

[H.A.S.C. No. 118-71]

**A REVIEW OF THE DEFENSE  
INTELLIGENCE ENTERPRISE'S  
POSTURE AND CAPABILITIES IN  
STRATEGIC COMPETITION AND IN  
SYNCHRONIZING INTELLIGENCE EFFORTS  
TO COUNTER THE  
PEOPLE'S REPUBLIC OF CHINA**

---

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND  
SPECIAL OPERATIONS

OF THE

COMMITTEE ON ARMED SERVICES  
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

---

HEARING HELD  
APRIL 11, 2024



---

U.S. GOVERNMENT PUBLISHING OFFICE

57-372

WASHINGTON : 2025

SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS

JACK BERGMAN, Michigan, *Chairman*

AUSTIN SCOTT, Georgia  
ELISE M. STEFANIK, New York  
TRENT KELLY, Mississippi  
RONNY JACKSON, Texas  
NANCY MACE, South Carolina  
MORGAN LUTTRELL, Texas  
CORY MILLS, Florida

RUBEN GALLEGO, Arizona  
WILLIAM R. KEATING, Massachusetts  
ELISSA SLOTKIN, Michigan  
SARA JACOBS, California  
JEFF JACKSON, North Carolina  
JENNIFER L. McCLELLAN, Virginia  
JIMMY PANETTA, California

CRAIG GREENE, *Professional Staff Member*  
WILL T. JOHNSON, *Professional Staff Member*  
OWEN MCGEARY, *Research Assistant*

# CONTENTS

---

|                                                                                                                               | Page |
|-------------------------------------------------------------------------------------------------------------------------------|------|
| STATEMENTS PRESENTED BY MEMBERS OF CONGRESS                                                                                   |      |
| Bergman, Hon. Jack, a Representative from Michigan, Chairman, Subcommittee on Intelligence and Special Operations .....       | 1    |
| Gallego, Hon. Ruben, a Representative from Arizona, Ranking Member, Subcommittee on Intelligence and Special Operations ..... | 2    |
| WITNESSES                                                                                                                     |      |
| Harris, Milancy D., Acting Under Secretary of Defense for Intelligence and Security, U.S. Department Of Defense .....         | 3    |
| Haugh, Gen Timothy D., USAF, Commander, U.S. Cyber Command, Director, National Security Agency .....                          | 5    |
| Kruse, Lt Gen Jeffrey A., USAF, Director, Defense Intelligence Agency .....                                                   | 6    |
| APPENDIX                                                                                                                      |      |
| PREPARED STATEMENTS:                                                                                                          |      |
| Harris, Milancy D. ....                                                                                                       | 25   |
| Haugh, Gen Timothy D. ....                                                                                                    | 30   |
| Kruse, Lt Gen Jeffrey A. ....                                                                                                 | 35   |
| DOCUMENTS SUBMITTED FOR THE RECORD:                                                                                           |      |
| [There were no Documents submitted.]                                                                                          |      |
| WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:                                                                      |      |
| Mr. Keating .....                                                                                                             | 81   |
| Ms. Jacobs .....                                                                                                              | 81   |
| Ms. McClellan .....                                                                                                           | 82   |
| QUESTIONS SUBMITTED BY MEMBERS POST HEARING:                                                                                  |      |
| Mr. Kelly .....                                                                                                               | 85   |



**A REVIEW OF THE DEFENSE INTELLIGENCE ENTERPRISE'S POSTURE AND CAPABILITIES IN STRATEGIC COMPETITION AND IN SYNCHRONIZING INTELLIGENCE EFFORTS TO COUNTER THE PEOPLE'S REPUBLIC OF CHINA**

---

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ARMED SERVICES,  
SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS,  
*Washington, DC, Thursday, April 11, 2024.*

The subcommittee met, pursuant to call, at 3:30 p.m., in room 2212, Rayburn House Office Building, Hon. Jack Bergman [chairman of the subcommittee] presiding.

**OPENING STATEMENT OF HON. JACK BERGMAN, A REPRESENTATIVE FROM MICHIGAN, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS.**

Mr. BERGMAN. Good afternoon. The subcommittee will come to order.

I ask unanimous consent that the chair be authorized to declare a recess at any time.

Without objection, so ordered.

Today we will hear from our witnesses on the Defense Intelligence Enterprise's Posture and Capabilities in Strategic Competition and in Synchronizing Intelligence Efforts to Counter the People's Republic of China.

The Department's efforts are focused on China as the priority of the National Defense Strategy, but once again, as we hold this hearing, the Russia-Ukraine conflict has been raging for more than 2 years; North Korea continues to test nuclear missiles; on October 7, Hamas conducted a surprise attack on Israel leading to a prolonged violent conflict that Iran has leveraged, using its proxies to attack U.S. forces in Iraq and Syria, while supporting the Houthi attacks on international shipping; and threats from terrorist organizations are still persistent across the globe.

The Defense Intelligence Enterprise has a challenging task to support the Department's efforts in strategic competition, counter China, and support the remaining Geographic Combatant Commanders to counter increased threats in their areas of operations, as well as their persistent counterterrorism efforts. This is by no means an easy task.

I am interested in understanding each of your roles in synchronizing these efforts and ensuring your organizations have the ability -- have the capabilities needed, are resourced appropriately, and what capability gaps exist.

I would like to welcome today's witnesses, all of whom are appearing before this subcommittee for the first time in their current capacities:

The Honorable Ms. Milancy Harris, Acting Under Secretary of Defense for Intelligence and Security; General Haugh, Director of National Security Agency, Chief of Central Security Service, and Commander of U.S. Cyber Command, and; Lieutenant General Kruse, Director of Defense Intelligence Agency.

In the interests of time, I ask the witnesses to keep their opening remarks to 5 minutes or less so that we will have more time for closed discussion.

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

**STATEMENT OF HON. JIMMY PANETTA, A REPRESENTATIVE FROM CALIFORNIA, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS**

Mr. PANETTA. Thank you, Mr. Chairman.

I appreciate this opportunity to be in this seat but also, and more importantly, to be part of this very, very important hearing. So, thank you for calling it. And thanks to all of the witnesses for your time today to appear in front of this subcommittee.

Before we start, though, I do want to take just a quick chance to highlight that all of the witnesses are relatively new to your positions. So, welcome and congratulations, as that really is a testament to your organizations that even as leaders transition on to other roles the people that make up our defense intelligence enterprise continue to do the great work to protect our country.

So, thank you.

Now, last year we had this same hearing and we opened up the hearing by saying the current global security environment is dynamic. Is dynamic. Not only has that not changed, it has become, I think we can all admit, even more dynamic.

We had the horrific attack on Israel by Hamas on October 7th, the ensuing conflict, and the humanitarian crisis, the malign actors that seek to exploit and expand on that conflict all across the Middle East.

We still have Russia as it continues its illegal and unjust war which has resulted in enormous damage to Ukraine, the people of Russia, and threatens the United States' interests.

We have Putin who remains defiant as he builds new partnerships to provide him the ability to continue that conflict.

We have Iran with its terrorist proxies and its nuclear program.

Then there is North Korea and its nuclear weapons.

And we have violent extremist organizations who continue to carry out deadly attacks, as we saw in Iran and Russia, and continue to fill the voids that are present in the continent of Africa.

And, of course, we have the Chinese Communist Party that continues to present a considerable challenge. Its willingness to act aggressively in contravention to international norms, coupled with its extensive efforts to modernize and to consolidate its control over the People's Liberation Army.

All of those are cause for concern, as coercive actions orchestrated by the CCP [Chinese Communist Party] continue to undermine both regional and global stability.

Based on my recent travel to the region with Chairman Bergman it was good to see, though, the firsthand partnerships that the United States has, and continue to grow and strengthen, and share intelligence to counter CCP's malignant efforts.

The Defense Intelligence Enterprise is a key component of the whole of government approach to containing all of these types of threats. Given that the global environment remains dynamic, now more than ever this committee remains committed to ensuring that your organizations have the resources and authorities required to carry out the duty that our country asks, our country demands of you. To effectively deal with those challenges and to recognize that we are in an era of Great Power competition, the Defense Intelligence Enterprise must be postured and ready to deal with all of those threats.

The Defense Intelligence Enterprise must remain agile, be collaborative across the enterprise, quickly provide releasable and actionable intelligence throughout the Department, and collaborate with our allies and with our partners.

That is why this hearing is important and why I look forward to hearing from all of our witnesses today.

Thank you, Mr. Chairman. I yield back.

Mr. BERGMAN. Thank you.

We will now hear from our witnesses, then move into the question and answer session. Immediately following one round of questions we will reconvene for the classified session which will take place in Rayburn Room 2337.

I now recognize Ms. Harris.

**STATEMENT OF THE HONORABLE MILANCY D. HARRIS, ACTING UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY, U.S. DEPARTMENT OF DEFENSE**

Ms. HARRIS. Chairman Bergman, Representative Panetta, and distinguished members of the subcommittee, it is a privilege to testify today on the current posture of the Defense Intelligence and Security Enterprise to confront the diverse array of global threats and challenges facing the United States of America and our allies and partners.

The intelligence and security experts across the Department of Defense work tirelessly to address current and future threats to our nation on a daily basis. On their behalf, thank you to the members of this subcommittee for your ongoing support and collaboration.

I am joined here today by the Director of the National Security Agency, Timothy Haugh, and Director of the Defense Intelligence Agency, Lieutenant General Jeffrey Kruse. They will be offering their intelligence-informed perspectives on how we support our warfighters and characterize the challenges facing the United States, our allies, and partners today and in the future.

We look forward to your questions on these challenges and how our enterprise is postured to meet them.

In addition to my remarks today, I have submitted a classified statement for the record detailing our fiscal year 2025 Military Intelligence Program budget request, providing further insight into our plans.

Our number one priority remains addressing our pacing challenge, the People's Republic of China. We seek a free and open Indo-Pacific Region that is peaceful and secure. Our network of regional allies and partners is deep, wide, strong, and committed to a shared vision of peace, stability, and deterrence.

The fiscal year 2025 President's Budget Request for the Military Intelligence Program postures the Defense Intelligence and Security Enterprise to support all of these efforts, and more.

The Department is also actively focused, with our NATO [North Atlantic Treaty Organization] allies, in support of Ukraine's defense against Russia's invasion. We must remain vigilant in safeguarding against a resurgent Russian threat to NATO, international security, and the rules-based order.

The Defense Intelligence and Security Enterprise is enabling the Department's response to the ongoing conflict between Israel and Hamas, as well as other crises in the Middle East involving the Houthis, Iranian-affiliated militia groups, and violent extremist organizations such as ISIS [Islamic State of Iraq and Syria] and Al Qaeda. We will continue to cooperate with allies and partners and leverage technology to build an enduring and sustainable counterterrorism posture to monitor and disrupt terrorist threats.

Regarding both the conflicts in Ukraine and Gaza, in order to continue the Defense Intelligence and Security Enterprise's support, it is vitally important that Congress approve the supplemental funding we have requested. That funding is urgently needed to support our allies and partners. If we walk away, that will signal that the United States is an unreliable partner and embolden would-be aggressors across the globe.

In our fiscal year 2025 budget request we seek to advance crucial programs in the following ways:

Providing the Department with an information and decision advantage over key adversaries, focused on the PRC [People's Republic of China];

Operationalizing defense intelligence and security partnerships across the Department, U.S. Government, our allies and partners, and the private sector;

Elevating security and counterintelligence to the maximum extent across the Department, and;

Identifying, recruiting, training, and retaining a workforce capable of supporting our mission requirements.

Finally, before I close I want to emphasize how critical it is for Congress to reauthorize Section 702 of the Foreign Intelligence Surveillance Act before it expires on April 19th.

Additionally, recently proposed legislation has sought to limit DoD's lawful and appropriate access to and use of commercially available information, or CAI, which is used to support the full spectrum of DoD [Department of Defense] missions. CAI is lawfully obtained by DoD and subject to stringent handling procedures to protect the privacy and civil liberties of U.S. persons.

It is important for the effectiveness of the Defense Intelligence and Security Enterprise that DoD and Congress have the opportunity to collaborate on legislation so as to preserve appropriate access to this data.

In summary, the President's Budget supports the Department's programs and authorities needed to address these global challenges, maintain our strategic advantages, and provide decision-makers and policymakers with information at the speed of relevance.

With that, I again thank the members of this subcommittee for your leadership and support. And I look forward to answering your questions here, and in our closed session.

I will now turn to General Haugh for his remarks.

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

Mr. BERGMAN. General Haugh, you are recognized.

**STATEMENT OF GENERAL TIMOTHY D. HAUGH, USAF, COMMANDER, U.S. CYBER COMMAND, DIRECTOR, NATIONAL SECURITY AGENCY**

General HAUGH. Chairman Bergman, Representative Panetta, and distinguished members of the committee, I am honored to be with you today representing the men and women of U.S. Cyber Command and the National Security Agency.

Defending the nation is the heart of our mission. The People's Republic of China poses a challenge unlike any our nation and allies have faced before, competing fiercely in the information domain. The men and women of U.S. Cyber Command and NSA continue to use the full scope of our authorities and the full spectrum of our capabilities to contest the threats posed by the PRC, imposing costs, denying benefits, and deterring the adversary.

We will continue to strengthen partnerships across the U.S. Government, with foreign partners, and with private industry so that we may operate anywhere we are needed. We are ready and postured to contest PRC malicious activities, at home and abroad.

While cyberspace threats have increased, we are ready to counter these threats with increased strength and capability. U.S. Cyber Command and NSA [National Security Agency] continue to use capabilities and partnerships to deny the PRC opportunities, frustrate their strategic efforts, and systematically eradicate intrusions. Our cybersecurity mission is protecting the Department of Defense and the Defense Industrial Base from adversary nation-states and ransomware attacks.

We are collaborating with U.S. Government partners and foreign partners to develop and execute intelligence-driven campaigns to counter adversary activities. In addition, we continue to identify and share adversary tools and tradecraft, enabling public and private partners to further defend against these threats.

Within U.S. Cyber Command and NSA we are making investments in our workforce. Our talented, agile, and diverse people represent an important competitive advantage across all of our mission sets. That is why we are committed to reducing the time our new applicants spend in the hiring process, and strengthening our

expertise, both in-house and through hiring, especially those with language and technical skills.

I remain focused on the reauthorization of Title VII of the Foreign Intelligence Surveillance Act, which is of paramount importance. FISA [Foreign Intelligence Surveillance Act] Section 702 is absolutely critical to our foreign intelligence mission. There is no substitute for this authority. The timely, actionable information it provides cannot be replicated by other means.

As you consider reauthorization, I look forward to discussion how this tool enables mission success and the controls we implement to ensure the protection of the privacy and civil liberties of the American people.

I would like to reiterate my appreciation for the opportunity to testify in front of you today, and for the committee's continued support of our mission and our people.

I look forward to our conversation.

[The prepared statement of General Haugh can be found in the Appendix on page 30.]

Mr. BERGMAN. Lieutenant General Kruse, you are recognized.

**STATEMENT OF LIEUTENANT GENERAL JEFFREY A. KRUSE,  
USAF, DIRECTOR, DEFENSE INTELLIGENCE AGENCY**

General KRUSE. Chairman Berman, Representative and today's Ranking Member Panetta, distinguished members of the subcommittee, thank you for this opportunity to discuss the Defense Intelligence Agency's assessment of the global security environment.

The complexity, trajectory, and rate of change in the national security arena is perhaps the highest and most consequential we have seen in our lifetime. How we respond matters, and our level of innovation, focus, and integration must match our adversaries stride for stride. We must position ourselves and our capabilities to meet the threats we see now and on the horizon, and not simply posture to repeat successes of the past.

DIA and our global workforce in more than 140 nations around the globe, partnered with our colleagues all across the nation and in the defense intelligence community are at the forefront of this task, collecting, analyzing, and operationalizing intelligence that underpins policy, diplomacy, acquisition and, when needed, combat operations.

It is an honor to join two of my colleagues in this endeavor, Honorable Harris and General Haugh, before the committee today.

In my first 2 months as the 23rd director of the Defense Intelligence Agency, I have taken a threefold approach to setting our course:

First, we are intensely integrated with and focused on meeting the needs of our warfighters and our allies and partners who are engaged in combat operations around the globe.

Second, we are addressing new and emerging security and intelligence challenges that fundamentally alter our operating environment, ranging from technology and artificial intelligence to cyber and biosecurity, to a growing number of adversaries who are interacting and partnering in ways and towards ends we have not seen before.

In these specific areas I have started three 90-day sprints addressing foundational military intelligence for cyber, the need for integrated force tracking in benign environments, and technical intelligence collection.

Finally, I have focused on partnerships, the one asset our adversaries simply cannot match. I have had more than 30 international engagements, to include hosting more than 70 foreign military representatives in my first 60 days. Simply stated, the scale of national security challenges require a new scale in effective national security partnerships.

My aim in this hearing is to crystallize these challenges and growing threats that we see and support this subcommittee in its critical work of defending the nation. One of the ways Congress can provide its most effective support and defense of the nation is to reauthorize Section 702 of the Foreign Intelligence Surveillance Act. Although DIA [Defense Intelligence Agency] collection does not operate under these specific authorities, our all-source analysis mission, our ability to operationalize intelligence, and our support to the Congress is dependent on those who do.

Thank you for the opportunity to appear before the subcommittee today. I am privileged to lead the Defense Intelligence Agency and represent the talented and dedicated global workforce.

We are grateful for your continued support. And I look forward to your questions.

[The prepared statement of General Kruse can be found in the Appendix on page 35.]

Mr. BERGMAN. Thank you.

I recognize myself for five minutes.

First one: question is for you, General Haugh.

Can you explain how your dual hat as Director of NSA and Commander of CYBERCOM [U.S. Cyber Command] has benefitted the intelligence community as well as the cyber community?

General HAUGH. Thank you very much for the question, Chairman.

So, from what the determination as to how we looked at the structure of both Cyber Command and NSA, so having a single leader that is able to lead both organizations. What it really benefits from both the intelligence community and from cyberspace is how we operate within the same operating domain within cyberspace and with common partners. We are able to have agility, we are able to operate with speed, and able to operate with a common intent.

What that really helps from an intelligence community perspective is that as we think about the campaigns that are going to be conducted in cyberspace we can start with how are we going to protect those key intelligence sources and methods that allow the nation to have insights, that allow our combatant commanders to have indications and warning, while able to generate outcomes in cyberspace that meet the demands of our warfighters.

That speed and agility was something that was looked at closely when, in July 2022, both the DNI [Director of National Intelligence] and the Secretary of Defense commissioned a joint study. They wanted to look at the dual hat construct.

Their conclusion was that it was in the best interests of the nation, and for many of those same reasons, to be able to move with speed and agility, the ability to have a common conversation, particularly with our foreign partners about how we partner together in cyberspace, and then how we can move aggressively when we see threats to the nation and the Department of Defense.

So, I have served in both organizations for the preponderance of my career and am very comfortable in terms of how we execute every single day for both our intelligence mission and our cyber mission.

Mr. BERGMAN. Thank you.

The next question is for all of you for a response.

The DNI and CIA [Central Intelligence Agency] produced an open-sourced intelligence strategy for 2024 to 2026 last month. How do each of you envision implementing the strategy, especially with the capability of AI [artificial intelligence] and machine learning, to (1) call down the trove of information into a manageable amount for further analysis, and (2) getting ahead and staying ahead of our adversaries?

So, please.

Ms. HARRIS. Thank you for the question.

I will take it from a little bit of the Department's perspective before deferring to the directors on their specific enterprise efforts.

From the Department's perspective, the DNI strategy is one part of how we think about the open source ecosystem. In the Department of Defense we are very focused on making sure we make the maximum use of open source information, to include commercially available and publicly available information.

And for the portions of the Department that sit in the IC [intelligence community], we are focused on making sure that there is a framework in which they understand how to use that information to the maximum degree possible.

General HAUGH. From the NSA perspective, we do not have an open source intelligence mission, but we certainly do leverage publicly available and commercially available information.

What we found most benefit from the overall strategy itself, it reaffirms how we handle information, how we use it, and then how we protect it in a manner consistent with all of our oversight, and all of our laws, all of our values. So, we leverage that information. It is a critical start point for us, and being able to, particularly, fill in gaps when we think about cyber threats. It is an area that we have leveraged very deeply and we will continue to follow the guidelines we have been given by the Department.

General KRUSE. Thank you for the question.

For DIA in particular, we are also designated as a Defense Intelligence Enterprise manager for open source intelligence. So, we do this mission each and every day. And as that enterprise manager we are also deeply involved in how the rest of the enterprise is able to pull together the tactics, techniques, procedures that are associated with this particular discipline.

The approach that DIA has taken since being designated as this is to take all the steps that are necessary to turn open source into the same kind of discipline that we see in signals intelligence, in

geospatial intelligence, in measurement and signals intelligence. How do we normalize that?

So, across the board DIA has put together a program, and it starts to deliver this year. And it is designed to put a structure around everything from requirements management, how do we do collection, what's the tradecraft associated with analysis, how do we do data management across multiple organizations? What does a training program look like, for whether it is us or whether it is the services that are doing open source?

And then, more importantly, how do we do the data cataloging? So, open source data is purchased or collected by one organization; we are not doing it across multiple organizations.

We will deliver on the first iteration of that later this year. And over a couple of years we intend to institutionalize open source across the Department.

Mr. BERGMAN. Thank you.

Mr. Panetta, you are recognized.

Mr. PANETTA. Thank you, Mr. Chairman.

General Haugh, Russia and China are using sophisticated hybrid and irregular warfare tactics while harnessing cyber and technological advantages, as we have seen over the past decade for sure.

It has been abundantly clear that also in Ukraine, where the forces have merged advanced technology with irregular warfare tactics to increase precision on the battlefield and control the information space.

To maintain our advantage the United States should be looking at new ways, similar to how the Ukrainians did it, to integrate our Special Forces capabilities with advancements in cyber and information operations.

General, can you explain how USCYBERCOM is working with SOCOM [U.S. Special Operations Command] to integrate cyber and soft capabilities?

And then, second, what is your assessment of Russia's utilization of both cyber and irregular warfare capabilities?

General HAUGH. Thank you very much for that question.

So, first, how do we think about our partnership with the U.S. Special Operations Command?

We look at that they are teammates in all of the missions that we consider. And so, first, both of us do things in support of the other combatant commands and our responsibilities. We will do those independently and we will conduct operations that are linked to those combatant commands.

But what we are increasingly finding, that there are times where we are able to look at something that the Geographic Combatant Commander needs, and if we work together with our Special Operations teammates, with our Space teammates, we can identify opportunities that allow us to produce an effect that would be larger than any of us operating independently.

Mr. PANETTA. Can you give me an example?

General HAUGH. So, there are things that we do in cyberspace that would require someone to be in theater and to leverage what a special operator would be doing in-country or in an environment that we don't reach as U.S. Cyber Command.

So, that is a partnership. We leverage that. And then we are able to extend our reach with our Special Operations partners.

That would be an example.

Mr. PANETTA. Thank you.

General HAUGH. The other area that in terms of Russia's evolution, your, your second part of your question, I think what we saw at the outset of the conflict is Russia operated in cyberspace in the same manner that they did in all the other domains. Not well planned, it was brute force.

But we also saw Ukraine take actions that we should learn from. They were very effective in moving their data outside of the country using Western cloud providers. Gave them resiliency.

And then they also drew upon any number of nations, including the United States, for additional cyber defense activities. So, they were very effective at the outset.

What we have seen is an evolution of how Russia continues to use their cyber forces. And I think one of the areas that we want to watch really closely is how they're using those forces from an intelligence aspect versus the cyber effect. And it is an area that we will want to watch closely and inform our European Command teammates.

Mr. PANETTA. Thank you.

General Kruse, last year we discussed the USCYBERCOM, NSA, China Outcomes Group and the DIA China Mission Group. Can you give us an update on those organizations and how they collaborate with these other?

And if you can answer as much as possible now, we can follow up in greater detail in the classified session, obviously.

General KRUSE. In this session I would certainly be happy to cover, in particular, the China Missions Group within DIA, a little bit of how we partner. And the -- I will certainly let General Haugh talk to the China Outcomes Group.

So, a little over a year ago my predecessor, after a series of studies, put together the requirement if China is our pacing threat, how do we integrate all the activities that we do, whether it is collection, whether it is analysis, whether it is protection of our own networks?

And how do we do that in a way that we can then build some campaigns to create the effects that we need, both to advance our interests, advance our collection, or to protect ourselves.

So, the China Mission Group that we put together pulls together for the first time all of our HUMINT [human intelligence] collectors, all of our analysis, all of our effects generators, if I could use that term in this environment, and stitches together what we might do with our service partners and with our interagency partners, to include the China Outcome Group, and very much focused on ensuring that we are taking, identifying collection gaps, and tasking either ourselves or others to fill those collection gaps in order to create the out-take, the outcomes that we need.

And one of our important partners is certainly the China Outcomes Group.

Mr. PANETTA. General Haugh, on the China Outcomes Group?

General HAUGH. So, the China Outcomes Group is a combined effort between NSA and Cyber Command to align our resources in

support of INDOPACOM [U.S. Indo-Pacific Command]. So, we have a series of priorities that we have been given by the INDOPACOM commander, and that has allowed us to really look at how would we provide intelligence today? How would we do that in a crisis? How do we think about network defense and cybersecurity, both for INDOPACOM and for their partners?

And then, if we get into a crisis, what are the things that U.S. Cyber Command and NSA can do to assist in generating options for the INDOPACOM commander?

That continues to work very well and very closely with the INDOPACOM team.

And I can give you more details in the closed session.

Mr. PANETTA. Thanks to all of the witnesses.

I yield back.

Mr. BERGMAN. Thank you.

Dr. Jackson, you are recognized for five minutes.

Dr. JACKSON of Texas. Thank you, Mr. Chairman. And thank you to our witnesses for being here today. Really appreciate your time.

Accurate and actionable intelligence for our Joint Force is a key component of all of our operations. A well-informed intelligence picture from the Defense Intelligence Enterprise will be key for decision-makers and military leaders in understanding the potential battle space in the Indo-Pacific should a conflict with China arise.

Similar to other resources across the Department, the Defense Intelligence Enterprise cannot neglect other AORs [area of responsibility] and miss an intelligence collection opportunity. The risks remain in those AORs and we have a duty to be properly postured.

My first question is while we must face -- while we must focus on countering the Chinese Communist Party and their coercive actions, there are very real threats to our national security that exist at our own southern border. In recent years we have seen a disturbing trend of known terrorists and Chinese military age males coming across our southern border.

As violent extremist organizations and our adversaries continue to become more bold and expand their reach, I am very concerned about the threats to our homeland. And our intelligence will ultimately prove to be probably our greatest defense against these possible threats.

General Kruse, I will start with you.

Do you have any concerns -- but I will ask this of all of you -- do you have any concerns about the threats that may have or potentially could come across our southern border based on the increased number of known terrorists and Chinese military age males who have crossed our border?

And how has that increased your workload?

And are we adequately resourced to remain vigilant regarding these threats while simultaneously focusing necessary resources on INDOPACOM?

General KRUSE. So, let me answer that two ways.

One is one of the advantages that DIA has in its very complex mission is that in addition to DIA itself at the headquarters, we also man the J2s [J-2 Joint Staff] at each of the combatant commands. And that gives us an ability to stay connected to each of

the combatant commands' threats, and that includes NORTHCOM and SOUTHCOM as you are tracking today.

So, we are infinitely involved, either directly at the headquarters or at the commands working the migration issues, the human issues or, in the other case you mentioned, PRC coming across the southern border.

We are always concerned about what may come across the southern border. We have not seen to date the things that would cause us to notify you of increased concern. But that is always a pathway.

And more to talk. I would be happy to talk more in detail when we get to the classified session.

Dr. JACKSON of Texas. Yes, sir. Thank you.

General HAUGH. Congressman, as we look at the southern border, we just recently participated, the DNI led a look at how could we, as an intelligence community, examine how we could better provide intelligence as it looks at fentanyl and how it makes its way to the United States.

As we look at that, I think from our perspective in the National Security Agency we are proud of the work that we have done to be able to illuminate threats. The area that I am probably the most concerned about is we are illuminating most of those threats from Section 702.

That has allowed us to see what it looks like for precursor chemicals coming from companies in China, how they make their way to Mexico, and then how criminal organizations can then move those.

So, I am concerned that we are going to lose our opportunity for those insights unless Section 702 is reauthorized.

Dr. JACKSON of Texas. Thank you. That is helpful.

Ma'am?

Ms. HARRIS. Thank you for the question.

I am confident that the Defense Intelligence Enterprise is fully engaged on these issues. Many of them are a whole of government effort. They cross domestic and foreign intelligence. And so, we have, I have full confidence that our agencies are fully engaged in that effort.

From my seat, I am constantly monitoring the resource trade-offs, that includes making sure we are making the right investments and we are not taking unnecessary trade-offs, particularly in the counterterrorism space.

Dr. JACKSON of Texas. Okay. I have one more question kind of related to that, to the funding issue.

But, you know, funding for Defense Intelligence Enterprise is split into two major components: the National Intelligence Program and the Military Intelligence Program. For fiscal year 2024 it looks like the National Intelligence Program is funded at 72.4 billion, and the Military Intelligence Program is funded at 29.3 billion, for a grand total of 101.7 billion.

For fiscal year 2024 the request actually appears to show a slight decrease, for a total funding of 101.6 instead of 101.7. When you factor in the record inflation that we have seen over the last few years, this is really a pretty severe cut.

So, my question is if I can get some more details on exactly what the issues are in the classified session. But I would like to ask each

of you real quickly, are we adequately resourcing the Defense Intelligence Enterprise?

How are we justifying cutting funding for the Defense Intelligence Enterprise at a time like this when we need to ensure that our intelligence is rock solid?

Ms. HARRIS. I am happy to go into further detail in the closed session. But I am confident that there has not been a decline in capability in the Military Intelligence Program, which is the portion I can speak to.

I think that the decline that you note is due mostly to phased program acquisitions and other factors which I am happy to dive into in further details. But I am confident that we have not made a reduction in capability, particularly within the MIP [military intelligence police].

Dr. JACKSON of Texas. Okay. I am out of time. But does one of you want to say something real quick? Otherwise I will yield back.

General HAUGH. I would prefer to talk about it in the closed session, if you don't mind, Congressman.

Dr. JACKSON of Texas. Yes, sir.

General KRUSE. I would be happy to do the same.

Dr. JACKSON of Texas. Thank you. I yield back. Thank you.

Mr. BERGMAN. Representative McClellan, you are recognized for 5 minutes.

Ms. MCCLELLAN. Thank you, Mr. Chairman, and Ranking Member Panetta, and to our witnesses for being here today.

Secretary Harris, one of the key take-aways from the post-9/11 era was the importance of our intelligence community working together and across agencies to tackle the threats that face the nation.

How did the Defense Intelligence Enterprise work to increase collaboration with the rest of the intelligence community in fiscal year 2024?

And what can we expect in fiscal year 2025?

Ms. HARRIS. Thank you for the question.

I think what I can offer is that I think we have only taken the lessons of the 9/11 era and applied them to new and different challenges. So, as I remarked before, I see the entire Defense Intelligence Enterprise really operationalizing our partnerships, which means we are no longer just working independently with partners but we are thinking about the way different agencies can partner with our allies and partners in service of common objectives.

I think you have heard already today some examples of joint work that is going on inside of the Department to make sure that we are approaching things with a new and different informed view that takes into, takes into account all of the different talents and capabilities that exist inside the Department and uses them to maximum effect.

Ms. MCCLELLAN. Thank you.

For each of you, what is the most pressing capability gap facing the Defense Intelligence Enterprise and your specific agency?

What are you doing to mitigate these gaps?

And what support do you need from us to help you do so?

General HAUGH. Congresswoman, I think from our perspective the areas that the Department has really asked us to look at is re-

siliency. How do we think about ensuring that we can deliver intelligence in competition and in crisis, and if deterrence fails, in conflict?

And I think those are areas that we are going to really examine closely. And those are things that you will see coming through the Department in terms of budget requests as we look at those areas the Secretary is asking us to focus on.

Ms. MCCLELLAN. Thank you.

General KRUSE. I think what I would offer is that our most pressing capability gap, really not just for us but for everyone, when asked this question I always actually go to a non-traditional route and I say the thing that I am most concerned about is our ability to protect our networks, our people, and our data.

So, whether that is a counterintelligence piece, whether it is security of our highly classified networks, whether it is the Defense Industrial Base, it is focused on those efforts that we need to do there.

We are all working those. And I think what you will see in the budget that has already been submitted are the kinds of programs that will help us in that regard.

Ms. MCCLELLAN. Thank you.

And, General Kruse, how is the Defense Intelligence Enterprise looking to incorporate emerging technology such as AI into its capabilities, and to ensure that these new capabilities will provide the most relevant information for our warfighters?

General KRUSE. Thank you for the question.

We have established an emerging and disruptive technologies organization that is focused really in three areas: one is on quantum, and that is doing some really good work on how others are using quantum computing, quantum comms, and quantum sensing.

We have an organization that is focused on biotechnology and biosecurity.

And then another group that is working specifically on AI and counter-AI. And we can certainly talk through what some of those lines of efforts might look like.

We also have a sort of a technology and long-range assessments organization that is looking out in the 5 to 20 year point to see what technology are in research and development stages that may not necessarily be military technologies yet but could be, if applied. And we track those through that position.

Ms. MCCLELLAN. And for some of the work that you are doing in the AI space, what steps are you taking to ensure that you can identify misinformation that our adversaries may be using through AI?

And the context of the question -- I know I am about to run out of time, so you may have to submit an answer later -- 5 years ago I was at a conference where an expert said that the ability of AI to detect misinformation was going to be outpaced by the ability of AI to create misinformation.

And I have been worried about that for five years. So, if you could provide some information on what you all are doing to try to get ahead of that?

General KRUSE. I would be happy either to take that for the record or answer that in classified session.

[The information referred to can be found in the Appendix on page 82.]

There is some important work. Your concerns are very valid. And it is an issue we have got to stay a step ahead of.

Ms. McCLELLAN. Thank you.

I yield back.

Mr. BERGMAN. Thank you.

Mr. Mills, you are recognized for five minutes.

Mr. MILLS. Thank you, Mr. Chairman.

Thank you to our distinguished guests for being here today.

We have got into a very bad habit of continuing our 1980s fashion of understanding warfare to only be kinetic, which has been a really big missed opportunity for us. Knowing that the evolution of warfare has truly gone to an economic, resourced, cyber supply chain, and even a non-kinetic influence operation campaign.

You know, I argue to many that we have been in a cold war for about 20-plus years with China as they continue to advance their influences, and also to degradate America's confidence in our currencies, or in developing nations that they are moving away from utilizing American goods as well as for using our currency as its primary source.

In knowing this, what is it that, in my belief personally with the China-Russia-Iran-North Korean geopolitical alignment, could we not utilize the quantum raters, especially looking at things like AI quantum entanglement, self-healing drone capabilities, and others, to be utilized in a very similar fashion to what President Reagan utilized the Space Race for against the Soviet Union, as a way to try to go ahead and economically cripple them, knowing the PRC's economics are not where they claim it is at, and seeing that they have more workforce strikes in the past years than they have in ever its history?

General HAUGH. So, Congressman, I will touch on the quantum discussion as a start point and then go wherever you would like to go.

So, as we think about quantum we are really thinking about it in two ways:

First, we have a research organization that has been involved in quantum research since its inception. Really sponsored some of those original studies that enabled the original qubit to be employed. So, we continue to partner with academia, with industry to look at what are the most appropriate applications when we think about quantum.

The other is how do we prepare the nation for a quantum computer to ensure that we have got quantum-resistant encryption?

So, NSA has published our first round of quantum-resistant encryption. That is an area that we want to work with the rest of the Department to ensure that we deploy so that we are prepared when the event that quantum computer is developed and employed. So, I think that is an area that we are certainly invested in. And we want to continue to advance.

Mr. MILLS. And you think that the quantum entanglement capability is advancing at a pace that will see us beat China in that race?

General HAUGH. I think this is one that is really difficult science. And so, I think it is one we want to make sure as a nation from our perspective, with the resources that we have, we will employ to continue to drive that research forward.

Mr. MILLS. I appreciate that.

Yeah, my hope is that we can get to a point where quantum entanglement can be utilized in a multi-drone fashion that would be able to be deployed to kind of leave our enemies blind, deaf, and dumb on the battlefield to give us that advantage for the warfighters abroad.

Ms. Harris, I wanted to ask you your thoughts on, you know, how can we leverage our JSOC [Joint Special Operations Command] capabilities, relationships with allies in the regions to counter China's efforts with regards to Africa?

Ms. HARRIS. I am happy to talk in a little bit more detail in closed session.

But I think what we have seen is that those partnerships are not just belonging to one organization. And I think where we have worked best is where our partnerships inside DoD are combined with those of our diplomats, and those of USAID [U.S. Agency for International Development], and other U.S. Government entities that are working in the region to really deepen the conversation, understand the different dynamics at play, and figure out how best to work together.

Mr. MILLS. And I guess kind of a follow-on to that because I am just curious is, you know, how can we shorten the decision-making process between the intelligence community and our respective agencies or teams on the ground?

Ms. HARRIS. Sir, I think that that is work that is ongoing every day. I think we have come a long way in shortening that cycle.

I think we have a focus right now in making sure we are sharing information quickly. We are proactively making sure that information is releasable to our partners, that conversations can happen at the lowest level classification that they need to. All of that speeds the pace of decision making and the ease of getting information out to our operators.

Mr. MILLS. And I know that you all, and again I also can speak to sitting in classified briefings and other areas where we have seen applies that play a very vital role with regards to preventing terrorist attacks by malign actors. But I would also argue that the FBI [Federal Bureau of Investigation], who has violated that, utilizing backdoor searches at least 287,000 times, without appropriate reforms these types of warrantless searches would be in direct violation of the Fourth Amendment.

Would you not agree?

Ms. HARRIS. I can speak to what the current bill offers, which I think is a meaningful set of reforms that gets at some of the concerns that have -- that you raise.

I think that we have made a number of reforms in response to concerns. But the bill right now is the most comprehensive reforms that we would have, will ever been made to Section 702.

Mr. MILLS. Well, I agree that there are some reforms. The FBI is reporting they have 98 percent compliance. But if you look at the over 200,000 violations they have, that is still over 4,000 a year

that they are violating with these illegal warrantless searches that are in direct violation of our Fourth Amendment.

And as constitutionalists and those who swear an oath, that is our job to protect our Constitution against all enemies foreign and domestic, and that means the violations that are by Government as well.

With that, I yield back.

Mr. BERGMAN. Mr. Keating, you are recognized for 5 minutes.

Mr. KEATING. Thank you, Mr. Chairman.

2 days ago The Wall Street Journal published a report about the private sales of Starlink assets and the shipping them, the shipping of them to Russians. Battlefield resources -- I am sorry -- battlefield sources in Ukraine.

Can you comment about the threat of these private sales, the public sales or through the black market and, you know, what the effect can be on the battlefield in Ukraine?

But also what it can be in the hands of non-state actors?

[The information referred to can be found in the Appendix on page 81.]

Ms. HARRIS. I am happy to discuss that question in more detail in a closed session.

I think we have a number of efforts ongoing to address some of these issues. But I would need to take that for the record, as not all of them fall within my remit within the Department.

Mr. KEATING. Just looking at the, you know, the forming axis of Russia, China, Iran, and North Korea together, and could you comment on their, to the extent you can publicly, on the information sharing that might have resulted in that closer relationship, and what we could do ourselves to do to try and make sure we are not falling into siloing things that we have in the past, and that we have on our part greater information sharing across the board given the expansion of the cooperation of those with that axis?

General HAUGH. So, I can take some of this, Congressman.

Because I think one of the things that we have worked really hard on since the beginning of Russia-Ukraine is how do we use intelligence to be able to have the greatest impact possible, and how all the elements of the CSAs[OM1] within the Department and within the community we are able to generate intelligence that can either be used by the Administration to identify what Russia is doing, but also to inform our combatant commands.

And I think we have really worked on the tradecraft of how do you use intelligence not just for military targeting but to create an outcome that gives some advantage? So, in this case, how do we expose those activities in a way that someone could take an action based on it?

And we could talk in a little bit more detail in the closed session.

Mr. KEATING. Do you think that -- Oh, go ahead. I am sorry.

Do you think that any of this information sharing is a threat, that particularly given Iran in the least, of sharing this with their proxy militia forces, malign forces that they have?

General HAUGH. So, I think from our perspective, or from my perspective as they collaborate it brings the potential for transfer of different technology or intelligence, we want to be able to limit that wherever we can.

General KRUSE. I would offer to -- it is a great question to kind of think through what is it that the coordinations in particular that you talked about, Russia, China, North Korea, and Iran, what are they doing now that they weren't doing before? And what are they increasing?

And I think what we have seen is the relationships that Russia has had to build in order to bring ammunition stocks and other weapons to them, some of the historic friction that has existed between those countries has going by the wayside.

And what we don't know is what is North Korea, what is China, what is Iran getting in return?

The information flow that we expect they are getting in return is more about technology, more about capabilities. It is less focused on sharing information about the U.S. But that said, they have shared common interests in their views of what is the role in the U.S. and future versus their roles in the future.

And I would be remiss if I did not go back to your question on Iran and proxies. We do see information sharing with Iran and their proxies, but it is more related about creating effects in the battle space that Iran would like to do that hide its hand.

Mr. KEATING. I think with the race that is going on between the development of artificial intelligence and then our ability to deal with that artificial intelligence, how to react to that on our own -- you will have to deal with this in classified, I understand -- but also on a general sense our enemies, some of the countries I just mentioned, are they in a situation where you see them developing that kind of capability, too, to counter that as well, to keep up with it on the responding side of it?

General KRUSE. I think what I would offer is there is at least two of those four countries that are deeply focused in that area. And in the classified session we can talk it in more detail.

Mr. KEATING. Okay. Well, thank you very much.

I yield back, Mr. Chairman.

Mr. BERGMAN. Ms. Jacobs, you are recognized for 5 minutes.

Ms. JACOBS. Thank you, Mr. Chairman. And thank you so much to our witnesses.

I know we talked a little bit about Africa and what we are doing there. I wanted to ask a little more specifically how we are sort of learning lessons and thinking strategically about maybe some of the things that we are missing in Africa, and making sure, you know, that we are looking not only at sort of targeting, but also the dynamics and population.

You know, for instance, despite all of the investments and access we have made in West Africa, the inter-agency was caught surprised by the coup in Niger despite the huge amount of military assets that we have in that country.

So, I guess, Lieutenant General Kruse, can you share how and why, as much as you can in open hearing, we didn't anticipate the coup in Niger; what lessons we have learned from that; and how DIA is working to ensure we are gathering intelligence that is more focused on local political and conflict dynamics, particularly in places where we do have big foreign military relationships?

General KRUSE. Thank you for the question.

And I would offer a little bit of framing and then the answer.

So, for me the framing that really has resulted in I think eight military coups in Africa since 2020 are tied to a combination of many things. It is humanitarian issues, it is food insecurity, it is migration, it is terrorism, it is a variety of things that no amount of military presence can, you know, overturn.

And so, when there is a military presence there, what that does allow us to do is one of the other organizations that we run, the Defense Attache Service, and the Defense Clandestine Service, and that does allow us to have a footprint with embassies in all of the nations around the globe, that allows us to have interagency conversations to see what it is that we can detect and what we can do about it.

And I think in a classified setting we can talk a little bit more about what we saw leading up to Niger and perhaps what we are doing about it.

Ms. JACOBS. Okay, great.

Are there any broad lessons learned on how you are doing things different based on sort of what happened in the Sahel with the eight coups over the past few years?

General KRUSE. I actually think it is too early to understand how those are playing out in a couple of areas. And there are a lot of activities still ongoing.

I think the biggest lesson for us almost goes back to one of the previous questions, which is to ensure while we are focused on China, while we are focused on some of the high-end adversaries, one of the critical responsibilities of the intelligence community is to be that guardrail and keep a pulse in some of those other areas.

And so, for us it is about maintaining attache presence and other presence and collection within the areas we have talked about.

Ms. JACOBS. Got it. Thank you.

And I know some of my colleagues have asked about AI already. I wanted to ask particularly about AI and sort of the ethical principles.

I know DoD has adopted ethical principles. I think that is great. I think there are still a lot of questions about how those principles translate into actionable guidelines. And one of the things we have been hearing a lot of concern about is around AI drones, particularly ones using facial recognition, used during military operations.

So, I guess a question is how accurate is the facial recognition technology used by the AI drones?

And what measures have been taken to ensure that it doesn't produce false positives? For whoever wants to answer.

Ms. HARRIS. I think we are going to have to take that question for the record.

[The information referred to can be found in the Appendix on page 81.]

What I can tell you is that the Department is committed to ensuring the ethical use of AI. I think you have seen that the Department has put that priority first and foremost by elevating the position of our chief data and AI officer to a direct report to the Secretary.

There is a focus in the Department to make sure we both understand the challenges those tools will face, we will face on the bat-

tlefield, but also how best to integrate them into military operations.

But I am happy to take back the question for more details.

Ms. JACOBS. Thank you. Yes, I would appreciate that.

And you may have to take this back, too, then. Is there anything put in place to ensure that AI drones do not accidentally target innocent civilians during military operations?

Ms. HARRIS. Again, I will take the specific question back for the record.

[The information referred to can be found in the Appendix on page 81.]

But I think as you have heard many seniors from the Department say just this week on The Hill, civilian protection is at the forefront of all of our operations.

Ms. JACOBS. Thank you.

Mr. Chairman, I yield back.

Mr. BERGMAN. Thank you. Well, they have called votes. And the open portion of the hearing is now adjourned.

We will reconvene in Rayburn 2337 for the classified session at the conclusion of which, which right now we are looking at walking off the floor about 4:45 or 16:45. I am not going to give it in Zulu time, so we will just leave it at those two to figure it out.

But we will all walk back from the floor to 2337 as soon as possible after that, and we will reconvene there in the classified session.

This portion is adjourned.

[Whereupon, at 4:24 p.m., the subcommittee was adjourned.]

---

---

# **A P P E N D I X**

APRIL 11, 2024

---

---



---

---

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

APRIL 11, 2024

---

---



Remarks as prepared for the Honorable Milancy Harris  
Acting Under Secretary of Defense for Intelligence and Security  
At the House Armed Service Committee Hearing  
Subcommittee on Intelligence and Special Operations  
April 11, 2024  
*(As of 04/11/2024)*

(U) Chairman Bergman, Ranking Member Gallego, and distinguished members of the Subcommittee, it is a privilege to testify on the current posture of the Defense Intelligence and Security Enterprise to confront the diverse array of global threats and challenges facing the United States of America and our allies and partners.

(U) The intelligence and security experts across the Department of Defense work tirelessly to address current and future threats to our nation on a daily basis. On their behalf, thank you to the members of this Subcommittee for your ongoing support and collaboration.

(U) I am joined here today by Director of the National Security Agency, General Timothy Haugh, and Director of the Defense Intelligence Agency, Lieutenant General Jeffrey Kruse. They will be offering their intelligence-informed perspectives on how we support our warfighters and characterize the challenges facing as the United States of America, our allies, and partners today and in the future. We look forward to your questions on these challenges, and how our Enterprise is postured to meet them. In addition to my remarks today, I have submitted a classified Statement for the Record detailing our FY25 Military Intelligence Program budget request, providing further insight into our plans.

Remarks as prepared for the Honorable Milancy Harris  
Acting Under Secretary of Defense for Intelligence and Security  
At the House Armed Service Committee Hearing  
Subcommittee on Intelligence and Special Operations  
April 11, 2024  
*(As of 04/11/2024)*

(U) Our number one priority remains addressing our pacing challenge, the People's Republic of China (PRC). We seek a free and open Indo-Pacific region that is peaceful and secure. Our network of regional allies and partners is deep, wide, strong, and committed to a shared vision of peace, stability, and deterrence. The FY25 President's Budget Request for the Military Intelligence Program postures the Defense Intelligence and Security Enterprise to support all of these efforts, and more.

(U) The Department also continues to be actively focused, with our NATO allies in support of Ukraine's defense against Russia's invasion. We must remain vigilant in safeguarding against a resurgent Russian threat to NATO, international security, and the rules-based order.

(U) The Defense Intelligence Enterprise is enabling the Department's response to the ongoing conflict between Israel and Hamas, as well as other crises in the Middle East involving the Houthis, Iranian-affiliated militia groups, and violent extremist organizations such as ISIS and Al Qaeda. We will continue to cooperate with our allies and partners and leverage technology to build an enduring and sustainable counterterrorism posture to monitor and disrupt terrorist threats.

(U) Regarding both the conflicts in Ukraine and Gaza, in order to continue the Defense Intelligence and Security Enterprise's support, it is vitally important

Remarks as prepared for the Honorable Milancy Harris  
Acting Under Secretary of Defense for Intelligence and Security  
At the House Armed Service Committee Hearing  
Subcommittee on Intelligence and Special Operations  
April 11, 2024  
*(As of 04/11/2024)*

that Congress approve the supplemental funding we have requested. That funding is urgently needed to support our allies and partners. If we walk away, that will signal that the United States is an unreliable partner and embolden authoritarians and would-be aggressors across the globe.

(U) In our FY25 budget request, we seek to advance crucial programs in the following ways:

- (U) Providing the Department with an information and decision advantage over key adversaries, focused on the PRC;
- (U) Operationalizing defense intelligence and security partnerships across the Department, U.S. Government, and our allies and partners, and the private sector;
- (U) Elevating security and counterintelligence to the maximum extent across the Department; and
- (U) Identifying, recruiting, training, and retaining a workforce capable of supporting our mission requirements.

(U) Finally, before I close, I wish to emphasize how critical it is for Congress to act to reauthorize Section 702 of the Foreign Surveillance Act before the short-term extension of that authority expires on April 19<sup>th</sup>. Additionally, recently proposed legislation in Congress has sought to limit DoD's lawful and appropriate access to and use of commercially available information, or CAI, which is used to support the full spectrum of DoD missions. CAI is lawfully obtained by DoD and

Remarks as prepared for the Honorable Milancy Harris  
Acting Under Secretary of Defense for Intelligence and Security  
At the House Armed Service Committee Hearing  
Subcommittee on Intelligence and Special Operations  
April 11, 2024  
*(As of 04/11/2024)*

subject to stringent handling procedures to protect privacy and civil liberties of U.S. persons.

(U) It is important for the effectiveness of the Defense Intelligence and Security Enterprise that DoD and Congress have the opportunity to collaborate on legislation so as to preserve appropriate access to this data.

(U) In summary, the President's Budget supports the Department's programs and authorities needed to address these global challenges, maintain our strategic advantages, and provide decision-makers and policymakers with information at the speed of relevance.

(U) With that, I again thank the Subcommittee for its leadership and support, and I look forward to answering your questions here, and in our closed session. I will now turn to General Haugh for his remarks, followed by Lieutenant General Kruse.

## MILANCY D. HARRIS

*Acting Under Secretary of Defense for Intelligence & Security (Acting USD(I&S))*



Ms. Milancy Harris is the Acting Under Secretary of Defense for Intelligence and Security (USD(I&S)).

Ms. Harris was sworn in as the Deputy Under Secretary of Defense for Intelligence and Security (DUSD(I&S)) on January 3, 2023. As DUSD(I&S), Ms. Harris is the deputy to the USD(I&S) who is the principal intelligence, counterintelligence, and security advisor to the Secretary of Defense (SecDef) and the SecDef's principal representative to the Intelligence Community.

Ms. Harris served as the Deputy Assistant Secretary of Defense for Irregular Warfare and Counterterrorism from February 2021 until December 2022. In that position, Ms. Harris was responsible for developing policy guidance and overseeing the implementation of all policies, strategies, and plans related to the employment of special operations forces in counterterrorism, unconventional warfare, irregular warfare, direct action, special reconnaissance, foreign internal defense, counter proliferation, sensitive special operations, and hostage and personnel recovery activities.

Ms. Harris previously spent 15 years with the U.S. Government focused on intelligence analysis and counterterrorism. Previous roles included serving as the Chief of Staff of the Directorate of Intelligence at the National Counterterrorism Center (NCTC), Director for Counterterrorism on the National Security Council staff, and as Deputy Director, Emerging Issues Division at the Office of the Director of National Intelligence. Ms. Harris began her career as an intelligence analyst and held positions at NCTC and the Defense Intelligence Agency focused on warning, information operations, and emerging technologies and served as an intelligence briefer for the Office of the Secretary of Defense. Outside of government, Ms. Harris' work focused on governance and institution building for technology companies.

Originally from Wisconsin, Ms. Harris earned Bachelor of Arts degrees in International Affairs and English Literature from Marquette University and possesses a Master of Arts degree in Political Management and a Graduate Certificate in International Security Studies from The George Washington University. She lives in Arlington with her husband, Caleb.

OPENING STATEMENT OF

GENERAL TIMOTHY D. HAUGH

COMMANDER, U.S. CYBER COMMAND  
DIRECTOR, NATIONAL SECURITY AGENCY  
CHIEF, CENTRAL SECURITY SERVICE

BEFORE THE 118TH CONGRESS

HOUSE COMMITTEE ON ARMED SERVICES SUBCOMMITTEE ON  
INTELLIGENCE AND SPECIAL OPERATIONS

APRIL 11, 2024



(U) Chairman Bergman, Ranking Member Gallego, and distinguished members of the Committee, I am honored to be with you today representing the men and women of U.S. Cyber Command and the National Security Agency.

(U) Defending the nation is at the heart of our mission. The People's Republic of China (PRC) poses a challenge unlike any our Nation and allies have faced before, competing fiercely in the information domain. The men and women of USCYBERCOM and NSA continue to use the full scope of both organizations' authorities and the full spectrum of capabilities to contest the threats posed by the PRC, imposing costs, denying benefits, and deterring the adversary. We will maintain and strengthen partnerships across the U.S. Government, with foreign partners, and with private industry so that NSA and USCYBERCOM are able to provide the necessary support in furtherance of the National Security Strategy and the National Defense Strategy. We are ready and postured to contest PRC malicious activities, at home and abroad.

(U) While cyberspace threats have increased, we are ready to counter these threats with increased strength and capability. USCYBERCOM and NSA continue to use capabilities and partnerships to deny the PRC opportunities, frustrate their strategic efforts, and systematically eradicate intrusions. NSA's and USCYBERCOM's cybersecurity mission is critical to protecting the Department of Defense and the Defense Industrial Base from adversary nation-states and ransomware attacks. We are collaborating with U.S. Government partners and foreign partners to develop and execute intelligence-driven campaigns to counter adversary activities. In addition, we

continue to identify and share adversary tools and tradecraft, enabling public and private sector partners to further defend against these threats.

(U) Within USCYBERCOM and NSA, we are making investments in our workforce. Our talented, agile, and diverse people represent an important competitive advantage across all our mission sets. That is why we are committed to reducing the time our new applicants spend in the hiring process, and strengthening our expertise, both in-house and through hiring, especially those with language and technical skills.

(U) I remain focused on the reauthorization of Title VII of the Foreign Intelligence Surveillance Act (FISA), which is of paramount importance. FISA Section 702 is absolutely critical to our foreign intelligence mission. There is no substitute for this authority – the timely, actionable information it provides cannot be replicated by other means. As Congress considers reauthorization, I look forward to discussing how this tool enables mission successes and the controls we implement to ensure the protection of the privacy and civil liberties of the American people.

(U) I would like to reiterate my appreciation for the opportunity to testify in front of you today and for this Committee's continued support of our mission. I look forward to our conversation.



## GENERAL TIMOTHY D. HAUGH

Gen. Timothy D. Haugh is Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service at Fort George G. Meade, Maryland.

Gen. Haugh received his commission in 1991 as a distinguished graduate of the ROTC program at Lehigh University. Gen. Haugh has commanded at the squadron, group, wing, numbered air force and joint levels. He served on staffs at major command, agency and combatant command headquarters.

### EDUCATION

1991 Bachelor of Arts, Russian Studies, Lehigh University, Bethlehem, Pa.  
1999 Master of Science, Telecommunications, Southern Methodist University, Dallas, Texas  
2005 Master of Science, Joint Information Operations, Naval Postgraduate School, Monterey, Calif.  
2010 Master of Science, National Resource Strategy with a concentration in Information Operations, Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C.

### ASSIGNMENTS

1. June 1992–December 1992, Student, Signals Intelligence Officer Course, Goodfellow Air Force Base, Texas
2. January 1993–September 1995, Flight Commander, 301st Intelligence Squadron, Misawa Air Base, Japan
3. October 1995–July 1998, Commander, Detachment 2, 544th Intelligence Group, Sabana Seca, Puerto Rico
4. August 1998–June 2001, Chief, Information Operations Technology Integration, Headquarters Air Intelligence Agency, Kelly AFB, Texas
5. June 2001–June 2004, Information Operations Project Officer, Headquarters U.S. Air Force, the Pentagon, Arlington, Va.
6. July 2004–September 2005, Student, Naval Postgraduate School, Monterey, Calif.
7. September 2005–June 2007, Director of Intelligence, Air Force Special Operations Forces, Hurlburt Field, Fla.
8. June 2007–June 2009, Commander, 315th Network Warfare Squadron, Fort George G. Meade, Md.
9. July 2009–June 2010, Student, Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C.
10. June 2010–June 2011, Chief, Intelligence, Surveillance, and Reconnaissance Division, 609th Air Operations Center, Al Udeid AB, Qatar
11. July 2011–July 2013, Commander, 318th Information Operations Group, Joint Base San Antonio-Lackland, Texas
12. July 2013–June 2014, Assistant Vice Commander, Air Force Intelligence, Surveillance, and Reconnaissance Agency, JB San Antonio-Lackland, Texas
13. June 2014–May 2016, Commander, 480th ISR Wing, JB Langley-Eustis, Va.
14. June 2016–June 2017, Deputy Commander, Joint Task Force-Ares, U.S. Cyber Command, Fort George G. Meade, Md.
15. June 2017–June 2018, Director of Intelligence, U.S. Cyber Command, Fort George G. Meade, Md.
16. June 2018–August 2019, Commander, Cyber National Mission Force, Fort George G. Meade, Md.
17. August 2019–October 2019, Commander, Twenty-Fifth Air Force, JB San Antonio-Lackland, Texas
18. October 2019–August 2022, Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber, JB San Antonio-Lackland, Texas
19. August 2022–February 2024, Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Md.
20. February 2024–present, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, Fort George G. Meade, Md.

### SUMMARY OF JOINT ASSIGNMENTS

1. June 2001–June 2004, Information Operations Project Officer, Headquarters U.S. Air Force, the Pentagon, Arlington, Va., as a major
2. June 2007–June 2009, Commander, 315th Network Warfare Squadron, Fort George G. Meade, Md., as a lieutenant colonel
3. June 2010–June 2011, Chief, Intelligence, Surveillance and Reconnaissance Division, 609th Air Operations Center, Al Udeid Air Base, Qatar, U.S. Central Command, as a colonel
4. June 2017–June 2018, Director of Intelligence, U.S. Cyber Command, Fort George G. Meade, Md., as a brigadier general
5. June 2018–August 2019, Commander, Cyber National Mission Force, Fort George G. Meade, Md., as a brigadier general



### EFFECTIVE DATES OF PROMOTION

|                                        |  |
|----------------------------------------|--|
| Second Lieutenant<br>December 09, 1991 |  |
| First Lieutenant<br>December 09, 1993  |  |
| Captain<br>December 09, 1995           |  |
| Major<br>September 01, 2002            |  |
| Lieutenant Colonel<br>March 01, 2006   |  |
| Colonel<br>August 01, 2011             |  |
| Brigadier General<br>November 02, 2016 |  |
| Major General<br>August 30, 2019       |  |
| Lieutenant General<br>October 11, 2019 |  |
| General<br>February 02, 2024           |  |

6. August 2022–February 2024, Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Md., as a lieutenant general  
7. February 2024–present, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, Fort George G. Meade, Md., as a general

**MAJOR AWARDS AND DECORATIONS**

Distinguished Service Medal  
Defense Superior Service Medal  
Legion of Merit with two oak leaf clusters  
Bronze Star Medal  
Defense Meritorious Service Medal  
Meritorious Service Medal with four oak leaf clusters  
Joint Service Commendation Medal with three oak leaf clusters  
Air Force Commendation Medal  
Air Force Achievement Medal

(Current as of February 2024)



UNCLASSIFIED

# 2024 WORLDWIDE THREAT ASSESSMENT

DEFENSE INTELLIGENCE AGENCY



ARMED SERVICES SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS  
UNITED STATES HOUSE OF REPRESENTATIVES

Jeffrey Kruse, Lieutenant General, U.S. Air Force  
DIRECTOR, DEFENSE INTELLIGENCE AGENCY

Prepared using information available as of 5 April 2024

UNCLASSIFIED

## INTRODUCTION

---

Chairman Bergman, Ranking Member Gallego, and Members of the Subcommittee:

Thank you for the invitation to provide the Defense Intelligence Agency's (DIA's) assessment of the global security environment.

Global instability is intensifying, fueled by accelerating competition among large nations, increasing collusion between historically nonaligned actors, HAMAS's 7 October 2023 attack, a rapidly evolving information and technology environment, and nondemocratic transitions of power. When coupled with the rapid military modernization efforts of our competitors and their drive to project hard power both regionally and around the globe, the world is growing more dangerous for the United States and our allies and partners. This dynamic environment is raising the risk of regional tensions and conflicts sparking broader vertical and horizontal escalation. It also amplifies the importance and advantages of the United States' robust alliances and partnerships across the world, which—measured in resolve, interoperability, and shared values—are unmatched by our competitors.

- > The PRC remains our pacing security challenge. Beijing is employing various political, economic, military, and information levers to intimidate and coerce countries in its region and to expand its military's global footprint, potentially holding U.S. operations at risk during a conflict. Beijing also is building its partnership with Russia on the strength of a shared rivalry with the United States, and expanding military cooperation through activities such as combined bomber patrols over the Pacific Ocean. During the next year, China is poised to advance its military capabilities, including in domains most critical to military operations against Taiwan and the United States, while improving its proficiencies as a joint force. This past year, Beijing advanced its longer-range missile development, expanded its space capabilities, and grew its naval fleet. PRC nuclear modernization is vastly outpacing efforts from even five years ago in both scale and complexity. The People's Liberation Army (PLA) has more than 500 operational nuclear warheads and probably will have more than 1,000 by 2030.
- > Russia faces a grinding war in Ukraine in which it continues to showcase its disregard for Ukrainian sovereignty and civilian infrastructure. With mounting casualties and costly equipment losses, Russia continues to look to suppliers, including Iran and North Korea, to enable capabilities such as attack unmanned aerial vehicles (UAVs). Moscow is playing for time as Russian President Vladimir Putin probably calculates that his forces can outlast the West's willingness to support Ukraine. Given the strain of the war, Russia's conventional military capabilities will remain diminished at least through 2024 as its defense industry focuses on refurbishing equipment and importing weapons to sustain its conflict in

## 2024 ANNUAL THREAT ASSESSMENT

Ukraine. However, Moscow will continue modernizing its nuclear deterrent capability and is expanding its nonstrategic nuclear weapons posture in Belarus.

- > The 7 October HAMAS attack in Israel has triggered regional instability that Iran sees as an opportunity to weaken Israel, threaten U.S. interests, and increase its own regional standing. Following the onset of the Israel-HAMAS conflict in October, Iran has amplified its support for militias in Iraq and Syria, which have conducted deadly UAV and rocket attacks against U.S. forces and are prepared to resume attacks with little to no warning. Iran is advancing its conventional military capabilities with increased range, accuracy, lethality, and reliability to improve Tehran's ability to strike U.S. and partner forces in the region; this is exemplified by recent Huthi attacks on maritime shipping vessels using Iran-supplied weapons. Iran also proliferates these weapons to regional allies to extend its own deterrent capabilities. Tehran is deepening its cooperation with Moscow and Beijing to blunt its own isolation and to build leverage.
- > Pyongyang has used the past year to expand its ties to Moscow and Beijing to bolster Kim Jong Un's regime and gain access to more advanced capabilities. North Korea's missiles and conventional weapons continue to hold U.S. forces and our allies in northeast Asia at risk while the Kim regime simultaneously seeks to improve its capability to threaten the U.S. homeland. In 2023, Pyongyang continued to diversify its missile and nuclear programs, introducing several new systems. Pyongyang unveiled a ballistic missile submarine and tested an underwater drone that it claimed can be nuclear-armed. Pyongyang also is adopting a more bellicose approach to Seoul, including its reunification policies and calling out South Korea as a separate state for the first time.
- > Transnational terrorist organizations, such as ISIS, have exploited the HAMAS attacks to mobilize their affiliates and supporters. They seek to retaliate against U.S., Israeli, and Jewish interests in response to Israeli operations in the Gaza Strip. Meanwhile, al-Qa'ida has launched the most aggressive propaganda campaign against Israel that we have seen since 2019 and also is seeking to conduct attacks to show solidarity with Palestinians.
- > Our adversaries continue to seek ways to inflict costs within the U.S. homeland. Both China and Russia work to maintain a capability to attack our critical infrastructure during a conflict and probe for access to our systems and supply chains to degrade our military advantage. Despite leadership losses, some transnational terrorist organizations still aspire to attack within the United States, either directly or through inspired actors.

As these threats against the United States persist, and our strategic competitors are emboldened through their cooperation, DIA's resolve to conduct exceptional intelligence operations and analysis that provides decision advantage to our Nation only deepens. I am privileged to lead this organization, and I want to assure you that DIA officers, who serve in more than 140 nations around the world, are dedicated to providing you the soundest insight into the strategic, operational, and tactical security threats confronting the United States. My aim in this hearing is to crystalize these threats and to support this committee in its critical work of defending the Nation. Thank you for your continued confidence. We are grateful for your vital support to DIA.

## CONTENTS

---

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| China .....                                                           | 1  |
| Military Modernization and Spending.....                              | 1  |
| Nuclear, Space, and Cyberspace Capabilities .....                     | 2  |
| Risks of Unsteady C2 and Accountability.....                          | 4  |
| Pressuring Taiwan.....                                                | 4  |
| Tension Along China's Periphery.....                                  | 5  |
| Global Military Presence.....                                         | 5  |
| Cooperation With Russia.....                                          | 6  |
| Outlook.....                                                          | 7  |
| Russia .....                                                          | 8  |
| Trajectory of the War in Ukraine.....                                 | 8  |
| Military Capabilities and Modernization.....                          | 9  |
| Global Military Activity .....                                        | 11 |
| Outlook.....                                                          | 12 |
| IRAN .....                                                            | 13 |
| Military Capabilities and Modernization.....                          | 13 |
| Cyber Capabilities.....                                               | 14 |
| Nuclear, Chemical, and Biological Activities.....                     | 14 |
| Defense Budget and Arms Acquisitions .....                            | 14 |
| Relations With Russia and China .....                                 | 15 |
| Role in Israel-HAMAS Conflict.....                                    | 15 |
| Outlook.....                                                          | 16 |
| NORTH KOREA .....                                                     | 17 |
| Military Capabilities and Modernization.....                          | 17 |
| Missile Research and Development and Weapons of Mass Destruction..... | 18 |
| Space and Cyberspace Capabilities .....                               | 18 |
| Outlook.....                                                          | 18 |
| TERRORISM .....                                                       | 19 |

## 2024 ANNUAL THREAT ASSESSMENT

|                                                |           |
|------------------------------------------------|-----------|
| ISIS.....                                      | 19        |
| Al-Qa'ida.....                                 | 20        |
| <b>SOUTH &amp; SOUTHEAST ASIA.....</b>         | <b>21</b> |
| Afghanistan.....                               | 21        |
| India.....                                     | 21        |
| Pakistan.....                                  | 22        |
| South China Sea.....                           | 23        |
| <b>MIDDLE EAST.....</b>                        | <b>24</b> |
| Iraq.....                                      | 24        |
| Yemen.....                                     | 25        |
| Syria.....                                     | 25        |
| Outlook.....                                   | 26        |
| <b>AFRICA.....</b>                             | <b>27</b> |
| North Africa.....                              | 27        |
| West Africa.....                               | 28        |
| East Africa.....                               | 28        |
| Central and Southern Africa.....               | 28        |
| <b>LATIN AMERICA.....</b>                      | <b>29</b> |
| Chinese, Russian, and Iranian Activity.....    | 29        |
| Venezuela.....                                 | 30        |
| Cuba.....                                      | 31        |
| Drug Trafficking.....                          | 31        |
| Refugee Flows and Migration.....               | 32        |
| <b>OTHER GLOBAL THREATS.....</b>               | <b>33</b> |
| Foreign Intelligence Service Activity.....     | 33        |
| Targeting Defense Critical Infrastructure..... | 33        |
| Advanced Technology.....                       | 34        |
| Global Health and Biodefense Trends.....       | 35        |
| Climate and Environmental Change.....          | 35        |

## CHINA

---

Beijing continues to advance its global capabilities to confront the United States and its allies across the diplomatic, informational, military, and economic domains. In March 2023, PRC President Xi Jinping told delegates to the Chinese People's Political Consultative Conference that "Western countries, led by the United States, have implemented comprehensive containment, encirclement, and suppression against us, bringing unprecedented severe challenges to our country's development." Xi is overseeing a whole-of-government effort to better prepare China for competition and confrontation with the United States and its allies in East Asia and around the world, and the PRC seeks to undermine popular and political support for U.S. military alliances and security partnerships throughout the world. This includes casting doubt on U.S. security alliances and partnerships, particularly those in the Indo-Pacific region, and labeling them as destabilizing and irreconcilable with PRC security interests. In addition, the PLA is undertaking efforts to modernize its capabilities and improve its near-term proficiencies as a joint force across all warfare domains so that it can effectively conduct a full range of military and information operations, including against U.S. and partner military forces. The PLA also is incrementally improving its power-projection capabilities to achieve its long-term goal of becoming a "world class military." However, global attention in 2023 to sudden removals of PLA leaders, unsafe PLA operating practices, and the public loss of a surveillance balloon cast doubt on Xi's ability to maintain reliable command and control (C2) and accountability of the PLA during a period of rising international tension.

### *Military Modernization and Spending*

China is rapidly advancing its military modernization and developing capabilities critical for potential, future military operations against Taiwan and the United States. These capabilities across land, sea, air, and emerging warfighting domains could enable Beijing to seize Taiwan by force and disrupt U.S. attempts to intervene. During his October 2022 speech at the opening ceremony of the 20th Chinese Communist Party (CCP) Congress, Xi reaffirmed his commitment to the PLA's 2027 modernization milestone to accelerate the technological development of the armed forces while modernizing the PLA's military theories, organizations, personnel, weapons, and equipment. In July 2023, Xi again emphasized this goal during a 2-day meeting with top military officials, noting the PLA aims to be a more efficient and combat-ready force by 2027.

- > The PLA Army—which is responsible for conducting operations ranging from firepower strike and mobile assault to all-dimension defensive actions—continues to modernize equipment with a focus on combined arms and joint training. The Army demonstrated a new long-range fire capability during its military response to the August 2022 congressional delegation visit to Taiwan, signaling its availability for use during a conflict with Taiwan.

## 2024 ANNUAL THREAT ASSESSMENT

- > The PLA Navy, the world's largest in terms of personnel, has increased its inventory of ships and submarines by 9 percent since 2022 to an overall battle force of more than 370 vessels, including more than 140 major surface combatants. The Navy's third aircraft carrier, launched in 2022, is expected to be operational in late 2024. The PLA Navy also commissioned its third YUSHEN class amphibious assault ship and, as of early 2023, probably had begun construction on a fourth YUSHEN class ship. These ships are advancing the PLA's ability to sustain operations in the Western Pacific, Indian Ocean, and beyond. This includes the Navy's growing aircraft carrier force—which extends the PLA's air defense coverage—and its increasingly sophisticated anti-ship cruise missiles equipped aboard submarines and surface combatants, which expand the threat posed to U.S. and allied forces to beyond the Second Island Chain.
- > The PLA Air Force—with more than 3,150 total aircraft—constitutes the region's largest aviation force and the third largest in the world, including approximately 2,400 combat aircraft, such as fighter jets, strategic and tactical bombers, multi-mission tactical aircraft, and attack aircraft. In 2023, the PLA Navy transferred many of its land-based aircraft to the Air Force, including 300 fighter jets, so the Navy could focus on improving its carrier-based air operations. The Air Force is evolving into a more technologically advanced, effective, and capable force that is proficient at conducting joint operations.
- > The PLA Rocket Force organizes, staffs, trains, and equips China's expanding land-based nuclear and conventional missile forces. The Rocket Force also fields various conventional mobile, ground-launched short-, medium-, and intermediate-range ballistic missiles and ground-launched cruise missiles (GLCMs). As of 2023, the Rocket Force had fielded approximately 1,000 short-range (SRBMs), 1,000 medium-range (MRBMs), and 500 intermediate-range ballistic missiles (IRBMs) as well as 300 GLCMs, compared with more than 600 SRBMs, 500 MRBMs, 250 IRBMs, and 300 GLCMs identified in 2022. The Rocket Force's conventionally armed anti-ship ballistic missile variant enables the PLA to conduct long-range precision strikes against ships in the western Pacific from mainland China. The PLA also may be exploring conventionally armed intercontinental-range missile systems, which would enable the PRC to threaten conventional strikes against the continental United States, Alaska, and Hawaii.
- > In March 2024, the PRC announced a nominal 7.2 percent annual military budget increase to USD \$232 billion, representing approximately 1.2 percent of its gross domestic product. The published military budget does not include details of expenditure breakouts, such as research and development and foreign weapons procurement, which means China's actual military-related spending is significantly higher than its announced defense budget.

### *Nuclear, Space, and Cyberspace Capabilities*

The PRC is rapidly diversifying and expanding its nuclear forces, vastly outpacing its modernization efforts of a decade ago in both scale and complexity. As of early 2023, the PLA possessed more than 500 operational nuclear warheads and probably will have more than 1,000 warheads by 2030. To support this stockpile growth, China probably will produce plutonium for its nuclear weapons

program using its new fast-breeder reactors (CFR-600s) and reprocessing facilities, despite publicly maintaining that these technologies are intended for peaceful purposes.

- > The PRC probably has completed the construction of its three new solid-propellant silo fields, which comprises at least 300 new intercontinental ballistic missile (ICBM) silos, and has loaded at least some ICBMs into these silos. This project, and the expansion of China's liquid-propellant silo force, is meant to improve the readiness of China's nuclear arsenal by moving to a launch-on-warning posture—called “early warning counterstrike”—where warning of an incoming missile automatically initiates a counterstrike. Inexperience with this early warning counterstrike capability coupled with the system's more compressed reaction timelines increases the risk of unintentional nuclear escalation during a crisis with the United States during the next three to five years.
- > The PRC also is updating its capability to deliver multimegaton warheads by fielding its new DF-5C silo-based, liquid-fueled ICBM. For the sea leg of its nuclear triad, in 2023, the PLA Navy continued to produce JIN class nuclear-powered ballistic missile submarines and fielded the longer-range JL-3 submarine-launched ballistic missile, rendering the JIN class capable of striking the continental United States from PRC littoral waters.

China's space and counterspace strategy is predicated on developing capabilities to offset a perceived U.S. over-reliance on space-based systems. China continues to dedicate significant resources to technologies, such as direct-ascent anti-satellite missiles, co-orbital satellites, electronic warfare, and directed-energy systems that can contest or deny an adversary's access to and operations in space during a conflict. During the past year, China cemented itself as a space launch leader, with only the United States conducting more launches. The PRC also added Azerbaijan, Belarus, Egypt, Pakistan, South Africa, UAE, and Venezuela to the International Lunar Research Station, a joint Chinese-Russian initiative to develop a lunar base for scientific research.

- > As of May 2023, China had 618 total satellites, including 347 remote-sensing/intelligence, surveillance, and reconnaissance (ISR) satellites, 73 communications satellites, and 49 navigation-related satellites.
- > China attempted 67 total space-related launches in 2023; 66 of its launches were successful. The United States conducted 114 launches in 2023. China's launch cadence was mostly on par with its 2022 performance of 64 launches, which resulted in 62 successful orbital launches.

PRC-based cyber intrusions continue to target information networks around the world, including U.S. Government systems, to steal intellectual property and data and develop access to sensitive networks. China uses its cyberspace capabilities to support intelligence collection against U.S. academic, economic, military, and political targets; to exfiltrate sensitive information from defense infrastructure and research institutes; and to lay the groundwork for malicious cyber activities and cyber attacks. The PLA has called for using space, cyber operations, and electronic warfare as weapons to paralyze adversary information systems during a conflict.

### *Risks of Unsteady C2 and Accountability*

Beijing struggles to maintain reliable C2 and accountability of its military forces and ensure safe operations in international air and maritime domains, all of which pose a threat to U.S. forces and interests. In January 2023, a military-linked, high-altitude surveillance balloon flew off course and crossed into the continental United States until it was shot down by a U.S. fighter aircraft. Also in 2023, a PLA pilot flew within 10 feet of a U.S. Air Force B-52 in international airspace over the South China Sea (SCS) and may have been unaware how close they came to causing a midair collision. Since 2022, the PLA has conducted more than 180 instances of coercive and risky air intercepts against U.S. aircraft in the Indo-Pacific region—more than in the previous decade. During the same period, the PLA committed approximately 100 coercive and risky maneuvers against ally and partner aircraft.

Beyond operational control, PRC leaders have struggled to hold the PLA administratively accountable, despite decades of anticorruption efforts. In 2023, Xi abruptly removed the PRC defense minister and senior Rocket Force officers, reportedly because of corruption surrounding weapons procurement and nuclear modernization, which could undermine PLA capabilities and weapon safety.

### *Pressuring Taiwan*

During the past year, PRC leaders have employed a range of pressure tactics against Taiwan and signaled its resolve to counter U.S.-Taiwan diplomatic and security cooperation. Beijing also continues to pressure Taiwan's diplomatic allies to cut ties with the island, with Nauru severing ties to Taiwan in January 2024. China has a range of military options to coerce Taiwan, including increasing the frequency and scope of its military presence operations, an air or maritime blockade, seizure of Taiwan's smaller outlying islands, joint firepower strikes, or a full-scale amphibious invasion of Taiwan. Beijing appears willing to defer the use of military force as long as it calculates that its unification with Taiwan ultimately can be negotiated, the costs of armed conflict would outweigh the benefits, and its stated redlines have not been crossed by Taiwan, the United States, or other countries.

- In April 2023, the PLA responded to former Taiwan President Tsai's transit of the United States and meeting with the then-U.S. House Speaker by sending at least 128 aircraft into the Taiwan Air Defense Identification Zone (ADIZ). PLA entries into the Taiwan ADIZ in 2023 slightly decreased to 1,641 events, compared with 1,733 in 2022. Concurrently, PLA aircraft Taiwan Strait centerline crossings increased to at least 712 events in 2023, compared with 552 in 2022, indicating a greater percentage of PLA ADIZ incursions included centerline crossings. Thus far in 2024, the PLA has conducted at least 332 Taiwan ADIZ entries and 111 centerline crossings, a slight reduction compared to the same time period in 2023.

### *Tension Along China's Periphery*

In 2023, the PRC continued to employ its Navy to patrol disputed areas in the South and East China Seas and used its Coast Guard to harass fishing activities, resupply missions, and hydrocarbon exploration operations, resulting in unsafe maritime incidents and escalating tensions with its neighbors. In 2023, PRC maps reintroduced a “ten-dash line” claim—revised from Beijing’s previously-claimed “nine-dash line”—which notably expanded the depiction of PRC claims over the Spratly and Paracel Islands and other land features in the SCS, including areas east of Taiwan.

- > Despite an international tribunal ruling in 2016 favoring the Philippines, China has continued efforts to disrupt the Philippines’ presence in the SCS, including at Second Thomas Shoal. In 2023, China’s efforts included Chinese Coast Guard and maritime militia boats using water cannons and conducting dangerous and aggressive maneuvering—which resulted in collisions with Philippine counterparts.
- > Beijing continues to use Coast Guard vessels and aircraft to patrol near the Japan-administered Senkaku Islands to compel Tokyo to concede its claim to the territory and the accompanying exclusive economic zone.

### *Global Military Presence*

Beijing is improving PLA systems to operate further from China for longer periods of time and establishing a more robust overseas logistic and basing infrastructure to sustain deployments at greater distances, which could potentially hold U.S. global operations or international commerce at risk during a conflict. Beijing is pursuing a mixture of military logistics models—including preferred access to commercial infrastructure abroad, exclusive PLA logistics facilities with pre-positioned supplies colocated with commercial infrastructure, and bases with stationed forces to support China’s overseas military logistic needs. Some of China’s Belt and Road Initiative (BRI) projects have potential military advantages, such as providing PLA access to foreign ports to pre-position the logistic support necessary to sustain more distant naval deployments in the Indian Ocean, Mediterranean Sea, and Atlantic Ocean.

- > In 2023, the PLA Navy more frequently operated worldwide, including a submarine deployment to the Indian Ocean, and continued its naval escort task force deployments to the Gulf of Aden. In October 2023, the 44th and 45th PRC naval task forces conducted missions in the Gulf of Aden.
- > Chinese officials attended Cambodia’s Ream Naval Base groundbreaking ceremony in 2022, and a PRC official has since confirmed that the PLA will have access to parts of the base. Beijing also probably has considered establishing PLA military logistics facilities in Angola, Bangladesh, Burma, Equatorial Guinea, Gabon, Indonesia, Kenya, Mozambique, Namibia, Nigeria, Pakistan, Papua New Guinea, Seychelles, Sri Lanka, Solomon Islands, Tajikistan, Tanzania, Thailand, and the UAE.

## 2024 ANNUAL THREAT ASSESSMENT

- > Beijing highlights the potential for these military logistics facilities to provide international public goods, such as humanitarian assistance and disaster relief, but its global military logistics network also provides the PLA new means to disrupt U.S. military operations and international commerce.

*Cooperation With Russia*

Driven by a common rivalry with Washington, Beijing and Moscow continue to demonstrate a close partnership through diplomatic, informational, military, and economic cooperation. These activities are intended to develop interoperable military capabilities, promote Beijing and Moscow as a political bloc against the West, and undermine security partnerships the United States maintains with regional countries, including the Australia, UK, and U.S. (AUKUS) agreement and the Quadrilateral dialogue with Australia, India, and Japan. Although Xi and Putin announced a “no limits partnership” ahead of the 2022 Winter Olympics in Beijing, Russia’s war in Ukraine has challenged China as it has sought to maintain official “neutrality” while privately supporting Moscow. In 2023, Beijing was particularly sensitive to advancing select areas of its partnership with Moscow while avoiding actions, such as overtly providing materiel or lethal military assistance, that might incur reputational or economic costs for Beijing.

- > Beijing has parroted Russian narratives when they align with China’s criticism of the United States and has refrained from condemning Russia’s conduct or referring to Moscow’s invasion as a “war.” China also has legitimized Russia’s role on the world stage by meeting with Russian leaders and continuing to work with Moscow in various multilateral fora, such as the United Nations (UN); Brazil, Russia, India, China and South Africa (BRICS); and Association of Southeast Asian Nations.
- > Russian assistance is helping to modernize China’s nuclear program, particularly by supplying it highly enriched uranium that can help it produce weapons-grade plutonium. In March 2023, China and Russia signed an agreement to continue cooperation on fast reactor and reprocessing technology development.
- > Despite Russia’s war in Ukraine, China and Russia continued a steady tempo of bilateral military exercises in 2023. This included a combined bomber patrol, a new naval exercise called North Cooperation-23, and a combined naval patrol to the Bering Sea. Since 2022, Russian military activity with China has included nine bilateral exercises and naval and bomber patrols. Although these exercises probably only marginally improved their capabilities and interoperability, they served as important demonstrations of both countries’ commitment to the partnership. In addition, China and Russia participated together in trilateral naval exercises with South Africa and Iran, both aimed at improving the participants’ military cooperation and maritime security near two critical sea lines of communication.
- > The PRC almost certainly is applying lessons from Russia’s war in Ukraine toward countering what it perceives as a U.S.-led containment strategy. Diplomatically, the Ukraine war probably reaffirmed to Beijing the importance of persuading countries that it

considers the “Global South” in Africa, Latin America, the Middle East, and the Indo-Pacific region to echo its narratives. The PLA also probably seeks to incorporate lessons from how Russia and Ukraine are employing influence operations in the conflict into its own doctrine. The effects of Western sanctions against Russia almost certainly have amplified China’s push for defense and technological self-sufficiency and financial resilience.

### *Outlook*

Xi’s travel to San Francisco in November 2023 to meet with the U.S. President were part of Beijing’s effort to stabilize tensions between the United States and China. However, it did not ultimately influence Beijing’s efforts to rapidly advance military capabilities and improve China’s multidomain approach to strategic competition with the United States. Across the Taiwan Strait, China is likely to put diplomatic, economic, and military pressure on Taiwan President-elect “William” Lai Ching-te—who will be inaugurated in May—to advance Beijing’s long-term objective of unification and deter any move by Taiwan toward independence. Along China’s periphery, Beijing is likely to respond with shows of military resolve in the face of neighbors resisting PRC territorial claims. Globally, Beijing will seek opportunities to exploit narratives that criticize Washington’s ability to manage global crisis and conflict. These efforts are aimed at presenting China as a responsible global leader, even as the substance of its global security role remains more rhetoric than action.

## RUSSIA

---

Russian President Vladimir Putin remains committed to prosecuting his war in Ukraine despite taking heavy losses and facing fierce resistance from Ukrainian armed forces. He seeks to eventually gain additional territory and prevent Ukraine from fully integrating with the West. Russia probably is able to continue military operations through 2024 as it retains sufficient manpower while producing, refurbishing, and receiving munitions and equipment from willing suppliers. Despite a brief but acute challenge to senior Russian leadership authority during the failed June 2023 armed insurrection of private military company (PMC) Wagner owner Yevgeniy Prigozhin, Putin has consolidated domestic support for the war and silenced internal dissent through a mix of incentives, coercion, and domestic propaganda portraying Russia as being under siege by the West.

### *Trajectory of the War in Ukraine*

Russia's February 2022 invasion has devolved into a war of attrition as both sides have experienced high casualties and strained their ammunition and equipment stockpiles. Despite Russia's high losses, Putin probably judges that his forces can outlast Western willingness to provide security and economic support. Throughout 2023, Russia conducted offensive operations in eastern Ukraine, demonstrating its intent to maintain military pressure on Ukrainian forces and to seize additional territory, even if only for small gains. Moscow probably will struggle to seize larger, strategically relevant swaths of additional territory in 2024 without a significant influx of additional personnel, which would risk straining the Russian economy and popular support.

- The war against Ukraine has proven costly to the Russian military, particularly to Russia's ground forces. Since the conflict's start, Russia has lost at least 7,400 ground combat vehicles, including at least 2,300 tanks and 19 naval vessels and approximately 200 aircraft. The significant amount of lost Russian conventional ground forces is likely to take years to reconstitute.
- Russia has incurred heavy personnel losses in Ukraine since the conflict began. After experiencing significant casualties early in the war among its highest readiness airborne and naval infantry forces, Russian casualties in 2023 consisted primarily of poorly trained and ill-equipped mobilized and contract soldiers.
- Moscow probably will continue to meter its use of precision-guided munitions (PGMs) because its production capacity cannot yet simultaneously support extensive offensive operations and reconstitution of prewar stocks. To remedy this, Moscow probably will continue to negotiate for the purchase of Iranian- and North Korean-supplied munitions.

- > Moscow also will continue to employ one-way attack UAVs to partially mitigate its PGM shortfall. To this end, Russia is boosting domestic UAV production, has imported UAVs directly from Iran, and also is assembling UAVs at an Iranian-equipped factory in Russia.

Following a period of heightened nuclear rhetoric from senior Russian leaders in late-2022, Putin has downplayed the possibility of a nuclear conflict in subsequent speeches and noted he saw no need to change Russia's nuclear doctrine, even though Russia has withdrawn its ratification of the Comprehensive Nuclear Test Ban Treaty. Nevertheless, an existential threat to the Russian state is cited in Russian doctrine and legal documents as justification for nuclear use, and the West cannot completely discount the possibility of Russia using nuclear weapons in Ukraine.

For at least the next year, Russia probably will continue to give priority to defending Russian-occupied areas in eastern and southern Ukraine and is likely to seek additional territorial gains, even if they are minimal and only incremental in nature. Putin probably is uninterested in a negotiated settlement that includes giving up Russian-occupied Ukrainian territory. Moscow also almost certainly would demand any settlement guaranteed Ukrainian neutrality or demilitarization.

#### *Military Capabilities and Modernization*

Russia's conventional military capabilities almost certainly will remain degraded through 2024 because of attrition from the Ukraine conflict. Moscow's defense industry is giving priority to refurbishing old equipment ahead of upgrading or producing new weapon systems, including aircraft, air defense networks, surface ships, and armored ground vehicles. The heavy losses to Russia's arsenal of modern equipment have forced Moscow to draw from Cold War-era equipment stocks, such as T-55 and T-62 tanks last produced in the 1970s, and obtain munitions from Iran and North Korea, including artillery shells and short-range missiles. Moscow's defense production remains strained by difficulty obtaining manufacturing components, inadequate repair facilities, and persistent underemployment in its defense sector.

- > The Russian Defense Ministry announced that it planned major reforms to military structures and capabilities through 2026 as a result of shortfalls identified during operations in Ukraine and in response to expansion of the North Atlantic Treaty Organization (NATO). In December 2022, Russian Defense Minister Sergey Shoygu announced a plan to expand Russia's military to 1.5 million troops by 2026, including 695,000 volunteer contract soldiers. However, Russia has a long history of failing to achieve its stated military reform and recruitment goals. In 2023, Russia's authorized troop strength was 1.3 million, but the fluid nature of Russian troop recruitment and casualty rates and Moscow's efforts to distort information about its war in Ukraine hinder our ability to accurately estimate Moscow's current military personnel figures.
- > Ongoing Russian Navy modernization efforts include outfitting older ships with modern KALIBR cruise missiles, continuing to build and field advanced submarines, and constructing new and upgraded basing infrastructure throughout the Arctic. In 2023, it

## 2024 ANNUAL THREAT ASSESSMENT

conducted a multifleet exercise, which included deploying a ship armed with hypersonic missiles near the United States. Despite losses incurred by its Black Sea fleet during the Ukraine war, Moscow will continue to use its navy to demonstrate commitment to its partners and showcase its global deterrent capability, and as a tool of global power projection during the next year.

- > Russia's Aerospace Forces have demonstrated poor proficiency during operations in Ukraine, resulting in substantial losses of equipment and veteran personnel that will take years to reconstitute. Overuse of aircraft, attrition, and poor force implementation probably will hamper aerospace operations inside Ukraine in 2024.
- > Russia is actively seeking to use ISR systems and electronic warfare to disrupt Ukraine's command, control, communications, and weapons guidance but has been unable to dominate the battlefield. Russia has employed its domestically produced Orlan UAVs and Iranian-provided Mohajer UAVs for this purpose.
- > Russian state and nonstate cyber actors have maintained a high volume of offensive cyber operations against Ukrainian networks and have achieved some disruptive effects. These actions indicate Moscow probably will continue to invest in modernizing its cyber capabilities.

Russia's space and counterspace strategy remains focused on maintaining access to space-based information assets while denying access to the adversary. Moscow has been hindered in its attempts to field more space capabilities because of international sanctions and export controls levied upon it in recent years. Given these limitations, Russia is focusing its available resources on developing counterspace capabilities, ranging from jamming to malicious cyber activities to direct-ascent and orbital antisatellite systems. In 2023, Russia unsuccessfully attempted to land a spacecraft on the moon as part of the International Lunar Research Station initiative.

Russia will continue to emphasize its military presence in the Arctic in 2024, maintaining its strategically defensive posture aimed at fortifying its Arctic territory against perceived threats from the United States and other nations. Since 2014, Russia has improved its posture in the Arctic across all military domains, enhancing its ability to defend the region against an attack and to respond to Western military operations along its periphery.

Modernizing its nuclear triad remains a long-term priority for Moscow. Russia also has expanded its nonstrategic nuclear weapons posture by placing weapons in Belarus. Putin claims warheads were delivered to Belarus in June; the new location does not extend the range of Russia's ability to deploy nonstrategic nuclear weapons. Russia also is developing the SS-X-29 and SS-27 Mod 2 ICBMs and DOLGORUKIY class ballistic missile submarine to maintain its nuclear deterrence capabilities. In addition to its nuclear arsenal, Russia maintains biological and chemical weapon programs and has used nerve agents in assassination attempts.

### *Global Military Activity*

Russia's decision to allocate the vast majority of its ground forces to invade Ukraine has degraded its ability to project power globally. Russia has curtailed some of its military exercises with foreign partners because of the demands of the war in Ukraine. In addition, Russia's military production demands and the reputational costs of its invasion are forcing Moscow to rely more on information operations, diplomatic overtures, and the use of nonstate paramilitary forces to garner influence globally. In 2024, Russia more frequently will turn to partners—such as Belarus, China, Iran, and North Korea—to demonstrate that it is not internationally isolated and to supply critical weapon components and mitigate its weapon shortages. In 2024, Russia plans to spend USD \$117 billion on defense, marking a 56-percent increase from 2023.

- > Moscow is seeking to expand its cooperation with Pyongyang in the economic, diplomatic, and defense spheres, which probably has already paid some dividends as North Korea has started to provide weapons to Russia for use in Ukraine.
- > Laden with heavy economic sanctions, Moscow is seeking to coordinate its energy production more closely with other energy-rich states in the Middle East. International isolation and resource shortfalls also have spurred Moscow to strengthen its relationship with Tehran. Iran has sent upwards of 1,000 one-way attack UAVs to Russia for use in Ukraine. The Russian military's physical presence in Syria and close partnership with the Bashar al-Asad regime provides Russia a power-projection tool in the Middle East and into the eastern Mediterranean. Putin uses his personal relationship with Turkish President Recep Tayyip Erdogan to manage tensions with Türkiye about Ukraine, to push back on U.S. presence in the region, and to coordinate security and diplomatic efforts in Syria.
- > In the Western Hemisphere, Russia probably will continue to engage its traditional partners in Cuba, Nicaragua, and Venezuela for economic deals and security partnerships. Moscow also probably intends to demonstrate its presence in the region through out-of-area, long-range aviation and naval deployments as a counter to U.S. presence near Russia's periphery. Russia's burgeoning outreach to Brazil, coupled with Foreign Minister Sergey Lavrov's visit to multiple Latin American countries in 2023, probably demonstrates its approach to leveraging its BRICS membership to improve partnerships in this region.
- > In Africa, Russia seeks to gain influence and advance its objectives through opportunistic arms sales, multilateral forums, military access agreements, resource extraction contracts, influence operations, and paramilitary group deployments. Following Prigozhin's 2023 armed insurrection, Moscow has attempted to replace PMC Wagner's presence in Africa with GRU-controlled paramilitary groups.

*Outlook*

Russia's conventional ground capabilities to deter, fight, or militarily compete with NATO probably will remain diminished for at least the next three years because the majority of combat-capable Russian maneuver units and other key conventional assets have been committed to the war in Ukraine. Moscow aims to avoid direct conflict with NATO but is able to employ asymmetric capabilities, such as cyber and information campaigns, against U.S. and other Western interests globally.

## IRAN

---

Tehran remains committed to ensuring the survival of its Islamic republic and positioning itself as a dominant regional power. Iran continues to modernize its military capabilities, enhancing its ability to project power and also deter potential adversaries. The regime, through the Islamic Revolutionary Guards Corps–Qods Force (IRGC-QF), continues to fund and equip militias, which have increased targeting of U.S. and partner interests in the region since the October 2023 HAMAS attack on Israel. Although Iran probably has not resumed its pre-2004 nuclear weapons program, it has pursued activities that would shorten the time required to produce sufficient weapons-grade uranium, should the regime make the decision to do so. Tehran's expanding ties to Moscow and Beijing have helped to reduce the regime's international isolation and counter the effect of sanctions.

### *Military Capabilities and Modernization*

Iran's conventional military strategy aims to strengthen Tehran's ability to hold U.S. and partner forces at risk while deterring adversary attacks and to retaliate if deterrence fails. For more than a decade, Tehran has given priority to developing ballistic and cruise missiles, surface-to-air missiles, and unmanned systems with increased range, accuracy, lethality, and reliability. Iran also proliferates these weapons to regional allies to extend its own deterrent-strike capabilities, orchestrate plausibly deniable strikes, and test equipment in combat.

- Tehran's missile force is increasingly augmented by Iran's UAVs and serves as the regime's primary conventional deterrent against attacks on its personnel and territory. Iran has a substantial inventory of ballistic and cruise missiles capable of striking targets as far as 2,000 kilometers from its borders. In 2023, Tehran focused on fielding a new generation of long-range systems to counter Israel and complement its robust inventory of accurate close- and short-range missiles. Since early 2023, the regime publicly unveiled three new missiles able to strike Israel from the western part of Iran, including a land-attack cruise missile and a ballistic missile Tehran has touted as hypersonic.
- Iran's space and counterspace strategy is focused on developing a more reliable launch capability; however, its strategy overall is less defined than China's or Russia's. Russian assistance has played a role in the development of Iran's space launch vehicle booster technology. In 2022, Russia built and launched a more sophisticated Khayyam remote-sensing satellite for Iran, and in October 2023, Moscow entered talks to launch additional Khayyam satellites and a communications satellite into geosynchronous Earth orbit.

### *Cyber Capabilities*

Iran views cyber operations as a means to supplement its conventional capabilities and engage adversaries in a deniable, low-cost manner. The regime is capable of a range of cyber operations, from information operations to destructive attacks against government and commercial networks worldwide. Iran's cyber operations against regional and Western entities—such as targeting Albania for hosting the Mujahedin-e Khalq (MEK) dissident group in 2022 or against Israeli-manufactured devices in the United States and Europe since the start of the conflict with HAMAS—demonstrate Tehran's continued ability and willingness to use cyber capabilities to advance its goals and threaten U.S. and partner interests.

### *Nuclear, Chemical, and Biological Activities*

Iran probably is not conducting the key activities necessary to produce a testable nuclear device, and Iran probably has not resumed its pre-2004 nuclear weapons program. However, in 2023, the regime continued to expand its stockpile of highly enriched uranium—which already is sufficient to produce several nuclear weapons—and to develop and operate advanced centrifuges. These activities have shortened the time required to produce sufficient weapons-grade uranium for a nuclear device from 10 to 15 days to probably less than one week—after a decision by Tehran to do so. This does not include the time necessary for Tehran to build a nuclear weapon.

- In 2023, Iran took some de-escalatory nuclear steps, such as delaying the installation of more advanced centrifuges, downblending some of its highly enriched uranium, and allowing the IAEA to reinstall some previously removed monitoring equipment. However, Tehran also has revoked some IAEA inspector accesses and not fully cooperated with the agency to resolve two outstanding safeguard issues, which impede previously agreed to IAEA supervision activities.

The United States has found Iran to be noncompliant with its obligations as a state party to the Chemical Weapons Convention and is concerned that Tehran is pursuing pharmaceutical-based offensive agents. Although Iran is a party to the Biological Weapons Convention, it probably has not abandoned its intention to conduct research and development of biological agents and toxins for offensive purposes.

### *Defense Budget and Arms Acquisitions*

Iran increased its defense budget from \$6.7 billion in 2021 to \$11.2 billion in 2023, which probably was driven in part by a desire to modernize its military equipment. Tehran's creation of a specific defense modernization fund in 2022, derived from euro-denominated oil revenues, probably will support Iran's purchase of foreign-supplied advanced conventional weapons, including more advanced fighter aircraft. In 2023, Iran received Russian YAK-130 trainer aircraft and agreed to purchase Russian Su-35 fighter aircraft, which would be a multigenerational technological leap

compared with the regime's current fighter inventory. Funding issues have delayed the delivery timeline for these fighter aircraft.

#### *Relations With Russia and China*

Since 2022, Iran has provided more than 1,000 Shahed-136 UAVs, as well as Shahed-131 and Mohajer-6 UAVs, to support Russia's war against Ukraine. In May, Iran began assisting Russia in establishing a Shahed-136 UAV production facility in Russia. Regime officials have cited the October 2023 expiration of missile exporting restrictions under United Nations Security Council Resolution 2231 as an opportunity to generate revenue and advance bilateral defense diplomacy. In 2023, Tehran marketed missiles to Moscow during a defense conference in Russia and directly to Russian Defense Minister Sergey Shoigu during a visit to Iran.

During the past year, China and Iran have deepened their economic, political, and military ties, probably to mitigate diplomatic isolation, blunt sanctions' effects, and counteract perceived Western hegemony. China remains Iran's leading oil purchaser and trading partner; this revenue partially shields the regime from the effects of international sanctions. Beijing's successful efforts in brokering Iranian-Saudi rapprochement in March 2023 signify new levels of diplomatic cooperation with Tehran. That same month, China and Iran conducted combined naval drills to strengthen military cooperation. In July 2023, Iran joined the China-led Shanghai Cooperation Organization, and in August, Iran successfully lobbied the BRICS for membership.

#### *Role in Israel-HAMAS Conflict*

Since the start of the Israel-HAMAS conflict in October 2023, Tehran has supported militia attacks against U.S. and Israeli interests in the region but also has calibrated these attacks to avoid being drawn into a direct conflict. Tehran almost certainly perceives an opportunity to weaken Israel and increase its own regional standing, including by driving a wedge between Jerusalem and its Arab neighbors and disrupting Israel-Saudi Arabia normalization talks. Surrounding countries, including the Gulf states, have limited capability to mitigate an escalation in Iranian and partner attacks that might threaten U.S. interests in the region.

- > The IRGC-QF provides guidance to the regime's partners and proxies in Iraq, Syria, Yemen, and Lebanon. Following the Israel-HAMAS conflict's onset, Iran-backed militias resumed UAV and rocket attacks targeting U.S. forces in Iraq, Jordan, and Syria. These attacks were suspended in February but could resume with little to no warning. Hizballah also has attacked Israel using artillery, rockets, and UAVs. In addition, Huthi forces in Yemen have conducted multiple attacks targeting Israel and maritime traffic in the Red Sea and Gulf of Aden with ballistic missiles, land-attack cruise missiles, and UAVs.

*Outlook*

During the next year, Iran will continue supporting its partners and proxies and probably is confident in its ability to use these groups to target U.S. and Israeli interests in a plausibly deniable manner. Separately, Iran almost certainly will continue assassination plotting against current and former U.S. officials in retaliation for the death of IRGC-QF Commander Qasem Soleimani and against Israeli and Jewish targets globally. Iran also will pursue advances to its conventional military capabilities—particularly its missiles and unmanned platforms—which probably will improve Tehran's ability to strike U.S. and partner forces in the region.

## NORTH KOREA

---

North Korea wields the missile and conventional capabilities to hold U.S. forces and allies in northeast Asia at risk and is maturing the capability to threaten the U.S. homeland with increasingly sophisticated weapons. These modernization efforts support North Korean leader Kim Jong Un's goal of building a military to credibly threaten and deter the United States and its allies. In line with that goal, this past year, North Korea launched a solid-propellant ICBM, developed more advanced unmanned systems, diversified missile launch platforms, and displayed what Pyongyang claimed is a new nuclear warhead design. Pyongyang also is reinvigorating its relationship with Moscow. In 2023, in his first trip abroad since 2019, Kim visited Putin in Russia to discuss security and space cooperation, and North Korea has since shipped at least a thousand shipping containers of equipment and munitions to Russia.

### *Military Capabilities and Modernization*

The Korean People's Army (KPA) almost certainly is able to mount a prolonged defense of North Korea's territory while imposing severe damage on an adversary using conventional, biological, chemical, and nuclear weapons. North Korea remains one of the most militarized nations in the world and has more than 1 million active-duty personnel and 7 million reserve and paramilitary personnel. However, resource constraints are restricting Pyongyang's efforts to upgrade its aging conventional military systems beyond its missile and unmanned vehicle programs. North Korea's economy and logistics infrastructure support its national defense goals, but the country's industrial system is poorly constructed and deteriorating.

- > The KPA Ground Forces is the military's largest element, and more than 70 percent of its forces are deployed near the demilitarized zone with South Korea. The KPA intends to modernize the Ground Forces with next-generation systems, but competing priorities have slowed production. The KPA Special Forces is highly trained, well equipped, and able to infiltrate several thousand personnel into South Korea to target critical U.S. and South Korean defense infrastructure in the event of a conflict.
- > The KPA Air and Air Defense Force probably can threaten U.S. and allied aircraft entering North Korean airspace, despite its aging aircraft, minimal training, and resource shortfalls. In 2023, Pyongyang revealed two advanced UAVs, representing significant progress in its unmanned ISR and strike capabilities.
- > The KPA Navy is an outdated, primarily littoral fleet that probably can defend North Korea's coastline to delay an amphibious invasion. In 2023, it tested its first unmanned underwater vehicle.

### *Missile Research and Development and Weapons of Mass Destruction*

The KPA Strategic Forces is North Korea's nuclear-armed missile force operating ballistic and cruise missile systems that can threaten the U.S. homeland, U.S. forces stationed in the Indo-Pacific, and our allies. During the past year, North Korea successfully launched four ICBMs—including a solid-propellant system—and also test-launched a submarine-launched strategic cruise missile, signaling progress toward Pyongyang's stated goals of improving its missile accuracy, range, and launch options. North Korea is diversifying its land- and sea-based launch systems, including launching a missile from a silo and revealing a ballistic missile submarine for the first time. Pyongyang continues to illicitly procure items for its missile program that it cannot produce domestically, often in cooperation with Chinese and Russian nationals. In March, Kim inspected what Pyongyang claimed was a tactical nuclear weapon, which is a development that would further diversify North Korea's nuclear delivery options.

### *Space and Cyberspace Capabilities*

Similar to Iran, North Korea's overarching space and counterspace strategy is ill-defined. North Korea's primary goal throughout 2023 was to place a reconnaissance satellite in orbit. Using its indigenously designed Chollima-1 space launch vehicle, North Korea attempted three launches and succeeded with its final launch in November 2023, placing its Malligyong-1 military reconnaissance satellite into orbit. North Korea claims the satellite gives it the ability to collect and process imagery of U.S. and allied military installations.

North Korea maintains a sophisticated ability to conduct disruptive and destructive cyber activities. Pyongyang's cyber capabilities also support the regime's goals of generating revenue through complex cryptocurrency theft and ransomware campaigns. Pyongyang seeks to use cyber espionage globally, probably to gain insight into adversary capabilities and policies and acquire information to aid weapons development. North Korea's cyber capabilities almost certainly enable it to fund its priority military modernization efforts at current levels and steal technology critical to those efforts.

### *Outlook*

Pyongyang's continued development of new military capabilities indicates that the regime probably will doggedly pursue its priority defense modernization goals through the next year. North Korea seeks to further entrench its nuclear program, advance its ability to threaten regional interests, and expand the reach and sophistication of its weapons that can strike the U.S. homeland. In support of these goals, North Korea almost certainly will continue conducting illicit activity to generate revenue and persist in its efforts to court cooperation with Moscow, using Russian ammunition shortages to gain favor toward expanding military cooperation.

## TERRORISM

---

Decentralized ISIS and al-Qa'ida attack plotting against U.S. and ally interests continues globally. At the same time, counterterrorism operations have eroded the leadership ranks of transnational terrorist groups, probably leaving few ISIS and al-Qa'ida leaders capable of galvanizing supporters globally and further straining the groups' global networks. In response, ISIS has obscured the identities of its senior leaders, a departure from its past efforts to demonstrate resilience by highlighting its leaders in propaganda. Similarly, Al-Qa'ida has not publicly named a new leader since the 2022 death of Ayman al-Zawahiri; the group's presumed leader, Sayf al-Adl, is located in Iran.

- > Despite these setbacks, ISIS and al-Qa'ida groups are adjusting to changes in counterterrorism pressure. Most ISIS branches and al-Qa'ida affiliates are improving their ability to attack U.S. interests as well as local populations and security forces in 2024, which ISIS demonstrated through deadly attacks in Iran in January and Moscow in March.
- > At least two affiliates, al-Qa'ida in Yemen and ISIS in Afghanistan, probably will continue to seek to inspire, enable, and direct attacks against the U.S. homeland and other Western countries in 2024. Decentralized ISIS and al-Qa'ida affiliates also may seek to exploit perceived weaknesses in travel or border security measures to direct attacks in the U.S. homeland. After the October 7 HAMAS attack in Israel, both ISIS and al-Qa'ida have continued to call for attacks against U.S., Israeli, Jewish, and European interests worldwide.

### ISIS

Since 2022, ISIS lost three self-proclaimed caliphs, with its leadership cadre in the Middle East now probably at its weakest point. ISIS also has lost key personnel across its global network, including a senior official in Somalia who was killed during a U.S. military raid in 2023. ISIS is adapting to the losses and probably will focus on expanding in Africa and strengthening the external attack capabilities of ISIS-Khorasan in Afghanistan.

- > In Somalia, ISIS personnel serve as a key hub for the organization's funding and operations globally. In the Sahel and West Africa, ISIS branches are expanding their attack capabilities, probably increasing the threat of collateral harm to U.S. persons in the region.
- > In Afghanistan, the Taliban regime is carrying out a counterterrorism campaign against ISIS-Khorasan, but this pressure is not preventing the group from developing capabilities to conduct attacks regionally and in the West.

## 2024 ANNUAL THREAT ASSESSMENT

*Al-Qa'ida*

Al-Qa'ida's failure to publicly name a new leader and to reinvigorate a centralized, transnational plotting approach probably will compel the group to sustain its focus on localized plotting against U.S. and partner interests through at least 2024. In the absence of strong central leaders, al-Qa'ida affiliates have focused on attacking local security forces and governments while messaging that al-Qa'ida maintains a global agenda.

- > During the past year, al-Qa'ida affiliates—rather than the group's core leadership—have coordinated and issued strategic messages for al-Qa'ida's global network, including propaganda following the 7 October HAMAS attacks and after instances of Quran desecrations in Europe, to portray it as a cohesive, unified organization.
- > Al-Qa'ida affiliates in the Sahel and Somalia are gaining strength, with al-Shabaab posing the most direct threat to U.S. forces in Africa. Al-Qa'ida in the Arabian Peninsula (AQAP) probably continues to seek ways to enable lone-actor threats to the U.S. homeland, most recently enabling an attack that killed three U.S. servicemembers at Naval Air Station Pensacola in 2019.

## SOUTH & SOUTHEAST ASIA

---

### *Afghanistan*

The Taliban is firmly in control of Afghanistan and is effectively combating ISIS-Khorasan and anti-Taliban resistance groups, although these groups still conduct sporadic attacks inside the country. Some local Taliban fighters continue to kill or arrest former Afghan government and military personnel, but senior Taliban leaders probably are not directing this campaign. The Taliban is restricting al-Qa'ida's and its affiliates' activities in accordance with the organization's perception of its Doha Agreement obligations. Discontent about Taliban emir Haybatullah Akhundzada's leadership style and hardline social policies, including restricting the activities of women and girls, has exposed some fissures within the Taliban but is unlikely to fracture the organization. The focus on improving internal security and reducing violence has enabled some foreign investment and expanded trade. Nonetheless, the Taliban's failure to create an inclusive government and persistent regional concerns about armed militant activity and human rights issues in the country are likely to stymie its efforts to achieve international recognition.

- > Beijing is investing in mining and establishing trade and infrastructure links with the Taliban, but it has expressed concern about terrorist threats from a number of groups in Afghanistan, including ISIS-K and the East Turkestan Islamic Movement.
- > Islamabad is frustrated with the Taliban's failure to curtail Tehreek-e Taliban Pakistan cross-border attacks targeting Pakistani interests. Pakistan's implementation of the Illegal Foreigners Repatriation Plan (IFRP), which instituted a late-October 2023 deadline for undocumented Afghans to leave Pakistan, was largely a response to these concerns. The IFRP's resumed implementation is likely to exacerbate persistent border-related tensions between the countries. Tehran similarly has expressed concern about border clashes and boundary resolutions and for Afghan migrants in Iran.
- > The Taliban has received humanitarian aid and infrastructure assistance for highways and dams from India, but New Delhi remains concerned about the Taliban's connections with Pakistani intelligence, extremist safe havens in Afghanistan, and human rights abuses.

### *India*

During the past year, India has showcased itself as a global leader by hosting the Group of 20 economic summit and demonstrated a greater willingness to counter PRC activity throughout the Indo-Pacific region. India has advanced partnerships in the Indo-Pacific with regional SCS claimants, such as the Philippines, through training and defense sales and deepened cooperation with the United States, Australia, France, and Japan. In 2023, India took steps to modernize its military to compete with China and reduce its dependency on Russian-origin equipment. India conducted sea trials for its first domestically produced aircraft carrier and also has negotiated with

## 2024 ANNUAL THREAT ASSESSMENT

several Western countries on the transfer of key defense technologies. In 2024, New Delhi probably will focus on securing its national parliamentary elections, maintaining economic growth, and building on its “Make in India” initiative as part of its military modernization effort—which is aimed at countering Beijing.

- > Bilateral relations between India and China remain tense following the 2020 Galwan clash that killed 20 Indian soldiers and at least five PLA soldiers. In October 2023, senior Indian and PLA Army officers failed to resolve disputes about the two remaining standoff locations in eastern Ladakh during their twentieth round of talks. Both sides maintain approximately 50,000–60,000 troops in the area and continue to improve their military infrastructure near the border.
- > India has maintained its neutral stance on Russia’s invasion of Ukraine. Russia remains India’s most substantial defense partner and New Delhi continues to acquire weapons from Moscow, such as the S-400 surface-to-air missile system, despite New Delhi’s desire to diversify its defense acquisition partnerships.

*Pakistan*

Pakistan has sustained its nuclear modernization efforts despite its economic turmoil. Terrorist violence against Pakistani security forces and civilians also rose last year. In 2023, militants killed approximately 400 security forces, a 9-year high, and Pakistani security forces have conducted almost daily counterterrorism operations during the past year. Pakistan’s contentious relationship with India continues to drive its defense policy. However, cross-border violence between the countries has decreased since their February 2021 recommitment to a cease-fire.

- > Islamabad is modernizing its nuclear arsenal and improving the security of its nuclear materials and nuclear C2. In October, Pakistan successfully tested its Ababeel medium-range ballistic missile.
- > Pakistan consistently receives economic investment and defense support from China. In 2023, both countries continued to support the China-Pakistan Economic Corridor (CPEC), although Islamabad’s economic challenges and militant threats to PRC personnel in Pakistan have hindered progress on the initiative. Islamabad conducted multiple joint military exercises with Beijing in 2023, including the third iteration of a joint naval exercise that aims to strengthen naval cooperation and security.
- > Pakistan has sought international support, including from the UN Security Council, to resolve its dispute with India about Kashmir. Separately, Islamabad and New Delhi have maintained an uneasy ceasefire along the shared Line of Control since February 2021.

*South China Sea*

During the past year, the Southeast Asian SCS claimants Brunei, Malaysia, the Philippines, and Vietnam and nonclaimant Indonesia have taken measures to protect their territorial sovereignty and work with several partners to uphold international law. The Southeast Asian SCS nations prefer to use diplomatic means to manage territorial disputes, but regional governments also have signaled a resolve to improve their maritime security presence in response to perceived sovereignty violations by China.

- > The Philippines' military is attempting to shift its focus from internal security to external territorial defense in response to China's growing aggression in the SCS. During the past year, the Philippines has experienced repeated instances of PRC harassment and aggression at Scarborough Shoal. PRC Coast Guard ships also have interfered with routine Philippine resupply missions to its military detachment on the grounded naval ship—BRP *Sierra Madre*—at the Second Thomas Shoal, including the use of water cannons and dangerous maneuvers. In the past year, the Philippine defense forces conducted combined patrols in the SCS with several regional partners, including the United States, Australia, and Japan.
- > Most Southeast Asian countries are concerned that great power rivalries will fracture the region and undermine Association of Southeast Asian Nations centrality. In response to intensifying tensions, most regional governments are reinforcing nonaligned and "friends to all" foreign policies to avoid choosing sides and to benefit from maintaining relations with a range of regional and other partners.

## MIDDLE EAST

---

The October 2023 HAMAS attack on Israel has marked an inflection point for the Middle East by ushering in broad regional instability, imperiling Israel, disrupting regional diplomatic advances, and intensifying threats against the United States. The ensuing conflict prompted a pause in Israel–Saudi Arabia normalization talks, the resumption of Shia militia attacks against Coalition forces in Iraq and Syria after a months-long hiatus, a deadly attack against U.S. forces in Jordan, Huthi attacks against commercial shipping vessels in the Red Sea and Gulf of Aden, and more frequent Hizballah cross-border attacks into Israel. The HAMAS attack and Israeli response also has triggered widespread public protests across the region, and governments with ties to Israel—including Egypt, Jordan, and multiple Gulf states—have sought to contain internal dissent amid greater public scrutiny. Meanwhile, Moscow and Beijing are seeking to shape regional dynamics to their advantage.

- > Russia hosted HAMAS leaders in Moscow as recently as January 2024, highlighting its longstanding support for the terrorist group. Egypt's dependence on Russian grain imports is a major factor in the country's food security, and Egyptian and Russian officials are discussing avenues for bilateral defense cooperation. The Asad regime in Syria continues to depend on broad support from Russia and Iran.
- > China seeks steady access to Middle Eastern oil and natural resources, which are vital to moving the PRC economy forward. Beijing also is advocating itself as an alternative to U.S. leadership in the Middle East by promoting trade and development through the Belt and Road Initiative, calling for international conferences on the Israeli–Palestinian dispute, and mediating diplomatic normalization efforts between Saudi Arabia and Iran.

### *Iraq*

One year after its formation, the Iraqi government—backed by several Iran-aligned political parties—is seeking to balance its relationships with Washington and Tehran, to reward Iranian-aligned Shia militias, and to address domestic problems, including economic instability, climate change, and drug trafficking. In August 2023, Washington and Baghdad reaffirmed Iraqi government support for the presence of U.S. and Coalition military advisers to assist in developing Iraqi security forces (ISF) capabilities and established a committee to plan the future of the Coalition's military mission. However, the Israel–HAMAS conflict spurred Iraqi elites to call for the expedited removal of U.S. forces from Iraq, citing U.S. support to Israel, which has put immense strain on Prime Minister Muhammad Shia al-Sudani's ability to constrain the Iran-backed militias in country. During the next year, the Iraqi government will contend with a myriad of domestic challenges, which will be exacerbated by regional tensions and will complicate U.S. advising to counter-ISIS operations.

- > During the past year, Shia militias have pressed the Iraqi government to force a withdrawal of U.S. troops from Iraq through political influence and public rhetoric. The militias also have conducted UAV, rocket, and missile attacks on U.S. facilities with little interference from the ISF, despite Sudani's public condemnation of the attacks.
- > ISIS in Iraq and neighboring Syria remain degraded despite the group's efforts to rebuild its capacity. The ISF's counterterrorism units have marginally improved their strike capabilities but still rely on Coalition forces for air, targeting, and intelligence support to conduct operations against ISIS.
- > The ISF is able to conduct wide-area clearance operations to constrain ISIS but probably will be unable to unilaterally sustain targeted operations against the group within the next year.

### *Yemen*

Huthi maritime attacks against targets in the Red Sea and Gulf of Aden almost certainly pose a direct or collateral threat to U.S. forces. Since October 2023, the Huthis have launched missile and UAV attacks against maritime vessels—including U.S. warships—and into Israeli territory. Some of the weapons used by the Huthis traversed Saudi, Jordanian, or Egyptian airspace or landed in those countries, or they were shot down by nearby U.S. and allied forces. The Huthis have sought to demonstrate support for Palestinians and Iran-aligned groups to their domestic constituents and the international community and have warned against any Saudi Arabian normalization with Israel. The Huthis probably judge that Israel will remain distracted from retaliating against attacks from Yemen for at least the duration of the Gaza conflict.

- > Iran-backed Huthis have engaged for more than a year in negotiations with Saudi Arabia to end the Yemen conflict. However, the Huthis are unwilling to make key concessions and remain prepared to restart major offensives within Yemen and cross-border attacks into Saudi Arabia to press the Saudi-led coalition (SLC) to concede to their demands. In addition, the Huthis remain capable of conducting—and poised to launch—maritime attacks on SLC infrastructure.
- > Separately, although AQAP has been displaced from some of its territory in southern Yemen, the group remains intent on targeting—and probably has some capability to threaten—U.S. and partner interests in the region.

### *Syria*

Syrian President Bashar al-Asad's regime has consolidated control of approximately 70 percent of its pre-civil war territory. The remaining opposition has kept its strongholds in northern Syria, and the threat from a degraded ISIS presence persists in central Syria. More than a decade of conflict has diminished Syria's military, and in 2024, the Syrian Army—with Russian and Iranian backing—probably will remain occupied with protecting the Asad regime from internal threats. Although the Asad regime probably intends to rehabilitate and modernize its forces, resource constraints

## 2024 ANNUAL THREAT ASSESSMENT

and competing security priorities probably will inhibit progress for at least the next year. The Asad regime, Russia, and Iran share intelligence and have fomented tribal violence against U.S. and partner forces in eastern Syria to press for a U.S. withdrawal from Syria.

- > Syria's normalization of relations with other Arab states and readmission into the Arab League in May 2023 ended Damascus's diplomatic isolation in the Middle East. President Asad probably judges this has improved his legitimacy and will accelerate the country's economic recovery, but Syria so far has failed to secure tangible economic benefits from the regional rapprochement.
- > Support from Russia and Iran remains critical to the Asad regime's stability; both countries provide military assistance against opposition elements, diplomatic backing, and economic aid. In 2024, their support probably will evolve to place a greater emphasis on rebuilding the Syrian military and economy.
- > In 2023, Asad made his first visit to China since the start of the civil war to secure investment and expand trade, although PRC investment is likely to remain minimal given Syria's poor infrastructure, persistent security concerns, and unstable economy.
- > As of late 2023, approximately 15.3 million people—about 70 percent of Syria's population—required some form of humanitarian assistance, a 5-percent increase from 2022. Syria hosts 6.8 million displaced persons, a number that is likely to increase, further straining international aid organizations' ability to provide adequate assistance to meet escalating needs.

### Outlook

The outcome of the Israel-HAMAS crisis probably will be the largest driver of the region's trajectory during the next year. Israel almost certainly will focus on reemphasizing deterrence vis-a-vis its adversaries and normalizing relations with other regional actors. Egypt is seeking ways to prevent spillover effects from the crises in neighboring states and territories, including not only Gaza and Israel but also Libya and Sudan. Elsewhere, talks between Saudi Arabia and the Huthis are unlikely to resolve key differences between warring parties, and the Huthis' ability and willingness to threaten sea lanes in the Red Sea and Bab al-Mandeb Strait will be the primary enduring threat to U.S. interests from Yemen. Gulf states probably will continue to diversify their defense and security relationships and are likely to expand their economic and security ties to China.

## AFRICA

---

In 2024, enduring instability that foments additional violence is likely to pose the most pressing security threat to U.S. interests in Africa. Against this backdrop, many African countries almost certainly will grapple with political and economic instability and humanitarian crises that grew in scope and complexity during 2023. Weak or predatory security forces, popular disenfranchisement, and feeble political institutions in many states probably will compel continued outreach to foreign countries to meet security and infrastructure needs. Parts of Africa continue to contend with terrorist activity as ISIS and al-Qa'ida branches conducted more than 5,000 attacks across the continent in 2023, which is on par with the 2022 attack figures. In 2023, these attacks represented approximately 85 percent of ISIS and al-Qa'ida's attacks worldwide, underscoring their capabilities in Africa and the inability of regional militaries to combat the groups effectively. Poor governance continues to create the conditions for destabilizing conflicts to metastasize and spread to neighboring countries in 2024.

- > Many African countries see China as an important economic partner, and several African countries attended the third BRI Summit in Beijing in October 2023. African countries also are deepening military and security ties to China, including infrastructure development that may benefit Beijing's military goals. In February, South Africa hosted the second iteration of a trilateral naval exercise with China and Russia. Some African countries also see Russia as an important security partner including , the Central African Republic and Mali, which continue to partner with Russian PMCs for security.
- > Amid the continent's security problems, some countries will continue to support international efforts to address challenges in Africa and beyond. Morocco and Tunisia, which have provided hundreds of troops to Africa-based UN peacekeeping operations, are poised to sustain their contributions in 2024. Kenya is poised to serve as a key U.S. security partner in and beyond East Africa, and it has pledged to send police to Haiti by 2024.

### *North Africa*

Moroccan-Algerian diplomatic ties remain severed with no sign of near-term rapprochement, and the low-intensity conflict between Morocco and the Algeria-backed Polisario Front continued unabated in 2023. North Africa remains a hub for immigration to Europe, with migrants transiting Tunisia and Libya to access dangerous routes across the Mediterranean Sea. The leader of al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) remains in Algeria where the group's efforts primarily focus on serving as a financial and communications facilitation hub for al-Qa'ida senior leadership and its subordinate Sahel-located affiliates. Despite al-Qa'ida leadership's regular communiqués urging action, AQIM attacks remain primarily defensive in nature and target local security forces.

## 2024 ANNUAL THREAT ASSESSMENT

In Libya, distrust lingers among rival militias despite some instances of cooperation, especially in response to flooding in September 2023. Senior officials in the self-described Libyan National Army (LNA) are engaging more frequently with Russian leaders, including with Putin, following the death of PMC Vagner owner Yevgeniy Prigozhin.

*West Africa*

West Africa continues its democratic backsliding trend, with military coups in Niger and Gabon in the past year and election irregularities that probably will exacerbate public discontent. The coup in Niger is detracting from counterterrorism operations in the Sahel and the ruling junta's focus on consolidating power, combined with the withdrawal of UN forces from Mali and conflict between the Vagner-supported Malian military and armed groups in the country's north, almost certainly will perpetuate a permissive operating environment for violent extremist organizations in 2024. Planned presidential elections this year in Chad, Ghana, Mali, and Mauritania, amid ongoing internal security and economic crises, probably will exacerbate pressure on governments that are already poorly postured to effectively respond to turmoil.

*East Africa*

In 2023, East Africa experienced multiple security crises that complicated humanitarian assistance efforts. Counterterrorism operations in central Somalia have slowed amid international concerns that Somali forces are not ready to assume duties from the African Union Transition Mission that are scheduled to hand off responsibilities in December 2024. In Sudan, fighting between military and paramilitary forces has spread to new areas since the outbreak of hostilities in April 2023, exacerbating a humanitarian crisis that the United Nations has called one of the worst in recent history. The Ethiopian government's Cessation of Hostilities Agreement with Tigray is holding, but its government is now contending with ethnic insurgent groups in the Amhara and Oromia regions.

*Central and Southern Africa*

During the past year, central Africa has faced heightened violence, jeopardizing already fragile humanitarian and economic situations. Tensions between the Democratic Republic of the Congo and Rwanda—as well as their use of armed proxies against one another—have escalated, creating conditions for direct conflict. The Central African Republic's reliance on PMC Vagner to maintain security has resulted in regular reports of human rights violations. Zimbabwe's August elections were rife with instances of fraud and the regime's intimidation of opposition and civil society members. In 2023, Mozambique's military and partner forces made gains against ISIS-Mozambique and claimed to have killed the group's leader, however, ISIS-Mozambique has resurged as some partner forces plan to withdraw beginning in June.

## LATIN AMERICA

---

Latin America continues to be a region where socioeconomic conditions make it attractive for our competitors trying to secure greater political, economic, or security influence, and transnational crime fosters insecurity and migration. The region's powerful transnational criminal organizations (TCOs)—which are responsible for most of the illicit fentanyl and other illegal drugs entering the United States—drive regional crime and perpetuate insecurity through drug trafficking, migrant smuggling, money laundering, arms trafficking, and corrupting security forces and public institutions.

- > South America's recent trend of electing left-leaning presidents was upended in 2023 when a right-leaning candidate defeated the incumbent economy minister in Argentina; Paraguay elected a conservative committed to maintaining strong ties to the United States and Taiwan; and Ecuador elected U.S.-friendly president Daniel Noboa.
- > Since January, Brazilian President Luiz Inacio Lula da Silva has focused on elevating Brazil as an influential regional and global leader by hosting a regional summit, meeting more than 50 leaders, and visiting 21 countries, including trips to Russia and China.
- > Haiti continues to experience worsening gang violence resulting in social and economic disruption. Kenya has committed to lead a UN-backed multinational security support mission and deploy 1,000 of its security forces to Haiti in 2024.
- > Mexico is scheduled to hold national elections in June 2024. As of early December 2023, both presidential frontrunners had met with the U.S. ambassador to Mexico and discussed maintaining positive bilateral relations through the next 6-year administration.

### *Chinese, Russian, and Iranian Activity*

Latin America is an important arena for China to cultivate influence and relationships and compete for favor in proximity to the United States as the region includes seven of the remaining 13 states that diplomatically recognize Taiwan. Economic engagement is a critical component of this strategy, and Beijing uses this engagement to access markets from which to source critical resources, such as lithium, and advance its BRI. Twenty-two Latin American countries are BRI signatories, including Honduras as recently as June 2023.

- > China's trade with Latin America increased by 70 percent during the past decade, and a majority of countries count China either as their largest or second-largest trade partner. China holds large market shares in strategic sectors, such as infrastructure development, public utilities, and telecommunications, and it has donated military equipment to Latin American countries.

## 2024 ANNUAL THREAT ASSESSMENT

- > Chinese state-owned enterprises control stakes in energy transmission and distribution infrastructure in a number of countries in the region. Similarly, the presence of PRC technology companies in Latin America—specifically within the region's existing 4G infrastructure—and their academic ties to some regional universities has ensured the PRC plays a prominent role in Latin America's 5G development. China also has increased its ground-based space facilities to 10 sites across 5 countries in the region to improve space-domain awareness of U.S. assets and counterspace capabilities.
- > Iran increased military activities in Latin America during 2023, deploying a Jamaran class guided-missile corvette to the region, signing a defense cooperation memorandum of understanding with Bolivia, and delivering fast-attack patrol vessels, typically equipped with anti-ship cruise missiles, to Venezuela.

Russia enjoys security engagement and influence with its historical strategic partners—Cuba, Nicaragua, and Venezuela—and is trying to maintain broader regional outreach through bilateral relationships and international fora. However, Moscow's war in Ukraine has drawn condemnation from the majority of countries in Latin America and the Caribbean, and Russia's military engagement with other partners in the region consists mainly of maintenance support for previously purchased Russian equipment.

- > Nicaragua seeks to deepen bilateral cooperation and military interoperability with Russia. Nicaragua is the only Latin American country that voted against the UN resolution condemning Russia's invasion of Ukraine; Bolivia, Cuba, and El Salvador abstained from voting.

### Venezuela

The regime of disputed Venezuelan President Nicolas Maduro continues to control all domestic institutions despite holding an approval rating under 20 percent and having an economy that has contracted 75 percent since he took office in 2013. The leading opposition candidate remains barred from running in the July 2024 presidential election.

- > In 2023, Maduro retained his two top military officers, citing their loyalty and contributions to the country. Security forces have focused on tackling domestic gangs rather than operations against a Revolutionary Armed Forces of Colombia dissident faction active in the country.
- > As of November 2023, more than 7.7 million Venezuelan migrants and refugees had been displaced globally, 85 percent of whom are dispersed throughout Latin America and the Caribbean. Colombia and Peru have the largest Venezuelan diaspora populations with nearly 2.9 million and more than 1.5 million migrants, respectively.
- > In 2023, Venezuela renewed its claim to the oil rich Essequibo region of Guyana; that claim dates to the 1890s and has been rejected in international arbitration. In April 2024, Maduro signed a law creating a new notional state that includes the entire region.

### *Cuba*

During the past year, socioeconomic conditions have deteriorated significantly, with worsening food and medical shortages and power outages that have amplified concerns about resulting civil unrest. Nonetheless, Cuban security forces and their affiliated cyber components are postured to suppress this growing domestic dissent and ensure the regime's survival for the next year.

- > Cuba relies on foreign partners—particularly China, Iran, Russia, and Venezuela—for military and economic support. Russia remains Cuba's preferred security partner and Havana receives assistance from Moscow to maintain its Soviet-era military inventory. During the past year, Cuba also has received fuel shipments from Mexico to help address its energy shortfalls.
- > Havana very likely is receptive to increased political, economic, energy, defense, and security cooperation with Beijing, Moscow, and Tehran because of concerns about domestic instability and perceived internal threats to the government of Miguel Díaz-Canel.

### *Drug Trafficking*

Mexican TCOs are the primary producers and traffickers of synthetic drugs—including fentanyl and methamphetamine—to the United States; they also traffic cocaine and heroin, contributing to historic numbers of drug-related deaths of U.S. citizens. Mexican TCOs also facilitate illegal migration over the United States' southwest border and contribute to high levels of violence and corruption in Mexico, affecting U.S. individual and commercial interests and the efficacy of Mexico's institutions. In 2024, Mexican TCOs probably will seek expansion into new global markets, primarily to European markets, to offset some decline in revenue from the saturated U.S. cocaine and synthetic drug market. Mexico's government remains a key partner to counter these violent TCOs and their illicit activities.

- > The amount of fentanyl seized at the U.S. southwest border increased by 85 percent in 2023. Fentanyl seizures have increased every year since 2019, with seizures at the southwest border surpassing heroin for the first time in 2021.<sup>6</sup> Fentanyl production remains elevated in Mexico despite Mexican TCOs announcing a ban on production in October 2023, probably hoping to alleviate Mexican government enforcement and extradition efforts.
- > According to the most recent statistics of the Centers for Disease Control and Prevention (CDC), reported U.S. drug overdose deaths remained elevated at 105,303 for the 12-month period ending in October 2023, but dipped slightly from 107,785 from the same time period ending in October 2022. The majority of these overdose deaths were related to fentanyl.

*Refugee Flows and Migration*

Fragile economic, security, political, and environmental conditions throughout the Western Hemisphere will remain the enduring factors driving migration within the region. Additional factors—including heightened xenophobia and misperceptions of U.S. immigration policies—also have contributed to persistently high migration levels.

- > In fiscal year 2023, more than 2.47 million irregular migrants were encountered at the U.S. southwest border, breaking the previous record of 2.37 million migrants in fiscal year 2022, according to U.S. Government data. Migrant flows through Panama serve as an early indicator of flows to the southwest border and surpassed 520,000 in 2023, breaking the 2022 record of 240,000 and demonstrating Panama's significance as a Western Hemisphere transit country toward the United States.
- > Before 2022, the majority of migrants were from Mexico and the Northern Central American countries of El Salvador, Guatemala, and Honduras. The past two years brought notable increases in migrants from countries such as Colombia, Cuba, Ecuador, Nicaragua and Venezuela, a trend that probably will continue through 2024.
- > Citizens from El Salvador, Guatemala, and Honduras experience severe poverty, worsening food security, and some of the highest homicide and violent crime rates in the world, which continue to drive emigration from these countries.
- > Higher levels of Haitians and Cubans have continued to migrate through maritime routes to the United States because of deteriorating socioeconomic conditions and U.S. immigration policies that are perceived as more favorable, and these trends probably will persist at elevated levels for at least the next year.

## OTHER GLOBAL THREATS

---

### *Foreign Intelligence Service Activity*

Adversary use of Ubiquitous Technical Surveillance (UTS) capabilities presents one of the most acute and generalized threats to DoD and U.S. Government personnel traveling or operating worldwide. UTS is the widespread collection, processing, and analysis of aggregated data captured from various sources that can identify patterns of activity that link persons to things, events, or locations. An increased interest in understanding consumer preferences paired with the capabilities of smart devices (phones, fitness trackers, video doorbells, etc.) have created a market based around data collection that incentivizes and enables companies to compile data on people, places, and organizations, which can adversely affect U.S. national security interests. Adversaries can collect financial transactions, communications, technology employed, or presence near a place of interest or sensitive location to compromise costly investments in our defense and intelligence capabilities. Increasing adversary use and proliferation of these capabilities will have profound implications for the mission, structure, and resources of the Defense Counterintelligence Enterprise for the foreseeable future.

### *Targeting Defense Critical Infrastructure*

Both Russia and the PRC have developed military doctrines to target U.S. critical infrastructure during a conflict with the United States. During the next 12 months, cyber threats from China will continue to pose a significant threat to U.S. defense critical infrastructure, which is consistent with trends we have observed since at least 2008. If a conflict were to occur, China probably would use cyber forces to disrupt, degrade, or destroy U.S. defense critical infrastructure. During a direct conflict, Russia also almost certainly would conduct malicious cyber activities on U.S. energy infrastructure and military sites, and if the conflict escalated, it would target critical infrastructure with precision-guided missiles. Along with the increasing threat from Chinese cyber operations, other foreign adversaries and domestic violent extremists also are able to pose a threat to DoD readiness by targeting defense critical infrastructure.

- > As of September 2023, Chinese cyber operations were more frequently attempting to collect against the U.S. defense-industrial base and other critical infrastructure. Russian cyber actors have gained operational experience conducting attacks against Ukraine's infrastructure, which probably will be used to inform cyber operation planning targeting United States interests during a conflict.
- > Since at least 2019, PRC nationals have attempted to gain access to U.S. military installations containing defense critical infrastructure. Although the vast majority of these attempts are deemed benign, a small percentage require further investigation. As of

## 2024 ANNUAL THREAT ASSESSMENT

September, PRC businesses and other entities had acquired more than 300,000 acres of agricultural land near U.S. military bases.

- > The proliferation of small, nonattributable unmanned aircraft systems (UASs) probably poses a threat to DoD facilities in the homeland. An increasing number of unidentified UASs have been detected at military training grounds, bases, and during exercises, suggesting adversaries probably use them for covert intelligence collection.

### *Advanced Technology*

Global advancements in artificial intelligence (AI), biotechnology, quantum sciences, and microelectronics pose a significant threat to U.S. technological advantage. Key adversaries recognize the potential for advanced technologies to enhance military processes, equipment, and forces, and dual-use breakthroughs in the commercial sector can enable even less capable states and nonstate actors to benefit. The PRC continues its state-led drive to dominate critical advanced technology fields, and the PLA is striving to integrate advanced technologies to enhance its forces and field disruptive military capabilities. The PRC also sponsors researchers and scientists who licitly and illicitly acquire intellectual property innovated by DoD-funded research programs. Russia maintains its strategic ambition to develop advanced technologies for military capabilities, but ongoing international sanctions and export controls will constrain its progress.

- > States are developing AI to improve decisionmaking support, enable quicker and more accurate ISR and targeting, tailor influence operations, advance cyber capabilities, and develop unmanned vehicles with higher levels of autonomy. Developing or acquiring software, hardware, and data that are optimized for military systems and processes will be key to any country's effectiveness in fielding these capabilities.
- > Researchers worldwide are pursuing dual-use biotechnologies that can support military applications, including human performance enhancements and human-machine integration for improved C2.
- > Quantum technologies—including computing, communications, and sensing—probably will provide militaries with advanced capabilities in decryption; positioning, navigation, and timing; and ISR. Although select research areas, such as sensing, are advancing more rapidly, non-governmental experts indicate that development of a quantum computer capable of decryption is unlikely in this decade.

Microelectronics continue to be the linchpin of technology competition and represent a critical chokepoint in adversary development and acquisition efforts. Access to high-end microelectronics underpins a state's ability to develop computing-intensive advanced technologies, such as AI and quantum. Although the United States and its allies maintain a technological advantage in manufacturing and design processes, ongoing adversary efforts to reduce foreign dependency constrain our opportunities to protect these critical technologies. The PRC continues to pour resources into securing its supply chain and developing domestic high-end microelectronics manufacturing capabilities. Export controls limit PRC access to U.S. and allied technologies and

are slowing its efforts, but Beijing has used less efficient techniques with legacy equipment and exploited policy loopholes to close the technology gap.

### *Global Health and Biodefense Trends*

Biological threats to national and economic security come not only from biological weapons but also from major disease outbreaks, continued increases in antimicrobial resistance, or the release of a deadly pathogen associated with a dual-use research of concern. To this end, the ongoing cholera outbreak in Haiti almost certainly has complicated the internal security situation, and outbreaks of African swine fever and avian influenza are straining world food supplies. Similarly, the potential use of biological weapons by state or nonstate actors remains a persistent threat to U.S. interests worldwide. The COVID-19 pandemic and ongoing conflicts have exacerbated many nations' medical infrastructure and their ability to respond to health threats.

The risk of laboratory accidents may be increasing with the rise in the number of laboratories around the world conducting high-risk life sciences research and research with potential pandemic pathogens without appropriate oversight. In a number of countries around the world, pathogens are stored in laboratories that lack appropriate biosecurity measures to prevent diversion by actors that wish to do harm. Beijing is expanding its network of high-containment laboratories both within China and helping to construct laboratories around the globe.

- > Advances in biotechnology, including synthetic biology, could make it easier to develop and use biological agents as weapons. New technologies, such as AI and genomic modification, have the potential to create more effective, resilient, and cost-efficient military and civilian applications while also creating new threat vectors for state and nonstate actors to exploit. For example, the same biological and chemical science advancements created to develop lifesaving medical countermeasures could also be used by adversaries to develop new or enhanced agents.
- > Russia's war against Ukraine has highlighted the strain that prolonged conflict can have on military medical capabilities to provide combat casualty care. In Ukraine, hospitals and medical facilities have been targeted, and medical evacuations by ground forces routinely come under attack by Russian forces. Forward medical teams need the capability to provide prolonged field care, more advanced resuscitation methods, and emergency stabilization surgeries on a larger number of patients before they can be moved away from the frontline area.

### *Climate and Environmental Change*

During the next decade, defense forces globally will need to expand planning efforts to address climate-linked effects on military readiness and operations, including for infrastructure, equipment, supply chains, logistics capacity, and the health and wellness of military personnel. Climate change also very likely will intensify natural disasters, regional instability, conflict, and geopolitical competition—increasing the scope of situations to which some militaries may have

## 2024 ANNUAL THREAT ASSESSMENT

to respond. This will strain resources as militaries are forced to address humanitarian and crisis situations, shifting focus away from conventional threats, training, and readiness.

- > Climate change is expected to alter storm and drought seasons, decrease freshwater availability, and increase water pollution—resulting in more widespread water insecurity. Water scarcity, shifting precipitation cycles, and climate shocks will hinder agricultural productivity and worsen food insecurity, very likely provoking conflict in some areas.
- > Natural disasters are the largest cause of internal displacements globally. Deteriorating environmental conditions will be a driver of migration, and remaining populations will be either unable or unwilling to move out of increasingly uninhabitable locations. Climate change disproportionately affects more vulnerable populations and poorer countries by compounding existing humanitarian crises.



## BIOGRAPHY



UNITED STATES AIR FORCE

## LIEUTENANT GENERAL JEFFREY A. KRUSE

Lt. Gen. Jeffrey A. Kruse is the Director of the Defense Intelligence Agency, Joint Base Anacostia-Bolling, Washington, D.C. As the Director of DIA, Lt. Gen. Kruse serves as the Department of Defense's senior military intelligence official supporting the Secretary of Defense, Chairman of the Joint Chiefs of Staff, military services, combatant commands and the Director of National Intelligence by providing intelligence, counterintelligence, enterprise management, acquisition support, secure communications and crisis support to policymakers and warfighters around the globe.

Prior to assuming his role at DIA, Lt. Gen. Kruse served as the Advisor for Military Affairs for the Director of National Intelligence and was awarded the National Intelligence Superior Service Medal. In this capacity—in partnership with executive leaders across DoD and the Intelligence Community—he oversaw and advocated for activities, capabilities and policies to drive enduring DoD-IC integration. Lt. Gen. Kruse also served as the Director for Defense Intelligence for Warfighter Support in the Office of the Under Secretary of Defense for Intelligence and Security.

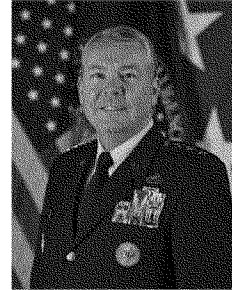
Lt. Gen. Kruse has extensive operational and combat experience in multiple theaters around the globe. He served as the Director of Intelligence for U.S. Indo-Pacific Command, deployed as the Director of Intelligence for Combined Joint Task Force-Operation Inherent Resolve in the Middle East and served as the Senior Special Advisor to the Commander of U.S. European Command and Supreme Allied Commander Europe. Throughout his career, Lt. Gen. Kruse commanded Air Force and joint units at the squadron, group and wing levels. Other assignments included serving as Chief of Legislative Affairs for U.S. Strategic Command and as a programmer, panel chair, and head of the Air Force's "Engine Room," which develops the service's annual budget.

## EDUCATION

1990 Bachelor of Arts, Political Science, Miami University, Oxford, Ohio  
 1991 Distinguished Graduate, Intelligence Officer Training, Goodfellow Air Force Base, Texas  
 1996 Honor Graduate, Master of Science, Strategic Intelligence, Joint Military Intelligence College, Washington, D.C.  
 1997 Distinguished Graduate, Squadron Officer School, Maxwell AFB, Ala.  
 2004 Master of Arts, National Security and Strategic Studies, with Highest Honors, College of Naval Command and Staff, U.S. Naval War College, Distinguished Graduate, Newport, R.I.  
 2008 Master of Science, National Security Strategy, National War College, National Defense University, Washington, D.C.

## ASSIGNMENTS OR CAREER CHRONOLOGY

1. April 1991–November 1991, Student, Intelligence Officer Training, Goodfellow Air Force Base, Texas  
 2. November 1991–December 1993, Chief of Intelligence, 682nd Air Support Operations Center, Shaw AFB, S.C.  
 3. January 1994–July 1994, Deputy Chief, Training and Tactics, 609th Air Intelligence Squadron, Shaw AFB, S.C.  
 4. July 1994–August 1995, Chief, Intelligence Section, 78th Fighter Squadron, Shaw AFB, S.C.  
 5. September 1995–September 1996, Student, Joint Military Intelligence College, Washington, D.C.  
 6. September 1996–September 1997, Instructor and Course Supervisor, Intelligence Applications Officer Course, Goodfellow AFB, Texas  
 7. September 1997–June 1998, Executive Officer, 17th Training Wing, Goodfellow AFB, Texas  
 8. June 1998–July 2000, Commander, 314th Training Squadron, Fort Huachuca, Ariz.  
 9. August 2000–January 2002, Chief, Strategic and Theater Targeting Sections, then Chief, Hard and Deeply Buried Targets Branch, U.S. Strategic Command, Offutt AFB, Neb.  
 10. January 2002–July 2003, Special Assistant to the Commander in Chief and Chief, Legislative Affairs, USSTRATCOM, Offutt AFB, Neb.  
 11. August 2003–June 2004, Student, College of Naval Command and Staff, Naval War College, Newport, R.I.  
 12. July 2004–April 2005, Chief, Intelligence Force Management Branch, Headquarters Air Combat Command, Langley AFB, Va.  
 13. May 2005–June 2006, Commander, Pacific Air Forces Air Intelligence Squadron, Hickam AFB, Hawaii  
 14. June 2006–June 2007, Deputy Director of Intelligence, Seventh Air Force, and Deputy Commander, 607th Air Intelligence Group, Osan Air Base, South Korea  
 15. July 2007–June 2008, Student, National War College, National Defense University, Fort Lesley J. McNair, Washington, D.C.  
 16. July 2008–February 2010, Chief, Information Superiority Division, then Chief, C2 and Cyber Superiority Division, Deputy Chief of Staff, Plans and Programs, Headquarters U.S. Air Force, Arlington, Va.



## EFFECTIVE DATES OF PROMOTION

|                                        |  |
|----------------------------------------|--|
| Second Lieutenant<br>December 16, 1990 |  |
| First Lieutenant<br>December 16, 1992  |  |
| Captain<br>December 16, 1994           |  |
| Major<br>January 01, 2002              |  |
| Lieutenant Colonel<br>May 01, 2005     |  |
| Colonel<br>October 01, 2008            |  |
| Brigadier General<br>June 08, 2015     |  |
| Major General<br>July 24, 2018         |  |
| Lieutenant General<br>August 16, 2020  |  |

17. March 2010–June 2010, Chief, Program Integration Division (“Engine Room”), Deputy Chief of Staff, Plans and Programs, Headquarters U.S. Air Force, Arlington, Va.
18. July 2010–July 2012, Commander, 361st Intelligence, Surveillance, and Reconnaissance Group, Hurlburt Field, Fla.
19. July 2012–June 2014, Commander, 480th Intelligence, Surveillance, and Reconnaissance Wing, Joint Base Langley-Eustis, Va.
20. June 2014–May 2015, Senior Special Assistant to the Commander, U.S. European Command and Supreme Allied Commander Europe, Mons, Belgium
21. June 2015–June 2016, Director of Intelligence, Combined Joint Task Force-Operation Inherent Resolve, Southwest Asia
22. July 2016–July 2019, Director for Intelligence, U.S. Indo-Pacific Command, Camp Smith, Hawaii
23. July 2019–August 2020, Director of Defense Intelligence (Warfighter Support), Office of the Undersecretary of Defense (Intelligence & Security), the Pentagon, Arlington, Va.
24. August 2020–February 2024, Director’s Advisor for Military Affairs, Office of the Director of National Intelligence, McLean, Va.
25. February 2024–present, Director, Defense Intelligence Agency, JB Anacostia-Bolling, Washington, D.C.

#### SUMMARY OF JOINT ASSIGNMENTS

1. August 2000–July 2003, Chief, Strategic and Theater Targeting and Chief, Hard and Deeply Buried Targets, then Special Assistant to the CINC and Chief, Legislative Affairs, U.S. Strategic Command, Offutt Air Force Base, Neb., as a captain and major
2. June 2014–May 2015, Senior Special Assistant to the Commander, U.S. European Command and Supreme Allied Commander Europe, Mons, Belgium, as a colonel
3. June 2015–June 2016, Director of Intelligence, Combined Joint Task Force-Operation Inherent Resolve (CJTF-OIR), Southwest Asia, as a brigadier general
4. July 2016–July 2019, Director for Intelligence, U.S. Indo-Pacific Command, Camp Smith, Hawaii, as a brigadier general and major general
5. July 2019–August 2020, Director of Defense Intelligence (Warfighter Support), Office of the Undersecretary of Defense (Intelligence & Security), the Pentagon, Arlington, Va., as a major general
6. August 2020–February 2024, Director’s Advisor for Military Affairs, Office of the Director of National Intelligence, McLean, Va., as a lieutenant general
7. February 2024–present, Director, Defense Intelligence Agency JB Anacostia-Bolling, as a lieutenant general

#### MAJOR AWARDS AND DECORATIONS

Defense Distinguished Service Medal  
 National Intelligence Superior Service Medal  
 Defense Superior Service Medal with three oak leaf clusters  
 Legion of Merit with two oak leaf clusters  
 Defense Meritorious Service Medal  
 Meritorious Service Medal with four oak leaf clusters  
 Joint Service Commendation Medal  
 Air Force Commendation Medal with oak leaf cluster  
 Army Commendation Medal  
 Joint Service Achievement Medal  
 Air Force Achievement Medal  
 Joint Meritorious Unit Award with four oak leaf clusters  
 Air Force Outstanding Unit Award with three oak leaf clusters  
 National Defense Service Medal with bronze star  
 Southwest Asia Service Medal with bronze star  
 Inherent Resolve Campaign Medal with two bronze stars  
 Global War on Terrorism Expeditionary Medal  
 Global War on Terrorism Service Medal  
 Korean Defense Service Medal  
 Nuclear Deterrence Operations Service Medal  
 Small Arms Expert Marksmanship (Pistol)  
 Kuwait Liberation Medal - Government of Kuwait

(Current as of March 2024)





---

---

**WITNESS RESPONSES TO QUESTIONS ASKED DURING  
THE HEARING**

APRIL 11, 2024

---

---



#### **RESPONSE TO QUESTION SUBMITTED BY MR. KEATING**

Ms. HARRIS. Russia utilizes black markets to obtain advanced technologies, consumer electronics, financial services, weapons, and other supplies that it is unable to acquire from domestic or legitimate international sources.

This includes commercial satellite communications services, which black market operators around the world have long sought to acquire. Russian entities operate illicit networks to circumvent sanctions, export controls, and other regulations to obtain prohibited goods and services. These black-market activities are not unique to Starlink services.

Rather, they reflect broader challenges of enforcing sanctions against both state actors and nonstate actors determined to acquire and employ weapons and sophisticated enabling capabilities in order to advance their objectives. The Department of Defense (DoD), in concert with other U.S. Government departments and agencies, and in close cooperation with the Government of Ukraine and SpaceX, has been investigating and disrupting these illicit Russian activities since they first became known several months ago.

SpaceX has cooperated with the U.S. Government and the Government of Ukraine and has been forward-leaning in providing information to support investigations and denying service to suspected illicit users. These cooperative efforts to disrupt Russian use of Starlink services continue, as Russian forces adapt and persist in efforts to regain their illicit access. [See page 17.]

#### **RESPONSE TO QUESTION SUBMITTED BY MS. JACOBS**

Ms. HARRIS. Facial recognition technology on drones continues to see significant advancements as new algorithms are improving accurate detection from higher altitudes, longer distances, and steeper angles; however, the accuracy can still vary based on these and other factors, such as lighting conditions in the environment.

To ensure all AI-enabled capabilities are used responsibly, the Department is working to improve the ability of operators to understand how well models perform on different tasks and in different environments, and how to use them most effectively in their mission. This work is guided by DoD's AI Ethical Principles and implemented through guidance and toolkits that provide hands-on, actionable steps AI developers and users can take to ensure responsible use of AI in DoD.

The DoD adopted AI Ethical Principles (Responsible, Equitable, Traceable, Reliable, and Governable) in February 2020. These principles reflect our nation's longstanding norms and values -- including those in the U.S. Constitution, Title 10 of the U.S. Code, and the Law of War, -- in the context of AI. These principles provide a foundation for the responsible design, development, deployment, and use of AI capabilities by the Department.

In 2021, Deputy Secretary Hicks provided additional guidance by publishing six Responsible AI (RAI) tenets -- RAI Governance, Warfighter Trust, AI Product and Acquisition Lifecycle, Requirements Validation, Responsible AI Ecosystem, and AI Workforce -- to direct the Department's holistic, integrated, and disciplined approach for RAI. The same memorandum created an RAI Working Council to develop lines of effort on how to operationalize the DoD AI Ethical Principles.

Then, in 2022, DoD released the Responsible AI Strategy & Pathway, which lays out the courses of action necessary to put the AI Ethical Principles into practice. As part of implementation, the Office of the Chief Digital and Artificial Intelligence Officer has developed and publicly published a Responsible AI Toolkit at <https://rai.tradewindai.com> to enable personnel in assessing the alignment of AI systems with the DoD's AI Ethical Principles and to mitigate issues or risks identified. [See page 19.]

Ms. HARRIS. DoD Directive 3000.09, Autonomy in Weapon Systems, establishes Departmental policy and assigns responsibilities for developing and using autonomous and semi-autonomous functions in weapon systems, including armed platforms that are remotely operated or operated by onboard personnel.

The directive establishes guidelines designed to minimize the probability and consequences of failures in autonomous and semi-autonomous weapon systems that

could lead to unintended engagements, which the directive defines as “[t]he use of force against persons or objects that commanders or operators did not intend to be the targets of U.S. military operations, including unacceptable levels of collateral damage beyond those consistent with the law of war, Rules of Engagement, and commander’s intent.”

For example, a weapon system accidentally engaging an innocent civilian during military operations would be an “unintended engagement.” DoD Directive 3000.09 was updated in January 2023. It supplements a variety of policies, processes, and frameworks in place across the Department to ensure the responsible use of weapon systems, including legal reviews of the intended acquisition, procurement, or modification of weapon systems for consistency with the Law of War.

Each of the DoD AI Ethical Principles is included in the current version of DoD Directive 3000.09 and the directive also provides generally that “[t]he design, development, deployment, and use of AI capabilities in autonomous and semiautonomous weapon systems will be consistent with the DoD AI Ethical Principles and the DoD Responsible Artificial Intelligence Strategy and Implementation Pathway.” DoD Directive 3000.09 provides for many measures to address the risk of unintended engagements.

For example, the directive calls for rigorous hardware and software verification and validation (V&V) and realistic system developmental and operational test and evaluation (T&E) as well as the establishment of training, doctrine, and tactics, techniques, and procedures applicable to the system in question.

In addition, autonomous weapon systems, with certain exceptions, must be approved by senior DoD officials through the review process outlined in Section 4 of DoD Directive 3000.09 “Autonomy in Weapon Systems” before formal development and again before fielding.

This holistic, case-by-case process includes, for systems incorporating AI capabilities, consideration of whether the deployment and use of the AI capabilities in the weapon system will be consistent with the DoD AI Ethical Principles and the DoD Responsible AI Strategy and Implementation Pathway. These criteria, along with several others, must be verified by senior DoD officials before systems undergoing review may be developed or fielded. [See page 20.]

#### **RESPONSE TO QUESTION SUBMITTED BY MRS. MCCLELLAN**

General KRUSE. [No answer was available at the time of publication.] [See page 15.]

---

---

**QUESTIONS SUBMITTED BY MEMBERS POST HEARING**

APRIL 11, 2024

---

---



#### QUESTIONS SUBMITTED BY MR. KELLY

Mr. KELLY. As you know, CYBERCOM's capability to comprehend and counteract malign influence campaigns from foreign adversaries, along with their narrative intricacies, is crucial for bolstering cognitive security in national defense. I commend the commendable efforts of the Cyber National Mission Force (CNMF) in identifying and thwarting malicious influence campaigns targeting the U.S.

The FY24 NDAA underscored the perpetual evolution and amplification of foreign adversary information and influence campaigns, highlighting an augmented necessity to comprehend the genesis of malign influence and disinformation, their dissemination and evolution, their channels to intended audiences, and their ensuing impact.

Acknowledging the FY24 NDAA's directive, the Department of Defense is tasked with evaluating and proposing recommendations regarding the establishment of a narrative intelligence center. CYBERCOM, particularly CNMF, has already demonstrated significant collaboration with industry and academic institutions in countering malign influence campaigns in this domain, and I welcome your sustained engagement in this endeavor.

When can we anticipate the recommendations for establishing a DoD national center for narrative intelligence, considering the evolving landscape of foreign adversary influence campaigns emphasized in the FY24 NDAA? Additionally, how do you intend to capitalize on the existing expertise of CYBERCOM, notably CNMF, in tandem with collaborations with universities and industry partners, to drive this initiative forward?

General HAUGH. U.S. Cyber Command (USCYBERCOM) is unaware of efforts to establish a DoD National Center for Narrative Intelligence and defers to the Department of Defense and applicable OSD offices, on further recommendations.

USCYBERCOM understands that, within the U.S. Government, the Foreign Malign Influence Center (FMIC) under the Director of National Intelligence (DNI), which was established per direction of previous NDAA's, is working on understanding foreign adversary influence campaigns and challenges from an intelligence perspective.

USCYBERCOM is also aware of growing interest in these challenges outside of the government, specifically in Academia and recent actions at the University of Mississippi to establish a National Center for Narrative Intelligence (NCNI). We understand this is a new, academia-driven effort, with the goal to partner with the private sector, U.S. government partners and other universities.

To date, our interactions have been limited and informal, but we are encouraged by Academia's interest and efforts in this area. This offers a potential partnership opportunity for the DoD, USCYBERCOM, CNMF, and other potential government partners, to work with academic partners for additional research and collaboration.

Finally, USCYBERCOM views the challenge of understanding adversary cyber-enabled influence campaigns as part of broader intelligence requirements supporting USCYBERCOM. USCYBERCOM remains highly interested in the establishment of a dedicated cyber intelligence center, which would include understanding the challenges of foreign cyber-enabled malign influence.

○