appendix on page 19.]

STATEMENT OF HON. TRENT KELLY, A REPRESENTATIVE FROM MISSISSIPPI, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

Mr. KELLY. In the interest of brevity, first of all, Lieutenant General Berrier, General Nakasone, Mr. Moultrie, Secretary Moultrie, I thank you all for being here. Thank you for what you do for America every day.

This is one of the most important posture hearings that I think that we have. I won't have a lot to say in the open session. I think the things we need to say are not for political purpose or those things.

I look forward to the closed session when you guys can tell us what you need to do the things that America needs you to do, and thank you and all the men and women who serve under you for their service.

Mr. GALLEGO. Thank you, Ranking Member Kelly. We will now hear from our witnesses and then move to question and answer session. Immediately following one round of questions, we will reconvene for the classified session which will take place in Rayburn 2212.

I will recognize Mr. Moultrie.

STATEMENT OF RONALD S. MOULTRIE, UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY, U.S. DEPARTMENT OF DEFENSE

Mr. MOULTRIE. Thank you, Chairman Gallego, Ranking Member Kelly, and distinguished members of the subcommittee. It is a privilege to testify on the current posture of the defense intelligence and security enterprise in addressing the threats facing the United States of America, its allies, and partners.

The Department of Defense's intelligence and security professionals work every day to address the current and future threats facing our Nation. On behalf—on their behalf, I wish to thank the members of this subcommittee for your continued support and partnership.

I am joined in my testimony today by General Nakasone and General Berrier. They will provide you a more comprehensive picture of how we support our warfighters as well as characterize the challenges we all face.

The Department of Defense trusts the intelligence community to respond to the threats that we will all hear about.

General Berrier.

[The prepared statement of Mr. Moultrie can be found in the Appendix on page 20.]

General BERRIER. Chairman Gallego, Ranking Member Kelly, distinguished members, I do have a statement here and I can forgo the statement if you would like to get to questions.

[The prepared statement of General Berrier can be found in the Appendix on page 25.]

Mr. GALLEGO. General, we will skip to questions.

General NAKASONE. Chairman, I will forgo my statement as well.

[General Nakasone did not submit a separate prepared statement for the record.]

Mr. GALLEGO. Great. Thank you. Appreciate [inaudible] all of our witnesses.

Thank you, and this is to all of our witnesses. I am interested in hearing about progress made to implement the FY22 reforms to better support combatant commanders' need for releasable intelligence. Given the situation in Ukraine, I will ask two sets of questions.

First, could you share specific examples of intelligence sharing to combat disinformation such as exposing Russia's false flags and intelligence sharing that could literally save lives?

Second, I would like to learn more about our intelligence sharing with Ukraine. Are we able to share intelligence in real time or near real time with Ukrainians and are they able to communicate with the U.S. and what do those communication channels look like?

If you can answer as much as possible now, we can also follow up in greater detail in the classified session.

Mr. MOULTRIE. Yes, Chairman Gallego, I would prefer to answer questions on the intelligence that we are sharing in terms of false flag and what we are doing in terms of near real time intelligence in closed session.

I would say that the intelligence that we are sharing and the work that we are doing to support the Ukrainian Government is making a difference. It is accurate, it is timely, and it is actionable. And so we think that we are supporting them in such a way that they are pleased with what we are providing. And I will forgo the rest of my comments until we get into closed session, sir.

General NAKASONE. Mr. Chairman, if I might—I will defer the specifics to closed session, but I think when we consider what the intelligence community writ large and our defense intelligence establishment has been able to do here, I would characterize it like this. Our ability to share intelligence is for a number of different consumers. First of all, the sharing of intelligence to build a coalition. Secondly, the sharing of intelligence to ensure that we shine a light on disinformation operations which you referred to before. And the third piece is how do we share information that is relevant, that is actionable, that is able to be utilized by the Ukrainians? All three of those areas I would tell you, I have never seen it better in the 35 years that I have spent in uniform.

General BERRIER. Chairman, I would say where we are at is—it is revolutionary in terms of what we have been able to do and I can provide great detail in terms of the how and what we are sharing in the closed session.

Mr. GALLEGO. Thank you. General Berrier, how is DIA [Defense Intelligence Agency], as the functional manager for open source intelligence for DOD, ensuring efforts are synchronized and coordinated to avoid duplicative data purchases?

General BERRIER. Chairman, the Open Source Intelligence Center assigned to DIA is working that very, very hard with the intelligence community. As you probably know, the CIA [Central Intelligence Agency] is the community manager for open source. DIA has been designated as the defense intelligence enterprise open source functional manager. We are taking that role on now and we are devising our way through really how we organize ourselves for the sharing of the information, the tools that we will use, the training in the tradecraft. And a big part of this is making sure that across the defense intelligence enterprise we are not getting ripped off for the data that we are purchasing, and putting a structure in place to allow us to understand what that data is, catalog it, and be able to understand who is paying for what.

Mr. GALLEGO. Thank you. General Nakasone, as you know, the NDAA [National Defense Authorization Act] requires that certain conditions be met prior to ending the dual hat of the commander of U.S. Cyber Command also serving as the director of NSA [National Security Agency]. There seems to be a natural partnership between the organizations, but I want to get your view on the future of the dual hat relationship. Is it realistic to expect either organization to operate independently?

General NAKASONE. So Chairman, if I might, I am approaching 4 years in the job and so I will reflect on my experiences. At the end of the day, this is a policy decision that obviously will be made by others. But my best military advice, as it was when I first came to the job and after 3-plus years in it, is the fact that through elections, through problems with Iran, through ransomware, and now with Russia/Ukraine, what the dual hat has allowed us to do is been able to take and be able to focus efforts from the National Security Agency and U.S. Cyber Command on very, very difficult problems—influence, ransomware, strategic competition—in one domain in cyberspace. We both operate there and being able to have action, being able to [have a] unity effort, and being able to have agility is what the dual hat has been able to allow me to do over the past 3-plus years.

Mr. GALLEGO. Sounds like a pretty good endorsement for me.

Ranking Member Kelly.

Mr. KELLY. Just really quick and Chairman Gallego asked this question, so it is more of a comment because you answered the question, General Berrier and General Nakasone, but open source is really important. Sometimes we just don't want to disclose how we know stuff and if it is open source, then we don't have to. A lot of times if it comes from the U.S. Government people tend to doubt it, but if it is from some other source other than the U.S. Government, it adds more credibility to it. And there are a lot of open source, and I have talked to several of those these weeks.

What I would like for you guys to do is what ways can—rather than contracting with a company to do certain things, can we not buy what we need when we need it? I.e., if we [inaudible] right now, are there satellite companies that can tell us, you know, how many bushels of corn are in Ukraine? Can they tell us the refugee flow? Can they do a lot of other things that we don't have to do, especially with some of the false flag information that Russia has been putting out? Can we go to those and say hey, we want to buy this information and have them put it out?

General BERRIER. Ranking Member Kelly, that is a great question and as we try to organize ourselves within the defense intelligence enterprise side of this, I think those are the questions we need to ask ourselves and pursue those strategies to be smarter, better, faster as we do this.

Mr. KELLY. Because I see open source, a lot of times it just adds credibility then rather than the other. And I guess the second question is I would have said in my opening comments that I had some, what extent are we able to collect meaningful intelligence over the horizon in Afghanistan? And also, are there open source things that can help us with that information that we can also use?

General BERRIER. Ranking Member, I would prefer to discuss the over-the-horizon mission in a closed session and there are open sources that we can use to help us in Afghanistan.

Mr. KELLY. And then the final question, just a general sense, we will discuss this more in the closed hearing, but overall, just for the public to see that they have to know we are going to closed session to talk about all of the important things. Overall, what does our budget look like or what does that look like? What is your request going to look like and what things, in a general sense, can you talk about here?

Mr. MOULTRIE. Yes, Ranking Member Kelly. Our budget, I think, is going to reflect the President's priorities. It will really focus on how we are focusing the enterprise on integrated deterrence; how we are still campaigning against our pacing challenges, China; and also how we are trying to build what I would call decisive information advantage to ensure that our policy makers, as well as our warfighters, have the information that they need to do the mission that is required of them every day, sir.

General NAKASONE. And Ranking Member, I would add to that, for us at the National Security Agency, as we look at it, we look at a budget that is going to be able to support us in competition, be able to support us in crisis, be able to support us in conflict because as a global power, we will be in many, many different phases of this throughout the next and many years to come.

Mr. KELLY. I yield back.

Mr. GALLEGO. Thank you, Ranking Member. Representative Scott is next.

Mr. SCOTT. I am sorry. I assumed it would go back to a Democrat. I do want to tell you I personally believe the intelligence back in December was the best collection job that I have seen in my 10 years in Congress with regard to Russia's plans for the Ukraine. And I do think and I know it was a big decision to declassify and to share it with the world. I do think that the world has benefitted from the declassifying and the sharing of that information so that they were prepared for—at least they expected it, maybe if we weren't prepared for it.

Under Secretary Moultrie, I have asked our different commanders for the various areas of responsibility to look at what a 5 percent and a 10 percent reduction in the global food supply means for the geopolitical stability around the world. I want to point out to you particularly that the Ukraine is responsible for putting 50 million metric tons of corn and wheat into the export markets. They are the largest supplier of food to the World Food Program.

If you look at what is happening in—there is tremendous civil unrest in Sri Lanka today which is 4,000 miles away from the Ukraine. I do think that the Defense Intelligence Agency needs to do an analysis of what a 5 percent and a 10 percent reduction in the global food supply looks like in the different areas of responsibility.

Russia is saying they are not going to export. They are the second-largest exporter of wheat in the world, if I am not mistaken, behind Ukraine. And you look at the whole Black Sea trade area, the food supply that comes through that area is effectively shut down. Belarus and Russia are the number two and number three potash suppliers which [is a] fertilizer for the world's crops.

And I kind of feel like Vladimir Putin has started World War III with regard to the global food supply and the geopolitical unrest that is going to come from that. And certainly, much respect for President Zelensky and the Ukrainian people for the fight they are putting up and I hope they keep fighting and I hope we keep giving them all of the intel they need and weapons that they would need to put up that good fight. But I am very worried about what this means for other areas of the world as well.

So we will be looking for that information from you as time pushes forward, but I do think that the U.N. [United Nations] is expecting tremendous political instability because of the food supply.

With that, I will save the remainder of my questions for a closed door, but I look forward to seeing that.

Mr. GALLEGO. Thank you, Representative Scott.

Representative Bacon.

Mr. BACON. Thank you. I did have some questions, too, on maybe the cost of sharing all this intelligence, but we will wait for the next closed thing.

But I do have a couple of questions for General Nakasone. I have a cyber defense bill that directs the Federal Government to do more to help defend private industry and our infrastructure. It passed out of committee unanimously. I know we have things like CISA [Cybersecurity and Infrastructure Security Agency]. We have got the FERC [Federal Energy Regulatory Commission]. But is there a bigger role for Cyber Command and NSA to help out in our private sector? The reason I say that, we had JBS attacked. We had the Colonial Pipeline attacked. And these folks can't go up against the intelligence services of Russia. They need your expertise. But your thoughts, sir?

General NAKASONE. So in terms of our role at the National Security Agency, I think, Congressman, you are well aware that one of our two missions is cybersecurity. Our focus has been outside of the United States foreign intelligence and being able to bring the insights of what cyber adversaries are doing outside of our country to be able to inform what is going on in the inside of our country. We have a responsibility as part of the defense industrial base to ensure the protection of that.

As you are well aware, 16 different sectors in our critical infrastructure, that is the one DOD is focused on. But for us, in general, I think the secret sauce that we bring at NSA is clearly what our adversaries are doing outside of the country and then being able to share it more broadly with obviously the interagency and the private sector.

Mr. BACON. Am I really down to 33 seconds?

Mr. GALLEGO. No. Go. Sorry about that.

Mr. BACON. Something happened here. That was the fastest 5 minutes I ever came across.

I would like to bring up another thing that was a big issue and I got elected in 2016 and swore the oath in 2017. There was a push to separate Cyber Command and NSA, make two different four-star headquarters. I always opposed it because being an old ISR [intelligence, surveillance, and reconnaissance] Air Force guy, I know how important NSA is to the Cyber Command mission. They are very much integrated. And if you had two four-stars going different directions, you'd have a dysfunctional situation. So is that discussion pretty much off the table now? Because I think—I like the way it is set up now.

General NAKASONE. So again, Congressman, that is really a discussion on the policy level that does come up at times. And I know that I have answered questions before a number of committees on that, but again, that is still something that is being considered.

Mr. BACON. Well, for what it is worth, I will oppose it and I hope the Congress does. You need unified direction and I think your leadership of both of those organizations provide that unified direction.

So, maybe I should have asked Mr. Moultrie that question, but sir, do you have any comments?

Mr. MOULTRIE. Yes, sir. I would say that from a Department of Defense perspective, we certainly recognize the value of the dual hat role that General Nakasone has played for the last 4 years and the role of Cyber Command and NSA over the last 12 years plus.

I believe that the dual hat will be looked at again, just by this administration just to ensure that we understand what the value-added is, but also what the impacts are. So that discussion is still ongoing within the Department today. We understand that there is sentiment on both sides to really not do any harm, but I believe that it will be looked at. I think it will be an objective look and we will make sure we brief that out to you, sir.

Mr. BACON. If I may just elaborate a little more. I mean, these cyber teams, the core of them are NSA folks. So if you have two four-stars with different visions and different direction, I don't see how you keep a unified direction for the cyber team? But that is just my 2 cents of being down at the O–5, O–6, O–7 level when I was in.

One last question is for General Berrier and General Nakasone. I flew the RC–135s, traditional ISR aircraft. There is a push among some to go to all fifth-gen [generation] type of collection capabilities, penetrating ISR? But we know day in and day out, we do not penetrate China's air space and we don't penetrate Russia's air space, right? So we still need some of that traditional ISR because that is what is the bulk of our collection.

So I guess my question is, are we keeping the right balance between the traditional ISR and penetrating ISR and do you see a need to maintain some of these older platforms?

General BERRIER. Congressman, with my Army hat on coming out of the G–2 job, there is this balance between ISR in competition and ISR in conflict. And certainly, as we are seeing this play out inside Ukraine, we would never fly those platforms into an envelope where they could get shot down or engaged. But certainly in competition, I think there is value for ISR platforms that can collect on the periphery and actually analyze and process that information.

General NAKASONE. Congressman, I would offer as the SIGINT [signals intelligence] functional manager for the defense intelligence establishment here, we need to have a variety of platforms, whether or not they are from space, whether or not they are airborne, whether or not they are terrestrial. All of these obviously stitched together for a very, very complex and very, very important look on what our adversaries are doing in many parts of the world.

So, I know the Chief of Staff of the Air Force is looking at a number of different platforms, but you know, from my perspective, having a wide variety of these platforms is really important for us to do our mission.

Mr. BACON. So you still keep a high priority for the RC–135?

Mr. GALLEGO. Mr. Bacon.

General NAKASONE. So I thank you Congressman——

Mr. BACON. It said a minute left.

Mr. GALLEGO. I rolled over from your last one. Thank you. We can take that in the briefing.

Representative Murphy.

Mrs. MURPHY. Thank you, Mr. Chairman, and thank you to the witnesses for being here today with us.

You know, one of the areas that I have been particularly interested in during my time in Congress is the use of deep fakes. We see them used here domestically, but also by our adversaries overseas. I secured some—I've requested—sorry, I secured some report language in the FY20 Intel Authorization Act on just getting a sense of how our adversaries have weaponized these deep fakes as a tool to shape the information environment.

And in fact, even recently, I saw that the Russians produced a deep-fake video of President Zelensky urging Ukrainians to stop fighting and that was broadcast on Ukrainian television yesterday. So we are seeing the use of it and the deployment of it quite broadly.

And so my question for you, General Nakasone, is how have you seen in your time that technology evolve? Where do you think it is headed? And then do you feel like our intelligence community is prepared or how are you preparing for the evolution of that threat?

General NAKASONE. So Congresswoman, I think you identified one of those key areas that I have seen over the past 3 years in this job which is the growth of influence operations by our adversaries. Deep fakes are the ability to use video and in some form or fashion that is intended to send a message is one of those ways.

So how are we doing it? At the National Security Agency, we are working very, very closely with our Research Directorate to understand the anomalies, understand the technology, understanding the key pieces of what we can determine what is real and what is fake.

But the other point really is that it goes to Ranking Member Kelly's point which is this is also an area where we are partnering very, very closely with the private sector that has done some very, very leading work that we have been able to obviously have discussions with them on that. So this is an area that we continue to watch very, very carefully, act very, very rapidly in, and I think we will have a number of different areas that we probably can discuss in closed session as well.

Mrs. MURPHY. Thank you, General. And Mr. Moultrie, I am a polyglot myself and I know that when I was in the private sector I often read open source information in language to get a full sense of what is going on and get the context of what is going on in a country or in a conflict.

I was wondering, you know, language, foreign language skills are clearly a tool that is important to the defense intelligence community and it is going to be increasingly, I think, an important part, especially as we look at great power competition. And so we are not just talking about Mandarin, but we are also talking about Tagalog, Indonesian, you know, other languages like that. It will be necessary for us to have it to be able to work with our partners, as well as to understand our adversaries.

I was wondering, you know, do you consider the defense intelligence enterprise's existing foreign language capabilities to be sufficient for today's great power competition? And if not, what are some areas in which we need to invest more? How do we get more analysts and operators who are proficient in foreign language?

Mr. MOULTRIE. Yes, Congresswoman, in terms of language, it is one of the more important things that we do and I will talk more about it—I would like to talk more about it in closed session.

When we look at the capabilities that we talk about here, regardless of the domain that we are talking about, whether it be space, whether it be ground, whether it be ISR, or whether it be cyber, our language capabilities are just absolutely essential.

So we actually are looking at it and as you said, the various languages, the competition languages, whether it be Mandarin or Russian or other languages that we are concerned about, regional languages such as Farsi or Urdu or Pashtu, those languages are all extremely important to us. There are some things that we are doing that are underway right now to help us not only gauge what we will need today, but what we will also need for the future. I would like to talk about that in more depth in closed session. Thank you.

Mrs. MURPHY. Thank you and I yield back.

Mr. GALLEGO. Thank you, Representative Murphy.

Representative Larsen.

Mr. LARSEN. Thank you, Mr. Chair. Maybe this can be answered in this session, this question. I understand the sensitivity around all the other things certainly.

But Secretary Moultrie, your office plays a critical role in the defense intelligence enterprise. Understanding the growth in your office in recent years, the GAO [Government Accountability Office] did a report last year in May citing several challenges with the oversight including governance bodies not operating as intended and so on. You know all of the issues.

Can you discuss a little bit what is being done to address those challenges that GAO identified and provide more active—to provide more active and effective oversight of the defense intelligence enterprise?

Mr. MOULTRIE. Yes, Congressman Larsen. The GAO report that you referenced, sir, from May of 2021 was something that we took to heart. We've looked at it and we've decided that we need to move out, we need to move out aggressively on it.

So what we are doing are four things, sir. We are looking at the roles, responsibilities, and functions in our organization, ensuring that we understand clearly what those components are.

And then we are trying, number two, to match what our people are actually doing to the roles that they should be doing to ensure that they are doing what we need to do to measure what is occurring within the defense intelligence and security enterprise, I'll add.

Thirdly, metrics. We need to make sure that we have metrics to see if we are adding value in terms of our oversight and governance role.

And then lastly, the people piece of this. Just ensuring that we have the right skill level, that we have the right backgrounds and focus on this are something that we are doing. We are being assisted in this by some independent analysis being done by IDA [Institute for Defense Analyses], independent analysis coming out of

Princeton. And we hope to have something back to you and to this committee in full by the fall of this year, sir.

Mr. LARSEN. That is great. Thanks. Related to Representative Murphy's questions about the kind of folks that you need, you mentioned language and maybe you have to answer in closed session, but in terms of subject matter or certain expertise, maybe on the technical side, what kind of work do you need to do to recruit folks into that part of the enterprise?

Mr. MOULTRIE. Congressman, the skill sets that our individuals need on the language side and analytic side run the gamut from being able to understand military operations, being able to understand economic issues, being able to understand diplomatic issues.

And so you can imagine that everything that we talk about, whether it be in our government and how we are moving economically, how we are looking at research, we have to understand that in some 100-plus languages around the world. And we have to understand that to the extent that our adversaries may talk about it. It is a daunting challenge and finding those skills, it is something that we have to compete for. So that is something that we are focused on. I will talk about that more in closed session, but it is a top priority of the intelligence community's and the defense intelligence enterprise's and we are working that jointly across not just the defense intelligence enterprise, but across the IC [intelligence community] and the interagency.

Mr. LARSEN. Okay, thanks. And finally, perhaps for General Nakasone, some of us—certainly I have been tracking the—strategic support forces in the Chinese PLA [People's Liberation Army] where cyber warfare as well as EW [electronic warfare] rests, and so on. Maybe this is an answer for the next session, but since it is being reorganized, kind of really stood up over the last several years, but really more traction over the last couple of years, whether or not you have seen an increased sophistication as opposed to just an increased investment from the PLA?

General NAKASONE. So Congressman, as you can well imagine, we track this very carefully and very closely. I would like to take this up in closed session just to talk about scope and scale [of] sophistication in what we are seeing, because I do think it probably can answer your question more fully.

Mr. LARSEN. That is great. Thank you. I yield back.

Mr. GALLEGO. Thank you. Representative Panetta.

Mr. PANETTA. Thank you, Mr. Chairman. Gentlemen, thank you for being here today.

Pivoting off or pivoting on to languages, Mr. Moultrie, can you explain what role the Defense Language Institute plays in some of this training that you talked about, please?

Mr. MOULTRIE. Well, Congressman, as a graduate of the Defense Language Institute some 40-plus years ago, and my wife is also a graduate—both Russian linguists, I might add—I can tell you it plays a critical role and so we see it more so today than we ever have, if you will.

When you look at what is going on in the Ukraine, having those individuals—you know, one of the challenges that we have, we appear to have, is focusing on the problem of today and not focusing on the problem that we might have tomorrow.

So the Defense Language Institute Foreign Language Center has played a key role. It is a place that I have tried to visit every year. I am planning to go out there again this year. They are that training ground for defense intelligence and security where we get the nation's best, most trained language.

And I am proud to say, as, you know, a person that has gone back there frequently, it is light years ahead of where it was when I was there. Individuals were doing in 12 weeks what I was doing in 36 weeks. It plays a key role and we want to make sure we are supporting it and we are going to do that across the enterprise, not just within the defense intelligence enterprise, but also personnel readiness and both with the National Security Agency, the Defense Intelligence Agency, and others in the Department of Defense.

Mr. PANETTA. Outstanding. And did I mention it is in my congressional district?

Mr. MOULTRIE. I know that, sir. Absolutely.

Mr. PANETTA. And thank you and I look forward to hosting you out there. If you do come out there, please let me know. I would be happy to host you as well.

Mr. MOULTRIE. Will do, sir.

Mr. PANETTA. Thank you. General Nakasone, just quickly, it seems that information operations sub-components appear to be fractured across the defense apparatus. And despite the forthcoming doctrine for operations in the information environment, there doesn't seem to be a jointly recognized idea on what information operations should prioritize.

Do you believe that establishing a sub-unified combatant command for information operations within USCYBERCOM could allow for joint information operations training and execution?

General NAKASONE. So Congressman, I am not sure it is a fit or a solution that is built to a sub-unified command. Here is what I do believe. We use information operations in every cyber mission that we do. It is that important to what is going on to be able to communicate a message to an adversary.

What I would say is we need more information operations-trained personnel that come to our command. That is one of the areas that I am working very, very closely with the services. I know my own service and other services have taken this on very seriously, but I think that is what we have to get to first is let's get more trained information operation specialists. Let's integrate them into our teams and instead of building a separate command, let's make sure that we understand that information operations spans an entire spectrum of what we need to do.

Mr. PANETTA. It sounds like you have a good idea. Do you have any more information on that plan as to what you can do to how you can improve training our forces to jointly employ information operations and operations in the information environment?

General NAKASONE. What I would like to do, Congressman, if I can is give you some very specific examples in closed session because I think this will clearly indicate the importance of what we are applying to it, and what the services have been providing and what we need more of.

Mr. PANETTA. Outstanding. Thank you. Gentlemen, thank you.

Mr. Chairman, I yield back.

Mr. GALLEGO. Thank you, and this concludes the open session. We will be moving directly over to 2212 for a classified session. Thank you.

[Whereupon, at 5:07 p.m., the subcommittee proceeded in closed session.]

APPENDIX

MARCH 17, 2022

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 17, 2022

Opening Statement of Hon. Ruben Gallego
Chairman, Subcommittee on Intelligence and Special Operations
Hearing on
Defense Intelligence Posture to Support the Warfighters and Policy Makers
March 17, 2022

Good afternoon. I call to order this hearing of the Intelligence and Special Operations Subcommittee of the House Armed Services Committee. I would like to welcome today's witnesses:

- Mr. Ronald Moultrie, Under Secretary of Defense for Intelligence & Security
- General Paul Nakasone, Director of the National Security Agency, Chief of the Central Security Service, & Commander of U.S. Cyber Command and
- Lieutenant General Scott Berrier, Director of the Defense Intelligence Agency.

I am pleased to see each of you today. This hearing takes place during a perilous time. Russia's invasion of Ukraine shows just how vulnerable our democratic alliances and partnerships are. It also reinforces the importance of the work being done by the defense intelligence enterprise – from exposing Russia's destructive disinformation to working with our allies and partners to share critical intelligence; and ensuring our intelligence apparatus is agile so that we can respond to the needs of each combatant commander.

Russia's violent assault on Ukraine's sovereignty threatens the world order and represents a dangerous level of aggression. As the situation in Europe unfolds, I am also concerned about China's threatening posture toward Taiwan; the threats we face from Iran and its proxies; and North Korea's persistent testing of ballistic missiles. We also continue to face threats from extremist groups who would, given the opportunity, strike us on our homeland.

We can only effectively combat these challenges with close collaboration with allies and partners, especially through our intelligence partnerships. I am interested in hearing today how the Defense Intelligence Enterprise is implementing reforms that this subcommittee included in the FY22 NDAA to ensure we are better postured to quickly provide releasable intelligence to combatant commanders to combat malign disinformation and support DOD messaging and influence operations.

In the interest of time, I ask the witnesses to keep their opening remarks brief so that we will have more time for the closed session.

With that, let me again thank our witnesses for appearing before us today. I now recognize Ranking Member Kelly for any opening remarks.

Remarks as prepared for the Honorable Ronald S. Moultrie
Under Secretary of Defense for Intelligence and Security
At the House Armed Service Committee Hearing
Subcommittee on Intelligence and Special Operations
March 17, 2022

FINAL SUBMITTED TO THE SUBCOMMITTEE

Chairman Gallego, Ranking Member Kelly, and distinguished members of the Subcommittee, it is a privilege to testify on the current posture of the Defense Intelligence and Security Enterprise in addressing the threats facing the United States of America, its allies, and partners.

The Department of Defense's intelligence and security professionals work every day to address the current and future threats facing our nation. On their behalf, I wish to thank the members of this Subcommittee for your continued support and partnership.

I am joined in my testimony today by Generals Nakasone and Berrier. They will provide you with a more comprehensive picture of how we support our warfighters as well as characterize the challenges we all face. The Department of Defense entrusts the Intelligence Community to respond to the threats you will hear about.

As the Under Secretary of Defense for Intelligence and Security, I am committed to strengthening and leveraging an integrated partnership between the Department of Defense and the Intelligence Community for the defense of our nation.

The United States is experiencing a period of rapid, profound, and dynamic change in the international landscape.

Although we have a strong national defense foundation, we know that without the much needed and continued investments in critical areas—including our intelligence and security portfolios—the Department risks eroding our competitive advantage over our rivals and adversaries.

It is our shared obligation to accelerate our Nation's advantage, act at the speed of relevance, and widen the gap between our capabilities and those of our competitors.

This is **a team effort**, and it **is** not and **cannot** be the work of any single organization.

We must work across the entire Defense Intelligence and Security Enterprise, which includes all the intelligence, counterintelligence, and security organizations within the Department of Defense.

Instead of revisiting the threat assessments provided by my colleagues, I would like to share with you how OUSD (I&S) plans to move forward.

Through our four "Big Plays," we will optimize our efforts, deliver meaningful outcomes, and maintain our Nation's strategic advantage. These Big Plays are:

- Providing an information and decision advantage to our leaders and warfighters;
- Operationalizing our partnerships within the Department, the interagency, and our allies and partners;
- Elevating security awareness and counterintelligence across the Department; and,
- Identifying, recruiting, training, and retaining a workforce capable of supporting the Department's I&S requirements.

We are confident that focusing our efforts in these areas will enable us to meet Secretary Austin's priorities, support our warfighters, and ensure our Nation's security.

We are also confident that the upcoming budget will reflect the requirements of the new National Defense Strategy and the National Security Strategy, and account for the resources that we need to implement these strategies.

The Department develops the Military Intelligence Program—or the MIP—with input from the Director of National Intelligence. Together, we align and synchronize national and defense intelligence capabilities, while avoiding unintentional duplication.

Last year, the President's $715 billion-dollar defense budget request included $23.3 billion for MIP. We believe that the resources requested in this year's budget will provide another opportunity to ensure our nation's strategic advantage.

Among my responsibilities is to provide oversight to the defense intelligence enterprise, including reform of existing programs and the start of new initiatives.

My focus is on supporting DoD decision makers and warfighters so they can fulfill their responsibilities.

Today, the Department is critically focused on responding to Russia's further invasion of Ukraine. During the Russian military buildup on the borders of Ukraine, the United States increased intelligence sharing with Ukraine, our NATO allies, and our key partners. The Department continues its support of a free and democratic Ukraine while minimizing the potential for further escalation.

We are ready, willing, and eager to discuss these efforts in closed session so that you can see how valuable and successful our intelligence efforts have been.

While focused on the immediate crisis, the Department must continue to lead in the 21st century information environment by adapting to:

- technological change;
- proliferation of global threats; and
- the changes in the velocity and volume of data.

We continue to shift our strategy to focus on our pacing challenge. We do so with an emphasis on performing at a speed and scale that exceeds that of our threats, while fine tuning our execution.

Consistent with the recommendations of the Government Accountability Office in its May 2021 report regarding OUSD(I&S) oversight, we are taking the following actions to clarify and update our Enterprise governance and oversight frameworks:

- Revising policy and strategic guidance to establish clear expectations for oversight;
- Codifying management roles and responsibilities to enable effective governance at the component level;
- Developing and incorporating a process to track and oversee enterprise performance and enhance accountability; and

- Establishing efficiencies in governance structures and processes to enable effective prioritization and oversight.

Beyond enhancing our governance of the DIE, we are also focused on improving our program management efforts.

For example, the Algorithmic Warfare Cross Functional Team (AWCFT, aka Project Maven) is DoD’s Artificial Intelligence/Machine Learning pathfinder for Defense Intelligence. It delivers current, state-of-the-art software and data capabilities to partnered warfighters and battlefield commanders.

Through rapid contracting and improved budgetary authorities, Project Maven worked with front line units, Services, and Combatant Commands to deliver operational capability using a field-to-learn approach. This has enabled rapid development of new capabilities at the speed of relevance to the front lines.

Recognizing Project Maven's success, the DoD has proposed transitioning the capability to NGA in FY23. This transition will amplify the reach and capacity of AI within the Defense Intelligence Enterprise, delivering a critical capability that will significantly increase our ability to operationalize GEOINT collection to meet future warfighter needs.

In these and other areas, the Department will align its defense posture with the budget, matching resource to strategy, strategy to policy, and policy to the will of the people.

The defense strategy aligns with our national priorities and creates synergy with the global efforts of our key partners and allies. At no time in recent history has this global cooperation been more important.

I wish to thank the Subcommittee for its leadership in critical national security issues, which is vital to our ongoing efforts. Thank you for the opportunity to testify today, and I look forward to your questions.

The Honorable Ronald Moultrie
Under Secretary of Defense for Intelligence and Security

Hon. Ronald Moultrie was sworn in as the Under Secretary of Defense for Intelligence and Security on June 1, 2021. In this role, he is the principal staff assistant and advisor to the Secretary of Defense for intelligence, counterintelligence, security, sensitive activities, and other intelligence related matters. Mr. Moultrie exercises authority, direction, and control on behalf of the Secretary of Defense over all intelligence and security organizations within the Department of Defense, including the National Security Agency, the Defense Intelligence Agency, the National Geospatial Intelligence Agency, the National Reconnaissance Office, the Defense Security Service and the intelligence components of the combatant commands and military services. He is also dual-hatted as the Director of Defense Intelligence in the Office of the Director of National Intelligence, and reports to the DNI in this capacity.

Mr. Moultrie was most recently the President and CEO of Oceanus Security Strategies (OSS), LLC, and served on the Biden-Harris Presidential Transition Team as a member of an Agency Review Team focused on national security. He retired from government as the National Security Agency's (NSA) Director of Operations. Moultrie also served in the Office of the Director of National Intelligence (ODNI), was a member of Central Intelligence Agency's (CIA) Senior Intelligence Service (SIS), and served as a Russian linguist and analyst in the U.S. Air Force. Moultrie served as a key Advisor to the Secretary of the Navy playing an instrumental role in the Cybersecurity Readiness Review. He subsequently led the crafting of a digital roadmap to better optimize the Department's focus on cybersecurity, data analytics and infrastructure, and emerging technologies such as AI/Machine Learning, 5 and 6G, and Quantum computing.

Moultrie earned a Masters of Science in Strategic Intelligence (MSSI), Russian studies, from the National Intelligence University, and a Bachelors of Arts, Business Management, from the University of Maryland, magna cum laude. Moultrie is the recipient of numerous awards to include a Presidential Rank Award, two Department of the Navy Distinguished Civilian Service Awards, the Director of National Intelligence's Seal Medallion, the National Intelligence Distinguished Service Medal, the National Intelligence Superior Service Medal, the CIA National Clandestine Service's Donovan Award, the National Reconnaissance Office (NRO) Gold Medal, three NSA Exceptional Civilian Service Awards, and two NSA's Meritorious Civilian Service Awards. While on active duty, Moultrie received the Defense Meritorious Service Medal and U.S. Air Force Meritorious Service Medal. Moultrie is married and lives in Maryland.

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT

ARMED SERVICES COMMITTEE

INTELLIGENCE AND SPECIAL OPERATIONS SUBCOMMITTEE

UNITED STATES HOUSE OF REPRESENTATIVES

Scott Berrier, Lieutenant General, U.S. Army

Director, Defense Intelligence Agency
2022

Information available as of 15 March 2022 was used in the preparation of this assessment.

CONTENTS

INTRODUCTION

Chairman Gallego, Ranking Member Kelly, and members of the committee, thank you for the invitation to provide the Defense Intelligence Agency's (DIA's) assessment of the global security environment and to address the threats confronting the Nation.

Strategic competition is intensifying because China, Russia, Iran, and North Korea have become more confident in the force modernization they have undertaken for years and perceive more opportunity to advance their ambitions. Both China and Russia perceive that the United States is a nation in decline as pretext for executing their ambitions globally.

The United States faces challenges from competitors who have and are developing new capabilities intended to challenge, limit, or exceed U.S. military advantage. These state and nonstate actors are selectively putting those capabilities into play globally and regionally. The threats those capabilities pose span all warfighting domains—maritime, land, air/air defense, electronic warfare (EW), cyberspace, information, and space/counterspace. They include more lethal ballistic and cruise missiles, growing nuclear stockpiles, modernized conventional forces, and a range of gray zone measures such as ambiguous unconventional forces, foreign proxies, information manipulation, cyberattacks, and economic coercion. Such gray zone measures are below traditional combat thresholds and often afford plausible deniability, but they enable actors to wage campaigns of aggression.

Today, strategic competitors and other challengers are advancing beyond gray zone measures and exerting increasing military pressure on neighboring states. Russia has invaded Ukraine, China is threatening Taiwan, and Iran—through its proxies—threatens neighbors in the Middle East and U.S. forces, while enriching uranium to new levels. North Korea continues to threaten South Korea, Japan, and the United States with nuclear-capable ballistic missiles of increased range and lethality. The threat from terrorist organizations will persist.

The security landscape in Afghanistan has changed. The United States faces a variety of security challenges in South Asia following the Taliban takeover of Afghanistan as regional dynamics shift. Since the withdrawal of U.S. forces in Afghanistan, countries like China, Russia, and Iran are working to damage U.S. credibility internationally and engage with the Taliban to pursue or develop outcomes favorable to their interests and ambitions.

Rapidly evolving technology, advances in special materials, high-performance computing, robotics, artificial intelligence (AI), and biotechnology will augment our adversaries' military capabilities, and pose additional challenges. China and Russia, in particular, are pressing ahead with advances in space and counterspace capabilities and using cyberspace to increase their operational reach into U.S. infrastructure. They continue to exploit the COVID-19 environment and conduct information warfare to undermine Western governments and compel economic and political outcomes in their favor.

Globally, terrorist groups have experienced significant losses; however, terrorism threats persist. COVID-19 will continue to threaten world health and stability and climate change will increasingly alter our operating environment. We must remain vigilant to protect our interests and those of our allies.

DIA officers fulfill the critical mission of providing strategic, operational, and tactical Defense Intelligence to our warfighters, defense planners, policymakers, and the acquisition community. The foundational intelligence that DIA, our colleagues across the Defense Intelligence Enterprise, and our allies and foreign partners provide on foreign military capabilities helps to translate national policy into executable military action and to inform the joint force.

I am privileged to lead DIA. My hope in this hearing is to help Congress and the Nation better understand the challenges we face and to support this committee in identifying opportunities to respond to these challenges. Thank you for your continued confidence. Your support is vital to DIA.

CHINA

China remains our pacing security challenge and has long viewed the United States as a strategic competitor. China is capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system. In a 2017 speech to the Chinese Communist Party (CCP) Congress, President Xi Jinping laid out two People's Liberation Army (PLA) modernization goals: to complete PLA modernization by 2035 and to transform the PLA into a military on par with the United States military by 2049. The PLA has already fielded sophisticated weapons and platforms in every warfare domain, instituted major organizational reforms to enhance joint operations, and improved its combat readiness, making it a credible peer competitor to the United States, its allies, and partners. These developments, along with future capabilities, are designed to provide options for China to dissuade, deter, or, if ordered, defeat U.S. and allied intervention during a large-scale, theater campaign such as a war over Taiwan. The PLA can conduct long-range precision strikes across domains, is demonstrating more sophisticated counterspace capabilities, and is accelerating the large-scale expansion of the PLA's nuclear forces. The accrual of China's national power, including military power, sets the conditions for Beijing to fully assert its preferences on a global scale. Its national strategy to achieve a broad range of developmental goals to establish China as a great power by 2049 is closely integrated with its ambition to make the PLA a military at least as strong as that of the United States.

In 2020, the CCP added a new milestone of 2027 for PLA modernization. This milestone is broadly understood as accelerating PLA mechanization; modernizing PLA command, control, computer, intelligence, and information systems; and expanding the PLA use of AI and other advanced technologies. These advances would give the PLA an improved ability to execute a number of military operations, including the invasion of Taiwan.

In 2022, President Xi Jinping will have an opportunity to demonstrate his consolidation of power in the CCP and set the conditions for his legacy among the CCP's most revered leaders. In late 2022, the CCP will hold its Party Congress where he will almost certainly be reappointed as General Secretary of the CCP and Chairman of the Central Military Commission for his third 5-year term. He will also almost certainly gain a third term as president of China at the spring 2023 National People's Congress because that body removed presidential term limits in 2018.

China's Military Capabilities

With a force that totals approximately 2 million personnel, the PLA is modernizing its capabilities and improving its proficiencies across all warfare domains so it can conduct a range of land, air, maritime, space, counterspace, electronic warfare, and cyber operations as a joint force. The PLA's evolving capabilities and concepts continue to strengthen its ability to fight and win regional wars against the United States, its allies, and partners, coerce Taiwan and rival claimants in territorial disputes, counter an intervention by a third party in a conflict along China's periphery, and project power globally.

The PLA Army has approximately 975,000 active-duty personnel in combat units. Last year, the Army accelerated its training and fielding of equipment from the already fast pace of recent years. The Army also strove to increase the realism of its training.

The PLA Navy is the largest navy in the world, with an overall battle force of approximately 355 ships and submarines, including more than 145 major surface combatants. The Navy largely comprises modern multirole platforms. In the near term, the Navy will have the capability to conduct long-range precision strikes against land targets from its submarine and surface combatants with land-attack cruise missiles, notably enhancing China's global power-projection capabilities. China is also enhancing its antisubmarine warfare inventory and training to protect the Navy's aircraft carriers and ballistic missile submarines.

The PLA Air Force and Navy constitute the largest aviation force in the region and the third largest in the world, with over 2,800 total aircraft (not including trainer variants or unmanned aerial vehicles (UAVs)) of which approximately 2,250 are combat aircraft (including fighters, strategic bombers, tactical bombers, and multimission tactical and attack aircraft). In October 2019, China signaled the return of the airborne leg of its nuclear triad after the Air Force publicly revealed the H-6N as its first nuclear-capable bomber with air-to-air refueling capabilities.

The PLA Rocket Force organizes, staffs, trains, equips, and operates China's strategic land-based nuclear and conventional missile forces, and its associated support forces and missile bases. The PLA is developing new intercontinental ballistic missiles (ICBMs) that will significantly improve its nuclear-capable missile forces and will require increased nuclear warhead production for multiple independently targetable reentry vehicle capabilities and general force growth. China is constructing at least three solid-propellant ICBM fields, which will cumulatively contain hundreds of new ICBM silos. The Rocket Force also continues to grow its inventory of road-mobile DF-26 intermediate-range ballistic missiles (IRBMs), which are able to conduct both conventional and nuclear precision strikes against ground targets as well as conventional strikes against naval targets. For regional strikes, the Rocket Force began to field its first operational hypersonic weapons system, the DF-17 hypersonic glide vehicle (HGV)-capable medium-range ballistic missile (MRBM).

China's Nuclear Modernization Efforts

During the next decade, China plans to modernize, diversify, and expand its nuclear forces. China is expanding the number of its land-, sea-, and air-based nuclear delivery platforms and constructing the infrastructure necessary to support this major expansion of its nuclear forces. They are supporting this expansion by increasing their capacity to produce and separate plutonium and constructing fast breeder reactors and reprocessing facilities. China likely intends to have about 1,000 deliverable warheads by the end of the decade and has probably already established a nascent nuclear triad with the development of a nuclear-capable air-launched ballistic missile and improve ground- and sea-based nuclear capabilities. The PLA intends to increase the peacetime readiness of its nuclear forces by moving to a launch-on-warning posture with an expanded silo-based force.

Other WMD

China probably has the technical expertise to weaponize chemical and biological agents and numerous conventional weapon systems that could be adapted to deliver these agents. China has consistently claimed that it has never researched, produced, or had biological weapons. However, China has engaged in potential dual-use biological activities—some of which raise concerns regarding their compliance with the Biological Weapons Convention (BWC)—and maintains sufficient biotechnology infrastructure to produce certain biological agents or toxins on a large scale. China has declared that it once operated a small offensive chemical weapons program. Although China maintains the program was dismantled, its chemical infrastructure is sufficient to research, develop, and procure some chemical agents on a large scale.

China's Approach to Taiwan

Since late 2020, the PLA has increased military pressure on Taiwan with frequent Air Force flights into Taiwan's air defense identification zone (ADIZ). The largest set of flights to date occurred on 4 October 2021; the Taiwan Defense Ministry claimed that a record 56 Chinese military aircraft, including fighter jets, antisubmarine warfare planes, and bombers crossed Taiwan's ADIZ in a single day. This year, China flew as many as 39 aircraft into Taiwan's ADIZ on 24 January 2022. Chinese officials justify these shows of force as reactions to a perceived deepening of U.S.-Taiwan cooperation.

Although China publicly advocates for peaceful unification with Taiwan, it has never renounced the use of military force. The circumstances under which China has historically indicated it would consider using force remain ambiguous and have evolved over time.

China has a range of options for military campaigns against Taiwan, from an air and maritime blockade to a full-scale amphibious invasion to seize and occupy some or all of Taiwan or its offshore islands. Beijing appears willing to defer the use of military force as long as it considers that unification with Taiwan can be negotiated and that the costs of conflict outweigh the benefits. Beijing argues that their credible threat of force is essential to maintaining the conditions for political progress on its terms and preventing Taiwan from moving toward independence. In January 2019, President Xi Jinping publicly reiterated China's longstanding refusal to renounce the use of force to resolve the Taiwan issue and staked China's position for peaceful unification under the model of "one country, two systems." In 2021, the PLA conducted joint amphibious assault exercises near Taiwan and continued to build capabilities that could contribute to a full-scale invasion.

China's Global Military Activities

Beijing wants its armed forces to take a more active role in advancing its foreign policy, highlighting the increasingly global character that Beijing ascribes to its military power. Chinese leaders have tasked the PLA to develop the capability to project power outside its borders and immediate periphery to secure China's growing overseas interests and advance its foreign policy goals. China is seeking to establish a more robust overseas logistics and basing infrastructure to allow the PLA to project and sustain military power at greater distances. Beyond its base in Djibouti, the PLA is pursuing additional military facilities to support naval, air, ground, cyber, and space power projection, including on Africa's Atlantic Ocean, Indian Ocean, Red Sea, and Mediterranean Sea coasts and other locations in the Middle East, Asia, and the Pacific.

China is the world's fifth-largest arms supplier and has sold UAVs to Saudi Arabia and the UAE, and co-produced fighter aircraft and submarines with Pakistan. The growth of China's global economic footprint, through programs like the Belt and Road Initiative (BRI), makes its interests increasingly vulnerable to domestic political transitions in countries participating in BRI, regional instability, transnational threats, natural disaster, disease, and climate threats. Some BRI projects create potential military advantages to protect China's growing interests, such as the PLA gaining access to selected foreign ports to pre-position the necessary logistics support needed to sustain naval deployments in waters as distant as the Indian Ocean, Mediterranean Sea, and Atlantic Ocean to protect its growing interests. BRI lending has slowed down significantly since its estimated peak from 2016 to 2017, in part because China has gradually shifted away from hard-infrastructure loans toward technology-focused investments.

China has increased activities and engagement in the Arctic region since gaining observer status in the Arctic Council in 2013. In January 2018, China published its first Arctic strategy that promoted a "Polar Silk Road" and declared China to be a "near-Arctic state." Later that year, China launched its second icebreaking research vessel, the *Xue Long 2,* which has since conducted both Arctic and Antarctic expeditions in 2020 and 2021 respectively.

Chinese-Russian Defense Relationship

China and Russia's strategic alignment continues to grow, as demonstrated by the recent Xi-Putin meeting ahead of the Winter Olympics. During the visit, the leaders signed a package of 15 bilateral agreements and issued a joint statement opposing a range of Western international security initiatives, including the U.S. Indo-Pacific Strategy and the Australia-U.S.-United Kingdom trilateral partnership. It further condemned NATO's "cold war mentality," and called for "non-interference in the internal affairs of other states."

This alignment has continued despite Russia's invasion of Ukraine. China is closely managing its messaging on the conflict, generally backing Russia's characterization as a conflict ultimately caused by U.S.-driven NATO expansion and disregard for Russia's security interests. However, Beijing is likely reluctant to fully back Russia in order to preserve its own economic relations with Europe and the U.S. No doubt, China is also keenly observing how the Russian campaign is conducted and how combat against determined resistance unfolds.

In step with the larger partnership, Beijing's defense relationship with Moscow has also strengthened. Throughout the COVID-19 pandemic, China and Russia maintained frequent high-level communication and stressed close strategic cooperation on global security and health issues. For 3 of the past 4 years, the PLA has participated in Russia's strategic command and staff exercise. Although China did not participate in Russia's 2021 strategic exercise, which was focused in western Russia, Beijing, for the first time, invited the Russian military to participate in a strategic campaign exercise in northwest China. China and Russia likely perceive further cooperation between the two militaries, including joint defense technology development, exercises, and other military modernization initiatives as advantageous to their respective interests. Despite continued military cooperation, China and Russia have denied any intent to enter into a formal alliance, apparently viewing the strategic effects of their current cooperation as sufficient to accomplish their goals.

China's Regional Relations

Tensions with India along the Line of Actual Control (LAC) continued in 2021, although no new significant confrontations took place. In February 2021, China asserted through its state-owned outlets that four PLA soldiers died during the June 2020 skirmish with India that also resulted in the death of 20 Indian soldiers. Despite agreements to disengage in spring 2021, both sides maintain troops along the LAC as corps commander–level negotiations have progressed slowly.

In 2021, Chinese and North Korean political and military diplomacy continued to be hampered by the COVID-19 pandemic. North Korea's forced isolation ceased almost all trade and people-to-people exchanges across the border, and the North Korean regime's paranoia about the risks of COVID-19 has prevented Chinese–North Korean diplomatic exchanges. China's objectives for the Korean Peninsula include stability, denuclearization, and the absence of U.S. forces near China's border. China's focus on maintaining stability on the Korean Peninsula involves preventing North Korea's collapse and military conflict on the peninsula.

Concerns about instability in Afghanistan probably are leading China to expand diplomatic engagement with the Taliban. On 25 October 2021, Chinese Foreign Minister Wang Yi met with senior Taliban officials in Doha, Qatar, marking the first high-level meeting between the two governments since the U.S. withdrawal from Afghanistan. Beijing cautiously proceeded with high-level meetings with the Taliban, probably to avoid the appearance of granting the Taliban de facto recognition.

China continues to pursue its maritime claims in the East and South China Seas, and in 2021, Beijing enacted a Coast Guard Law that included expansive language on jurisdiction and use-of-force authorities. The dispute between China and Japan over the Senkaku Islands and overlapping exclusive economic zone and continental shelf claims persists with no progress toward resolution. Japan remains concerned about the persistent presence of Chinese Coast Guard ships and fishing vessels in disputed East China Sea waters and rejects China's claim of sovereignty.

In the South China Sea, China claims sovereignty over the Spratly and Paracel Islands and other land features within its ambiguous self-proclaimed "dashed line." Its claims are disputed in whole or part by Brunei, the Philippines, Malaysia, and Vietnam. Beijing continues to employ the Navy, Coast Guard, and its maritime militia to patrol the region and harass the oil and gas exploration operations of rival claimants. In response to China's continued assertive actions against foreign fishing ships, Indonesia, Malaysia, the Philippines, and Vietnam publicly reject Beijing's claims and invoke international law in support of their maritime sovereign rights.

China's Defense Economics

In 2022, China announced a 7 percent increase from its 2021 annual defense budget, continuing more than 20 years of annual defense spending increases and sustaining its position as the second-largest military spender in the world. China's published military budget omits several major categories of expenditures and its actual military-related spending is higher than what it states in its official budget.

China's economic development supports its military modernization through the resources of their growing national industrial and technological base, the availability of funding for larger defense budgets, and deliberate party-led initiatives such as Made in China 2025 and China Standards 2035. In documents detailing the 14th 5-Year Plan (2021 to 2025), Chinese planners announced a shift to a new development concept they call "dual circulation." Dual circulation is focused on accelerating domestic consumption as a driver of economic growth, shifting consumption to higher-end manufacturing, and creating breakthroughs in key technologies along critical high-end global supply chains. It also places emphasis on mutually reinforcing foreign investment in key technologies to provide the capital and technology necessary to advance domestic technological innovation in support of China's security and development objectives.

China pursues its military-civil fusion (MCF) development strategy to blend its economic, social, and security development strategies to build an integrated national strategic system and capabilities to support its national rejuvenation goals. The MCF strategy includes objectives to develop and acquire advanced dual-use technology for military purposes, deepen reform of the national defense science and technology industries, and serve a broader purpose by strengthening all of China's instruments of national power.

This year, Chinese leaders will be focused on the upcoming Party Congress and almost certain continuation of Xi Jinping's leadership for a third term. In the wake of last year's 100th anniversary of the founding of the Chinese Communist Party and this year's Olympics, Beijing probably will attempt to portray China as an increasingly powerful, stable, and prosperous state, while trying to manage an increasingly complex regional and global security environment and avoid any blame for COVID-19. While holding the CCP up to the Chinese populace as the primary driver for China's success, Chinese leaders probably will continue to address a number of security priorities including the growing competition with the United States, fallout from the Russian invasion of Ukraine, pressuring Taiwan to unify with the mainland, solidifying its position in disputed regions, and increasing its ability to protect Chinese interests abroad.

RUSSIA

Russia's invasion of Ukraine clearly signals the re-emergence of a more hostile and militaristic Russia that seeks to overturn the U.S.-led rules based post-Cold War international order, expand its control over the former Soviet empire, and reclaim what it regards as its rightful position on the world stage. Russian military capabilities have been used to violate not only the sovereignty and independence of Ukraine, they pose an existential threat to U.S. national security and that of our allies. Russia's military strength allows Moscow to challenge U.S. global standing and undermine our democracy as it seeks to shape a new world order that is more favorable to its interests and consistent with its authoritarian model.

Leadership Views and Goals

Russia views the United States and NATO as the primary threats to its national security and geopolitical ambitions, and Moscow has sought to develop a modern, capable military designed to counter perceived threats and achieve its objectives in this new era of great-power competition. Russia views a powerful, survivable nuclear force as the foundation of its national security, and its modernized general purpose forces as critical to meet any conventional military threat and project Russian power abroad. At the same time, Russia continues to develop a diverse toolkit of indirect actions such as information confrontation, private military companies, and other covert actions that are designed to weaken the United States and its allies, coerce and threaten its neighbors, and influence or subvert political and diplomatic decisionmaking processes. These tactics are tailored to take advantage of Russian strengths and exploit U.S. vulnerabilities and have allowed Russia to compete effectively in international politics well above its relative power. Russia has taken on an increasingly alarmist view of NATO's presence along its borders, claiming the alliance uses operations and deployments near Russia to stage long-range strike platforms to test its defenses, and threaten a decapitating first strike. In the past year, Russia has publicly expanded its claim that NATO is encroaching on its borders, messaging that it needs security guarantees and regards any NATO presence in countries Moscow considers within its sphere of influence, such as Ukraine, to be unacceptable. Russia is now engaged in direct military action against Ukraine, employing the majority of its conventional ground forces, ground- and air-launched missile attacks, and some of its naval forces to prevent what it undoubtedly sees as a major political-military catastrophe, a Ukraine more deeply aligned with NATO.

Russian Military Capabilities

Russia is modernizing its military forces across all services. President Vladimir Putin continues to tout the development of fifth-generation fighters, state-of-the-art air and coastal defense missile systems, new surface vessels and submarines, advanced tanks, modernized artillery, and improved military command and control (C2) and logistics. Russia's modernization is intended to ensure Russia can field a military capable of engaging in the full spectrum of warfare to deter or defeat a wide scope of threats, but initial setbacks in Ukraine call some of Putin's narrative into question.

Russia continues to improve capabilities for its Ground Forces, Airborne Forces, and coastal troops. It is upgrading main battle tanks (MBTs) and introducing new MBTs, artillery, and multiple rocket launchers to its arsenal. Russia has also steadily increased its number of battalion tactical groups (BTGs)—the Ground Force's primary maneuver element. In 2021, Russia's Defense Minister claimed its force structure could generate 168 BTGs, which is a 75 percent increase from the 96 BTGs it claimed it could generate in 2016.

Russia is also in the process of restructuring its Ground Forces located near its borders with NATO countries, and it added upwards of 20 new units or divisions in the Western Military District by the end of 2021. However, reports of undermanned Russian formations in the initial days of the invasion suggest that many of these units have yet to achieve full combat capability, and given losses in Ukraine, will probably face significant problems doing so.

Russia's Aerospace Forces (VKS) have steadily modernized, adding more fourth-generation aircraft, modern strategic and tactical surface-to-air missiles (SAMs), new radars and UAVs, and increased training and pilot proficiency. Russia's VKS modernization combined with combat operations in Syria have substantially improved its capability to conduct close air support, sustainment, C4ISR, precision strike and interdiction in limited operations, but may not yet have been promulgated across the force. New and upgraded SAMs and radars have increased Russia's over-the-horizon target fidelity and its capability to identify and respond to activity approaching Russia's borders.

For Russia's general purpose forces navy, Moscow has fielded the ultra-quiet, cruise-missile carrying Severodvinsk II class SSGN *Kazan*—accepted into service in 2020—and SSGN *Novosibirsk*, which Russia's Pacific Fleet service will likely accept within the coming months to provide a new platform capable of threatening North America from the Pacific Ocean. Russia is also making significant progress fielding hypersonic weapons and announced in November, after successfully completing testing, that the Tsirkon hypersonic antiship missile would enter into service in 2022.

Russia's Nuclear Modernization Efforts

As of November 2021, Russia claims to have upgraded 86 percent of its nuclear triad and is developing several novel nuclear-capable systems designed to overcome ballistic missile defense systems and ensure that Russia can credibly inflict unacceptable damage on the West. Russia is developing new ballistic missile submarines, arming its heavy bombers with high-precision cruise missiles, and developing more capable ICBMs. Russia has also already fielded some of the novel weapons systems announced by President Putin in 2018, including an ICBM-launched hypersonic glide vehicle and an air-launched ballistic missile. A new heavy ICBM, a transoceanic torpedo, and an intercontinental cruise missile—all nuclear armed—may be fielded later this decade. Russian Long-Range Aviation has remained active and is on track to receive new Tu-160 Blackjack bombers and upgrade existing platforms to deliver advanced hypersonic and precision-strike weapons at intercontinental ranges.

Russia is also making progress in modernizing its conventional and nuclear C2 capabilities. During Russia's 2020 and 2021 annual capstone military exercises, Moscow demonstrated an improved ability to pair reconnaissance and conventional strike systems to increase lethality. Russia also advanced its use of automated C2 systems to speed command decisionmaking. In November 2020, President Putin highlighted the impending completion of a new and highly survivable command center that can withstand attacks by nuclear forces.

Nuclear Policy and Arms Control

Russia views nuclear weapons as primarily for deterrence but maintains the right to use such weapons in response to what it views as an existential threat. Russian military and deterrence doctrine consistently outlines the conditions under which Moscow would consider using nuclear weapons, which include existential threats of hypersonic missiles, weapons of mass destruction, or massed conventional strikes to the Russian homeland or its allies. In late February, following a large Russian strategic forces exercise and Russia's invasion of Ukraine, President Putin ordered his military leadership to put the deterrence forces of the Russian military on "special combat duty," a term appearing to refer to heightened preparations designed to ensure a quick transition to higher alert status should the situation call for it. Putin stated this was in response to "leading NATO nations" making aggressive statements about Russia. This order and other recent comments by Russian leaders highlighting Russia's nuclear arsenal are likely intended to intimidate. They also reflect Moscow's doctrinal views on the use of tactical, non-strategic nuclear weapons to compel an adversary into pursuing an off-ramp or negotiations that may result in termination of the conflict on terms favorable to Russia, or deter the entry of other participants when Russian offensive progress of its conventional forces looks like it might be reversed or the conflict becomes protracted.

Russia has a mixed record on arms control compliance, violating treaties it sees as overly constraining and adhering to those aligned with its strategic interests. In January 2021, Russia and the United States agreed to extend the New START Treaty, and Russia adheres to New START's central limits and verification regimes because the treaty allows Moscow to maintain relative strategic nuclear parity with the United States, constrain U.S. nuclear force growth, and avoid a more costly arms race. By contrast, Russia continues to support the SSC-8 ground-launched, theater range, nuclear-capable cruise missile program that prompted the U.S. Government to conclude Moscow was in violation of the Intermediate Range Nuclear Forces (INF) Treaty. Russia also formally withdrew from the Open Skies Treaty in December 2021. In future negotiations, Russia may attempt to use the development of systems such as the Kinzhal hypersonic, maneuvering, dual-capable, air-launched ballistic missile; the Burevestnik nuclear powered, nuclear-armed cruise missile; or counterspace weapons as leverage to gain concessions from the United States and NATO.

Russia almost certainly maintains biological and chemical weapon programs. Since 1992, Russia's BWC Confidence-Building Measure (CBM) submissions have remained incomplete and misleading. It only partially acknowledges the former Soviet Union program, maintains its secrecy efforts, and has not provided sufficient evidence that key biological and chemical weapon program activities have been dismantled. The United States is unable to certify that Russia has met its obligations for providing complete declarations of its chemical weapons production and development facilities, and its stockpile. Furthermore, the United States Government asserts that Russia is not in compliance with its obligations under the Chemical Weapons Convention (CWC) in part because of its use of a nerve agent—referred to as Novichok—in the attempted assassination of former Russian Main Intelligence Directorate (GRU) intelligence officer Sergey Skripal and his daughter in March 2018. In August 2020, Russian Federal Security Service (FSB) officers used a Novichok nerve agent to poison Russian opposition leader, Aleksey Nalvanyy.

Threats to Ukraine and the other Soviet Union Successor States

Russia is determined to restore a sphere of influence over Ukraine and the other states of the former Soviet Union which is a key driver for Russian military aggression against Ukraine. Intent on bringing Kyiv back into its orbit, Russia has launched a multi-axis, combined arms invasion of Ukraine, dedicating the vast majority of their conventional forces for seizing large swaths of Ukrainian territory and replacing the government in Kyiv. Despite greater than anticipated resistance from Ukraine and relatively high losses in the initial phases of the conflict, Moscow appears determined to press forward by using more lethal capabilities until the Ukrainian government is willing to come to terms favorable to Moscow. Stiff Ukrainian resistance is leading Russia to resort to more indiscriminate methods that are destroying cities, infrastructure, and increasing civilian deaths.

Russia's success in Ukraine, or lack thereof, probably will impact its ability to wield stronger influence over other Soviet successor states. The Kremlin likely calculates that a victory over Ukraine will compel most of the Soviet successor states to align themselves more closely with Moscow, but a military setback for Russia or a lengthy drawn-out campaign in Ukraine probably will have the opposite effect.

Regardless of the outcome in Ukraine, the Kremlin remains sensitive to what it perceives as Western regime change efforts in Belarus and continues to press Belarusian President Aleksander Lukashenko to integrate more deeply with Russia. Lukashenko's approval for Russia to use Belarus as a staging ground for Russian troops to invade Ukraine signals his willingness to concede to Russia's demands. In Central Asia, Moscow is also trying to exploit the U.S. withdrawal from Afghanistan and Central Asian concerns about a potential spillover of Afghan-based instability into the region to convince these states to expand their political-military cooperation with Russia. In January, Moscow demonstrated such cooperation and its role in the region by sending Collective Security Treaty Organization (CSTO) member troops into Kazakhstan on the request of Kazakh leadership to quell domestic protests.

Russia-China Ties

Russia continues to deepen its ties to China in an effort to curtail U.S. power and influence. Relations between Moscow and Beijing are probably their deepest since any time before the Sino-Soviet split. Both countries coordinate on high-priority geopolitical issues to maximize their power and influence while bilateral military cooperation continues to evolve—punctuated by a growing number of combined military exercises. In 2018, Moscow included the Chinese military in its largest annual exercise, VOSTOK-2018, for the first time. Since then, China has participated in two other Russian capstone exercises, conducted two combined bomber patrols over the Sea of Japan, and circumnavigated Japan together in October 2021, marking their first combined maritime patrol.

The January Xi-Putin meeting, which resulted in 15 bilateral agreements and a joint statement opposing Western international security initiatives, probably reflects Putin's intent to blunt the force of Western sanctions and strengthen the voice both countries use to espouse anti-western narratives. Moscow probably views Beijing as its most capable geopolitical partner, an alternative financial clearinghouse, and a key ally at the United Nations to undercut Western messaging and offset the harshest impact of sanctions. The extent to which China will help Russia mitigate the effects of sanctions as Russia's economy declines further is not clear. However, Putin probably views his relationship with Xi as critical to alleviating the departure of credit card companies, creating a viable alternative to SWIFT, signing further energy deals, and leveraging Chinese technology.

An Increasingly Assertive Actor Abroad

Russia continues to pursue its national security interests and geopolitical ambitions aggressively across the globe, acting from a position of increased confidence and emboldened by its perception that the United States is in a period of decline. Russia is steadily expanding its international profile, increasing its engagement with select countries in Asia, the Middle East, Africa, and Latin America and is working to diminish U.S. influence around the globe. The Kremlin is seeking to establish military bases and air and naval access agreements with states in these regions to enhance its power projection capabilities and increase its regional influence.

The Kremlin's engagement with Pyongyang centers on the preservation of regional stability and promotion of Russia's status on the peninsula. Russia has advocated for a comprehensive and negotiated settlement and opposes the use of force. Moscow agreed to UN sanctions against Pyongyang in 2017; however, Moscow sometimes skirts compliance issues because of business interests and a fear of destabilizing the North Korean regime. In addition, Russia coordinates its North Korea-related diplomacy with China, including a bilateral "Road Map" for peace, an initiative since 2017 that has aimed to reduce tensions on the Peninsula through a dual-track approach to advance denuclearization and establish a peace mechanism.

In the Middle East, Moscow continues to provide Syria with military, diplomatic, and economic support, while seeking to broker an end to the Asad regime's international isolation and lobbying for economic aid to assist in Syria's reconstruction. The Kremlin likely calculates this support along with its military presence in Syria will ensure its sway over the Asad regime, cement Moscow's status as Syria's preeminent foreign partner, and bolster Russian regional influence and power projection capability. Russia and Turkey continue to downplay their disagreements and compartmentalize their divergent foreign policy objectives in Syria and elsewhere in the region.

Russia also continues to expand its involvement in Africa, highlighted by the activities of Russian oligarch Yevgeniy Prigozhin and his Private Military Company Vagner. Vagner has conducted combat operations in the Central African Republic since 2017, Libya since 2019, and deployed to Mali in December 2021. More broadly, Russia uses arms sales, training, and bilateral defense agreements to establish lasting relationships on the continent. To enhance its power-projection capabilities and increase its regional advantage, Moscow continues to pursue military bases and air and naval access agreements in Africa, such as the planned naval logistics facility in Sudan.

In Latin America, Moscow is focused largely on strengthening military ties with its traditional partners Cuba, Nicaragua, and Venezuela, offering training, arms sales, and weapons maintenance support. Russia has also threatened to increase its military presence in the region in response to U.S. support for Ukraine. Moscow continues to support disputed Venezuelan President Nicolas Maduro with military and economic assistance, largely to protect its economic investments and thwart perceived efforts to remove President Maduro from power. Russian engagement with other Latin American governments remains minimal, but the Kremlin is open to opportunities for more extensive engagement.

Russia views the Arctic as a security and economic priority, seeking to exploit Arctic natural resources and develop the Northern Sea Route as a major international shipping lane. Russia is refurbishing Soviet-era airfields and radar installations, constructing new ports and search and rescue centers, and building up its fleet of conventionally- and nuclear-powered icebreakers. Russia is also expanding its network of air and coastal defense missile systems to strengthen its antiaccess/area-denial capabilities in the region. In May 2021, Russia assumed the two-year rotating Chairmanship of the Arctic Council, an association of the eight Arctic nations intended to preserve the Arctic as a zone of peace and constructive cooperation. Russia intends to use the platform to attract investment in its Arctic projects and defend its national interests.

Looking ahead, Russia will continue to pose a multifaceted threat to U.S. national security and its ability to lead and shape international developments while Russia's invasion of Ukraine will have immediate and long-term consequences for European security and stability.

Protracted occupation of parts of Ukrainian territory threatens to sap Russian military manpower and reduce their modernized weapons arsenal, while consequent economic sanctions will probably throw Russia into prolonged economic depression and diplomatic isolation that will threaten their ability to produce modern precision-guided munitions. As this war and its consequences slowly weaken Russian conventional strength, Russia likely will increasingly rely on its nuclear deterrent to signal the West and project strength to its internal and external audiences.

Russia's aggression in Ukraine is reviving fears of a more imperial and militaristic Russia, prompting requests from NATO allies for assurances that U.S. security guarantees will be honored. U.S. partners in the former Soviet Union will also look to the United States for signs that they are not being abandoned while adjusting their policies to coexist with a stronger and more emboldened Russia. Russian military modernization efforts will progress even as initial timelines for some programs may have to adjust to likely new economic realities, and Moscow will continue to blend traditional displays of military might with other coercive political, economic, cyber, and information confrontation measures to achieve its geopolitical interests, delineate its redlines, and compel the United States to take its concerns more seriously. Moreover, U.S. efforts to undermine Russia's goals in Ukraine, combined with its perception that the United States is a nation in decline, could prompt Russia to engage in more aggressive actions not only in Ukraine itself, but also more broadly in its perceived confrontation with the West.

IRAN

Iran is the primary state challenger to U.S. interests in the Middle East because of its increasingly sophisticated military capabilities, broad proxy and partner networks, and demonstrated willingness to use force against U.S. and partner forces. Iran's national security strategy aims to ensure the continuity of clerical rule, maintain internal stability, secure its position as a dominant regional power, and achieve economic prosperity. Tehran employs a complex set of diplomatic, military, and security capabilities, including unconventional forces that recruit and train partners and proxies to achieve its objectives and conventional forces that can impose high costs on adversaries. Tehran probably calibrates its attacks to pressure adversaries and proportionally retaliate for real or perceived transgressions against Iran, while attempting to prevent escalation to full-scale conflict. Iranian officials continue to perceive that they have not sufficiently retaliated for the 8 January 2020 death of former Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) Commander Qasem Soleimani, and probably are planning covert actions against U.S. officials to retaliate for his death while attempting to maintain plausible deniability and minimize escalation. Iran probably will continue to focus on unconventional attacks or minimally deniable actions, such as cyberoperations, rather than overt conventional retaliation to counter Western pressure.

Iranian Military Capabilities

Iran’s conventional military strategy is based on deterrence and retaliation. If deterrence fails, Iran probably would seek to demonstrate strength by striking its adversaries. Iran fields the region’s largest arsenal of UAVs and missiles and has increasingly relied on UAVS, likely because they are inexpensive, versatile, and Iran probably believes they sometimes allow for plausible deniability. Iran has emphasized improving UAV accuracy, lethality, and over-the-horizon capabilities. Iran also proliferates UAV equipment and training to proxy and partner networks, which provides Tehran a deniable means of attacking U.S. and partner interests throughout the Middle East.

Iran routinely uses its naval forces to monitor U.S. and allied naval operations off its coast—including near the Strait of Hormuz—and occasionally engages in dangerous and unprofessional interactions. Since 2019, Iran’s naval forces have become more brazen and have seized, sabotaged, and attacked merchant ships in the region—in some cases retaliating for Israeli and allied activities.

Some Iranian missiles are able to strike targets 2,000 kilometers from Iran’s borders, and it has demonstrated the willingness to use them. Iran continues to increase the accuracy and lethality of its ballistic missile force, including short-range ballistic missiles (SRBMs) with increasing range and antiship capability and MRBMs with accuracy and warhead improvements. Since at least 2016, Iran has unveiled antiship cruise missiles launched from aircraft and submarines, mobile air defense systems, and several land-attack cruise missiles that fly at low altitudes and can attack a target from multiple directions, complicating missile defense. Iran continues to develop space launch vehicles with boosters that could be capable of ICBM ranges if configured for that purpose. Tehran also aspires to build, launch, and operate satellites and has attempted to place several experimental satellites into orbit—including the successful April 2020 launch of Iran's first military reconnaissance satellite.

Iran is a party to the CWC and BWC. However, since 2018, the United States Government has found Iran to be noncompliant with its CWC obligations due to its failure to declare its transfers of CW, its complete list of Riot Control Agents (RCAs), and failure to submit a complete list of chemical weapons production facilities. The United States Government is also concerned that Iran is pursuing pharmaceutical-based agents for offensive purposes.

In 2021, Iran conducted arms sales negotiations with Russia, China, and North Korea. These negotiations probably reflect Iran's military modernization priorities—missile, naval, UAV, and air defense forces—but Tehran also may pursue more robust air power and EW capabilities based on lessons learned from recent conflicts.

Iran's Regional Military Activities

Regionally, Tehran continues to provide advisory, financial, and materiel support to partner and proxy networks in Iraq, Lebanon, Syria, and Yemen to build strategic depth, facilitate attacks against United States' and its regional partners' interests, and guarantee Iran's long-term regional influence. Tehran has leveraged its relationships to attack the continued U.S. presence in the region and is attempting to force a U.S. military drawdown. Esmail Ghani, the IRGC-QF commander, has advanced the regional lines of effort he inherited in January 2020 from his predecessor, Qasem Soleimani.

In 2021, Iran began using more aggressive measures and novel tactics—including targeting Israeli-associated commercial shipping—as part of a new strategy to counter Israel. Tehran has increasingly relied on UAVs to fulfill this strategy and has conducted or enabled at least six UAV attacks against Israeli interests in the past year. Iran also seeks to prevent Israel from normalizing its relations with Arab states, combining threats from its proxies and partners with diplomatic outreach.

In Iraq, Iran seeks to ensure that Iranian-aligned Shia militia groups maintain military and political influence. Iran has improved militia capabilities and increased their operational independence. In 2021, Iraqi militias used Iranian-provided one-way UAVs to attack U.S. targets for the first time and have modulated subsequent attacks based on political circumstances. Iran has directed temporary pauses in militia attacks to manage escalation and improve the militias' political prospects in response to Iraq's October 2021 elections. Militias conducted multiple UAV and indirect fire attacks on U.S. forces in January to increase pressure on the United States to withdraw.

In Lebanon, Tehran works with Lebanese Hizballah—its most important and capable substate partner—to project power and bolster regional Shia militants' capabilities. Iran acts as Hizballah's primary patron, and their strategic interests rarely diverge.

In Syria, Iran seeks to secure a lasting economic and military presence while deterring continued Israeli strikes on Iranian interests. During the past year, Tehran has demonstrated its willingness to target U.S. forces in Syria. Since 2019, Iranian-backed forces have conducted several rocket attacks against U.S. and coalition partners in Syria. In October 2021, Iranian forces in Syria struck U.S. forces with multiple UAVs in the most sophisticated attack against a U.S. military base in the country to date, reportedly in retaliation for an Israeli airstrike that used airspace near the At Tanf area.

In Yemen, Iran continues to support the Huthis with advisers and weapons to facilitate complex and long-range attacks against Saudi Arabia and United Arab Emirates (UAE) in order to pressure the Saudi-led coalition. In the past year, Iran supplied the Huthis with one of its most advanced one-way–attack UAVs, the Shahed-136, which provides Iran and the Huthis a long-range strike option capable of reaching Israel. In January, the Huthis attempted multiple UAV and missile attacks against the UAE, including a successful attack on 17 January which killed three, wounded six, destroyed three oil tankers, and caused a fire at the Abu Dhabi International Airport. The Huthis claimed the January attacks as retaliation for UAE-backed Yemeni forces regaining key territory in Shabwah and southern Marib governorates and threatened additional strikes, demanding the UAE end its involvement in the conflict.

Iran has continued its regional activities despite U.S. sanctions being reimposed in 2018, which has impeded Tehran's access to traditional government funding streams, including oil exports. Iran has worked to circumvent sanctions, but currency depreciation, high inflation, and unemployment continue to plague its economy. Iran's 2021 defense budget is substantially larger than its previous five defense budgets, but fiscal constraints very likely will prevent it from fully funding its planned expenditures.

Tehran Nuclear Development Efforts

Tehran also has continued to reduce its adherence to the Joint Comprehensive Plan of Action (JCPOA) to gain leverage in talks and revive the deal on terms favorable to Iran. Tehran has halted some transparency measures for its nuclear program and enriched uranium up to 20 and 60 percent, beyond the JCPOA limit of 3.67 percent. Iran also has conducted research and development with advanced centrifuges and has produced small quantities of enriched uranium metal for the first time.

During the next year, Tehran probably will respond to U.S. and partner operations in a manner it determines is similar or proportional to avoid risking unmanageable escalation. Tehran's response probably would seek to demonstrate strength, reduce Western regional influence, and reestablish deterrence following repeated attacks on Iranian interests in Iran and Syria. Such responses probably will include deniable attacks, cyberoperations, or nuclear-related actions. Iran probably will seek to avoid escalation they expect would undermine JCPOA negotiations or impede their goal of compelling a U.S. withdrawal from the region.

NORTH KOREA

North Korea remains a serious challenge for the United States and its allies. North Korea has the capability of holding U.S. and allied forces at risk with missiles capable of carrying nuclear, chemical and biological payloads and its large conventional military. North Korean leader Kim Jong Un is committed to preserving his regime and the further development of military capabilities with destructive power and expanded reach. To this end, North Korea is modernizing and expanding its missile force to more accurately target U.S. and allied interests in the Asia-Pacific region and across the continental United States. Since early 2021, North Korea has tested a new railborne missile launch capability, missiles it claims have an HGV payload, a new SRBM, a new submarine-launched ballistic missile (SLBM), and a new long-range cruise missile. Since January 2022, North Korea tested eight missile systems including an ICBM, IRBM, purported HGVs, railborne missiles, cruise missiles, and multiple types of solid-propellant SRBMs, to showcase its commitment to advancing and diversifying its missile program. Pyongyang also continues to shift to solid-propellant missiles, allowing for more rapid employment than existing liquid-propellant missiles. In January 2021, Kim Jong Un announced plans to modernize North Korea's military over the next 5 years. Specific goals included developing multiple independently targetable reentry vehicles, an HGV, solid-propellant ICBMs, reconnaissance satellites, a nuclear-powered submarine, a more powerful hydrogen bomb, and making their nuclear weapons tactical. Pyongyang also remains committed to its nuclear-weapons program. North Korean leadership likely views expanding its strategic nuclear and missile deterrents as essential to ensuring regime security and enabling coercive military threats and actions.

Since ascending to power in 2011, Kim Jong Un has solidified his rule by raising the public prominence of his regime, installing a cadre of loyal military and political advisers, and bolstering control over the North Korean population—steps that Kim probably expects will enhance his legitimacy at home and abroad and ensure long-term regime security. Kim has reinforced the approach of his father and grandfather that focuses on maintaining repressive domestic controls to shield his regime from internal threats—including crackdowns on access to outside information, intensive ideological indoctrination, and enforcement through a pervasive security apparatus to counter external influences. Personnel shuffles, purges to enact sweeping policy changes, and public speeches justifying his policies have also allowed Kim to ensure elite support and reinforce fealty to him throughout his tenure. In January 2021, the

Korean Workers' Party (KWP) elected to change Kim Jong Un's title from Chairman of the KWP to General Secretary of the party, a title also held by Kim Il Sung and Kim Jong Il.

North Korea's Military Capabilities

North Korea's military force has long been plagued by resource constraints and aging equipment and probably reduced training during the past year to prevent the spread of COVID-19. Despite these limitations, North Korea maintains a capable military of ground, air, navy, special operations, and missile forces. These forces are almost certainly postured to maintain a credible defense of its territory and execute lethal, limited objective attacks, but they are not able to support a sustained conflict or reunify the Korean Peninsula.

The Korean People's Army (KPA) Ground Forces remain the core of North Korea's military power and the primary means by which Pyongyang threatens Seoul. The KPA ground units comprise approximately 1,000,000 active-duty personnel and have thousands of long-range artillery and rocket systems arrayed along the demilitarized zone to be able to strike South Korea without warning. It is also developing more accurate multiple rocket launchers with ranges extending to South Korean and U.S. bases farther south on the peninsula.

North Korea's Air and Air Defense Forces consist of more than 900 combat aircraft and can fly strike missions against targets in South Korea with fighters, bombers, and possibly UAVs. It is developing or procuring a variety of UAVs, some of which have been used for reconnaissance missions over South Korea and could be equipped with rudimentary armaments. Its air defense forces maintain a dense network of integrated systems, providing overlapping, redundant territorial coverage.

The North Korean Navy is primarily a coastal defense force and is capable of conducting limited short-term offensive and defensive operations. It maintains one of the world's largest submarine forces. While most of its submarines are of older design, it launched a new ballistic missile submarine with a single launch tube in 2015, and tested a new SLBM in 2016 and another model in 2021, in an effort to build its naval deterrent.

North Korea's Strategic Force controls a wide selection of SRBMs, MRBMs, IRBMS, and ICBMs and has stated each represents a nuclear-capable class. North Korea's Strategic Force is one of the most rapidly modernizing elements of its national military, and if training and development are sustained and pursued consistently forcewide, it could become one of North Korea's most capable military arms. North Korea maintains robust chemical warfare (CW) and biological warfare (BW) capabilities. North Korea, which is not a member of the CWC, probably has a CW program with up to several thousand metric tons of CW agents and the capability to produce nerve, blister, blood, and choking agents. North Korea probably could employ CW agents by modifying a variety of conventional munitions, including artillery, rockets, and ballistic missiles as well as unconventional, targeted methods such as the use of a chemical agent in the 2017 assassination of Kim's half-brother Kim Jong Nam. North Korea has a dedicated, national-level effort to develop BW capabilities and has developed, produced, and possibly weaponized BW agents. North Korea probably has the capability to produce sufficient quantities of biological agents for military purposes upon leadership demand. Though a signatory to the BWC, North Korea has failed to provide a BWC confidence building measure report since 1990.

North Korea's economy and logistics infrastructure support national defense considerations, but the systems are poorly constructed and deteriorating. While it has made recent progress on hydroelectric power and improving power generation, North Korea continues to experience chronic electricity shortages. As a country, it possesses extensive indigenous capability for defense industrial output but uses illicit foreign procurement for some components and technology. North Korea also continues to expand the world's largest and most fortified underground facility (UGF) program, estimated to consist of thousands of UGFs and bunkers that are designed to conceal and protect leadership, C2 assets, WMDs, ballistic missiles, military forces and assets, and defense industries.

North Korea continues to violate international sanctions by procuring dual-use goods for its WMD and missile programs, illicitly importing refined petroleum and exporting proscribed commodities—such as coal and military equipment—despite its extreme border restrictions. Since 2018, North Korea has acquired refined petroleum in excess of the amount allowed under United Nations Security Council (UNSC) resolutions through vessels using illicit ship-to-ship transfers and direct deliveries of petroleum using third-country tankers. Prior to the pandemic, evasion of sanctions stabilized North Korea's fuel supplies and prices; however, widespread shortages caused by the pandemic-driven border closures continue to affect price volatility and depletion of its stockpiles. Evading sanctions has also allowed a continued revenue flow that has historically funded its nuclear and ballistic missile programs. Pyongyang remains a willing supplier of conventional arms, military equipment, and almost certainly missile technology, flouting UNSC sanctions to generate revenue from arms exports. North Korea uses intermediaries and front companies to mask exports to the few arms buyers undeterred by international interdiction efforts, including Iran, Syria, and Uganda. North Korea may also resume arms sales to Burma, considering North Korea's need for cash and Burma's limited arms trade options after the February coup.

North Korean Cyber Capabilities

North Korea possesses a sophisticated hacking program that supports the regime's goals of generating revenue and advancing its defense capabilities. North Korea's cyberactors also conduct espionage for the regime, while sidestepping sanctions. They generate currency through criminal enterprises such as cryptocurrency theft, ransomware, and hacking-for-hire. Revenue from these operations probably supports weapons development and production and overall regime survivability. North Korea conducts cyberespionage globally against foreign officials, academics, and defense and aerospace industries, probably to gain insight into adversary capabilities and acquire information to aide Pyongyang's own weapons development. In addition, its cyberactors continue to collaborate with foreign cybercriminals, demonstrating an ability to use third-party accesses and resources to further North Korean cyber missions. North Korea maintains the ability to conduct disruptive and destructive cyberattacks.

North Korea's external engagements probably will remain stagnant in early 2022, and its relationships do not appear to contribute significantly to its defense establishment or to boost military readiness. International sanctions against North Korea probably dampened potential partner interest in expanding ties. Pyongyang's internal efforts, such as border tightening to mitigate the spread of COVID-19 and crackdowns to increase population control, probably also hindered foreign engagement in 2021. North Korea has signaled it may loosen some border restrictions in 2022 to address ongoing food insecurity and depressed economic conditions. Its only formal defense agreement is with China: the 1961 Sino–North Korean Treaty of Friendship, Cooperation, and Mutual Assistance. In October 2021, Kim Jong Un appeared to reinforce the importance of this agreement in a letter to his Chinese counterpart in which he pledged support for China's fight against confrontational moves by hostile forces (presumably the United States). Russia, which provided substantial military assistance and equipment to North Korea during the Soviet Era, has largely curtailed its defense relationship with Pyongyang. North Korea probably sees Russia as less important than China as a regional partner.

We expect North Korea to continue its nuclear, missile, and military modernization efforts in 2022 as it emphasizes bolstering its strategic deterrence and countering the military capabilities of the U.S.–South Korean alliance. Kim Jong Un will likely use these developments to try to increase his leverage in any potential negotiations with the United States. North Korea will probably continue to justify its actions by using U.S. policy, South Korea's military modernization, and combined U.S.–South Korean military exercises as pretext to normalize North Korea's military advancements. To demonstrate North Korean strength and resolve, leadership could consider further missile testing of various ballistic and cruise missiles, conduct a cyberattack, or test another nuclear device. Such actions would probably also depend on North Korean leadership's calculation between developing military capabilities and seeking to apply pressure on the United States and South Korea to advance its political objectives. In addition, Kim Jong Un's calculation may also involve an expectation for significant diplomatic or economic backlash, particularly with ICBM testing.

TERRORISM

Status of the Salafi Jihadist Movement

Twenty years after 9/11, the Salafi jihadist movement's unifying leaders are mostly dead, the threat to the United States homeland is much diminished and the movement's priorities are mainly local, probably preventing a return to its 2015 peak within the next 2 years. ISIS and al-Qa'ida, however, are able to inspire or enable opportunistic attacks against the United States and U.S. interests. Lone-actor attacks by Salafi jihadists, with little or no warning, are more likely to occur than directed attacks. Salafi jihadist group leaders who give high priority to directing attacks in the West, such as al-Qaida, probably will need at least 1 to 2 years to conceptualize, develop, and execute complex plots. ISIS-Khorasan could develop a capability to attack the United States within the next year, if the group prioritizes such an attack. Salafi jihadist groups probably can accelerate the timeline of directed attacks in the West to as little as 4 to 6 months by pursuing plots that are simple to execute. Leadership intent probably is a more critical driver for initiating directed plots against the West than a terrorist group's control of territory or freedom of movement.

Islamic State of Iraq and ash-Sham

In 2021, ISIS maintained 17 publicly recognized branches worldwide and claimed responsibility for attacks in dozens of countries. Earlier this year, ISIS emir Hajji Abdallah died during a U.S. military operation in Syria. ISIS retains a C2 structure that allows the group to withstand his death and preserve its ability to oversee local operations and its expanding global presence. In Iraq and Syria, the ISIS insurgency progressed unevenly during the past 2 years, in part because of their senior leadership losses; however, the group remains a substantial threat to security in these countries. ISIS is also seeing opportunities in Afghanistan, where the group has gained considerable personnel and resources since the Taliban takeover and been emboldened since its 26 August attack on Hamid Karzai International Airport in Kabul. These gains include prisoners freed from Afghan prisons in mid-August, which increased the group's manpower and capabilities. If ISIS-Khorasan leaders give priority to external attacks, the group probably can use this influx of resources and personnel to develop the capability to attack the U.S. homeland within the next year. The ISIS narrative continues to emphasize the group's attacks and regional expansion—especially in Africa—where ISIS branches have conducted attacks against Western targets and have partial territorial control. The group's continued growth in Africa will spread instability and increase the threat to U.S. interests on the continent.

Al-Qa'ida

Al-Qa'ida's capabilities have been significantly weakened; further, the group probably is on a declining global trajectory after years of organizational resilience and lacks leaders who have global jihadist appeal. The deaths of senior leaders, unfavorable operating environments, and sustained counterterrorism pressure have hurt the group during the past 2 years. Al-Qa'ida's Iran-based senior leaders oversee its global network and issue guidance to al-Qa'ida affiliates on media releases and strategy. In the newly Taliban-controlled Afghanistan, al-Qa'ida's capabilities are weak, and the group probably is focused on recovery while considering its strategy for the future. Al-Qa'ida leaders have called for obedience to the Taliban, which has publicly declared that Afghanistan will not be used for transnational attacks. If al-Qa'ida decides to reverse course, the group likely will require at least 1–2 years to rebuild its external operations capabilities in Afghanistan to mount an attack against the West, should it choose to prioritize external operations. Al-Qa'ida's regional affiliate in Afghanistan—al-Qa'ida in the Indian Subcontinent (AQIS)—struggles to conduct local attacks and is experiencing leadership losses. The group's future trajectory probably depends on the Taliban regime's restrictions. In 2021, al-Qa'ida made gains in Sub-Saharan Africa, where it now controls large swaths of Burkina Faso, Mali, and

Somalia and is attempting to gain footing in littoral West Africa. Al-Qa'ida in the Arabian Peninsula has lost personnel and territory during the past 2 years to counterterrorism pressure and internal actions aimed at ferreting out suspected spies. In 2022, the group's global enterprise probably will continue to focus more on regional priorities in the Middle East, Africa, and Asia than on attacks in the West.

Lebanese Hizballah

Lebanese Hizballah's Islamic Jihad Organization (IJO)—the group's primary overseas attack unit—remains an integral element of Iran's threat network. Hizballah probably will direct an IJO attack in the homeland or against U.S. interests abroad only if Hizballah or Iran perceives a threat to the group's existence. Hizballah almost certainly will maintain the IJO to deter foreign aggression, particularly from Israel and the United States. In 2022, the IJO will probably continue its focus on recruiting and training new members, refining its capabilities, and improving its operational security in Latin America, Africa, and Southeast Asia.

Racially/Ethnically Motivated Violent Extremists (RMVEs)

In the last decade, other extremist ideologies reemerged in the West, with sociopolitical factors and perceived grievances fueling transnational RMVE movements and probably driving RMVE attack strategies that threaten Western governments and civilians. Disrupted plots within the past 2 years include those against U.S. military personnel. RMVEs exploit the information environment by spreading extremist propaganda and proliferating conspiracy theories online to attract new members and strengthen the extremist identity of others with similar beliefs across the globe. RMVE movements have been seeking to recruit current and former military members with varying levels of success.

DISEASE AND CLIMATE THREATS

COVID-19 Pandemic

Since its onset, COVID-19 has killed over 6 million people across the globe. In the past year, there have been multiple COVID-19 waves, with the most recent—driven by the Omicron variant—just beginning to subside. During the next 6 months, countries or regions without sufficient non-pharmaceutical intervention practices—such as social distancing and mask wearing—or vaccine supplies probably will see the most dramatic waves.

Limited and fragmentary data has led the Intelligence Community (IC) to maintain multiple theories on the origin of COVID-19. Four elements and the National Intelligence Council assess with low confidence that the virus likely emerged from a natural interaction between an animal infected with the virus and a human; one IC element assesses with moderate confidence a laboratory origin is more likely and three other IC elements are unable to arrive at either conclusion without additional information. All agencies agree the virus was not developed as a biological weapon and most agree that it was not genetically engineered. China continues to obscure all investigations into the origins of COVID-19 that would assist in making a definitive assessment, preventing the release of information such as data on early cases, access to potential host species, or documents from internal investigations—behavior indicative of a desire to keep COVID origins secret.

As of February, there were at least 337 candidate COVID-19 vaccines in clinical development worldwide, with at least 142 in human clinical trials. Russia's Sputnik V COVID-19 vaccine has still not received World Health Organization prequalification; the review previously stalled because of missing data. Despite this, Russia has marketed Sputnik Light as a single-dose vaccine and more recently as a booster for other COVID-19 vaccines. Chinese vaccine manufacturers claim that their Sinovac and Sinopharm vaccines have demonstrated 50- to 79-percent effectiveness in protecting individuals against COVID-19, but cases of resurgence in some countries that have heavily relied on Beijing’s vaccines call these claims into question.

The COVID-19 pandemic—especially new variant case surges, such as Omicron—has strained medical capabilities worldwide, prompting many nations to seek foreign medical assistance and deploy military medical assets to augment domestic responses. Medical personnel shortages have been a primary factor hindering worldwide COVID-19 responses, especially as the pandemic has caused widespread health care worker infections and deaths, burnout, and resignations. The emergence of novel respiratory viruses capable of causing sustained human-to-human transmission on multiple continents, like COVID-19 and its variants, continues to pose the greatest enduring infectious disease risk to U.S. personnel.

Climate Change

Climate change is an important factor in the current and future operating environment for the Joint Force, affecting foreign nations’ internal stability and military capabilities. We assess that climate change will increasingly exacerbate risks to U.S. national security interests as physical impacts increase and geopolitical tensions mount about how to respond. The physical effects of climate change are likely to intensify cross-border geopolitical flashpoints, including a growing risk of conflict over cross-border migration and water, food, and mineral resources. We also assess the potential for instability and possibly internal conflict in developing countries will increase, in some cases creating additional demands on U.S. military resources—particularly for humanitarian assistance and disaster relief operations. The most vulnerable countries in Africa, Asia, Latin America and the Caribbean, and the Middle East that are dealing with the physical effects of climate change will continue to request military and nonmilitary assistance from the United States to help manage and mitigate those issues.

REGIONAL SECURITY ISSUES

MIDDLE EAST

China and Russia will continue to challenge the United States for influence in the Middle East as the perception of waning U.S. engagement leads regional allies to seek alternatives to U.S. support to counter threats, particularly from Iran. Roughly half of Chinese oil and gas imports come through the Persian Gulf, and China also relies on sea lines of communication through the Suez Canal and Red Sea to maintain access to European markets. Beijing is particularly focused on building economic and diplomatic ties with key states, including UAE, Saudi Arabia, Iran, and Egypt. Russia has sought to build upon its success in Syria to expand its regional influence and serve as a geopolitical counterweight to the United States in the Middle East, advertising itself as a reliable arms supplier, security partner, and mediator.

Iran and its regional allies, likewise perceiving a reduced U.S. commitment to the region, are emboldened to use military force to increase their influence and diminish U.S. influence. Traditional drivers of unrest—authoritarian leaders, insufficient economic opportunity, and corruption—remain and are compounded by terrorism, hybrid military threats, Iranian activity, and the persistent pandemic.

Syria

After more than a decade of civil war, Syria is beginning to reemerge from its international isolation as some Middle East, European, and Asian countries work toward closer diplomatic and economic ties with Damascus. This year's high-level engagements between Syria and China indicate an interest by both sides to enhance cooperation, particularly on counterterrorism efforts and Syria's reconstruction—despite uncertainty surrounding possible returns on Chinese economic investment. Economic and security cooperation between Damascus and Beijing is unlikely to supplant the Asad regime's reliance on Iran and Russia during the next 2–3 years.

Syria and its allies probably are best positioned to shape the conflict’s trajectory in their favor during the next year. Following the March 2020 cease-fire agreement, cease-fires around the country largely have held and military operations have waned, despite many areas of the country remaining outside the Asad regime’s control. The frontlines are likely to remain mostly static for at least the next 6 months. Syria probably will not resume a major offensive without explicit political and military support from Russia, judging from Syria’s previous reluctance to engage directly with the Turkish military in sustained combat. Damascus is building relationships with local tribes in the east to foment unrest against the Syria Democratic Forces (SDF), undermine Kurdish-led governance, weaken the U.S. relationship with tribes, and conduct deniable attacks on the SDF and coalition forces. Syria’s economic crisis has degraded living conditions and fueled a low-level insurgency in regime-controlled southwest Syria, but sustained Iranian and Russian support probably will prevent the insurgency from posing an existential threat to Damascus.

The SDF relies on Russia and the United States to forestall additional Turkish operations and buy time to negotiate reconciliation terms with Damascus. Russia continues to exploit SDF vulnerabilities to gradually expand the Asad regime’s presence in the northeast and strengthen Asad’s leverage in future reconciliation negotiations.

The Syrian opposition almost certainly is incapable of threatening regime stability and instead seeks to defend its remaining territory in the north and support Turkey’s objectives in Syria to maintain Ankara’s support. Turkey’s direct military support to the opposition during the past several years has solidified Ankara’s control over the opposition.

Turkey’s activities in northeastern Syria include restoring infrastructure, conducting patrols and road checks, clearing mines and IEDs, and conducting counterterrorism raids. Turkey blames the Kurdish People’s Protection Unit (YPG) for conducting attacks in northeastern Syria targeting the Turkish-supported opposition and resulting in civilian casualties. Turkey views the YPG as the Syrian affiliate of the Kurdistan Workers' Party and an existential threat to Turkish internal and border security.

Russia almost certainly will maintain a long-term military and economic presence in Syria, affording it access to natural resources and continued use and expansion of its military presence, which enables its regional power projection capabilities. Moscow seeks to normalize relations between the international community and Damascus with the goal of encouraging outside investment and reconstruction efforts while mitigating the impact of U.S. sanctions on the Asad regime.

Iran remains committed to securing its strategic interests in Syria, including ensuring the stability of the Asad regime and preserving access to Levant-based partners and proxies, particularly Hizballah. Hizballah's primary objectives in Syria are to maintain security along the Lebanon-Syria border, stage for a potential conflict with Israel, and preserve resupply nodes from Iran. Iranian-backed forces remain critical-force multipliers for proregime operations across Syria and for holding territory in the east. Iranian officials also intend to wield influence in postconflict Syria, particularly through reconstruction contracts and a permanent Iranian military presence.

Iraq

Iraq held early national elections in October 2021 and is currently going through the government formation process, which may take months. The Sadrists, led by Shia cleric Muqtada al-Sadr, are the largest political bloc, winning roughly 70 of the 329 seats in the Council of Representatives and will most likely lead the government's formation. The Sadrist platform emphasizes Iraqi sovereignty and is focused heavily on removing foreign actors, reducing other Shia militias' domestic influence, diversifying foreign partnerships, and normalizing relations with the Arab world. Iran-backed Shia political parties performed poorly in the October 2021 elections and are seeking to negotiate a power-sharing agreement with Sadr to retain their influence in Iraq's government. Iran-backed parties led protests against the election results from October to December 2021, which sparked a deadly clash with Iraqi security forces and led to an Iranian-backed militia using quadcopters to attack the prime minister's residence in the International Zone in early November 2021.

The threat to U.S. and coalition forces from Iran-backed Shia militias remains high as militias continue to demand the withdrawal of U.S. forces from Iraq. In 2021, Shia militias began using one-way-attack UAVs and armed quadcopters to target U.S., U.S. partner nation, and Iraqi government interests, demonstrating their capability and intent to employ advanced Iran-provided weapons. Shia militants considered 31 December 2021 to be a deadline for the withdrawal of U.S. troops and conducted seven UAV and indirect fire attacks during January. Iraqi militia leaders have publicly pointed to the U.S. withdrawal from Afghanistan as evidence that regular attacks against U.S. forces will catalyze a U.S. departure.

Iraqi security forces (ISF) probably will maintain counter-ISIS operations absent coalition support for at least 1 year, although coordination among the various ISF elements will be inconsistent, judging by the operations undertaken during this year. Throughout 2021, the ISF has demonstrated its ability to conduct effective counter-ISIS operations independently, but it still seeks support from coalition forces when its own capabilities are insufficient. In late 2021, the Kurdish Ministry of Peshmerga and the Iraqi Army continued plans to form and deploy two joint Iraqi-Peshmerga brigades to eliminate ISIS from the disputed territories near the Iraqi Kurdistan Region (IKR).

Finally, the Kurdistan Regional Government (KRG) almost certainly will continue to experience several systemic weaknesses, including Kurdish dynastic rule, challenges paying government salaries, and a bifurcated and partisan system of military C2. The KRG faces external security threats from Iran-backed militias and from ISIS as well as ongoing Turkish and Iranian strikes targeting opposition groups in the IKR. Since early 2021, the Kurdistan Democratic Party has accused Iran-backed Shia militias of carrying out several UAV and rocket attacks in the IKR, primarily near Erbil International Airport. Separately, last year, the second largest Kurdish party, the Patriotic Union of Kurdistan, went through a leadership struggle that risked armed conflicts between factions.

ISIS in Iraq and Syria

In Iraq, ISIS maintained a steady pace of attacks during the past year, although at a slightly lower level than the year before. Coalition and Iraqi counterterrorism operations inflicted losses on several of the group's key leaders in Iraq, but its basic C2 structure remains intact. ISIS probably benefited from Shia militia attacks during the past year that forced the coalition to prioritize force protection, intermittently disrupting counter-ISIS operations. As in years past, ISIS has operated most freely in north-central Iraq where the mountainous terrain impedes effective counterterrorism operations by the ISF. It has shown increased ability to conduct occasional high-profile attacks in Baghdad, such as suicide bombings, but not the ability to sustain such attacks. ISIS also has made targeted efforts to foment sectarian tension in Sunni-Shia communities, which the group believes will increase its popular support among Sunnis. Still, the group enjoys little overt popular support and relies mainly on coercion to obtain money, supplies, and access to populated areas.

In Syria, ISIS continues to operate as a clandestine insurgency with most of the group's activities and attacks occurring in the largely rural areas of central Syria, consisting of rudimentary hit-and-run style attacks on static checkpoints and frequently traversed highways. It remains capable of conducting sporadic, high-casualty attacks despite reduced attack levels this year, probably resulting from consistent counterterrorism operations from the U.S.-backed SDF, pro-regime forces, and rival extremist groups. To increase its ranks, ISIS has focused its efforts on smuggling ISIS-affiliated families from internally displaced person camps in northern Syria and freeing ISIS prisoners from SDF-run detention facilities. On 20 January, ISIS attacked Al-Hasakah Prison and freed an undetermined number of its members, underscoring the importance the organization places on rebuilding its capabilities.

Yemen

In 2021, the Iranian-backed Huthis rebels regularly attacked Saudi Arabia with UAVs and missiles and gained control of additional territory from the Saudi-led coalition in northern Yemen. The Huthis, with Iranian support, improved their military capabilities, using more advanced UAVs and missiles to target Saudi Arabian bases, air defense, and infrastructure. In 2021, the Huthis continued ground operations to seize control of Marib City, the Yemeni government's last military and economic stronghold, and advanced into resource-rich Al Bayda and Shabwah Governates and along the west coast in Al-Hudaydah. The Yemeni government and the anti-Huthi coalition remain weakened by internal divisions and persistent humanitarian and economic issues. As a result, the Huthis are growing increasingly confident in their position based on their military success.

Lebanon

Lebanon's economic and internal security crises very likely will worsen during the next year. Beirut has been unable to manage its sharply declining economy, sustain critical services, or address its underlying governance problems, which is eroding government legitimacy and driving increased crime and violence. Lebanese Armed Forces and other security forces have experienced a 90-percent reduction in the U.S. dollar value of their budgets, which has limited their ability to respond to security incidents, including increased sectarian violence. Hizballah is publicly blaming the economic crisis in Lebanon on U.S. sanctions, which it describes as a "siege" against the country. It is watching for threats from perceived domestic rivals, Israel, or the United States and is preparing to respond if its core interests are threatened. Hizballah is trying to maintain the political supremacy of its coalition in parliament while avoiding being drawn into sectarian violence with political rivals.

Egypt

Egypt remains focused on Ethiopia's progress toward the development and filling of the Grand Ethiopian Renaissance Dam (GERD), which Cairo views as an existential threat, as it depends on the Nile for approximately 97 percent of its water resources. Egypt will closely monitor the GERD's construction and continue to call upon the international community to intervene and secure a legally binding agreement for filling and operating the dam ahead of the next round of filling in summer 2022. Egypt has maintained its position for the use of diplomacy to settle the GERD dispute and will refrain from addressing the conflict in Ethiopia to preserve Cairo's good neighbor policy. In 2021, foreign terrorist organizations continued to conduct attacks in Egypt, and they almost certainly will remain active in 2022. Although attacks have decreased from the past 2 years, this year terrorist attacks in Egypt have been concentrated in North Sinai, where the Egyptian Armed Forces are engaged in counterterrorism operations against ISIS-Sinai.

SOUTH ASIA

The U.S. retrograde from Afghanistan will have security reverberations globally, particularly in South Asia, as states seek to recalibrate relations, violent extremist organizations capitalize on reduced U.S. counterterrorism pressure, and the Taliban regime attracts U.S. adversaries as diplomatic partners. Meanwhile, the Taliban regime will struggle to avert a humanitarian catastrophe brought on by multiple simultaneous crises, including ongoing economic collapse, mass-scale displacement, severe drought, and a food crisis that puts 23 million Afghans at risk of extreme hunger or famine, according to the United Nations.

Afghanistan

Since capturing Kabul on 15 August, the Taliban regime has announced the formation of ministries and appointments to senior leadership positions. The regime's caretaker cabinet comprises over 50 exclusively male and mostly-Taliban military officials, a small number of religious scholars, and non-Taliban members who were not part of the previous Afghan government. The Taliban regime is seeking the return of skilled Afghans to help with technical aspects of running the government. Despite public claims of amnesty for all Afghans, the regime has committed small-scale reprisal killings, violence, and intimidation against former Afghan National Defense and Security Forces (ANDSF) members and former Afghan government employees; however, we assess the reprisals are limited to the local level and not directed by Taliban senior leadership. Limited infighting at senior levels has emerged over power-sharing arrangements, but the Taliban regime likely will not fracture in the coming year.

The Taliban regime claims to be exercising oversight over foreign fighters and some violent extremist organization (VEO) members in Afghanistan, primarily through its intelligence apparatus and activity restrictions that include living in areas approved by the Taliban and seeking permission to travel. The Taliban is opposed to ISIS-Khorasan and has targeted and arrested ISIS-Khorasan members believed responsible for attacks—although the regime has not been able to stop ISIS-Khorasan operational planning to prevent attacks. The regime seeks to portray that it is capable of delivering on counterterrorism assurances and providing nationwide security and likely will downplay the threat of ISIS-Khorasan in Afghanistan. During the next year, ISIS-Khorasan will focus attacks on sectarian, regime, and infrastructure targets to destabilize the Taliban and expand its operations throughout Afghanistan.

The Taliban regime is pursuing closer relationships with regional states, including Russia, China, Uzbekistan, and Iran, but it probably will continue to prioritize its sovereignty over obtaining international recognition and aid. In October, Acting Deputy Prime Minister Mullah Abdul Ghani Berader met with Chinese Foreign Minister Wang Yi to discuss humanitarian aid, sanctions relief, and China's security concerns. As of November, the Taliban regime had secured its removal from Russia's list of terrorist organizations and reached agreements with Iran and Pakistan to expand their economic and political relationships.   In response to recently perceived threats to its sovereignty—neighboring

Tajikistan's support for the anti-Taliban resistance and other perceived interference—the regime deployed forces to its northern border.

Our adversaries are seeking to capitalize on the U.S. withdrawal from Afghanistan through actions that attempt to erode U.S. credibility in the world. For example, immediately following the U.S. withdrawal from Afghanistan, Moscow amplified its messaging that the retrograde was a failure and that the United States is an unreliable partner and a declining power. Russia has used this moment to improve its regional position by claiming to enhance the capabilities of its bases in Kyrgyzstan and Tajikistan, holding regional exercises, and increasing its engagements with longstanding partners such as India. Similarly, Chinese officials and state media outlets used the U.S. withdrawal from Afghanistan as an opportunity to portray the United States as an unreliable partner and declining power since August. Tehran views the U.S. withdrawal as an opportunity to expand its influence in Afghanistan, but is also wary that instability could cause additional refugee flows into Iran and increase risks to Afghan minority communities it supports. Tehran is engaging with the new Taliban regime as Kabul's de facto government to secure its interests, which include expanding trade, securing the Iran-Afghan border, managing refugees, and countering ISIS-Khorasan.

Regional Security Impacts

As of late October, the Taliban regime was sending fighters, including specialized units, to secure Afghanistan's borders, and had met with Turkmenistan over increasing their respective border security efforts. As of December, Iran had hosted an additional 300,000 Afghan refugees since the Taliban takeover; combined, Pakistan and Iran host approximately 2.3 million Afghan refugees, most of whom arrived before 2021. In mid-November, India, Iran, Kyrgyzstan, Turkmenistan, Tajikistan, Kazakhstan, Uzbekistan, and Russia met to discuss growing concerns about Afghanistan, border security and a possible refugee crisis. In October and November, Russia led CSTO exercises in Tajikistan along

Dushanbe's border with Afghanistan, and in November, Kazakhstan and Uzbekistan participated in joint military exercises along Uzbekistan's border with Afghanistan.

Taliban Military

As of November, Taliban fighters were using weapons, vehicles, and equipment left by former ANDSF units, including UH-60 and Mi-17 helicopters, and have demonstrated the capability to conduct ground operations and move troops with their very nascent air force capabilities. The Taliban regime has begun to professionalize its military, but there is almost no chance it will achieve a professional force within its 2-year goal.

In 2022, the Taliban regime likely will maintain control of Afghanistan through the use of force. The regime is likely to be more focused on suppressing any internal unrest to secure the regime's survival than bending to external pressures.

Pakistan

Pakistan currently views instability in Afghanistan as its most pressing concern and will likely prioritize preventing spillover into Pakistan in the next year and beyond. Although Pakistan has not formally recognized the Taliban regime, Islamabad seeks to maintain positive relations with them, and it is providing humanitarian assistance, international outreach, and technical support to achieve this. Pakistan views the Taliban as a strategic asset, useful for securing its interests in Afghanistan. However, Islamabad's ability to shape Taliban behavior will probably diminish because the group no longer relies on its safehavens in Pakistan.

Pakistan remains vulnerable to attacks by a variety of anti-Pakistan militant groups, including Tehrik-e-Taliban Pakistan (TTP), ISIS-Khorasan, and Baloch separatists. Pakistan's military continues to execute operations against these militant groups and remains concerned about their ability to conduct small-scale attacks and occasional high-profile attacks inside the country. Since 2020, TTP has consolidated factions and increased its attack tempo. In November 2021, TTP agreed to a 1 month cease-fire with Pakistan, but announced it would not extend it further due to perceived Pakistani violations of the terms of the agreement. Fighting resumed in early December 2021, with dozens of deadly attacks.

Islamabad's tense relationship with India will continue to drive Pakistan's defense policy. Pakistan's relations with India remain strained since a high-profile anti-India militant attack in the Union Territory of Kashmir in February 2019. New Delhi's August 2019 revocation of Kashmir's semiautonomous status added to these tensions. However, cross-border violence has decreased since February 2021, when both countries recommitted to a cease-fire. India and Pakistan have not made meaningful progress toward a long-lasting diplomatic solution since then.

Pakistan perceives nuclear weapons as key to its national survival, given India's nuclear arsenal and conventional force superiority. Pakistan very likely will continue to modernize and expand its nuclear capabilities by conducting training with its deployed weapons and developing new delivery systems in 2022.

China is Pakistan's most reliable partner and primary source of military, economic, and diplomatic support. Islamabad has publicly supported China on its handling of the COVID-19 pandemic, treatment of Uyghur Muslims, and other regional security issues. China is Pakistan's most important defense partner and largest supplier of military equipment. China has also invested an estimated $46 billion in the China-Pakistan Economic Corridor—a series of infrastructure projects constituting the flagship of China's BRI.

During the next year, Pakistan is very likely to continue its focus on securing its interests in Afghanistan, while also seeking to expand its relationship with Beijing. Tensions with India probably will remain elevated.

India

Throughout 2021, New Delhi continued to implement foreign policy aimed at demonstrating India's role as a leading power and net provider of security in the Indian Ocean region. India seeks to promote prosperity and ensure stability in the Indo-Pacific region by seeking strategic partnerships to build influence through bilateral and multilateral mechanisms such as the Quadrilateral Security Dialogue and the Association of Southeast Asian Nations. New Delhi seeks to deepen intelligence and operational cooperation on cybersecurity, protect critical information infrastructure, prevent adversary manipulation of public opinion, and to create standards and norms that protect and secure data governance. Following the collapse of the Afghan government, New Delhi is increasingly concerned about potential attacks against India—empowered by a Taliban-controlled Afghanistan—by terrorist groups such as Lashkar-e-Tayyiba and Jaish-e-Mohammed. The evacuation of Indian personnel from Afghanistan degraded its resources to monitor potential threats and cultivate influence over regional stability.

Despite recommitting to the 2003 cease-fire, India remains postured to respond to perceived militant threats, and it has continued counterterrorism operations inside Indian-administered Kashmir. Occasional skirmishes between Indian and Pakistani troops will continue, and a high-profile attack in India by Pakistan-based terrorists risks an Indian military response.

Chinese-Indian relations remain strained following the fatal clashes in summer 2020 between their respective forces along the Western sector of the disputed LAC. During 2021, both sides held multiple rounds of high-level diplomatic and military talks that resulted in a mutual pullback of forces from several standoff points. However, both sides maintain close to 50,000 troops along with artillery, tanks, and multiple rocket launchers, and both are building infrastructure along the LAC.

New Delhi is pursuing an extensive military modernization effort encompassing air, ground, naval, and strategic nuclear forces with an emphasis on domestic defense production. India is taking steps to establish Integrated Theater Commands that will improve its joint capability among its three military services. Since 2019, Prime Minister Narendra Modi has given priority to strengthening the country's economy by expanding its domestic defense industry, including establishing a negative import list to curtail defense purchases from foreign suppliers. India's longstanding defense relationship with Russia remains strong, holding their first "2+2" format talks in December—a joint foreign and defense ministerial that India previously only held with the United States, Japan, and Australia. India has maintained a neutral stance on the Russia-Ukraine conflict and continues to call for peace.

As of October 2021, India's military was seeking to procure advanced surveillance systems to better safeguard India's land and sea borders and boost its offensive and defensive cyber capabilities. In December, India received its initial delivery of the Russian S-400 air defense system, and it intends to operate two in its western theatre by April 2022. India continued to develop its own hypersonic, ballistic, cruise, and air defense missile capabilities, conducting multiple tests in 2021. India has a growing number of satellites in orbit, and it is expanding its use of space assets, likely pursuing offensive space capabilities.

Burma

Since the February 2021 military coup, Burma remained in a state of emergency and growing civil unrest, which we expect to continue this year. The military junta arrested senior National League for Democracy leaders President Win Myint and State Counselor Aung San Suu Kyi, who currently face convictions on charges of alleged corruption, bribery, and election fraud to bar them from future political office. Since the spring, civil disobedience protests have evolved into an increasingly aggressive, multifront, armed resistance of rural and urban militias who seek the end of military rule. These groups, in varying levels of collaboration with the popular shadow government, join numerous ethnic armed groups operating within Burma, adding complexity to decades of internal conflicts. Beijing has visibly embraced the regime, offering some support in international organizations and resuming infrastructure projects it had previously pursued with the civilian-led government.

The military regime almost certainly will manipulate conditions to ensure it remains in power to prevent a return to civilian-led, democratically elected government in prospective August 2023 elections. In the next year, Burma's internal conflicts between the regime, resistance factions, and ethnic armed groups likely will continue as the regime and the armed civilian resistance remain entrenched and are unwilling to negotiate.

AFRICA

Many African nations continue to struggle with internal and external pressures driven by political instability, food instability, economic downturns, and expanding domestic insecurity. Internal and regional conflicts expanded in several African regions and countries in 2021—most notably in East Africa. Terrorism remains an active destabilizing influence with al-Qa'ida-affiliated terrorist groups and ISIS gaining influence and in many cases territorial control in the Sahel, Mozambique, Nigeria, Somalia, and elsewhere on the continent.

African states have engaged with a variety of foreign actors, including China and Russia, largely out of a pragmatic desire to maximize assistance and diversify foreign support. African leaders' security challenges provide China and Russia opportunities to expand their influence across the continent. China is the largest trading partner of all African states combined, and economic downturns throughout the continent in 2021 drove increased African receptivity to Chinese political, security, and economic engagement to offset budget shortfalls and deliver tangible infrastructure and economic results. Growing security cooperation between China and African states is rooted in requirements for security assistance to counter various threats such as extremists, pirates, illicit traffickers, and state and nonstate adversaries. Many African nations are also receptive to Russia's outreach as a security partner and tend to purchase Russian arms because they are relatively inexpensive, arrive quickly, and are not subject to extensive vetting and end-use monitoring. Since 2014, Russia has signed at least 19 military cooperation deals in Sub-Saharan Africa for training and cooperation in counterterrorism, peacekeeping, and counterpiracy operations. In addition, some African governments turn to Russian private military companies to receive training for their forces, to augment security operations, or to enhance their security. African responses to Russia's invasion of Ukraine vary on a country-by-country basis, but countries such as the Central African Republic and Mali remain willing to work with Russia and Russian private military companies.

North Africa

Libya's rival factions have remained deadlocked in central Libya since June 2020, when the eastern-based Libyan National Army (LNA) retreated from its military campaign to capture Tripoli. A cease-fire between the LNA and Tripoli-based Government of National Unity (GNU), codified in October 2020, remains in place. The LNA and GNU have made progress toward easing tensions through the Joint Military Commission, which includes five military representatives from each side, but they have not made significant progress toward achieving military unification or removing foreign military forces in the country. The presidential election scheduled for 24 December 2021 and parliamentary elections planned for February 2022 were postponed indefinitely, primarily because the candidates included controversial Libyans in leadership roles or with ties to the former Qadhafi regime.

Turkey has advocated for free, fair, and credible elections in Libya. Ankara maintains Turkish forces and Syrian proxies in Libya and says it is in favor of a measured withdrawal of its proxies but is seeking Russian private military company Vagner to withdraw first. Ankara has also resisted calls for Turkish forces to withdraw alongside other foreign forces because it maintains the Turkish presence falls under bilateral agreements with the legitimate government of Libya. Moscow seeks to secure arms sales, oil agreements, and military access by building a defense relationship with Libya. Since 2019, Vagner has conducted combat operations on behalf of the LNA, with aircraft and air defense equipment provided by the Russian Defense Ministry. Moscow is balancing its military support to the LNA with diplomatic outreach to the GNU, probably to secure Russian interests regardless of the future structure of the Libyan state.

Since November 2020, Morocco's military has been engaged in a low-intensity conflict in Western Sahara against Algeria-backed Polisario insurgents, who demand a referendum on the territory's status overseen by the United Nations Mission for the Referendum in Western Sahara. Algeria cut diplomatic relations with Morocco in August 2021 and tensions have since increased. In early November a Moroccan UAV strike killed three Algerians, and shortly thereafter, Morocco signed a security cooperation agreement with Israel.

In July 2021, Tunisian President Kais Saied invoked an emergency constitutional measure to suspend parliament and dismiss most of the government. Saied defended this measure as necessary to end the political standoff and address socioeconomic concerns. He appointed a prime minister in October and plans to hold a referendum on a new constitution in July and parliamentary elections in December 2022.

West Africa and the Sahel

Terrorist threats in West Africa continue to expand throughout the Sahel and Lake Chad Basin as security forces struggle to make counterterrorism gains while addressing competing sources of internal political and social instability. The January 2022 military takeover in Burkina Faso is the latest in a series of destabilizing events in the region and underscores the tumultuous and fragile state of some West Africa governments, which are already struggling to adapt to increasing threats. The al-Qa'ida–affiliated group Jamaat Nusrat al-Islam wal-Muslimin continues to increase attacks in Sahelian states, especially

Burkina Faso and Mali, and to threaten littoral countries, while ISIS-Greater Sahara is focused on rebuilding itself in Niger after leadership losses and setbacks in 2020 and 2021. ISIS-West Africa mostly defeated Boko Haram in 2021, incorporating many former Boko Haram fighters in the process and allowing the group to expand its area of influence and continue attacks on regional security forces in the Lake Chad Basin.

In February 2022, France announced its intent to withdraw its forces from Mali and reposition its Sahel counterterrorism mission to Niger. During the past year, regional security efforts, such as the G5 Sahel Joint Force and the Multinational Joint Task Force in the Lake Chad Basin, have made little progress curbing terrorist activity and expansion because of resource constraints and operational shortcomings. These shortcomings and the longstanding instability in the region present opportunities for China and Russia to increase influence through expanded foreign military sales, counterterrorism training, and other security assistance initiatives. In December 2021, Vagner personnel deployed to Mali—ostensibly at the behest of Mali's transitional government to conduct security operations. This presence has the potential to disrupt ongoing counterterrorism and stabilization efforts in the region.

East Africa

During the past year, East Africa has experienced heightened instability because of the conflict in Ethiopia, a military takeover in Sudan, political tensions in Somalia, and a sustained terrorist threat from al-Shabaab and ISIS groups. Conflict in Ethiopia continues. In late 2021, Tigrayan forces advanced toward Addis Ababa, threatening the federal government, worsening a humanitarian crisis, and elevating the risk of wider ethnic violence, but have since retreated. The crisis threatens to spill over into neighboring countries as Ethiopia's longstanding tensions with Egypt and Sudan over the GERD, Eritrea's military involvement in the Tigray conflict, and an unresolved border dispute between Ethiopia and Sudan present potential flashpoints. In Sudan, a military takeover of the government in November 2021 disrupted political progress the country had made following the establishment of a civilian-led transitional government and removal from the U.S. Government's State Sponsors of Terrorism list. Postponed presidential elections in Somalia have raised political tensions in the country, which at times has led to fighting between armed groups in Mogadishu and distracted from the counterterrorism fight against al-Shabaab.

Al-Shabaab remains the primary terrorist threat in the region, and the group continues to exploit the security vacuum caused by undergovernance, internal political tensions, and the slow progress of establishing Somali security forces. Al-Shabaab operates as a shadow government in the areas it controls, while continuing to attack security forces and civilians, and deliberately targeting U.S. and Western personnel and interests in the region. The much smaller ISIS-Somalia primarily operates from the Golis Mountains area of Puntland, using IEDs and assassinations to target Somali and Puntland government and security forces and civilian targets.

Central and Southern Africa

The Central Africa region faced heightened violence and an expanding regional terrorist threat during the past year, which jeopardizes fragile humanitarian, economic, and political situations. In the Central African Republic, Russian private military contractors and government forces regularly commit human rights violations while fighting antigovernment armed groups. In the Democratic Republic of the Congo (DRC), ISIS-DRC's increasing violence against government and UN security forces and civilians is driving a humanitarian crisis and risks spreading primarily into Uganda, which experienced five ISIS-DRC attacks between October and November 2021.

In 2021, most countries in southern Africa experienced economic turmoil because of the effects of the COVID-19 pandemic, which exacerbated instability and constrained counterterrorism capacity. In Mozambique, ISIS-Mozambique expanded operations, conducting deadly attacks and temporarily taking terrain that threatened Western economic interests in the oil-rich province of Cabo Delgado. Maputo requested Rwanda and the Southern African Development Community deploy security forces in July and the European Union sent a training mission in November. In South Africa, ISIS elements have used the country as a conduit for illicit financial transactions. In July, South Africa deployed 25,000 troops—the most deployed domestically since 1994—in response to unrest because of inequality and the jailing of former President Jacob Zuma on corruption charges. In Zimbabwe, the political system and economy grew more fragile, as President Emmerson Dambudzo Mnangagwa failed to implement promised reforms.

LATIN AMERICA

Latin American countries continue to face a number of stressors that stretch their security forces' capabilities. These stressors include COVID-19 issues, contracting economies, expanding transnational organized criminal networks, rising violent crime rates, and food insecurity, all of which contribute to increased levels of migration and instability. Cuba, Venezuela, Nicaragua, and other countries maintain autocratic structures and reject calls for democratic participation in governance. The resulting instability has enabled China and Russia to make inroads into the region through offers of medical, economic, and military assistance. Beijing and Moscow probably will seek to expand this influence by continuing offers of aid and support to address the region's myriad issues while taking advantage of corruption and nepotism to expand their influence in governing structures.

Venezuela

Disputed President Nicolas Maduro's regime continues its firm grip on all domestic institutions—including the military—despite a 15-percent approval rating and an economy that has shrunk 75 percent during his tenure. The opposition has been unable to organize a large-scale antiregime protest since 2019. Opposition political parties are considering new leadership after failing to unseat the regime in 3 years. Venezuelan military leaders remain steadfast in their support for Maduro with active duty or retired officers holding a third of his cabinet positions. Security forces, however, almost certainly will struggle to confront various internal threats such as urban gangs and foreign illegal armed groups, including elements of the Revolutionary Armed Forces of Colombia dissidents. Venezuela's worsening humanitarian conditions likely will spur continued migration from the country. Since 2014, more than 5 million people have left Venezuela and the UN projects an additional 3 million will leave in the next year.

Cuba

The Cuban regime uses its security forces and cyber capabilities to quell dissent, while relying on foreign partnerships—including those with China and Russia—for military and economic support. Havana is very likely receptive to increased political, economic, and military cooperation with Moscow and Beijing because of concerns about perceived threats to the Miguel Diaz-Canel administration. Russia is Cuba's military partner of choice and Havana has accepted loans from Moscow to maintain Soviet-era military equipment. Havana's relations with Beijing are mostly economic, with some bilateral professional exchanges and military training support.

Transnational Crime

Criminal networks will continue to challenge Latin American governance. The COVID-19 pandemic exacerbated security challenges as criminal actors exploited overburdened security forces and soaring unemployment. Despite short-term operational disruptions caused by the pandemic, criminal groups have adjusted and been able to resume near pre-pandemic operational levels. Chinese, Russian, and Iranian actors, some of whom are government-sponsored, routinely conduct illicit financial activities in the region. Mexican transnational criminal organizations (TCOs) produce and traffic illicit drugs that dominate the U.S. market. From October 2019 through September 2021, fentanyl seizures by volume at the U.S. Southwest Border increased more than 130 percent, surpassing heroin for the first time. In 2021, nearly 10 million counterfeit pills were seized in the United States, a 430-percent increase since 2019. Colombian-origin cocaine supplies most of the U.S. market, primarily trafficked by Mexican TCOs. Bogota is almost certainly going to try to build on its October 2021 capture of Gulf Clan leader Dario Antonio Usuga, the country's most wanted drug trafficker, as a means to reduce drug flows. Violence from longstanding disputes between rival organizations over drug trafficking routes and other illicit revenue sources will continue to challenge Colombian security forces.

Refugees and Immigration

Fragile economic, security, political, and environmental conditions will remain the enduring factors driving regional migration. A mix of military, paramilitary and police forces—especially those in Mexico and northern Central America—have added personnel to their ranks during the past year to address associated security needs. Since January, other factors, such as increasing xenophobia throughout the region against migrants, loosened COVID-19–related border and movement restrictions, perceptions of a more permissive U.S. immigration policy, and better job opportunities have contributed to above-average migration levels. From October 2020 to October 2021, there were more than 1.73 million migrants encountered at the southwest U.S. Border, a 278-percent increase from 2020 and a 77-percent increase from 2019. Citizens from El Salvador, Guatemala, and Honduras experience severe poverty, insecurity, worsening food security, and some of the highest violent crime rates in the world. Since January 2020, migration from countries other than Mexico and northern Central America—largely from Brazil, Cuba, Ecuador, Haiti, Nicaragua, and Venezuela—has contributed to higher migrant encounter levels, a trend that probably will continue through 2022.

Chinese and Russian Presence

During the past year, China modestly increased its security presence and influence in the region. Chinese technology firms dominate the Safe City market in Latin America, and China also enhanced its ties with countries in the region by sending COVID-19 vaccines and medical supplies. Many regional militaries still view the United States as the security partner of choice, but they are receptive to increasing Chinese engagement—especially those receiving donated Chinese equipment and free military education. Russia values its security engagement and influence in Latin America with its historical partners—Cuba, Nicaragua, and Venezuela—while maintaining broad regional outreach through bilateral relationships and international fora. Russia has delivered humanitarian aid to Cuba and issued loans so the Cuban military can maintain its Soviet-era military equipment. Russian President Vladimir Putin has overseen the deepening of security ties with Managua, and several Nicaraguan laws passed prior to the November elections appear to be modeled after Russian statutes that have been used to suppress dissent. In January, Russia's deputy foreign minister suggested that Russia was open to deploying military infrastructure to Venezuela or Cuba amid tensions with Ukraine. Other Russian officials claimed that Venezuela was prepared to provide Moscow unspecified military-technical assistance in the event Russian-U.S. relations were to deteriorate.

TRANSNATIONAL THREATS

CYBERSPACE

Cyberspace has emerged as an inseparable and indispensable element of modern great-power competition. What nations once achieved through traditional tools of national power, such as diplomacy, informational means, military force, and economic pressure, can now be gained through malicious software programs and hacking tools. Adversaries are probing and exploiting our military and intelligence networks, conducting sustained targeting of social media to manipulate personnel and monitor movement of U.S. forces, and attempting to compromise the U.S. defense-industrial networks to steal weapon systems technology, while criminals are conducting cyberattacks against U.S. critical infrastructure. Russia will probably use artificial intelligence to develop autonomous cyber capabilities to optimize offensive cyberoperations and automate social media operations designed to exacerbate social divides. The 2021 ransomware attacks by Russian cybercriminals, including several that targeted the U.S. oil and food industry, exemplifies the potential danger to U.S. critical infrastructure. Our adversaries undoubtedly noted the impact on U.S. oil production and distribution and the ensuing psychological effects they had on the U.S. public. China is concentrating on improving its information systems and cyberwarfare capabilities, and is seeking to leverage emerging technologies such as big data, AI, and 5G telecommunications to do so. Effective integration of data obtained through intrusions of U.S. information systems and networks and those of its allies and partners could provide China with timely insights that yield intelligence and military advantage. The PLA's emphasis on an integrated approach to using advanced technologies in the cyber domain could improve its ability to conduct cyberspace operations in the near term. The PLA believes modern warfare—as a confrontation between complex systems—demands the ability to implement joint operations across all warfare domains, including cyberspace. China and Russia also have agreements to increase cyber capabilities of other countries creating the potential for new threat platforms in the future.

SPACE AND COUNTERSPACE

China and Russia are intent on undercutting U.S. global space leadership, and Iran and North Korea will continue using EW to deny or degrade U.S. space-based communications and navigation.

China's rapidly growing space program is second only to the United States in numbers of operational satellites, both civilian and military. Beijing is strengthening its science and technology sector and international relationships, and it is modernizing its military through advances in space systems and space-related R&D. China seeks space superiority through its steadily advancing space and counterspace programs to support its military objectives and overall national security goals. China publicly advocates for the peaceful use of space and for agreements at the United Nations on the nonweaponization of space while it continues to improve its counterspace weapons. In addition to improvements in counterspace technology, Beijing has enacted military reforms to integrate cyberspace, space, and EW into joint military operations. China's 2007 antisatellite (ASAT) missile test destroyed a defunct weather satellite, indicating the PLA's ability to target low Earth orbit (LEO) and potentially even geosynchronous Earth orbit satellites. China is developing other sophisticated space-based capabilities like the Shijian-17—a satellite with robotic arm technology that is potentially capable of grappling other satellites—and multiple ground-based laser systems that are capable of blinding or damaging satellites. China very likely is also developing a variety of satellite jammers to disrupt targeted satellites. Since at least 2006, China's government-affiliated academic community began investigating aspects associated with space-based kinetic weapons—a class of weapon used to attack ground, sea, or air targets from orbit.

Russia derives a considerable amount of national pride as a longstanding space power and considers itself deserving of international leadership on any space issue. Moscow considers U.S. dependency on space to enable power projection as a vulnerability it can exploit during a conflict, and it has concluded that gaining and maintaining supremacy in space has a decisive impact on the outcome of future conflicts. Russia also is developing and has fielded counterspace weapon systems—including several ground-based lasers—that can deny, damage, and defeat U.S. space-based systems to reduce U.S. military effectiveness and control conflict escalation if deterrence fails. In November, Russia successfully launched a Nudol ASAT missile and destroyed a Soviet-era satellite—creating more than 1,500 pieces of trackable debris and tens of thousands of pieces of lethal but nontrackable debris. This debris will endanger the spacecraft of all nations in LEO for years to come and may endanger the lives of astronauts and cosmonauts on the International Space Station and China's Tiangong space station.

North Korea and Iran have nascent space programs supporting civilian and military goals, with both nations experiencing limited success in placing earth-observation satellites into LEO using largely unreliable space launch vehicles. The development of space launch vehicles probably has a secondary purpose of testing ballistic missile technology under the guise of peaceful use of space as such testing produces data applicable to the development of long-range and multistage ballistic missiles, including ICBMs. In January 2021, North Korean state-owned media announced Pyongyang is conducting full-scale aerospace work, with Kim Jong Un claiming North Korea had designed a military reconnaissance satellite to launch in the near future. Iran's Project 505 probably is an attempt to remedy prior launch failures by buying an imagery satellite system from Russia; however, this system is not yet in orbit.

North Korea and Iran recognize the value of military space, and they will attempt to deny adversary use of space during a conflict. Pyongyang has conducted GPS and communications jamming, and Tehran publicly acknowledges its capabilities to do the same—with Iran possibly contributing to the proliferation of jamming equipment. North Korean cyberactors have conducted numerous cyberoperations against foreign partner and U.S. Government networks, including against aerospace industry and space enterprises, which could enable North Korean weapon and space system development and procurement programs through technology theft.

NUCLEAR WEAPONS

The number of states with nuclear weapons has grown since the end of the Cold War, and countries with mature nuclear weapons programs are increasing the stockpile and/or the capabilities of weapons in their programs. All of these countries are modernizing their legacy stockpiles by incorporating advanced technologies to penetrate or avoid missile defense systems. Countries are also developing nuclear weapons with smaller yields, improved precision, and increased range for military or coercive use on the battlefield.

Russia and China probably will significantly expand their nuclear warhead stockpiles during the next decade. The anticipated expansion in Russia's stockpile is primarily driven by nonstrategic nuclear weapons growth. Russia probably has up to 2,000 nonstrategic nuclear warheads, in addition to approximately 1,450 deployed warheads on strategic systems covered by New START. Beijing accelerated its nuclear expansion. China will likely have about 1,000 deliverable nuclear warheads by 2030. Other nations such as Pakistan, North Korea, and India continue to advance their nuclear programs, although the programs are not as complex as in Russia and China.

Iran does not have a nuclear weapons program, but it is advancing its uranium enrichment program beyond prescribed JCPOA limits, shortening the time that Tehran would require to produce sufficient weapons-grade uranium for a single nuclear device—should Tehran decide to do so.

The proliferation of dual-use, WMD-applicable goods, knowledge, and technology will continue to present a direct threat to U.S. and allied interests by complicating U.S. force projection capabilities, countering Western missile defense systems, and improving adversarial targeting capabilities. Specialized procurement networks acquire dual-use goods, materials, technologies, and expertise for WMD programs and delivery systems for countries of concern, such as China, Iran, North Korea, Pakistan, and Russia. These networks remain resilient and adaptable in the face of a vast international framework of sanctions, export controls, and other prohibitions limiting the purchase or transfer of certain WMD-applicable goods to specific countries or entities. Such efforts directly support the advancement, development, expansion, and survivability of WMD capabilities around the world.

FOREIGN INTELLIGENCE

DoD faces an extremely sophisticated global foreign intelligence threat environment from an increasing number of state and nonstate actors that are becoming more complex and diverse and substantially threaten DoD personnel, information, operations, supply chains, technologies, and critical infrastructure. China, Russia, Iran, and North Korea compose the majority of these global threats, but the rapid development of globally available and affordable advanced technologies is accelerating the capabilities and numbers of state and nonstate actors posing intelligence threats to DoD interests. DoD and U.S. Government officials also continue to face reports of anomalous health incidents (AHIs)—often referred to in the press as Havana Syndrome—that are affecting the personal safety of officers and their families and U.S. Government missions. The IC has assessed that U.S. adversaries are not engaged in a sustained global campaign involving hundreds of incidents to harm or collect intelligence on U.S. personnel. We continue to investigate possible attribution for a subset of cases and analyze potential causal mechanisms. U.S. adversaries extensively use human intelligence and a wide variety of technical means to surveil DoD personnel and operations around the world. Their proliferation of some technologies—such as Safe City surveillance systems and facial recognition capabilities—can enable them to track and observe DoD personnel and activities, including in locations where U.S. adversaries do not maintain a physical presence.

U.S. adversaries have become adept at using multiple vectors to gain access to or manipulate the DoD supply chain to enable exploitation, sabotage, or subversion. These vectors include using foreign and U.S. laws and regulations to access proprietary or commercial data stored within national borders; evading U.S. Government scrutiny by concealing companies' ties to foreign governments or intelligence services. U.S. adversaries also leverage third-party relationships among companies to conceal foreign entities' involvement in the supply chain and create opportunities for foreign intelligence entities to access or manipulate the DoD supply chain; and they exploit companies tied to foreign governments that pursue monopoly power in their industries to gain access to the DoD supply chain.

Russia, China, and Iran also use multiple avenues to collect on U.S. R&D of emerging and disruptive technologies, primarily to support their own domestic military R&D efforts, threatening to undermine the DoD's future advantages on global battlefields. In addition, U.S. adversaries use multiple methods to collect information on DoD critical infrastructure, which they almost certainly would target during a conflict to degrade DoD's ability to execute and sustain operations.

U.S. adversaries will use emerging technologies—such as AI, big data analytics, cloud computing, advanced unmanned and autonomous systems, Safe City surveillance systems, and wearable electronics—in ways that intend to substantially diminish U.S. advantage in multiple domains. The global proliferation of surveillance technologies, coupled with AI, will offer governments the ability to automate monitoring capabilities to surveil more people, more often. Deployment of 5G networking and

Internet of Things advancements will further enable broad-based surveillance technologies, giving them the bandwidth and on-board analytic capabilities to quickly push greater amounts of higher quality sensor data.

ADVANCED TECHNOLOGY

Rapid technological advancement combined with a global society increasingly eager and willing to integrate new technologies into everyday life likely will drive the incorporation of technology into novel military capabilities faster than any other time in the modern era. With the exception of the United States, only China and Russia have the resources and strategic ambition to incorporate advanced technologies throughout all domains and their forces intended for global deployment. Beijing and Moscow view the development of these technologies as a race in which leaders in a technical field could develop military capabilities faster than their adversaries do to gain the advantage.

China's science and technology (S&T) ecosystem is a multipronged, whole-of-government system that incorporates S&T development from both the commercial and military sectors. China's military-civil fusion strategy, which emphasizes the open sharing of S&T resources and transfer of technology between civilian and defense industries, blurs the distinction between these supply chains. The emergence of the civilian sector as a dominant player developing next generation technology very likely will continue, notably in fields where China has already reached peer or near-peer levels, such as AI, high-performance computing, quantum information sciences, and biotechnology. China aspires to be the world leader in emerging and disruptive technologies by 2035 to sustain its economic growth and develop military capabilities that outmatch those of the United States. Beijing's long-term strategy of rapid, indigenous S&T development of cutting-edge technology, combined with licit and illicit foreign technology acquisition, very likely has positioned China at the forefront of numerous scientific fields.

China's Brain Project is a state-sponsored initiative that seeks to enhance human-machine decisionmaking systems by combining computer-based AI and brain science. The PLA is pursuing related brain science research to enable warfighter enhancement through brain-computer interfaces, devices that directly connect the human brain to computers, and cognition enhancement research. PLA researchers pursue cognitive enhancement through use of pharmaceutical and brain stimulation technologies.

By contrast, Russia more narrowly focuses its research efforts on technologies to match, counter, or offset perceived advantages of the United States and other potential adversaries. Despite the Russian defense industry's massive size and Moscow's efforts to increase development of indigenous capabilities, Russia is challenged both organizationally and technically to produce the high-tech subcomponents required for advanced weapons. These limitations likely stem from severe funding, resource, talent, and infrastructure constraints on the country's S&T sector.

CONCLUSION

The military environment is defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest continuous stretch of armed conflict in our Nation's history. Defense Intelligence must focus on the entire spectrum of conflict and across all warfighting domains to detect and correctly characterize key foreign developments and inform our Defense decisionmakers with timely, relevant insight.

Lieutenant General Scott D. Berrier, USA
Director, Defense Intelligence Agency

LTG Scott D. Berrier arrives to DIA as the 22nd Director and came from the Department of the Army where he served as the 46th G-2. In that role, he was the principal military intelligence and counterintelligence adviser to the Secretary and Chief of Staff of the Army, and the Army's Intelligence Community representative.

He is a career intelligence officer having served as the "2" at every level from Battalion to Combatant Command. The depth of his leadership experience ranges from Company Commander to Commanding General and Senior Mission Commander. His Army, Joint Service, and Special Operations assignments include service throughout the United States, the Republic of Korea, Iraq, and Afghanistan.

LTG Berrier earned a Bachelor of Science Degree in History from University of Wisconsin – Stevens Point, a Master of Science Degree in General Studies from Central Michigan University, and a Master of Science Degree in Strategic Studies from the United States Army War College.

His awards and decorations include the Distinguished Service Medal (1OLC), Defense Superior Service Medal (2OLC), Legion of Merit (1OLC), and Bronze Star Medal (1OLC). LTG Berrier also earned the Parachutist Badge, Air Assault Badge, and Ranger Tab.

LTG Berrier and his wife, Annie, began their Army journey in 1987 at Fort Richardson, Alaska. They have two sons, Cole and Connor. Cole and his wife (Mika) currently serve in the office of Senator Brian Schatz. Lieutenant Connor Berrier is a Naval Intelligence Officer serving as the Flag Aide for the Navy N2/6.

General Paul M. Nakasone
Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service

General Paul M. Nakasone assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service in May 2018.

He previously commanded U.S. Army Cyber Command from October 2016 - April 2018.

A native of White Bear Lake, Minnesota, GEN Nakasone is a graduate of Saint John's University in Collegeville, Minnesota, where he received his commission through the Reserve Officers' Training Corps.

GEN Nakasone has held command and staff positions across all levels of the Army with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan.

GEN Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command. He has also commanded a company, battalion, and brigade, and served as the senior intelligence officer at the battalion, division and corps levels.

GEN Nakasone has served in Joint and Army assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. His most recent overseas posting was as the Director of Intelligence, J2, International Security Assistance Force Joint Command in Kabul, Afghanistan.

GEN Nakasone has also served on two occasions as a staff officer on the Joint Chiefs of Staff.

GEN Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.

GEN Nakasone's awards and decorations include the Distinguished Service Medal (with oak leaf cluster), the Defense Superior Service Medal (with three oak leaf clusters), Legion of Merit, Bronze Star, Defense Meritorious Service Medal (with oak leaf cluster), Army Commendation Medal, Joint Service Achievement Medal (with oak leaf cluster), Army Achievement Medal (with four oak leaf clusters), Joint Meritorious Unit Award, Iraq Campaign Medal, Afghanistan Campaign Medal, Combat Action Badge, and the Joint Chiefs of Staff Identification Badge.

GEN Nakasone and his wife are the proud parents of four children, who form the nucleus of "Team Nakasone."

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 17, 2022

QUESTIONS SUBMITTED BY MR. KELLY

Mr. KELLY. Project Maven was created in 2017 to automate the identification of data collected through imagery and full motion video and ultimately improve the speed and accuracy of our targeting. Five years since its inception, and with a pending transfer to NGA for ownership and oversight, has Project Maven reached full operational capability?

Can you provide an overview of the remaining milestones for Project Maven to reach full operational capability and be fielded to operational units across DOD?

Has Project Maven been used as the primary geospatial analysis and target identification tool in any settings outside of training exercises?

Has Project Maven developed operational algorithms to identify the conventional military weapons and equipment of our near-peer adversaries?

Mr. MOULTRIE. [The information is classified and retained in the committee files.]

QUESTIONS SUBMITTED BY MR. SCOTT

Mr. SCOTT. What is DIA's backlog of Russian language military books and journals that need to be translated? What resources in terms of dollars, personnel, and equipment would be needed to clear this backlog?

General BERRIER. DIA does not have a backlog of Russian language military books or journals to be translated.

Mr. SCOTT. What is DIA's backlog of Chinese language military books and journals that need to be translated? What resources in terms of dollars, personnel, and equipment would be needed to clear this backlog?

General BERRIER. DIA does not have a backlog of Chinese language military books or journals to be translated.

Mr. SCOTT. Is there a need for additional Coast Guard attachés especially if the U.S. Coast Guard was better resourced in terms of dollars and personnel?

General BERRIER. [The information is classified and retained in the committee files.]

Mr. SCOTT. What can be done to enhance Foreign Military Exploitation (FME)?

General BERRIER. [The information is classified and retained in the committee files.]

Mr. SCOTT. What shortfalls exist in the collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information?

General BERRIER. [The information is classified and retained in the committee files.]

Mr. SCOTT. The field of DIA History is vast and so much remains unwritten. What are the gaps in DIA's historical literature because earlier studies were inadequate or are outdated, or because topics have been more or less ignored?

General BERRIER. (U) Background on DIA History efforts and some existing challenges:

- (U) Although there are numerous early histories of DlA, they focus on the organizational structure of the Agency and not its capacity to achieve its roles and missions.
- (U) DIA's many missions and global footprint mean its historians struggle to develop true expertise in every mission area.
- (U) Virtually no organizations within DIA create their own histories or metrics of success that are accessible for study (the MARC's recent "Year in Review" is one excellent exception that we hope to see more of).
- (U) DIA organizations have a high turnover rate, with military personnel assignments lasting approximately two years, and the rotation of DIA civilians for purposes of professional development.
- (U) DIA records are not well organized and a large-scale digitization effort is just beginning, making historical research a challenging task.
- (U) The level ofresources and support provided to DIA's History Branch has varied over the decades. In a few periods, a single or couple of historians have been responsible for the entire mission of the branch. Note that the History branch

activities extend beyond writing history products and include supporting a range of other missions.

- (U) Establishment of the new DIA Museum has required significant resources since 2016 and produced video and podcast series such as "The Historians" and "DIA Connections."
- (U) Many DIA History products are published only on an internal DIA platform (The Daily, The Communique, workforce emails) and are not publicly available on DIA.mil. Limited resources have hindered History Branch's ability to write in-depth histories. For example, historical writing requires substantive investigation and time. Consequently, DIA has not yet been able to address gaps in historical writing, particularly on subjects since 9/11.

(U) Some significant gaps that History Branch hopes to study as soon as possible, include:

- (U) 1980s Latin American operations, including drug interdiction

(U) Mission Services support functions—Logistics, Facilities, Human Resources and Equal Opportunity:

- (U) War in Afghanistan/Operation Enduring Freedom (OEF; 2001–2021)
- (U) War in Iraq/Operation Iraqi Freedom and NEW DAWN (OIF, NEW DAWN; 2003–2011) (Note: an extensive survey of DIA in OIF/NEW DAWN is nearing completion.)
- (U) 2002 Operation Enduring Freedom—Horn of Africa
- (U) 2002—Insurgency in the Maghreb
- (U) 2003–2010—War in Darfur—support to African Union and United Nations
- (U) 2004–2007, 2012–2013—Central African Republic Bush Wars—support to MINURCAT (UN Mission in the Central African Republic and Chad) and MICOPAX (Mission for the consolidation of peace in the Central African Republic) CEEAC/ECCAS (Economic Community of Central African States)

(U) Various African missions:

- (U) 2007—Operation Enduring Freedom—Trans Sahara
- (U) 2008—Djiboutian-Eritrean border conflict
- (U) 2009—Boko Haram's armed rebellion against Nigeria's government

- (U) 2008—South Ossetia War, in which Russia invaded Georgia; and NCMI predicted the invasion
- (U) 2008–2009 Gaza War
- (U) The rise and fall of ISIS over many waypoints, 2006 to 2017:
- (U) 2006—Islamic State of Iraq forms from Al Qaeda in Iraq
- (U) 2010—Baghdadi takes control of the group
- (U) 2013—Baghdadi relocates to Syria, and re-names the group Islamic State of lraq and Syria
- (U) 2014—ISIS takes control of Raqqa, Syria, which becomes its de-facto capital; ISIS takes control of Mosul and the Mosul Dam in Iraq; ISIS declares caliphate; Baghdadi named caliph.
- (U) 2015—Iraqi forces regain Iraq's largest oil refinery from ISIS; Kurdish forces regain Sinjar, Iraq; SECDEF Carter announces U.S. special operation forces supporting Iraqi and Kurdish fighters in Iraq; last ISIS stronghold in Aleppo province falls.
- (U) 2016—Iraqi forces retake Ramadi; Iraqi troops regain Fallujah, Iraq; operation to retake Mosul begins.
- (U) 2017—Syrian troops retake Palmyra; U.S.-backed coalition announces offensive to retake Raqqa; Iraq reclaims mosque in Mosul, and the Iraqi Prime Minister claims that the caliphate has fallen and declares Mosul fully liberated.

(U) Lastly, there are some DIA studies that would benefit from significant updating, including:

- (U) DIA budgets
- (U) DIA chartered missions
- (U) DIA leaders and mission priorities

Mr. SCOTT. If you had to create a recommended reading list just for the field of counterintelligence, what books would you recommend?

General BERRIER. (U) Below is an unclassified reading list compiled by DIA counterintelligence (Cl) analysts, which can provide insight into the field of counterintelligence. Although not exhaustive, the list provides a great introduction and background into counterintelligence.

(U) A Wilderness of Mirrors: Intrigue, Deception, and Secrets that Destroyed Two of the Cold War's Most Important Agents—David C Martin

(U) Rise and Kill First: Secret History of Israel's Targeted Assassinations—Ronen Bergman

(U) Active Measures: Secret History of Disinformation and Political Warfare—Thomas Rid
(U) The Year of Armageddon: The Pope and the Bomb—Gordon Thomas
(U) Spy Handler: Memoir of a KGB Officer—Victor Cherkashin
(U) Merchants of Treason—Thomas B. Allen, Norman Polmar
(U) The Angel: the Egyptian Spy that Saved Israel—Uri Bar Joseph
(U) Red Sea Spies—Raffi Berg
(U) To Catch A Spy—James Olson
(U) Talking to Strangers: What We Should Know About People We Don't Know—Malcolm Gladwell;

General
(U) The Great Game: The Myth and Reality of Espionage—Frederick Hitz
(U) Spies: The Secret Agents Who Changed the Course of History—Ernest Volkman
(U) A Century of Spies—Jeffrey Richelson
(U) Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda—Robert Wallace and H. Keith Melton

Background on US Intelligence Agencies
(U) For the President's Eyes Only—Christopher Andrew
(U) Roosevelt's Secret War—Joseph Persico
(U) The Agency—John Ranelagh
(U) Wedge: The Secret War Between the FBI and CIA—Mark Riebling
(U) Inside the CIA—Ronald Kessler

Background on Foreign Intelligence Agencies
(U) The Sword and the Shield—the Mitrokhin Archive—Christopher Andrew and Vasili Mitrokhin
(U) KGB—Christopher Andrew and Oleg Gordievsky
(U) Every Spy a Prince—Dan Raviv and Yossi Melman
(U) Chinese Intelligence Operations—Nicholas Eftimiades
(U) Her Majesty's Secret Service: The Making of the British Intelligence Community Christopher Andrew
(U) Venona—John Haynes and Harvey Klehr
(U) The Haunted Wood—Allen Weinstein
(U) The New Nobility—Andrei Soldatov
(U) The Charm School—Nelson Demille

Major Spy Cases
(U) Breaking the Ring—[the Walker family case] John Barron
(U) The Rosenberg File—Ronald Radosh and Joyce Milton
(U) Perjury—[the Alger Hiss case] Allan Weinstein
(U) Confessions of a Spy—[the Ames case] Pete Earley
(U) Spy—[the Robert Hanssen case] David Wise
(U) Triple Agent: the al-Qaeda Mole who Infiltrated the CIA—Joby Warrick
(U) Widows: Four American Spies, the Wives They Left Behind, and the KGB's Crippling of American Intelligence—William R. Corson, Susan B. Trento, and Joseph J. Trento

Biographies and Memoirs
(U) Spymaster—Clarence Ashley
(U) The Main Enemy—Milt Bearden
(U) Anthony Blunt—[British art historian and Soviet spy; a member of the "Cambridge Five"] Miranda Carter
(U) Witness—Whittaker Chambers
(U) Cold Warrior—[on James Angleton] Thomas Mangold
(U) Red Spy Queen—[on Elizabeth Bentley] Kathryn Olmstead
(U) A Secret Life: the Polish Officer, His Covert Mission, and the Price He Paid to Save His Country—Benjamin Weiser
(U) Alger Hiss's Looking Glass Wars—Edward White
(U) The Double-Cross System—John Cecil Masterman

Mr. SCOTT. Could you give us DIA's best estimate of how many precision-guided weapons Hezbollah now has in its arsenal? How do you assess the status of Iran's efforts to provide Hezbollah with indigenous manufacturing capability for PGMs? How big of a threat do you see this Iranian precision-guided missile project being to U.S. interests and what will you do to thwart it in Lebanon and elsewhere?

General BERRIER. [The information is classified and retained in the committee files.]

QUESTION SUBMITTED BY MR. BACON

Mr. Bacon. The FY22 Department of Defense appropriations bill includes $62.1 to fully fund the top FY22 unfunded priority of “Hardening Department of Defense Networks”—which was also fully authorized in the FY22 NDAA. Some of these funds are intended to enable full, DOD Information Network-wide deployment of Internet Operations Management (IOM) capability. Does Jt Force Headquarters DOD Information Network (JFHQ–DODIN) have the concept of operations and associated planning material to enable swift operationalization of this capability once procured, and what is the expected implementation timeline for deployment of IOM?

General Nakasone. (U) The funding provided for Internet Operational Management (IOM) aligns to my command’s priority to consistently modernize our ability to command and control in cyberspace at speed. I am grateful for this additional funding to accelerate the adoption of this capability and to enable an enhanced understanding of our public internet-facing DODIN cyberspace terrain.

JFHQ–DODIN has already begun detailed planning required to implement this capability across the DODIN and to ensure we achieve sustained operational effectiveness. Once procured, full implementation is expected within 12–24 months.

○