

S. HRG. 119–109

**OPEN HEARING:
THE 2025 ANNUAL
THREAT ASSESSMENT OF THE U.S.
INTELLIGENCE COMMUNITY**

HEARING
BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
OF THE
UNITED STATES SENATE
ONE HUNDRED NINETEENTH CONGRESS
FIRST SESSION

MARCH 25, 2025

Printed for the use of the Committee on Intelligence



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

60–885

WASHINGTON : 2026

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res 400, 94th Cong. 2d Sess.]

TOM COTTON, Arkansas, *Chairman*

MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho

SUSAN M. COLLINS, Maine

JOHN CORNYN, Texas

JERRY MORAN, Kansas

JAMES LANKFORD, Oklahoma

MIKE ROUNDS, South Dakota

TODD YOUNG, Indiana

TED BUDD, North Carolina

RON WYDEN, Oregon

MARTIN HEINRICH, New Mexico

ANGUS S. KING, JR., Maine

MICHAEL F. BENNETT, Colorado

KIRSTEN E. GILLIBRAND, New York

JOHN OSSOFF, Georgia

MARK KELLY, Arizona

JOHN THUNE, South Dakota, *Ex Officio*

CHARLES E. SCHUMER, New York, *Ex Officio*

ROGER F. WICKER, Mississippi, *Ex Officio*

JACK REED, Rhode Island, *Ex Officio*

RYAN TULLY, *Staff Director*

WILLIAM WU, *Minority Staff Director*

KELSEY S. BAILEY, *Chief Clerk*

C O N T E N T S

March 25, 2025

OPENING STATEMENTS

Tom Cotton, U.S. Senator from Arkansas	Page 1
Mark R. Warner, U.S. Senator from Virginia	3

WITNESSES

The Honorable Tulsi Gabbard, Director of National Intelligence; Accompanied by: John Ratcliffe, Director, Central Intelligence Agency (CIA); General Timothy D. Haugh, USAF, Director, National Security Agency/Central Se- curity Service (NSA/CSS); Kashyap P. Patel, Director, Federal Bureau of Investigation (FBI); Lieutenant General Jeffrey A. Kruse, USAF, Director, Defense Intelligence Agency (DIA)	6
Prepared Statement	11

SUPPLEMENTAL MATERIAL

AP article dated March 21, 2025	23
Annual Threat Assessment of the U.S. Intelligence Community Report	52

OPEN HEARING: THE 2025 ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

TUESDAY, MARCH 25, 2025

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in Room SH-216 in the Hart Senate Office Building, in open session, the Honorable Tom Cotton, Chairman of the Committee, presiding.

Members Present: Senators Cotton (presiding), Warner, Cornyn, Moran, Lankford, Rounds, Young, Budd, Wyden, Heinrich, King, Bennet, Gillibrand, Ossoff, Kelly, and Reed (*Ex Officio.*)

OPENING STATEMENT OF HON. TOM COTTON, A U.S. SENATOR FROM ARKANSAS

Chairman COTTON. The hearing will come to order.

Good morning. Welcome to the Senate Intelligence Committee's annual worldwide threats hearing.

I would like to begin by welcoming our esteemed panel of witnesses: the Director of National Intelligence, Tulsi Gabbard; the CIA Director, John Ratcliffe; the FBI Director, Kash Patel; the Director of the National Security Agency and Commander of U.S. Cyber Command, General Tim Haugh; and the Defense Intelligence Agency Director, Lieutenant General Jeffrey Kruse. Thank you for your appearance and thank you for your leadership.

I also want to recognize the hard work and dedication of the thousands of men and women in our intelligence community whom you are here to represent today. Their successes are seldom celebrated, their accomplishments are often unseen, but our Nation is grateful to each one for the vital work they do to keep our Nation safe, prosperous and free.

Our annual worldwide threats hearing allows for the American people to receive an unvarnished and unbiased account of the real and present dangers that our Nation faces. As we will hear from our witnesses, many of the threats we face are truly existential. Communist China is actively working to replace the United States as the world's dominant superpower. China uses coercive military, economic and influence operations short of war to shape a world favorable to its interests and hostile to ours. These methods include the biggest peacetime military build-up in history, rapidly expanding its nuclear forces, providing critical assistance to help Russia withstand U.S. sanctions, obscuring its role in accelerating the spread of COVID-19 beyond Wuhan, turning a blind eye to Chinese companies that enable the production of fentanyl flooding into

the United States, and putting space weapons on orbit among other tactics.

Iran despite setbacks inflicted on its so-called “axis of resistance” by Israel over the last year still aims to destroy what it calls the “little Satan,” the State of Israel, and what it calls the “great Satan,” the United States. It continues to arm Yemeni rebels to attack global shipping, though these outlaws have suffered terrible losses over the last 2 weeks thanks to the decisive action by President Trump and our brave troops.

I commend the President, Mike Waltz, Pete Hegseth, and his entire national security team for these actions.

Iran also continues its decades-long effort to develop surrogate networks inside the United States to threaten U.S. citizens. Furthermore, Iran’s nuclear program continues to pace. It is actively developing multiple space launch vehicles which are little more than flimsy cover for an intercontinental ballistic missile program that could hit the United States in a matter of years. But all this will soon come to an end. The Supreme Leader of Iran now faces a stark choice thanks to President Trump. The Supreme Leader can fully dismantle his nuclear program or he can have it dismantled for him.

Finally, today’s report also acknowledges that illicit drug production endangers the health and safety of millions of Americans. For the first time, the Annual Threat Assessment lists foreign illicit drug actors as the very first threat to our country. As the report highlights, Mexican-based cartels using precursors produced in China continue to smuggle fentanyl and synthetic opioids into the United States. Last year alone, these deadly drugs tragically killed more than 52,000 Americans—more than the number killed in attacks by foreign terrorists or foreign nations.

Given these threats, we have to ask, are our intelligence agencies well postured against these threats?

I am afraid the answer is no, at least, not yet. As the world became more dangerous in recent years, our intelligence agencies got more politicized, more bureaucratic, and more focused on promulgating opinions rather than gathering facts. As a result of these misplaced priorities, we have been caught off guard and left in the dark too often.

I know that all of you agree that the core mission of the intelligence community is to steal our adversaries’ secrets and convey them to policymakers to protect the United States. At the same time, it is not the role of intelligence agencies to make policy, to justify presidential action, or to operate like other Federal agencies. After years of drift, the intelligence community must recommit to its core mission of collecting clandestine intelligence from adversaries whose main objective is to destroy our Nation and our way of life. The reason is not that our intelligence community lacks dedicated patriots who show up to work every day to protect the American people. On the contrary, it has an abundance of them. The reasons are a misuse of resources, bureaucratic bloat, a default to play it safe, and a past administration that prioritized social engineering over espionage. Coupled with recent failures, the findings in today’s worldwide threat report should be a wake-up call to get our house in order. The status quo is proving inadequate to provide

the President and Congress with the intelligence needed to protect the American people. As more storms gather, America's intelligence capabilities require urgent reform and revitalization.

As the Chairman of this Committee, I look forward to working with each of you to strengthen America's intelligence edge and refocus our intelligence community on its core mission, stealing secrets. The American people deserve nothing less. We have assembled an impressive team to get this done, and I look forward to hearing your comments.

Now I recognize the Vice Chairman for opening remarks.

OPENING STATEMENT OF THE HON. MARK R. WARNER, A U.S. SENATOR FROM VIRGINIA

Vice Chairman WARNER. Thank you, Mr. Chairman, and good morning, everybody. I want to thank all the witnesses for being here.

I've got to say, I have been on the Committee now for 14 years, and this year's assessment is clearly one of the most complicated and challenging in my tenure on the Committee.

Now, I want to get into that in a moment, but I want to first of all address a recent story that has broken in the news. Yesterday, we stunningly learned that senior members of this administration and according to the reports, two of our witnesses here today, were members of a group chat that discussed highly sensitive and likely classified information that supposedly even included weapons packages, targets, and timing, and included the name of an active CIA agent. Putting aside for a moment that classified information should never be discussed over an unclassified system, it is also just mind boggling to me that all these senior folks who are on this line and nobody even bothered to check security hygiene 101, who are all the names? Who are they?

Well, it apparently included a journalist. And no matter how much the Secretary of Defense may want to disparage him, this journalist had at least the ethics to not report, I think, everything he heard.

The question I raise is, like, everybody on this Committee gets briefed on security protocols. You are told don't make calls outside of SCIFs of this kind of classified nature. We don't know and we are going to ask, obviously, Director Gabbard is the executive in charge of all keeping our secrets safe. Were these government devices? Were these personal devices? Have the devices been collected to make sure there is no malware?

There is plenty of declassified information that shows that our adversaries China and Russia are trying to break into encrypted systems like Signals.

I will just say this. If this was the case of a military officer or an intelligence officer and they had this kind of behavior, they would be fired. As I think this is one more example of kind of sloppy, careless, incompetent behavior particularly towards classified information, that this is not a one-off or a first time error.

Let me take a couple minutes and review some of the other reckless choices that this administration has made regarding our national security. We all recall, it seems like it wasn't that long ago, less than 2 months ago, in the first two weeks the administration

canceled all U.S. foreign assistance. Now, some may say, how bad can that be? It is foreign assistance.

Well, U.S. foreign assistance paid for the units in Ukraine to provide air defense to civilian cities being attacked by Russia. Foreign assistance paid for guarding camps in Syria where ISIS fighters are detained. Foreign assistance paid for programs abroad that ensured that diseases like Ebola don't come home. And until recently, it paid for the construction of a railway in Africa that would have helped give the United States much needed access to critical minerals in Congo. Now that project—China is going to try to finance it.

As well, in the first two weeks, Director Patel, the administration fired several of our most experienced FBI agents, including the head of the Criminal Investigative Division, the head of the Intelligence Division, the head of the Counterterrorism Division, the heads of the New York, Washington, and Miami field office—all individuals who were distinctly and directly responsible for helping to keep America safe. The irony of it was the currently and recently dismissed head of the Counterterrorism Division was involved in disrupting the ISIS attacks planned for Oklahoma City and Philadelphia, and helped lead the effort to bring to justice the key planner of the Abbey Gate bombing in Afghanistan that killed 13 U.S. servicemen and 150 civilians. That very Abbey Gate effort was actually praised by the President in his State of the Union Address. Yet, the administration's response to these agents', I believe, good works and years of service, was to force these folks out.

It is hard to imagine how that makes our country safer. Nor can I understand how Americans are made more secure by firing more than 300 staff at the National Nuclear Security Administration, including those responsible for overseeing the security and safety of the nuclear stockpile; or by ousting 130 employees at CISA, the agency directly responsible for trying to take on China's Salt Typhoon attack. Again, after Salt Typhoon, I would have thought folks on that group chat might have thought twice.

Or, how we were made safer by sacking 1,000 employees at the CDC and NIH who were actually directly working to keep our country safe from disease, and by pushing out hundreds of intelligence officers.

The amazing thing is, our intelligence officers, they are not interchangeable like a Twitter Coder. These intelligence officers, our country makes twenty to \$40,000 of investment just in getting a security clearance. It literally goes into six figures when you take the training involved. Can anyone tell how firing probationary individuals without any consideration for merit or expertise is an efficient use of taxpayer dollars?

And just to make clear that yesterday's story in *The Atlantic* was not this rookie one-off, it is a pattern. I want to acknowledge that Director Ratcliffe was not here in his position when this took place; but again, earlier in the administration when a nonclassified network was used, thereby exposing literally hundreds of CIA officers' identities—those folks can't go into the field now. How does that make our government more efficient?

You know, again, this pattern of an amazing cavalier attitude towards classified information is reckless, sloppy, and stunning. Per-

haps what troubles me most is the way the administration has decided we can take on all our problems by ourselves without any need for friends or allies.

I agree that he has got to put America's priorities first, but "America First" cannot mean America alone. The intelligence we gather to keep Americans safe depends on a lot of allies around the world who have sole access to sources we don't have. That sharing of information saves lives, and it is not hypothetical. We all remember because it was declassified last year when Austria worked with our community to make sure to expose a plot against Taylor Swift in Vienna that could have killed literally hundreds of individuals.

However, these relationships are not built in stone. They are not dictated by law. Things like the Five Eyes are based on trust, built on decades. But so often that trust is now breaking literally overnight. Yet, suddenly, for no reason that I can understand, the United States is starting to act like our adversaries are our friends. Voting in the U.N. with Russia, Belarus, and North Korea—that's a rogues gallery if I ever heard of one—treating our allies like adversaries, whether it is threats to take over Greenland or the Panama Canal, a destructive trade war with Canada, or literally, threatening to kick Canada out of the Five Eyes, I feel our credibility is being enormously undermined with our allies, who I believe and I think most of us on this Committee regardless of party believes makes our country safer and stronger. But how can our allies ever trust us as the kind of partner we used to be, when we without consultation or notice, for example, stop sharing information to Ukraine in its war for survival against Russia?

Or, how can our allies not only not trust our government but potentially not our businesses with such arbitrary political decisions? Let me give you a few examples.

As a result of a lot of work in this Committee and others in Congress, we made sure America's commercial space industry is second to none. From space to launch to commercial sensing and communications, the United States has taken a record lead. Yet overnight, this administration called into question the reliability of American commercial tech industry when Maxar and other commercial space companies were directed to stop sharing intelligence with Ukraine.

I am going to tell you—I've been a business guy, I can't say longer than being an elected official, but pretty close—that shockwave across all of commercial space and frankly not just commercial space, I've heard it from some of our hyperscalers in the tech community has sent an enormous chill. Who is going to hire an American commercial space company—government, or foreign business—with the ability to have that taken down so arbitrarily? It is not just in the case of commercial space, we see that Canada, Germany, Portugal have all been saying they are rethinking buying F-35s. I heard directly from Microsoft and Google and Amazon, they have questions whether they can still sell their services. We have seen foreign adversaries and friends take advantage of this riff in our national security areas and our scientists.

Germany has already put out ads trying to attract some of our best scientists who have been riffed. And the Chinese intelligence agencies are posting on social media sites in the hopes of luring in-

dividuals with that national security clearance who have been pushed out perhaps arbitrarily to come into their service.

So, no, the Signal fiasco is not a one-off. It is unfortunately a pattern we are seeing too often repeated. I fear that we feel the erosion of trust from our workplace, from our companies and from our allies and partners. It can't be put back in the bottle overnight. Make no mistake, these actions make America less safe.

Thank you, Mr. Chairman.

Chairman COTTON. Before I turn to the witnesses' hearing, I want to welcome everyone in our large audience today. I also want to note that we will not tolerate any disruptions of the witnesses' testimony or Senators' questions and the witnesses' answers. You will note that we have a large contingent of Capitol Police in the room.

Any disruptions either opposed or in favor to the witnesses will result in prompt removal from the hearing room, and my encouragement to the U.S. Attorney to throw the book at the person disrupting the hearing. No offense, but we all came to hear the witnesses, no one else in the room.

Director Gabbard, I understand you will make a statement for the panel of witnesses.

STATEMENT OF TULSI GABBARD, DIRECTOR OF NATIONAL INTELLIGENCE

Director GABBARD. Thank you, Mr. Chairman, Vice Chairman, Members of the Committee. Thanks for the opportunity for us to be here to present you the intelligence community's 2025 Annual Threat Assessment.

I am joined here this morning by my colleagues from the CIA, DIA, FBI, and NSA. Our testimony offers the collective assessment of the 18 U.S. intelligence elements making up the U.S. intel community, and draws on intelligence collection and information available to the IC from open source and private sector and the expertise of our analysts. This report evaluates what the IC assesses most threatens our people and our Nation's ability to live in a peaceful, free, secure, and prosperous society.

As you know, we face an increasingly complex threat environment that is threatening us here at home and our interests abroad.

I will begin by focusing on what most immediately and directly threatens the United States and the well-being of the American people—non-State criminal groups and terrorists putting American lives and livelihood at risk. Then I will focus on the key nation-states who have the capability to threaten the interests of the United States.

In this complex environment, non-State and State actors are able to exploit or take advantage of the effects of each other's activities. Conventional and asymmetrical capabilities even the traditionally weakest of actors are able to acquire from available advanced technologies creates an even more complex and serious threat landscape.

First, I will highlight the threats presented by several non-State actors. Cartels, gangs, and other transnational criminal organizations in our part of the world are engaging in a wide array of illicit activity, from narcotics trafficking to money laundering to smug-

gling of illegal immigrants and human trafficking which endanger the health, welfare, and safety of everyday Americans. Based on the latest reporting available for the yearlong period ending October, 2024, cartels were largely responsible for the deaths of more than 54,000 U.S. citizens from synthetic opioids. Mexico-based transnational criminal organizations, or TCOs, are the main suppliers of illicit fentanyl to the U.S. market and are adapting to enforcement and regulatory pressures by using multiple sources and methods to procure precursor chemicals and equipment primarily from China and India, many of which are dual-use chemicals used in legitimate industries.

Independent fentanyl producers are also increasingly fragmenting the drug trade in Mexico. The availability of precursor chemicals and ease of making illicit fentanyl have enabled independent actors to increase illicit fentanyl production and smuggling operations in Mexico.

Cartels are profiting from human trafficking and have likely facilitated more than 2 million illegal immigrants encountered by law enforcement at the U.S. Southwest border in 2024 alone, straining our vital resources and putting the American people at risk. Criminal groups drive much of the unrest and lawlessness in the Western hemisphere. They also engage in extortion, weapons and human smuggling, and other illicit and dangerous revenue-seeking operations including kidnappings for ransom, forced labor, and sex trafficking. These and other human traffickers exploit vulnerable individuals and groups by promising well-paying jobs while confiscating their identification documents. They operate in the shadows exploiting lawlessness in various areas and using coercion and intimidation to control their victims.

While these key drivers of migrants are expected to persist, heightened U.S. border security enforcement and deportations under the Trump administration are proving to serve as a deterrent for migrants seeking to illegally cross U.S. borders. U.S. Border Patrol apprehensions along the Southwest border in January 2025 dropped 85 percent from the same period in 2024.

Transnational Islamist extremists such as ISIS, al-Qaida, and affiliated jihadi groups continue to pursue, enable, or inspire attacks against the United States and our citizens abroad and within the homeland to advance their ultimate objective of establishing a global Islamist caliphate. This includes heightened efforts to spread their ideology to recruit and radicalize individuals in the U.S. and the West. While the New Year's Day attacker in New Orleans had no known direct contact with ISIS terrorists, he was influenced and radicalized by ISIS ideological propaganda, as one example.

Al-Qaida and its affiliates continue to call for attacks against the United States as they conduct attacks overseas. These jihadist groups have shown their ability to adapt and evolve including using new technologies and tactics to spread their ideology and recruit new followers.

A range of non-State cyber criminals are also targeting our economic interests, critical infrastructure, and advanced commercial capability for extortion, other coercive pursuits, and financial gain. These actors use a variety of tactics including phishing, ransomware, and denial of service attacks to disrupt our systems

and steal sensitive and lucrative information, using available technologies and U.S. cyber vulnerabilities. Ransomware actors last year, for example, attacked the largest payment processor for U.S. healthcare institutions. Another set of criminal actors conducted cyberattacks against U.S. water utilities. Some of these non-State cyber actors also operate as proxies for or emulate similar activities carried out by major State actors. While these non-State cyber actors often seek financial and intellectual property gains, they also carry out cyber operations for espionage purposes, targeting our critical infrastructure.

Turning to key State actors, the IC sees China, Russia, Iran, and North Korea engaging in activities that could challenge U.S. capabilities and interests, especially related to our security and economy. These actors are in some cases working together in different areas to target U.S. interests and to protect themselves from U.S. sanctions.

At this point, the IC assesses that China is our most capable strategic competitor. Under the leadership of President Xi Jinping, the People's Republic of China seeks to position itself as a leading power on the world stage, economically, technologically, and militarily. Beijing is driven in part by a belief that Washington is pursuing a broad effort to contain China's rise and undermine CCP rule. China's most serious domestic challenge is probably China's slowing economy and potential instability if socioeconomic grievances lead to large-scale unrest. Growing economic tensions with the United States and other countries could also weigh on China's plans for economic growth and domestic job creation.

China's military is fielding advanced capabilities, including hypersonic weapons, stealth aircraft, advanced submarines, stronger space and cyber warfare assets, and a larger arsenal of nuclear weapons. While it would like to develop and maintain positive ties with the United States and the Trump administration to advance its interests and avoid conflict, China is building its military capability in part to gain advantage in the event of a military conflict with the United States around the issue of China's efforts toward unification with the Republic of China or Taiwan. China's military is also expanding its presence in the Asia Pacific region with a focus on disputed territorial claims in both the East China and South China Seas.

Beijing is advancing its cyber capabilities for sophisticated operations aimed at stealing sensitive U.S. Government and private sector information and prepositioning additional asymmetric attack options that may be deployed in a conflict. China's cyber activities have been linked to multiple high-profile breaches, including last year's massive compromise of U.S. telecom infrastructure, commonly referred to as Salt Typhoon.

Beijing currently dominates global markets and strategically important supply chains, for example, with the mining and processing of several critical minerals. In December, China imposed an export ban to the United States on gallium, germanium, and antimony, all of which are important to the production of semiconductors and our defense technologies. This is in direct response to U.S. export controls on chips designed to broadly limit PRC access to advanced chips and chip-making equipment.

China also aims to compete in other critical global industries, including AI, legacy semiconductor chip production, biomanufacturing and genetic sequencing, and medical and pharmaceutical supply production. Leveraging often heavily state-subsidized production at greater scale, lower costs, and weaker regulatory standards than required in the West, Beijing's strategy has given it a leading position in many parts of these sectors and supply chains that support them. In 2023, for example, China had five first in class domestic drug approvals and three FDA approvals.

Turning to Russia, Russia's nuclear and conventional military capabilities along with its demonstrated economic and military resilience make it a formidable competitor. Moscow has more nuclear weapons than any other nation that can inflict catastrophic damage on the United States and the world in the event of a major war that Russian leaders fear put them and their regime at serious risk. In late 2024, Russia announced updates to its nuclear doctrine, expanding the conditions under which Russia would consider using nuclear weapons. Russia is building a more modern and survivable nuclear force designed to circumvent U.S. missile defense through reliable retaliatory strike potential. Russia intends to deter the U.S. by holding both the U.S. homeland at risk and by having the capabilities to threaten nuclear war in a conflict. Russia has developed advanced cyber capabilities and has attempted to preposition access to U.S. critical infrastructure for asymmetric options and make it a persistent cyber threat. Russia's cyber activities have been linked to multiple high-profile breaches, including the 2023 hack of Microsoft. Russia is also fielding new capabilities in antisatellite weapons meant to degrade U.S. and allied space infrastructure. Among Russia's most concerning developments is a new satellite intended to carry a nuclear weapon as an anti-satellite weapon, violating longstanding international law against such activity and putting the U.S. and global economy at risk.

Iran continues to seek expansion of its influence in the Middle East, despite the degradation to its proxies and defenses during the Gaza conflict. Iran has developed and maintains ballistic missiles, cruise missiles, and UAVs including systems capable of striking U.S. targets and allies in the region. Tehran has shown a willingness to use these weapons, including during a 2020 attack on U.S. forces in Iraq and in attacks against Israel in April and October 2024. Iran's cyber operations and capabilities also present a serious threat to U.S. networks and data.

The IC continues to assess that Iran is not building a nuclear weapon and Supreme Leader Khomeini has not authorized a nuclear weapons program that he suspended in 2003. The IC continues to monitor closely if Tehran decides to reauthorize its nuclear weapons program.

In the past year, we have seen an erosion of a decades-long taboo in Iran on discussing nuclear weapons in public, likely emboldening nuclear weapons advocates within Iran's decisionmaking apparatus. Iran's enriched uranium stockpile is at its highest levels and is unprecedented for a State without nuclear weapons. Iran will likely continue efforts to counter Israel and press for U.S. military withdrawal from the region by aiding, arming, and helping to reconstitute its loose consortium of like-minded terrorists and mili-

tant actors which it refers to as its “axis of resistance.” Although weakened, this collection of actors stills presents a wide range of threats including to Israel’s population, U.S. forces deployed in Iraq and Syria, and to U.S. and international military and commercial shipping and transit.

North Korean leader Kim Jong Un is pursuing stronger strategic and conventional capabilities that can target U.S. forces and allies in the region as well as the U.S. homeland to bolster North Korea’s leverage and stature, defend its regime and achieve at least tacit recognition as a nuclear weapons power.

Kim’s recently cemented strategic partnership with Russia supports these goals by providing him greater financial, military, and diplomatic support; reduce reliance on China; and providing North Korean forces and weapons systems authentic war fighting experience. Kim views his strategic weapons advances since 2019, its deepening ties with Russia, and North Korea’s economic durability as strengthening his negotiating position against Washington’s demands for denuclearization and lessening his need for sanctions relief. North Korea is probably prepared to conduct another nuclear test on short notice and continues to flight test its ICBMs to demonstrate their increasing capabilities as leverage in future negotiations.

Since 2022, China, Russia, Iran, and North Korea have grown closer. Removing the accelerant of the war in Ukraine is unlikely to revert these bilateral relationships to a prewar 2021 baseline, leaving room for new strategic priorities and world events to create new incentives or challenges to their currently high levels of cooperation.

Russia has been a catalyst for much of this expanded cooperation driven heavily by the support it has needed for its war effort against Ukraine, including protection from U.S. and Western sanctions. In addition to its exchange of military and other resource capabilities with North Korea, Russia has relied more heavily on China’s financial and defense industry backing and also has increased combined military exercises with China to signal shared fortitude against the United States and U.S. allies in the Asia Pacific region.

With Iran, Russia has also expanded financial ties to mitigate sanctions. Iran has become a critical military supplier to Russia, especially of UAVs in exchange for Russian technical support for Iranian weapons, intelligence, and advanced cyber capabilities.

In conclusion, the threats that we see to U.S. national security are both complex and multi-faceted and put the lives, safety, and well-being of the American people at serious risk. As the heads of the American people’s intelligence community, we will continue to provide the President, Congress, and our warfighters with timely, unbiased, relevant intelligence to keep the United States secure, free, prosperous, and at peace.

To the American people specifically, our intelligence community exists to serve you, and to ensure your safety, security and freedom.

Thank you.

[The prepared statement of the witness follows:]

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
FROM THE OFFICE OF STRATEGIC COMMUNICATIONS

Tulsi Gabbard, Director of National Intelligence
Congressional Testimony
Annual Threat Assessment of the U.S. Intelligence Community
March 25, 2025

Chairman Cotton, Vice Chair Warner, Members of the Committee, thank you for the opportunity to present to you the Intelligence Community's 2025 Annual Threat Assessment, joined by my colleagues from CIA, DIA, FBI, and NSA.

Our testimony offers the collective assessment of the 18 U.S. intelligence elements making up the U.S. Intelligence Community and draws on intelligence collection, information available to the IC from open-source and the private sector, and the expertise of our analysts.

This report evaluates what the IC assesses most threatens our people and our nation's ability to live in a peaceful, free, secure and prosperous society. We face an increasingly complex threat environment that is affecting us here at home, and our interests abroad.

I'll begin by focusing on what most immediately and directly threatens the United States and the wellbeing of the American people -- non-state criminal groups and terrorists putting American lives and livelihood at risk, followed by key nation states who have the capability to threaten the interests of the United States. In this complex environment, non-state and state actors are able to exploit or take advantage of the effects of each other's activities. Conventional and asymmetric capabilities even the traditionally weakest of actors are able to acquire from available advanced technologies creates an even more complex and serious threat landscape.

First, I will highlight threats presented by several non-state actors. Cartels, gangs, and other transnational criminal organizations in our part of the world are engaging in a wide array of illicit activity, from narcotics trafficking, to money laundering, to smuggling of illegal immigrants and human trafficking, which endanger the health, welfare, and safety

UNCLASSIFIED

UNCLASSIFIED

of everyday Americans. Based on the latest reporting available, for a year-long period ending October 2024, cartels were largely responsible for the deaths of more than 54,000 U.S. citizens from synthetic opioids. Mexico-based transnational criminal organizations (TCOs) are the main suppliers of illicit fentanyl to the U.S. market and are adapting to enforcement and regulatory pressures by using multiple sources and methods to procure precursor chemicals and equipment primarily from China and India, many of which are dual-use chemicals used in legitimate industries. Independent fentanyl producers are increasingly fragmenting the drug trade in Mexico. The availability of precursor chemicals and ease of making illicit fentanyl have enabled independent actors to increase illicit fentanyl production and smuggling operations in Mexico.

Cartels profit from human-trafficking, and likely facilitated more than 2 million illegal immigrants encountered by law enforcement at the U.S. southwest border in 2024, straining vital resources and putting the American people at risk. Criminal groups drive much of the unrest and lawlessness in the Western Hemisphere. They also engage in extortion, weapons and human smuggling, and other illicit and dangerous revenue-seeking operations, including kidnappings for ransom, forced labor, and sex trafficking. These and other human traffickers exploit vulnerable individuals and groups by promising well-paying jobs and confiscating identification documents. They operate in the shadows, exploiting lawlessness in various areas, and by using coercion and intimidation to control their victims.

While key drivers of migrants are expected to persist, heightened U.S. border security enforcement and deportations under the Trump administration are proving to serve as a deterrent for migrants seeking to illegally cross U.S. borders. U.S. Border Patrol apprehensions along the southwest border in January 2025 dropped 85% from the same period in 2024.

Transnational Islamist extremists, such as ISIS and al-Qa'ida, and affiliated jihadi groups, continue to pursue, enable, or inspire attacks against the United States and our citizens, abroad and within the Homeland, to advance their ultimate objective of establishing a global Islamist caliphate. This includes heightened efforts to spread their ideology to recruit and radicalize individuals in the U.S. and the West. While the New

UNCLASSIFIED

UNCLASSIFIED

Year's Day attacker in New Orleans had no known direct contact with ISIS terrorists, he was influenced and radicalized by ISIS ideological propaganda, for example. Al-Qa'ida and its' affiliates continues to call for attacks against the United States, as they conduct attacks overseas. These jihadist groups have shown an ability to adapt and evolve, including using new technologies and tactics to spread their ideology and recruit new followers.

A range of non-state cyber criminals are also targeting our economic interests, critical infrastructure, and advanced commercial capability for extortion, other coercive pursuits, and financial gain. These actors use a variety of tactics, including phishing, ransomware, and denial-of-service attacks, to disrupt our systems and steal sensitive and lucrative information, using available technologies and U.S. cyber vulnerabilities. Ransomware actors last year, for example, attacked the largest payment processor for U.S. healthcare transactions, and another set of criminal actors conducted cyber attacks against U.S. water utilities.

Some of these non-state cyber actors also operate as proxies for or emulate similar activities carried out by major state actors. While these non-state cyber actors often seek financial and intellectual property gains, they also carry out cyber operations for espionage purposes, targeting our critical infrastructure.

Turning to our key state-actors, the IC sees China, Russia, Iran, and North Korea engaging in activities that could challenge U.S. capabilities and interests, especially related to our security and economy. These actors are, in some cases, working together in different areas to target U.S. interests and protect themselves from U.S. sanctions.

At this point, the IC assesses that China is our most capable strategic competitor. Under the leadership of President Xi Jinping, the People's Republic of China seeks to position itself as a leading power on the world stage, economically, technologically and militarily. Beijing is driven in part by a belief that Washington is pursuing a broad effort to contain China's rise and undermine CCP rule.

China's most serious domestic challenge is probably China's slowing economy and potential instability if socioeconomic grievances lead to large-scale unrest. Growing

UNCLASSIFIED

economic tensions with the United States and other countries could also weigh on China's plans for economic growth and domestic job creation.

China's military is fielding advanced capabilities, including hypersonic weapons, stealth aircraft, advanced submarines, stronger space and cyber warfare assets, and a larger, arsenal of nuclear weapons. While it would like to develop and maintain positive ties with the United States and the Trump Administration to advance its interests and avoid conflict, China is building its' military capability, in part, to gain advantage in the event of a military conflict with the United States around the issue of China's efforts toward unification with the Republic of China, Taiwan. China's military is also expanding its presence in the Asia-Pacific region, with a focus on disputed territorial claims in both the East China and South China Seas.

Beijing is advancing its cyber capabilities for sophisticated operations aimed at stealing sensitive U.S. government and private sector information, and pre-positioning additional asymmetric attack options that may be deployed in a conflict. China's cyber activities have been linked to multiple high-profile breaches, including last year's massive compromise of the U.S. telecommunications infrastructure, also referred to as Salt Typhoon.

Beijing currently dominates global markets and strategically important supply chains, for example with the mining and processing of several critical minerals. In December, China imposed an export ban to the United States on gallium, germanium, and antimony, all of which are important to the production of semiconductors and defense technologies. This was in direct response to U.S. export controls on chips designed to broadly limit PRC access to advanced chips and chipmaking equipment.

China also aims to compete in other critical global industries, including AI, legacy semiconductor chip production, biomanufacturing and genetic sequencing, and medical and pharmaceutical supply production. Leveraging often heavily state-subsidized production at greater scale, lower costs, and weaker regulatory standards than required in the West, Beijing's strategy has given it a leading position in many parts of these sectors and supply chains supporting them. In 2023, China had five first-in-class domestic drug approvals and three FDA approvals.

UNCLASSIFIED

Turning to Russia: Russia's nuclear and conventional military capabilities, along with its demonstrated economic and military resilience, make it a formidable competitor. Moscow has more nuclear weapons than any other nation, that could inflict catastrophic damage on the United States and the world in the event of a major war that Russian leaders feared put them and their regime at serious risk. In late 2024, Russia announced updates to its public nuclear doctrine, expanding the conditions under which Russia would consider using nuclear weapons.

Russia is building a more modern and survivable nuclear force designed to circumvent U.S. missile defense through reliable retaliatory strike potential. Russia intends to deter the U.S. by both holding the U.S. homeland at risk and by having the capabilities to threaten nuclear war in a conflict.

Russia has developed advanced cyber capabilities and has attempted to pre-position access on U.S. critical infrastructure for asymmetric options and make it a persistent cyber threat. Russia's cyber activities have been linked to multiple high-profile breaches, including the 2023 hack of Microsoft.

Russia is also fielding new capabilities and antisatellite weapons meant to degrade U.S. and allied space infrastructure. Among Russia's most concerning developments is a new satellite intended to carry a nuclear weapon as an antisatellite weapon, violating longstanding international law against such activity and putting the U.S. and global economy at risk.

Iran continues to seek expansion of its influence in the Middle East, despite the degradation to its proxies and defenses during the Gaza conflict. Iran has developed and maintains ballistic missiles, cruise missiles, and UAVs, including systems capable of striking U.S. targets and allies in the region. Tehran has shown a willingness to use these weapons, including during a 2020 attack on U.S. forces in Iraq and in attacks against Israel in April and October 2024. Iran's cyber operations and capabilities also present a serious threat to U.S. networks and data.

The IC continues to assess that Iran is not building a nuclear weapon and Supreme Leader Khamenei has not authorized the nuclear weapons program he suspended in

UNCLASSIFIED

UNCLASSIFIED

2003. The IC is closely monitoring if Tehran decides to reauthorize its nuclear weapons program. In the past year, we have seen an erosion of a decades-long taboo in Iran on discussing nuclear weapons in public, likely emboldening nuclear weapons advocates within Iran's decision-making apparatus. Iran's enriched uranium stockpile is at its highest levels and is unprecedented for a state without nuclear weapons.

Iran will likely continue efforts to counter Israel and press for a U.S. military withdrawal from the region by aiding, arming, and helping to reconstitute its loose consortium of like-minded terrorist and militant actors, which it refers to as its "Axis of Resistance." Although weakened, this collection of actors still presents a wide range of threats, including to Israel's population, U.S. forces deployed in Iraq and Syria, and to U.S. and international military and commercial shipping and transit.

North Korean Leader Kim Jong Un is pursuing stronger strategic and conventional capabilities that can target U.S. forces and allies in the region, as well as the U.S. Homeland, to bolster North Korea's leverage and stature, defend the regime, and achieve at least tacit recognition as a nuclear weapons power. Kim's recently cemented strategic partnership with Russia supports these goals by providing him greater financial, military, and diplomatic support; reduced reliance on China and the need to defer to Beijing's terms for support; and providing North Korean forces and weapons systems authentic warfighting experience.

Kim views his strategic weapons advances since 2019, deepening ties with Russia, and North Korea's economic durability as strengthening his negotiating position against Washington's demands for denuclearization and lessening his need for sanctions relief.

North Korea is probably prepared to conduct another nuclear test on short notice and continues to flight test ICBMs to demonstrate their increasing capabilities as leverage in future negotiations.

Since 2022, China, Russia, Iran and North Korea have grown closer. Removing the accelerant of the war in Ukraine is unlikely to revert these bilateral relationships to a pre-war, 2021 baseline, leaving room for new strategic priorities and world events to create new incentives or challenges to their currently high levels of cooperation. Russia

UNCLASSIFIED

UNCLASSIFIED

has been the catalyst for much of this expanded cooperation, driven heavily by the support it has needed for its war effort against Ukraine, including protection from U.S. and Western sanctions. In addition to its exchange of military and other resource capabilities with North Korea, Russia has relied more heavily on China's financial and defense industry backing, and also has increased combined military exercises with China to signal shared fortitude against the United States and U.S. allies in the Asia-Pacific region. With Iran, Russia has also expanded financial ties to mitigate sanctions. Iran has become a critical military supplier to Russia, especially of UAVs, in exchange for Russian technical support for Iranian weapons, intelligence, and advanced cyber capabilities.

In conclusion, the threats we see to U.S. national security are both complex and multifaceted, and put the lives, safety and wellbeing of the American people at serious risk.

As the heads of the American people's Intelligence Community, we will provide the President, Congress, our warfighters, and the American people the timely, unbiased, relevant intelligence to keep the United States secure, free, prosperous and at peace.

To the American people, specifically, our Intelligence Community exists to serve you, and ensure your safety, security, and freedom.

Thank you.

UNCLASSIFIED

Chairman COTTON. Thank you, Director Gabbard.

As I mentioned in my opening remarks, the Annual Threat Assessment for the first time lists cartels and traffickers as the very first threat.

Director Patel, I am pleased to say that the FBI's Little Rock field office has been doing its part in addressing this threat. The field office, along with other Federal, State and local law enforcement agencies, have arrested nearly 300 immigrants in my State in 2025 so far. Could you provide some color about the nature of the threat these illegal immigrants have posed not just to Arkansas, but our Nation, perhaps including some of the details of the horrific offenses they have committed against the American people.

Director PATEL. Thank you, Mr. Chairman.

(A disruption occurred in the Hearing Room.)

Chairman COTTON. The witness will suspend.

That protester was a Code Pink lunatic, saying the greatest threat to world peace is funding Israel. I will observe for the benefit of the audience here and on television that Code Pink is funded by Communist China as well, which simply illustrates—speak up now so you can be removed as well, whoever is saying that.

(A disruption occurred in the Hearing Room.)

Chairman COTTON. If anyone else would like to join them, speak now, please, so we don't have any more disruptions.

As I was saying, the fact that Communist China funds Code Pink which interrupts a hearing like this about Israel, simply illustrates Director Gabbard's point that China, Russia, Iran, North Korea, and other American adversaries are working in concert to a greater degree than they ever have before.

Director Patel, back to my question. Could you give us some color about threat that illegal migrants have posed not only to my State which has resulted in nearly 300 arrests in 2025 but also to the Nation at large?

Director PATEL. Thank you, Mr. Chairman, Mr. Vice Chairman, and Members of the Committee. I appreciate the time to address you all.

Specifically to Arkansas, Senator. The priorities at the FBI which I identified during my confirmation hearing and since is attacking violent crime along with national security, and every single State in this country is a border State. Arkansas is no exception. Allow me to highlight the work of the men and women of the FBI and State and local law enforcement in the State of Arkansas. Since February 5th alone, we have 220 illegal immigrants arrested on charges varying from violent offenses, weapons offenses, narcotics offenses and serious violent felonies; 253 separate individuals have been charged related to those offenses. And here is something I want the American people to hear about narcotics, and countering narcotics. Thousands of pounds of narcotics were seized in these three weeks in the State of Arkansas—thousands, worth tens of millions of dollars—everything from fentanyl, to meth to cocaine to heroin to marijuana and more, and also including manufactured drugs.

The FBI does have the biggest footprint in Arkansas, but we could not achieve this mission without our State and local law enforcement partners, which has been one of the priorities since I

took the helm at the FBI. They provide the greatest ground level intelligence to conduct these operations in Arkansas and in every single State across the Union. Since February 5, we have assisted with the arrests of hundreds of criminals and illegals throughout your State, and that was just a 3-week operation. Prior to that, Senator, there was a bust of 17 Federal indictments relating to a meth lab in the State of Arkansas in the Southwest corner of your State. All of those individuals are now facing prosecution for hundreds of pounds of illegal opioids, guns, and other illicit material. So, we will continue to do that work. We will work seven days a week, 365 days a year, not just in your State, Mr. Chairman, but in every State.

Chairman COTTON. Thank you, Director Patel.

As Director Gabbard highlighted from the Annual Threat report, Director Ratcliffe, many if not most of the chemical precursors for deadly fentanyl produced by Mexican drug cartels originates in China. China, of course, is a techno-totalitarian police State. They have technology to monitor their own people that Soviet Russia could have only imagined. Is there any reason, Director Ratcliffe, to believe that China could not monitor and crack down on this flow of chemical precursors to Mexico if it chose to do so?

Director RATCLIFFE. Thank you, Senator, for the question. No, there is nothing to prevent China, the People's Republic of China, from cracking down on fentanyl precursors. As you well know, Senator, one of the reasons that they don't is that there are more than 600 PRC-related companies that produce those precursor chemicals in an industry that generates \$1.5 trillion. That is one of the reasons that we see the Chinese efforts to affect the fentanyl precursors are really limited in nature and intermittent in nature and not a dedicated effort to enforce their own laws and regulations to crack down on this.

Chairman COTTON. Thank you, Director Ratcliffe. But I have many more questions I could ask, but I am going to try to lead by example and stay within the 5-minute limit.

For the benefit of Senators, I remind everyone there is a vote scheduled at noon. I hope to finish the open portion of this hearing before that vote closes, after which time we will move to the closed portion. The Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman. I will be happy to take your extra 13 seconds. But I want to go back to what I addressed at the outset. This was not only sloppy and not only violated all procedures, but if this information had gotten out, American lives could have been lost. If the Houthis had this information, they could reposition their defensive systems. So I want to get a little more information about this.

Director Gabbard, did you participate in a group chat with the Secretary of Defense and other Trump senior officials discussing the Yemeni war plans?

Director GABBARD. Senator, I don't want to get into——

Vice Chairman WARNER. Ma'am, were you on?

Director GABBARD [continuing]. This conversation——

Vice Chairman WARNER. So you are not going to be willing to address—are you denying—answer my question, ma'am. You were not "TG" on this group chat?

Director GABBARD. I am not going to get into the specifics of the delivery.

Vice Chairman WARNER. Would you acknowledge whether you were on this group chat?

Director GABBARD. Senator, I am not going to get into the specifics.

Vice Chairman WARNER. Why are you not going to get into the specifics? Is it because it is all classified?

Director GABBARD. Because it is currently under review by the National Security Council.

Vice Chairman WARNER. Because it is all classified? If it is not classified, share the texts now.

Director GABBARD. As the White House previously stated——

Vice Chairman WARNER. Is it classified or nonclassified information on these texts?

Director GABBARD. I can confirm——

Vice Chairman WARNER. Director Ratcliffe, were you on the group chat?

Director RATCLIFFE. Senator, I was on a Signal messaging group.

Vice Chairman WARNER. You were the John Ratcliffe on that chat?

Director RATCLIFFE. I was. Can I provide some context on that?

Vice Chairman WARNER. Thank you, but I have a series of questions——

Director RATCLIFFE. So, but I think it is important, because at the outset you made some comments about Signal messaging using encrypted apps.

So that we are clear, one of the first things that happened when I was confirmed as CIA Director was Signal was loaded on to my computer at the CIA, as it is for most CIA officers.

One of the things that I was briefed on very early, Senator, was by the CIA records management folks about the use of Signal as a permissible work use. It is. That is a practice that preceded the current administration to the Biden administration.

Vice Chairman WARNER. Director Ratcliffe, I have a series of questions. If you are making the statement——

Director RATCLIFFE. To your point——

Vice Chairman WARNER. If you are making the statement that Signal is a secure channel.

Director RATCLIFFE. No. Can I answer that?

Vice Chairman WARNER. Sir, I've got a series of questions.

Director RATCLIFFE. It is encryption.

Vice Chairman WARNER. I understand encryption.

Director RATCLIFFE. It is permissible to use to communicate and coordinate for work purposes, provided——provided, Senator, that any decisions that are made are also recorded through formal channels. So those were procedures that were implemented.

Vice Chairman WARNER. Director Ratcliffe——

Director RATCLIFFE. My staff implemented those processes, followed those processes, complied with those processes, and finally——just please. So my communications to be clear in a Signal message group were entirely permissible and lawful and did not include classified information.

Vice Chairman WARNER. Well, we will make that determination, because if it is not classified, share the texts with the Committee. Let me go on.

Director GABBARD, you are the security executive and set access guidelines for classified information. Did you contact the Defense Secretary or others after this specific military planning was put out and say: Hey, we should be doing this in a SCIF?

Director GABBARD. There was no classified material that was shared in that Signal chat.

Vice Chairman WARNER. No classified material? Share it with the Committee. You can't have it both ways. These are important jobs. This is our national security, bobbing and weaving and trying to filibuster your answer. So please answer the question. If this was—Director Gabbard, if this was a rank and file intelligence office who did this kind of careless behavior, what would you do with them?

Director GABBARD. I would reiterate there was no classified material that was shared in that Signal—

Vice Chairman WARNER. Ma'am, if there was no classified materials shared, and if there is no classified materials, you can't even answer the question whether you were on the chat. This is strangely familiar, and I think my colleagues remember, when you couldn't answer the question "Is Edward Snowden a traitor?"

Ma'am, I have serious doubts about your—

Anyway, Director Gabbard, I am going to give you this, tweeted just 11 days ago, and I am quoting you: "Any unauthorized release of classified information is a violation of the law and will be treated as such."

So, if this information is classified, what are you going to do?

Director GABBARD. Senator, two points here. First of all, there is a difference between inadvertent release versus—

Vice Chairman WARNER. Careless and sloppy.

Director RATCLIFFE [continuing]. Malicious leaks of classified information. Second point is, there was no classified information on the Signal group chat.

Vice Chairman WARNER. And this Committee will seek to get that information.

Director Patel, my time is about up and I am going to use my 12 seconds that the Chairman gave me.

Director Patel, did the FBI launch an investigation into any of this?

Director PATEL. Senator, I was just briefed about it late last night I and don't have an update.

Vice Chairman WARNER. I would like to get an answer by the end of the day.

Chairman COTTON. At this point in the ordinary course of affairs, I would recognize Senator Collins. She asked me to express to you that she is under the weather this morning. She regrets her absence, but anticipates submitting written questions, to which I would request your prompt replies.

Senator Cornyn.

Senator CORNYN. Director Gabbard, I applaud President Trump's efforts to try to bring an end to the war between Russia and Ukraine.

I want to read a statement out of the Annual Threat Assessment and just confirm that you agree with this. It says: Russia views its ongoing war with Ukraine as a proxy conflict with the West, and its objective to restore Russian strength and security, and its near abroad against perceived U.S. and Western encroachment has increased the risks of unintended escalation between Russia and NATO.

Do you agree with that statement; and that is in the Annual Threat Assessment, correct?

Director GABBARD. Correct.

Senator CORNYN. I would like to refer to an AP story, Associated Press, dated March 21, 2025. The title of the article is: "Western officials say Russia is behind a campaign of sabotage across Europe. This AP map shows it."

Mr. Chairman, I would like to ask unanimous consent that this be made part of the record.

Chairman COTTON. Without objection. [The document was submitted for the record, as follows:]

[Western officials say Russia is behind a campaign of sabotage across Europe. This AP map shows it](#)

Emma Burrows

March 21, 2025

Western officials have accused Russia and its proxies of staging dozens of attacks and other incidents across Europe since the invasion of Ukraine three years ago, according to data collected by The Associated Press.

They allege the disruption campaign is an extension of Russian President Vladimir Putin's war, intended to sow division in European societies and undermine support for Ukraine.

The AP documented 59 incidents in which European governments, prosecutors, intelligence services or other Western officials blamed Russia, groups linked to Russia or its ally Belarus for cyberattacks, spreading propaganda, plotting killings or committing acts of vandalism, arson, sabotage or espionage since the Feb. 24, 2022, invasion.

The incidents range from stuffing car tailpipes with expanding foam in Germany to a plot to plant explosives on cargo planes. They include setting fire to stores and a museum, hacking that targeted politicians and critical infrastructure, and spying by a ring convicted in the U.K.

Richard Moore, the head of Britain's foreign intelligence service, called it a "staggeringly reckless campaign" in November.

It is often difficult to prove Russia's involvement, and the Kremlin denied carrying out a sabotage campaign against the West. But more and more governments are publicly attributing attacks to Russia.

The alleged disruption has a double purpose, James Appathurai, the NATO official responsible for the alliance's response to such threats, told the AP.

One is to create "political disquiet" and undermine citizens' support for their governments and the other is to "undercut support for Ukraine," said Appathurai, deputy assistant secretary-general for Innovation, Hybrid, and Cyber.

During the investigation, the AP spoke to 15 current officials, including two prime ministers, and officials from five European intelligence services, three defense ministries and NATO, in addition to experts.

The AP plotted the incidents on a map to show the scope of the alleged campaign, which experts say is particularly worrying at a time when U.S. support for Ukraine is wavering and European allies are questioning Washington's reliability as a security partner and ally.

What is happening?

The cases are varied, and the largest concentrations are in countries that are major supporters of Ukraine.

Some incidents had the potential for catastrophic consequences, including mass casualties, as when packages exploded at shipping facilities in Germany and the U.K. Western officials said they suspected the packages were part of a broader plot by Russian intelligence to put bombs on cargo planes headed to the U.S. and Canada.

In another case, Western intelligence agencies uncovered what they said was a Russian plot to kill the head of a major German arms manufacturer that is a supplier of weapons to Ukraine.

European authorities are investigating several cases of damage to infrastructure under the Baltic Sea, including to a power cable linking Estonia and Finland. Finnish authorities detained a ship, suspected of being part of Russia's "shadow fleet" used to avoid sanctions, after that cable and others were damaged.

When a fake French Defense Ministry website claimed citizens were being called up to fight in Ukraine, a French minister denounced it as Russian disinformation. German authorities suspect Russia was behind a campaign to block up scores of car tailpipes ahead of national elections, according to a European intelligence official who spoke on condition of anonymity to discuss sensitive matters.

Officials from Estonia, Poland, Latvia and Finland, meanwhile, have accused Russia and Belarus of directing migrants to their borders.

Putin's spokesperson, Dmitry Peskov, told the AP that the Kremlin has never been shown "any proofs" supporting the accusations and said "certainly we definitely reject any allegations."

How AP documented the cases

The AP scoured through hundreds of incidents suspected to be linked to Russia since Moscow's invasion that were reported in open sources such as local media and government websites.

They were included in AP's tally only when officials drew a clear link to Russia, pro-Russian groups or ally Belarus. Most of the accusations were made to or reported by AP, either at the time they occurred or during the course of this investigation. Fourteen cases were reported by other news organizations and attributed to named officials.

In about a quarter of the cases, prosecutors have brought charges or courts have convicted people of carrying out the sabotage. But in many more, no specific culprit has been publicly identified or brought to justice.

A 'bolder' approach

Countries have always spied on their enemies and long waged propaganda campaigns to further their interests abroad. But since the invasion of Ukraine, Moscow has become "bolder," hitting the West with sabotage, vandalism and arson in addition to the tactics it previously used, including killings and cyberattacks, said Elisabeth Braw, an expert on the attacks at the Atlantic Council in Washington.

"The way you can weaken a country today is not by invading it," she said.

China has also been accused of espionage and cyber operations in Europe, and The Wall Street Journal reported that Ukrainian authorities were responsible for blowing up the Nord Stream 1 and 2 pipelines in 2022. Kyiv has denied this.

"Multiple countries engage in hybrid operations," said David Salvo, managing director of the Alliance for Securing Democracy at the German Marshall Fund. "Russia is the overwhelming culprit in Europe."

How to respond — even as US support wavers

A coordinated approach — especially sharing intelligence — is critical to tracking and countering the threats, Appathurai said.

That cooperation — never easy since intelligence is not shared collectively across NATO members — faces new challenges now, as the Trump administration increasingly questions the role of the alliance, embraces Russia and spars with its European partners.

Still, as the scale of the campaign becomes clearer, some nations are becoming more assertive.

Appathurai pointed to the approach to suspected sabotage in the Baltic Sea, where NATO has launched a mission to protect critical infrastructure.

“If we are to have a chance of stemming the threat,” Braw said, “then we have to work together.”

Senator CORNYN. The document that AP compiled, and I presume this is through open sources, documented 59 incidents, “including cyber attacks, spreading propaganda, plotting killings, or committing acts of vandalism, arson, sabotage or espionage.”

Is that consistent with your understanding and impression of what Russia is currently engaged in in Europe?

Director GABBARD. Senator, I haven’t seen that specific article, but I can confirm that we assess Russia’s attempts to conduct such sabotage activities in Europe.

Senator CORNYN. Thank you.

One of the things that I am most concerned about, following some of the discussions between Russia and Ukraine and United States and our other allies, obviously, as I said, peace between Ukraine and Russia is the desirable end-state. I think you have to be—you would have to be crazy to say otherwise; but I also want to talk a little bit about the unexpected or maybe unintended consequences of European insecurity. I know the incoming Chancellor of Germany has talked about the possibility that Germany might share its nuclear weapons with Ukraine and suggested that the UK would be part of that. I know that Poland has talked about acquiring nuclear weapons and perhaps other European countries to make up for what they view as a receding of the American umbrella of protection.

General Kruse, what would be the result of the proliferation of nuclear-weapon armed countries in Europe if, in fact, that would occur as a result of the perception of European insecurity?

LTGEN KRUSE. Senator, thank you for the question. One of the things that the intelligence community works very hard on is to understand who has nuclear weapons throughout the planet, and as discussed in the opening statements by both the Chair and by Director Gabbard, the proliferation and the increase in the types and the lethality of nuclear weapons is one of the things that we have to track and we as a Nation are going to have to face. And it has changed dramatically in the last 5 years and will continue to change over the next 5 years.

The addition of additional countries which have their own deterrence policies and will act in a nuclear dialogue or the presence of those weapons, the security of those weapons, the movement and the threat of use of those weapons complicates the environment by which all of us will operate and will complicate all of the decisions by which all future conflict and the political decisions that we support for the decision makers.

Senator CORNYN. It makes the world a more dangerous place, does it not?

LTGEN KRUSE. Senator, yes, it does.

Senator CORNYN. And just by way of history, Ukraine used to have the third-largest arsenal of nuclear weapons on the planet, but as a result of negotiations between Russia and Ukraine and the United Kingdom, the Budapest Memorandum documented a commitment by Russia and the United States to protect the territorial integrity of Ukraine in exchange for them giving up their nuclear weapons.

Did I correctly summarize the content of the Budapest Memorandum back in 1994?

LTGEN KRUSE. Yes, Senator, you did. And Ukraine willingly gave up its weapons for the protection of others.

Senator CORNYN. Thank you very much.

Chairman COTTON. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Obviously, my colleagues and I feel very strongly about the war planning meeting over unclassified phones. Obviously reckless, obviously dangerous, both the mishandling of classified information and the deliberate destruction of Federal records are potential crimes that ought to be investigated immediately. And I want to make clear that I am of the view that there ought to be resignations starting with the National Security Adviser and the Secretary of Defense.

Director Ratcliffe and Director Gabbard, have you participated in any other group chats with senior Trump administration officials in which classified information was shared using phones that weren't cleared for such information? Question for the two of you.

Director RATCLIFFE. Senator, thank you for the question. Your question was have I participated in any "other" group chats sharing classified information. To be clear, I haven't participated in any Signal group messaging that relates to any classified information at all.

Senator WYDEN. Okay. Director Gabbard?

Director GABBARD. Senator, I have the same answer. I have not participated in any Signal group chat or any other chat on another app that contained any classified information.

Senator WYDEN. Yeah, and I just think it is important to follow through here. Will the two of you cooperate with an audit to confirm that that is the case?

Director GABBARD. I have no objection.

Director RATCLIFFE. Senator I will certainly comply with any follow-up that the National Security Council would deem appropriate; but again, to be clear, the use of Signal message end-to-end encryption applications is permissible and was in this case used permissibly at least to my understanding, and in a lawful manner.

Senator WYDEN. The seriousness of this is so clear that is why I want to have an audit and both of you had gave me an answer indicating that you would be open to it and I appreciate it.

Director Patel, you weren't in this particular group chat, but have you participated in any chats on unclassified phones with other administration officials relating to national security, and if so, on what other topics?

Director PATEL Thank you for the, question, Senator, and not that I can recall.

Senator WYDEN. Okay.

Question I have for you, Director Gabbard, involves this question of Elon Musk wasn't going to see the military's China war plans because you said he "has business in China," and he perhaps he would be susceptible to that, and that was his comment. So as DNI you are responsible for security clearance policy across the government. Under your watch, how are you going to go about carrying out this obligation because I think it obviously is a very significant one in terms of American national security?

Director GABBARD. Thank you, Senator.

As you know, the office of the Director of National Intelligence provides oversight over these different 18 intelligence elements. Leaders within those elements are empowered with that responsibility to uphold the trust that the American people have placed in them. In this example that you have cited both Secretary Hegseth as well as President Trump completely denied the assertion that Elon Musk was going to receive any kind of classified war plan brief pertaining to China or any other country.

Senator WYDEN. So on the question of whether the President has the prerogative to get clearances is really the area that I want to touch on, because you are formally responsible for security clearance policies and that is why I am asking about it. So can a President decide who gets a clearance?

Director GABBARD. Yes.

Senator WYDEN. What about your role? You are formally responsible for security clearance policies.

Director GABBARD. That is also true.

Senator WYDEN. So how do you resolve it?

The President just gets his way?

Director GABBARD. The elected President and Commander in Chief has the authority to provide a security clearance to those who he deems necessary.

Senator WYDEN. Mr. Chairman and Ranking Member, I think we have to have a further discussion on this and figure out what the ground rules are. I think it is clear what the Director says. I just think we need more clarity, because I think you have the formal responsibility for security clearances and now we have heard that this is somehow going to be the President's project, and I think we ought to have further discussions. Thank you, Mr. Chairman.

Chairman COTTON. Senator Lankford.

Senator LANKFORD. Mr. Chairman, thank you.

Thank you, all of you, in your service to the country. It matters. There are a lot of citizens in our country right now that have much greater security in their life because of the work that you do and the people that are working around you do, so I just want to say I appreciate that for the folks in Oklahoma. They would definitely want me to be able to say thank you for your service.

Let me ask a couple of questions on this.

Director Gabbard, let me start with you on this. Iran has been listed as one of the top sponsors of terrorism for a very long time. They are the primary armorers of Hezbollah, Hamas, the Houthis. They are arming the Russians to be able to kill Ukrainians. They continue to be able to destabilize the region and just in recent days when many nations in the Gulf region have talked about how to provide greater stability, Iranian leadership stepped out and made very clear statements, they want a one-State solution for Israel and that is to drive out all Jews. So this continues to be an issue not just for the region but for Americans in particular. So my question is, on the sanctions and the effect of sanctions, what we know about the Iranian response. Under the Biden administration, those sanctions were turned down. Quite frankly, Iran has been able to sell \$90 billion in oil on the global market to be able to rearm itself and others in the region. Now sanctions are now going back on to Iran again. What do we know about the effect of those sanctions?

Director GABBARD. Thank you, Senator, for the question. These sanctions have just begun to be reinstated, so the full effects have not yet borne fruit; but the message that the President has sent with his maximum pressure campaign is certainly heard.

As the Chairman mentioned in his opening remarks, President Trump recently sent a letter to the leader of Iran expressing his interest in direct talks in order to try to de-escalate and prevent war, prevent Iran from gaining a nuclear weapon, but also stated there would be military consequences if there was no direct negotiations. So President Trump is continuing to carry out his vision and mission of peace through strength acting in the best interests of the American people. We will see what choices are made from here.

Senator LANKFORD. Thank you.

Director Patel, during the last administration and the very open border policy that they had, we had some years including 2022 and 2023 where there were 70,000 individuals that were released into the country that were identified as “special interest” aliens. This is something that this Committee and Homeland Security Committee tried over and over again to get details on. The Biden administration was unwilling to share any of the details of the special interest aliens, which led to a great amount of frustration. The comment came often back to us that the FBI was going to track all these individuals and to be able to identify them, even though it was 70,000 a year that were coming into the country.

You just walked into this position and trying to get your feet on the ground and so many different issues that are outstanding on that. I raise to you the issue of individuals that are currently illegally present in the country going through a process but are listed as special interest aliens. By definition from the administration, those are individuals that we don’t know their level of risk, but they are considered a national security risk, but we don’t know anything else about them from there. So how are you trying to get on top of the number of people that are criminal aliens in the country, but also these special interest aliens that come from terrorist areas?

Director PATEL. Thank you, Senator. I appreciate your question. As far as the FBI is concerned, you hit on it—criminal. So we are focused across our interagency partners at DHS, ICE, CBP, CISA and elsewhere to identify through our information sharing networks that we have stood up with State and local law enforcement to provide us the details on any criminal evidence relating to any of the individuals you highlighted, and if there is a nexus there, a case will be opened by the line agents who predicate a lawful and factual basis to do so; and we will further refer that matter to the Department of Justice for prosecution. We are reviewing all of these cases anew and we will report back to you, Senator, with some fidelity on the outcome of that process.

Senator LANKFORD. Okay, thank you. Are you getting good feedback from social media technology companies and cooperation from them on illegal activities that are promoted on their site? All the different sites have rules and standards for what can and cannot be done on that, but for instance on the border areas, many of the sites are allowing child trafficking or they are allowing basically

the hiring of Americans to come be drivers and such. And they know this is being circumvented. Are they working with you on that to be able to take illegal content off their sites?

Director PATEL. Thank you, Senator.

We have engaged directly at the top levels of all the private sector software communities and social media companies and they have been very helpful because they have known, they have been told that this is a priority for me at the FBI to work with them because they have so much information to share back with us. Now that is of course just on the public systems. We were not talking about the dark net.

Senator LANKFORD. Thank you, Mr. Chairman.

Chairman COTTON. Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

Director Ratcliffe, I want to start with you. Who determined that the content of this discussion on Signal was not classified?

Director RATCLIFFE. Senator, I guess I am not——

Senator HEINRICH. Well, for example——

Director RATCLIFFE. I can speak to my personal knowledge, there was no classified.

Senator HEINRICH. There was an agent mentioned as part of this story. Normally, that would be classified information. So I guess what I'm asking is, did you just determine it was not classified or was there any declassification after the fact?

Director RATCLIFFE. So, to be clear, so everyone understands the process. As we talked about, Signal is a permissible use.

Senator HEINRICH. I understand that.

Director RATCLIFFE. And it is used at the CIA and has been approved by the White House for senior officials.

Senator HEINRICH. And appropriate for many conversations.

Director RATCLIFFE. And recommended by CISA for high level officials who would be targeted by foreign adversaries to use end-to-end encrypted apps whenever possible, like Signal. In this case what the National Security Adviser did was to request through a Signal message that there be coordination.

So you mentioned the name of a CIA active officer, correct? So——

Senator HEINRICH. I didn't mention the name, I mentioned the existence of that.

Director RATCLIFFE. And in the article the implication was that somehow that was improper. That was not the case.

So a CIA officer was not operating under cover—so the request for coordination was for a staff member to coordinate on the high-side. So I communicated the name of a CIA officer not operating under cover, completely appropriate, who does openly and routinely coordinate with the White House as a member of my staff. So the information that there was something inappropriate was clearly incorrect.

Senator HEINRICH. Did it occur to you that given the sensitive nature of this discussion, that it could just move to the high-side?

Director RATCLIFFE. So that was clearly, Senator, I think, the intent, was that this was initially set up by the National Security Adviser with the instruction that send a point of contact and then you

will be provided with information further on the high-side for high side communication.

So I think clearly it reflects that the National Security Adviser intended this to be as it should have been, a mechanism for coordinating between senior level officials, but not a substitute for using high-side or classified communications for anything that would be classified, and I think that is exactly what did happen.

Senator HEINRICH. So, I am curious. Did this conversation at some point include information on weapons packages, targets, or timing?

Director RATCLIFFE. Not that I am aware of.

Senator HEINRICH. Director Gabbard, same question.

Director GABBARD. Same answer, and defer to the Department of Defense on that question.

Senator HEINRICH. Well, those are two different answers.

But you are saying that was not part of the conversation.

Director GABBARD. Not to my knowledge.

Senator HEINRICH. Precise operational issues were not part of this conversation?

Director GABBARD. Correct.

Senator HEINRICH. Okay. I want to ask you, Director Gabbard, something on a very different track here, which is, I very much agree with the conclusion of the ATA that foreign illicit drug actors are a major threat in the United States, and many of you have spoken to this today.

Is the IC wrong in its omission of Canada as a source of illicit fentanyl in the ATA? I was surprised, given some of the rhetoric that there is no mention of Canada in the ATA.

Director GABBARD. Senator, the focus in my opening and the ATA was really to focus on the most extreme threats in that area, and our assessment is that the most extreme threat related to fentanyl continues to come from and through Mexico.

Senator HEINRICH. So the President has stated that the fentanyl coming through Canada is massive and actually said it was an "unusual and extraordinary" threat, and that was the language that was used to justify putting tariffs on Canada. I am just trying to reconcile those two issues. Is it an unusual and extraordinary threat or is it a minor threat that doesn't even merit a mention in the Annual Threat Assessment?

Director GABBARD. Senator, I don't have the numbers related to Canada in front of me at this time. I would like to get back to you on the specifics of that answer.

Senator HEINRICH. It is less than 1 percent of the fentanyl that we are able to interdict; but if you have different information I would very much welcome that.

Chairman COTTON. Senator Budd.

Senator BUDD. Thank you all for being here. And Director Gabbard, prior to your role here, we had a big storm in western North Carolina, and you were among those first from outside our State to show up. So thank you for your work there and thank you for your ongoing work there and that of your family as well. It was good to see them out in western North Carolina last week, so thank you.

Director Haugh, so what do we need to do in regards to Volt Typhoon. There was a lot of prepositioning that went on there. So where are we with that and what do we need to do in regards to our power companies, whether it is generation or distribution, Duke Energy in my home State or even the rural electric co-ops. What have we learned and what can I tell them?

General HAUGH. Senator, 99 percent of the critical infrastructure in the United States is controlled by private companies. That really drives us to talk about how do we partner with industry and with the commercial sector, in this case, the power sector.

Volt Typhoon began when industry came to the intelligence community and said: We are seeing anomalous activity. Can you help us to gain context? And we were able to bring context to that to be able to understand what the threat was and to ultimately be able to identify who was behind that threat.

Since that time, we have continued to work very closely with industry to be able to determine what are the right ways for us to be able to pursue these threats within networks to enable the interagency, to enable our partners, and industry to be able to pursue them. That is the approach we have to take. It is a collaboration between the government and industry to be able to eradicate these threats and we have continued to pursue them together since our first identification and notification related to this particular threat.

Senator BUDD. Thank you. What have you done on the offensive side here in regards to I think there were three, Salt Typhoon, Volt Typhoon and even Flax Typhoon? Maybe there were others, but those are the three that are known.

General HAUGH. Senator, I have been given really clear guidance in terms of what the Secretary of Defense expects in terms of our aggressive approach to be able to restore deterrence, and I look forward to talking with you about that in the closed hearing.

Senator BUDD. I look forward to that.

Directors Gabbard, Ratcliffe, and Patel, again, thank you all for being here. So, as you all are keenly aware, Section 702 of FISA is an extremely useful authority to help keep our Nation safe. I also know that we need to rebuild the American people's trust and confidence that such authorities are not being misused by the intelligence community to unlawfully target Americans. So, since taking over your respective agencies, can you tell me and tell the American people how effective the recent changes have been in protecting privacy and civil liberties of each and every American, and then if you will comment on how useful the authority is in generating the intelligence that actually protects the homeland. We will start with you, Director Gabbard.

Director GABBARD. Senator, Section 702 which authorizes the foreign collection of non-U.S. persons outside of the United States continues to be one of our most effective collection tools to ensure our national security. There are a number of reforms that the Senate passed that Congress passed last year that have proven to strengthen the protections of Americans' Fourth Amendment rights.

In the short time I have been in this seat, I have seen a few examples of that directly, most recently through the FISA Court call-

ing in an amici to come in and weigh in on a dispute regarding provisions that would further protect Americans' Fourth Amendment rights. I will be visiting our friends at the NSA next week and doing a quote unquote "ride along" to observe directly how those reforms that Congress passed are being implemented to protect Americans' civil liberties. I look forward to reporting back after I have had that opportunity.

Senator BUDD. Thank you. Director Patel.

Director PATEL. Thank you, Senator.

With my background in FISA and 702, I just want to clearly delineate between FISA Title I, III, and 702 collection. We need to both ardently defend its use but also ardently support reforms that allow the American public to entrust that those charged with those capabilities are not violating the Fourth Amendment or any other violation. Speaking of Title I, Title III, when it comes to U.S. persons, I have already included an amendment in terms of FBI language to make sure when a U.S. person is targeted, that the FBI, specifically, is responsible for culling through all exculpatory information that is reasonably known and satisfying that burden and stating it in the application.

When it comes to 702, Senator, some of the biggest enterprise efforts we have had to thwart, national security risk would not have occurred if 702 collection had gone dark. And the FBI continues to use that information to protect the homeland. We have had multiple takedowns in the last six months based on 702 and inter-agency collection processes but we just need to ensure the American public—and I am working with my team—and even in the 702 sphere that Americans' information is protected.

Senator BUDD. Thank you all. I look forward to the discussion in the closed session.

Chairman COTTON. Senator King.

Senator KING. Thank you, Mr. Chairman.

Director Gabbard, I didn't intend to get into the Jeffrey Goldberg story, but something you said has sort of puzzled me. According to open source reporting, at 11:44 on the morning of March 15, Secretary Hegseth put into this group text a detailed operation plan including targets, the weapons we were going to be using, attack sequences, and timing. And yet you have testified that nothing in that chain was classified.

Wouldn't that be classified? What if that had been made public that morning before the attack took place?

Director GABBARD. Senator, I can attest to the fact that there were no classified or intelligence equities that were included in that chat group at any time.

Senator KING. So the attack sequencing and timing and weapons and targets you don't consider should have been classified?

Director GABBARD. I defer to the Secretary of Defense and the National Security Council on that question.

Senator KING. Well, you are the head of the intelligence community, and you are supposed to know about classifications. So your testimony very clearly today is that nothing was in that set of texts that were classified.

I will follow up on Senator Wyden's question. If that is the case, please release the whole text stream so that the public can have

a view of what actually transpired on this discussion. It is hard for me to believe that targets and timing and weapons would not have been classified.

Let me move on.

You approved this report, this annual report, prepared by the Office of the Director of National Intelligence. Is this submitted to the White House routinely in anticipation of its public release?

Director GABBARD. I don't know what you mean by submitted routinely.

Senator KING. Was this report submitted to the White House before its release today?

Director GABBARD. It was submitted to them once it was completed. I think probably around the same time it was sent to all of you.

Senator KING. I want to move on.

One note that surprised me. I have been on this Committee now for, this is my 13th year. Every single one of these reports that we have had has mentioned global climate change as a significant national security threat, except this one. Has something happened?

Has global climate change been solved?

Why is that not in this report, and who made the decision that it should not be in the report when it has been in every one of the 11 prior reports?

Director GABBARD. I can't speak to the decisions made previously, but this Annual Threat Assessment has been focused very directly on the threats that we deem most critical to the United States and our national security. Obviously, we are aware of occurrences within the environment and how they may impact operations, but we are focussed on the direct threats to Americans' safety, well being, and security.

Senator KING. How about how they will impact mass migration, famine, dislocation, political violence, which is the finding, by the way, of the 2019 Annual Threat Assessment under the first Trump administration. You don't consider that a significant national security threat?

Director GABBARD. For the intelligence community, being aware of the environment that we are operating in is a given. What I focused this Annual Threat Assessment on and the IC focused this threat assessment on are the most extreme and critical direct threats to our national security.

Senator KING. Well, let me ask you a direct question. Who decided climate change should be left out of this report after it has been in the prior 11.

Director GABBARD. I gave direction to our team at ODNI to focus on the most extreme and critical national security threats that we face.

Senator KING. Did your direction include no comments on climate change.

Director GABBARD. Senator, as I said, I focused on the most extreme and direct national security threats—

Senator KING. That is not a response to a my question.

Director GABBARD [continuing]. that we face.

Senator KING. Did you instruct that there be no finding in terms of climate change in this report?

Director GABBARD. I don't recall giving that instruction.

Senator KING. Final questions in a few short seconds that I have left. You all concede and it is in the report repeatedly about the cyber danger from China, from Russia, from Iran. Why then is the administration deconstructing CISA; 130 people fired, General Haugh talked about the importance of public-private cooperation. That section of CISA seems to have been disestablished. What possible policy reason is there for undermining CISA's relationship to the States with regard to elections and to the private sector with regard to cybersecurity, when the cybersecurity threat is only growing?

Anybody want to tackle that?

Director GABBARD. I won't speak for all of my colleagues here, but I don't believe any of us have any insight into those specific staffing decisions that have been made.

Senator KING. Well, let me ask you this question. The report has found explicitly growing cyber threats including to elections from Russia, China, Iran. Do you believe that it is in the national interest to diminish our capacity to deal with those cyber issues, yes or no?

Director GABBARD. President Trump is focused on effects and making sure that the people that we have and the resources that we have are focused on our national security. He and his team recognized that more people doesn't necessarily always mean better effects. Those are some of the things that are driving the changes that we are seeing across the administration is getting all of our agencies back and focused on our core mission.

Senator KING. General Haugh, do you agree? Sorry, my time is up.

Chairman COTTON. Senator King, your time has expired.

Senator KING. Thank you.

Chairman COTTON. Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman.

First of all, thank you all for your service to our country.

With regard to the issues surrounding Signal, I am going to address it, but I am going to address it in the closed session so we can get more in depth into that issue.

In the meantime, I want to direct my first question to Director Ratcliffe. As the debate continues in Washington regarding spectrum, what can you share in this unclassified setting regarding the critical nature of spectrum to national security interests generally?

Director RATCLIFFE. Thanks for the question, Senator. I know this is an issue of great interest to the Senate—the potential auction of commercial space on spectrum. Those, as you correctly point out, the discussions about spectrum, I will start out by saying there are national security implications from such an auction if it were to take place, to both the DOD and the IC.

I think the discussions that we need to have, in a classified setting, I can relate to you that the direction from early meetings that we have had is that the discussion about where that might take place would not affect specifically CIA or IC equities and I hope that is the case where the discussion goes, but I think we need to be concerned that a public auction, that bands at certain levels

would have an impact on our ability to deliver an accurate intelligence picture.

Senator ROUNDS. In other words, there are parts of the spectrum which simply cannot be shared with the commercial?

Director RATCLIFFE. That is correct. And we can talk about the specific reasons why in a classified setting that would cause a diminishment of our ability to deliver a good threat picture to the Commander in Chief.

Senator ROUNDS. And in some cases life or death consequences involved?

Director RATCLIFFE. Absolutely.

Senator ROUNDS. Director Patel, first of all, I just want to thank you for what you are doing, and I know there is a number of items in your previous life that you did that simply can't be discussed; but nonetheless, we appreciate what you have done for our country already.

Today, I want to just talk to you about, we have seen a series of public news reports about ISIS threats within the United States and there have been several successful interdictions—Oklahoma City, Philadelphia, New York. Although the question remains as to the total number of ISIS operatives who were able to breach porous borders in the months and years before policy changes in this January—January of 2025, to what extent is the FBI tracking operatives who remain in the United States today, and what is the FBI doing to track them down?

Director PATEL. Thank you, Senator. I appreciate your question and your comments. So the priorities at the FBI since I took over have been violent crime and national security, and this speaks directly to national security.

The direction for the FBI is to track down any individuals with any terrorist ties whatsoever, whether it be ISIS or another foreign terrorist organization, and now to include the new designations of the cartels down south and elsewhere.

So, the FBI is utilizing our joint terrorism task force which are situated in all 55 Field Offices, but the key to success there is our partnership with State and local law enforcement who have the ground level intelligence on some of these operatives. And as you have highlighted, we have already shut down numerous threats and we've identified publicly, where permissible, these threats on individuals and where they are coming from and the I think the FBI is doing a very good job right now in collecting this information through our interagency process and we will continue to thwart every bad actor affiliated with a terrorist organization or otherwise.

Senator ROUNDS. Thank you.

And Director Haugh, first of all, Okay. You talked a little bit already about the problem with Salt Typhoon, but what I want to really get into is the things that are moving right now that you haven't had a chance to address, and in particular Cybercom 2.0, and the need to accelerate that particular plan moving forward. Can you talk just briefly—I've got 40 seconds left. Talk to us a little bit about how critical 2.0 is in terms of countering the cyber activity that is going on due to nefarious actors.

General HAUGH. Senator, what we were asked to do by Congress was to look at what is the force generation model for the Department of Defense to be able to generate cyber forces.

Based off of that request, I produced a recommendation for the Secretary that outlined three critical things which is really how we manage the talent, how we develop the talent in the Department, and also how we equip that talent underpinned by compute and AI.

We brought that plan initially back to Secretary Hegseth. He told us to go faster. We delivered him that plan, and now, based off his guidance, we will now begin to move forward with the rest of the Department.

Senator ROUNDS. Thank you.

Thank you, Mr. Chairman.

Chairman COTTON. Senator Bennet.

Senator BENNET. Thank you, Mr. Chairman.

Thank you very much for holding this hearing, and thank you for being here.

Director Ratcliffe, it sounds to me like your testimony today and the DNI's testimony is that there was nothing wrong at all with the Signal thread that you were on; that it didn't include any targeting information or battle sequence. That is your testimony. That is your testimony. And I am a little staggered that that is your view, Director Ratcliffe. Does the CIA have any rules about the handling of classified information, yes or no?

Director RATCLIFFE. Yes.

Senator BENNET. Thank you, Director Ratcliffe. Do you agree, Secretary of Defense Pete Hegseth said this morning when asked by members of the press what had happened, he said this morning in Hawaii that Atlantic Editor-in-Chief Jeff Goldberg is a quote "deceitful and highly discredited so-called journalist who has made a profession of providing hoaxes time and time again."

Do you share that evaluation, the Secretary of Defense's evaluation of Jeff Goldberg as a journalist?

Director RATCLIFFE. Senator, I didn't see those comments. I don't know Jeff Goldberg.

Senator BENNET. Do you share that view of the Secretary of Defense?

Director RATCLIFFE. I don't have a view.

Senator BENNET. Okay. Assuming that he has that view, I am curious about whether—You are the CIA Director. This has happened. We know it's happened. Did Jeff Goldberg somehow—was it—did he create a hoax that allowed him to become part of this Signal thread?

Please answer the question. Don't insult the intelligence of the American people. Did he invite himself to the Signal thread?

Director RATCLIFFE. I don't know how he was invited. Clearly he was—

Senator BENNET. Clearly it was—finish your sentence, please.

Director RATCLIFFE. Clearly he was added to the Signal group. Your question is—

Senator BENNET. So you don't know that the President's National Security Adviser invited him to join the Signal thread?

Everybody in America knows that; does the CIA Director not know that?

Director RATCLIFFE. I've seen conflicting reports about who added the reporter to the Signal messaging group.

Senator BENNET. Do you think it is perfectly appropriate that there was a reporter added, especially one that the Secretary of Defense says is "deceitful," "highly discredited," a "so-called journalist who has made a profession of peddling hoaxes over and over again"?

Is your testimony that it was appropriate that he was added to this Signal thread.

Director RATCLIFFE. No, of course not.

Senator BENNET. Why did you not——

Director RATCLIFFE. Hold on, Senator. Let me——

Senator BENNET. No, you answered the——

Director RATCLIFFE. You are mischaracterizing my testimony.

Senator BENNET. You answered the question. Let me ask you: When he was added to the thread, you are the CIA Director, why didn't you call out that he was present on the Signal thread?

Director RATCLIFFE. I don't know if you use Signal messaging app.

Senator BENNET. I do. I do—not for classified information, not for targeting, not for anything remote.

Director RATCLIFFE. Neither do I, Senator. Neither do I, Senator.

Senator BENNET. Well, that is what your testimony is today.

Director RATCLIFFE. It absolutely is not, Senator. Weren't you listening at the beginning when I said that I was using it as permitted. It is permissible to use——

Senator BENNET. I agree that is your testimony.

Director RATCLIFFE. Yeah.

Senator BENNET. I agree that is your testimony. You asked me if I used it, and I said not for targeting, not for classified information.

Director RATCLIFFE. And I said I don't either.

Senator BENNET. I also know Jeff Goldberg. I don't use it to communicate with him, but you thought it was appropriate.

By the way, I think he is one of the more outstanding journalists in America, but I am shocked to find him on a thread that he is reading in the parking lot of a grocery store in Washington, DC. And your testimony as the Director of the CIA is that it is totally appropriate.

Director RATCLIFFE. No.

Senator BENNET. Is it appropriate that the President——

Director RATCLIFFE. That is not what I——

Senator BENNET. Go ahead, please.

Director RATCLIFFE. When did I use the word "appropriate".

Senator BENNET. Well, go ahead, please.

Director RATCLIFFE. Well, I didn't.

Senator BENNET. So everybody in America——

Director RATCLIFFE. So, clearly, Senator——

Senator BENNET. Is what your testimony is. This is just a normal day at the CIA where we chat about this kind of stuff over Signal. In fact, it is so normal, that the last administration left it here for us. That is your testimony today.

Director RATCLIFFE. That's your testimony, Senator.

Senator BENNET. That is not my testimony. That is what you said.

Director RATCLIFFE. I didn't say any of those things that you related, Senator.

Senator BENNET. I heard you say it. Let the American people decide.

Director RATCLIFFE. Well, you just mischaracterized it. Are you going to give me a chance to—

Senator BENNET. Is it appropriate—Did you know that the President's Middle East adviser was in Moscow on this thread while you were, as Director of the CIA, participating in this thread? Were you aware of that? Are you aware of that today?

Director RATCLIFFE. I am not aware of that today.

Senator BENNET. This sloppiness, this incompetence, this disrespect for our intelligence agencies, and the personnel who work for them is entirely unacceptable. It is an embarrassment.

Director RATCLIFFE. Senator.

Senator BENNET. You need to do better. You need to do better. Thank you.

I am being gaveled by the Chairman and I apologize for going over my time.

Chairman COTTON. Senator Young.

Senator YOUNG. Thank you all for being here. I will be asking some follow-up questions, clarifications about this Signal episode in a closed setting, and try and work with all of you to bring clarity to that situation. It appears to me there are some unanswered questions. It will take some time, I think, to get there in a more dispassionate setting.

Director Gabbard, I am going to begin today asking you some questions about emerging technologies. It has been a real point of emphasis, I know, of our broader national security community for a period of time. We know that PRC is making generational investments in certain emerging tech—AI, biotech, and other areas of technology to reduce their vulnerability against any supply chain disruptions and to lead the world in some areas.

As the IC assesses, the PRC is seeking to quote "become a global S&T superpower, surpass the United States, promote self-reliance, and achieve further economic, political, and military gain."

Director Gabbard, can you describe the actions China is taking to operationalize that IC assessment in ways that directly target the security and prosperity of everyday Americans?

Director GABBARD. Senator, what we know is that they are trying to use these capabilities as a means to continue to exploit vulnerabilities within our own critical infrastructure and our cyber technology.

Critical infrastructure is a key area of concern, given what we know has already been exploited; these asymmetric attacks that have been placed within our critical infrastructure that are of serious concern given how they could be exploited especially during a time of conflict.

We know that they are experiencing a boom in their generative AI capability and are competing very heavily against our own AI capabilities. Obviously, AI can and will be used across a multitude of every sector of our society, both here as we are in our own coun-

try, and we expect China to be able to continue to do the same there.

Senator YOUNG. So, two key areas of vulnerability to the United States conceivably, susceptibility to cyber attacks and China's leveraging of AI towards misinformation and increasingly into the physical realm, they can pose threats to us as well.

As follow-up, Director Ratcliffe, we have had Huawei, we've had TikTok, what do you believe will be the next point of technological friction in competition between the U.S. and China?

What should Members of Congress be looking for?

Director RATCLIFFE. Senator, I think I can answer this question more fully in the classified setting. What I would say is it relates to the issue of emerging technologies and matters of quantum computing and quantum sensing, and our ability to stay ahead of China in the technological curve with respect to those issues.

I would be happy to get into that in further detail in a classified setting.

Senator YOUNG. Excellent. We will dive into that.

Director Haugh—general, how do you see biotech playing into this broader competition?

General HAUGH. I think it is an area that from our perspective has increasingly been a priority as we all understand the approach that China has taken and also to ensure that as we think about the President's priorities in terms of both economic and technology security, we are certainly as a community following DNI's guidance that we are increasingly putting our resources to be able to ensure that we understand where China is investing in those resources and how that will impact our economy and over all, the overall health of our national security.

Senator YOUNG. Thank you, General.

Director Gabbard, not a lot of time left on this end but I have a little crypto interest I want to communicate to you. Can you share with this Committee how we are positioned to disrupt foreign cyber efforts to steal cryptocurrency such as the North Koreans have successfully done?

If others would like to pull this thread and weigh in on this question very briefly, that would be great.

Director GABBARD. Senator, we are obviously aware of North Korea's revenue generating by stealing cryptocurrency has had a significant effect on North Korea's capabilities. I defer to our technical experts on the actions that are being taken.

General HAUGH. Senator, I think this would be a great topic when we go to closed session.

Senator YOUNG. It is going to be a busy closed setting, yes. Director Patel?

Director PATEL. I agree with the General. In closed session I can provide some details.

Senator YOUNG. It is what you get when you visit with a bunch of spies. All right, Chairman.

Chairman COTTON. Senator Kelly.

Senator KELLY. Thank you, Mr. Chairman.

I am going to come back to the topic of the day here, the Signal chain as reported by *The Atlantic*.

Ms. Gabbard and Mr. Ratcliffe, you each testified that there was no information operational in nature, no classified information. So, I want to ask each of you a series of questions. Just respond yes or no.

I will start with Ms. Gabbard. In the Signal chain that we have been talking about, was there any mention of a target in Yemen?

Director GABBARD. I don't remember mention of specific targets.

Senator KELLY. Any generic target?

Director GABBARD. I believe there was discussion around targets in general.

Senator KELLY. Mr. Ratcliffe.

Director RATCLIFFE. I think that is consistent with my recollection. Again, I don't have access to that.

Senator KELLY. Was there any mention, Ms. Gabbard, of a weapon or weapons system?

Director GABBARD. I don't recall specific weapons systems being named.

Senator KELLY. I am not talking about specific—any weapon or weapons system.

Director GABBARD. I don't recall specific names of systems or weapons being used or named within the chain.

Senator KELLY. Well, I am not asking whether—I don't want you to tell me what the specific weapon was, but any weapon at all.

Mr. Ratcliffe, same question.

Director RATCLIFFE. I don't recall.

Senator KELLY. How about anything about timing, Ms. Gabbard?

Director GABBARD. I don't recall specific timing.

Senator KELLY. Was there any mention—

Director GABBARD. And I won't get into the detail of the conversation, but obviously there was a significant amount of planning and internal discussions that had occurred prior to and outside of this Signal chat.

Senator KELLY. Mr. Ratcliffe, you are nodding your head. Any mention of any military unit whatsoever, Mr. Ratcliffe.

Director RATCLIFFE. Not that I recall.

Senator KELLY. Ms. Gabbard.

Director GABBARD. Not that I recall.

Senator KELLY. Okay. I understand that DOD policy prohibits discussion of even what is called "controlled unclassified information" or CUI on unsecured devices.

Are both of you aware of that DOD policy?

Director GABBARD. I haven't read that policy.

Director RATCLIFFE. Not familiar with the DOD policy, but I would say that the Secretary of Defense is the original classification authority for DOD in deciding what would be classified information.

Senator KELLY. Ms. Gabbard, does the intelligence community have a policy that prohibits discussion of controlled unclassified information?

Director GABBARD. Yes.

Senator KELLY. It does. Okay. Controlled unclassified information, according to DOD, includes information that is information that has not been approved for public release. Would you—of what

has been disclosed publicly of the Signal chain, would either of you feel that that would be approved for public release?

Ms. Gabbard.

Director GABBARD. The discussion that took place in that Signal chat group was a conversation reflecting national security leaders and the Vice President around the President's objectives.

Senator KELLY. So, yes or no, would you approve that for public release?

Director GABBARD. I don't feel I can answer that question here.

Senator KELLY. Because of the nature of this hearing?

Director GABBARD. Because of the nature of a private discussion that took place between individual leaders in our government.

Senator KELLY. It would make sense that you would not approve it for public release, wouldn't it?

Director GABBARD. There are other factors that would go into that consideration.

Senator KELLY. Okay. Mr. Ratcliffe, yes or no.

Director RATCLIFFE. I wouldn't approve the release of classified information. Again, as I've said—

Senator KELLY. I am not talking about classified information, Mr. Ratcliffe. I am talking about information that has not been approved for public release, that is information that is considered controlled unclassified information.

Director RATCLIFFE. The principals that would have been on that would have been individuals capable of approving that for public release.

Senator KELLY. I got 20 seconds. The deliberation as to whether or not we should launch a strike on another country, would you consider that classified information, Ms. Gabbard?

Director GABBARD. The information was not classified.

Senator KELLY. This is—I am not talking about this. I am just talking about deliberation from principals as to whether or not we should launch a strike on another country. Would you consider that classified information? I am not talking about what happened this week.

Director GABBARD. There are other factors that would go into determining that classification.

Senator KELLY. Mr. Ratcliffe, the deliberation between principals in our national security apparatus about whether or not to strike another country, would you consider that to be classified information.

Director RATCLIFFE. Predecisional strike deliberations should be conducted through classified channels.

Senator KELLY. Thank you.

Thank you, Mr. Chairman.

Chairman COTTON. If I may, I just want to return, Mr. Ratcliffe, to your answer there in part of Senator Kelly. It has been raised on several occasions now in this hearing about whether classified information was discussed in this chat; and you mentioned about the Secretary of Defense being what you called the original classification authority?

Director RATCLIFFE. Correct.

Chairman COTTON. I think it is important for the public to understand that although you and Director Gabbard are original clas-

sification authorities on many matters, you are not that for all matters that might be classified in the government; is that right?

Director RATCLIFFE. That's correct.

Chairman COTTON. So, if the Secretary of State has classified sensitive diplomatic details, that is his authority. If the Secretary of Energy has sensitive classified information about our national laboratories, that is his authority; and the two of you can't speak to other departments who have their own original classification authority and which, of course, as Director Gabbard said, ultimately rests with one person, the President of the United States; is that correct?

Director RATCLIFFE. That's correct.

Chairman COTTON. I just wanted to clarify that.

It looks like the Vice Chairman wants to weigh in as well.

Vice Chairman WARNER. Just very briefly.

I mean, I think it strains the audience and the watching public's credibility. If we are talking about timing, packages, that somehow this would be okay to put out, or just frankly, senior American officials trashing Europe. I have been around this for a while. This is not information you generally put out, and the notion that there is not even acknowledgment of "hey, gosh, we screwed up" is stunning to me. And the idea somehow that none of this was classified but we can't talk about it here—you can't have it both ways.

Chairman COTTON. I think the witness's point is they can't speak for every official in the government who has original classification authority.

Vice Chairman WARNER. Mr. Chairman, I don't—that is not what—I am not trying to litigate that.

I am trying to litigate on the face, unless as Senator Bennet said, this reporter is somehow making this all up. I think the White House has acknowledged that the text chain he submitted was authentic—it strains my mind to think, it strains my mind if the shoe had been on the other foot what my colleagues would be saying about this. And again, we are going to get to the bottom of it. I appreciate your comments, but you both testified under law that there is nothing classified in that information. In a sense, I have not heard any one of you say: Gosh, we screwed up. We will find out. This is too important to our national security, and again, I know we have more Members to cross.

Chairman COTTON. They testified, is my understanding—correct me if I am wrong, that there is no intelligence community classified information; is that correct?

Director RATCLIFFE. That's correct.

Chairman COTTON. Is that correct, Director Gabbard?

Director GABBARD. Yes, Chairman.

Senator KING. (Off microphone.) That is not correct. She said repeatedly there was nothing classified. Period.

Vice Chairman WARNER. Period.

You can't have it both ways. Again, we will see. I cannot believe this is not going to come out. And if it is not classified, again, we would ask you to make it—give it to the public today. I am sure one of your aides back there have probably got it on paper. If you got it here and it is not classified, stand by your position. Or is this

just one more example of a careless approach to how we keep our secrets in this administration.

Chairman COTTON. With apologies, to Senator Moran.

Senator MORAN. Thank you, Mr. Chairman, and thank you to our witnesses for being here.

I want to explore a little bit about Ukraine, and I will direct this to Director Ratcliffe or Director Kruse. The ATA assesses that “the grinding war of attrition in Ukraine will lead to a gradual but steady erosion of key positions on the battlefield.”

Are Ukrainian forces at any significant risk of collapse this year?

LTGEN KRUSE. Before I turn it over to Director Ratcliffe, I think both sides are working through the equipment that they need, the industrial base they need to be able to support that and the personnel that are required to man that equipment and man the frontlines. As we see the battle space in various portions, whether it is in Kursk or any of the four Oblasts, we see areas where Kyiv will struggle to prevent the slow attritional grind. We do not see an imminent collapse in any of the line of control battle spaces at this point.

Senator MORAN. And then, vice versa. That answers my question, unless you want to add something, Director.

Whatever advantages in manpower and materiel they have, can Russia maintain its operational tempo without significant changes to how it is conducting the war?

LTGEN KRUSE. I think our assessment from a military perspective is that Russia has the ability to sustain its campaign longer than Kyiv would. Now when that timeline hits, we do not have an assessment of, but I believe that if this were to go on for more than the remainder of this year, both sides would have a significant challenge maintaining their defense industrial base as well as their operational ops tempo.

Senator MORAN. Longer than this year.

LTGEN KRUSE. That is correct, and they will each have difficulty at various points throughout the spring, summer, and fall, as well.

Senator MORAN. Thank you.

Director Ratcliffe, ATA says continuing the Russia-Ukraine war perpetuates strategic risk to the United States of unintended escalation to a large-scale war and heightened insecurity among NATO allies. What are the strategic risks to the United States if Russia were to achieve its maximalist objectives via a peace agreement?

Director RATCLIFFE. Achieve via a peace agreement?

Senator MORAN. Yes.

Director RATCLIFFE. Well, I think that clearly the negotiations that are going on reflect that President Trump is seeking a cessation of the war on terms that will end the war permanently. From an intelligence community standpoint, and specifically with regard to CIA assets, we have taken steps to support that—the President’s goal of an enduring peace.

To General Kruse’s comments, I agree with his assessment and generally the public assessment that Russia has the battlefield advantage, is grinding forward slowly. I want to comment on that, however, to say that with regard to the Ukrainian resistance, the Ukrainian people and the Ukrainian military have been underestimated for a period of several years now, and ultimately I am con-

vinced from my reflections in observing from an intelligence standpoint that they will fight with their bare hands if they have to, if they don't have terms that are acceptable to an enduring peace.

Obviously, to the point of maximalist goals, President Trump has communicated that he is aware of the dangers of that—of Russia getting what they want. And I think that the peace talks that are taking place would reflect, if successful—and they are making progress—that both sides would not get everything that they want and no one's maximalist goals would be achieved.

Senator MORAN. Thank you both.

In the short time that I have, I am going to skip a question that I intended to ask but ask the Director of the FBI.

Director, I chair the subcommittee that appropriates money for the Department of Justice, including the FBI. It has been our practice that the FBI Director as well as the Attorney General appear before our committee each year, and I would want to make certain that you do not foresee any challenges that I will have in your presence when you come to speak—when we invite you to come to speak about your budget.

I think when you visited in the office you made yourself often available, pleased to talk to Congress. We are getting ready for the appropriations process to begin. The budget the President intends to submit is seemingly months away—weeks away, long weeks away. And we may ask you to testify about your priorities now or sooner than that. Is that a challenge for you that we ought to be aware of?

Director PATEL. From the FBI, no, as long as the Department of Justice and Attorney General are good with it.

Senator MORAN. Thank you.

Chairman COTTON. Senator Reed.

Senator REED. Thank you very much, Mr. Chairman.

Director Ratcliffe, you have repeatedly made the point that there was no classified information contained in any of these discussions that were reported in the Atlantic Monthly; is that correct?

Director RATCLIFFE. No, that is not correct, Senator. What I related is that any information that was related from my perspective or that I observed from the intelligence perspective was not classified information.

With respect to the assertions and the allegations that there was strike packages or targeting information or things that relate to DOD, as I pointed out, the Secretary of Defense is the original classification authority for determining whether something is classified or not, and as I understood from media reports, the Secretary of Defense has said the information was not classified.

Senator REED. Are you aware that the Secretary of Defense declassified this information prior to the discussion?

Director RATCLIFFE. I am not.

Senator REED. Director Gabbard, you indicated—at least the impression that I got was that there was no classified information discussed; is that correct?

Director GABBARD. Senator, my answer is the same as the Director of the CIA.

Senator REED. The question has to be posed to Secretary Hegseth whether he declassified the information and at what point he did declassify it; do you agree?

Director GABBARD. Yes, I defer questions to the Secretary of Defense.

Senator REED. Okay. Director Patel, are you conducting an investigation of this—these discussions and activities?

Director PATEL. Thank you, Senator. As I informed the Vice Chairman on the same question, I found out about this late last night, early this morning. So, I don't have an update for you on that.

Senator REED. Thank you. When you get an update, we would appreciate it very much.

Director PATEL. Yes, sir.

Senator REED. Director Gabbard, were you overseas during any parts of these discussions?

Director GABBARD. Yes, Senator, I was.

Senator REED. Were you using your private phone or a public phone for these Signal discussions?

Director GABBARD. I won't speak to this because it is under review by the National Security Council. Once that review is complete I am sure we will share the results with the Committee.

Senator REED. What is under review? It is a very simple question, your private phone or an officially issued phone. What could be under review?

Director GABBARD. The National Security Council is reviewing all aspects of how this came to be, how the journalist was inadvertently added to the group chat, and what occurred within that chat across the board.

Senator REED. So you are not going to disclose anything about whether you used a phone.

Director Ratcliffe, there is an indication that the CIA has warned recently retired personnel about the vulnerabilities of Signal and other encrypted messaging applications. If that is the case, why were you discussing these issues on Signal?

Director RATCLIFFE. Senator, Signal use, as I said repeatedly, is permissible for work purposes.

I've never said that end-to-end encryption apps like Signal are a substitute for classified systems, and I was not discussing classified information in this setting.

Senator REED. But as you have indicated previously, perhaps the Secretary of Defense was discussing classified information and only he can be held accountable in terms of whether it was classified or declassified of what he formally spoke, is that accurate?

Director RATCLIFFE. Well, I didn't say it that way.

I said the Secretary of Defense is the original classification authority, and my understanding is that his comments are that any information that he shared was not classified.

Senator REED. But you have no way to verify that?

Director RATCLIFFE. I don't.

Senator REED. Again, this is a very troubling example, and a great lapse in our intelligence, in our discussion.

One further point: If you are not aware of any classified information on the discussions back and forth, would it be appropriate for

the author to release the entire text of what he heard or transcribed?

Director RATCLIFFE. I think the author has released—my understanding—essentially, almost all of the information as it has been related to me.

I don't know what calculation the author made with regard to what information would be released or not. But again, I can again confirm that with respect to the communications that were related as to me, there was no classified information.

Senator REED. According to the article, quote, "the message contained information that might be interpreted as related to actual and current intelligence operations" and the author did not disclose that information. So, the question would be if he disclosed everything he heard, in your view—

Director RATCLIFFE. That wouldn't be classified information. I know the context of what that is, and I think the author said "might be interpreted as related to" intelligence information. It was not classified information.

Senator REED. So it goes back to my point, if he released all this information he did not release, he could do so without any liability at the Federal level?

Director RATCLIFFE. I think you are asking for a legal answer I am not able to give you.

Senator REED. Mr. Patel, can you opine?

You are a lawyer and you are the Director of the FBI. Would he face any legal liability if he released the information?

Director PATEL. Because of the questions you and the Vice Chairman have put to me, I am not going to prejudge the situation. And that legal call is ultimately for the Department of Justice.

Senator REED. Thank you. Thank you very much, Mr. Chairman.

Chairman COTTON. Senator Ossoff.

Senator OSSOFF. Thank you, Mr. Chairman, and thank you all for joining us and for your service.

Just to make sure I understand some of the basics here. So, Director Ratcliffe, you were a member of the Houthi PC small group Signal chain, correct.

Director RATCLIFFE. I was.

Senator OSSOFF. And so was the Vice President, the Secretaries of State and Defense, the National Security Adviser, and Ms. Gabbard; correct?

Director RATCLIFFE. I believe so. I don't have a list of who was invited, to be honest.

Senator OSSOFF. So was national political reporter Jeffrey Goldberg, correct?

Director RATCLIFFE. I don't know that.

Senator OSSOFF. Yes, you do.

Director RATCLIFFE. I don't know Jeffrey Goldberg, and I have already testified, I don't know whether or how he was added.

Senator OSSOFF. Okay. Well, he was a member of the Signal chain, and the discussion included the Vice President's private opinion on the wisdom of proposed U.S. strikes in Yemen, correct?

Director RATCLIFFE. I don't recall.

Senator OSSOFF. Vance: "I think we are making a mistake. I am not sure the President is aware of how inconsistent this is with his

message on Europe. Right now there is a strong argument for delaying this a month.”

You don’t recall?

Director RATCLIFFE. As you—As you read that—

Senator OSSOFF. You don’t recall seeing that?

Director RATCLIFFE. I don’t.

Senator OSSOFF. It included the private opinions of the Secretary of Defense on the timing of strikes in Yemen, correct?

Director RATCLIFFE. I don’t recall.

Senator OSSOFF. Director Ratcliffe, surely you prepared for this hearing today. You are part of a group of principals, senior echelons of the U.S. Government in now a widely publicized breach of sensitive information.

You don’t recall whether the vice-president opined on the wisdom of the strikes? That is your testimony today under oath?

Director RATCLIFFE. In that setting, I don’t recall.

Senator OSSOFF. Here is what Secretary Hegseth said: “Waiting a few weeks or months does not fundamentally change the calculus. Two immediate risks on waiting. One this leaks and we look indecisive. Two, Israel takes an action first or Gaza’s ceasefire falls apart and we don’t get to start this on our own terms.”

Your testimony is that you don’t recall the Secretary of Defense sending that message or reading it?

Director RATCLIFFE. I recall there being an exchange. I don’t recall the specifics as you are reading it.

Senator OSSOFF. Well, let’s put it this way. Director Ratcliffe, a discussion by senior U.S. officials on the timing and risks of a proposed military campaign, and disagreements between the President and the Vice President about U.S. plans and intentions would be of obvious interest to foreign intelligence services, would it not?

Director RATCLIFFE. Yes.

Senator OSSOFF. And they were discussing the timing of sending U.S. air crews into enemy air space where they faced an air defense threat; correct?

Director RATCLIFFE. I am going to—Senator, defer to the other principals that you are referring to about what the meaning and context of what—

Senator OSSOFF. Director Ratcliffe, they are talking about the timing of U.S. air strikes, correct?

Director RATCLIFFE. Yes.

Senator OSSOFF. And therefore the timing of sending U.S. air crews into hostile air space; correct?

Director RATCLIFFE. Yes.

Senator OSSOFF. And therefore the time period during which enemy air defenses could target U.S. air crews flying in enemy air space; correct?

Director RATCLIFFE. I don’t know that.

Senator OSSOFF. You do know that. Let me ask this question, General Haugh.

You lead America’s signals intelligence collection. Would the private deliberation of foreign senior officials about the wisdom and timing of potential military action be a collection priority for you and the U.S. intelligence community?

General HAUGH. Senator, it is our job to do indications and warning for both the plans and intentions of adversary leaders and for military commanders.

Senator OSSOFF. And would not information about the timing of air strikes allow a military to preposition or cue air defense systems to shoot down enemy aircraft?

General HAUGH. I think, Senator, from our perspective, any advanced warning is something that we certainly are trying to protect.

Senator OSSOFF. Director Ratcliffe, this was a huge mistake, correct?

Director RATCLIFFE. No.

Senator OSSOFF. A national political——

Director RATCLIFFE. Hold on.

Senator OSSOFF. No, no, you hold on.

Director RATCLIFFE. Let me answer.

Senator OSSOFF. No, No. Director Ratcliffe, I am asking a yes-or-no question and now you will hold on. A national political reporter——

Director RATCLIFFE. You can characterize it how you want——

Senator OSSOFF [continuing]. Was made privy to sensitive information——

Director RATCLIFFE. The White House was clear that——

Senator OSSOFF [continuing]. About imminent military operations against a foreign adversary——

Director RATCLIFFE [continuing]. There was an inadvertent mistake of adding a reporter.

Senator OSSOFF. And that wasn't a huge mistake?

[Cross talk.]

Director RATCLIFFE. Well, I think—they characterized——

Senator OSSOFF. This as an embarrassment. This is utterly unprofessional. There has been no apology. There has been no recognition of the gravity of this error.

And, by the way, we will get the full transcript of this chain and your testimony will be measured carefully against its content.

Thank you, Mr. Chairman.

Chairman COTTON. I thank the witnesses again for their appearance today.

I sense the Vice Chairman has something to add.

Vice Chairman WARNER. I do.

Chairman COTTON. So I will recognize him, briefly.

Vice Chairman WARNER. Well, again, I thank the witnesses, but what you are saying doesn't make sense on the face of it.

Everybody knows.

At least, Director Ratcliffe, you had the courtesy of acknowledging you were on the chain.

Director Gabbard wouldn't even touch that, even though we have got her initials.

If you want a comparison, think back to the beginning of the Ukraine war when the United States in concert of our then-ally the United Kingdom declassified a lot of Putin's battle plans that allowed the Ukrainians to push back successfully on the Russian invasion. How was that? That was gone through a real process of declassification.

As Senator Ossoff clearly made the point, this information out potentially where our adversary could reposition its defenses and the unwillingness of the individuals on this panel who were on the chat to even apologize or acknowledge what a colossal screw-up this is speaks volumes.

Chairman COTTON. Thank you to our witnesses for your appearance.

A few administrative matters. As I mentioned earlier, Senator Collins is under the weather. She regrets she cannot be here for your testimony.

Senator Risch, likewise, had to preside over a hearing of the Foreign Relations Committee to include the nomination of my former Governor, Mike Huckabee, a Great American and a great friend of Israel, to be the next Ambassador to Israel. He also regrets he cannot be here. I anticipate he would have written questions, as well. I would urge you all to respond to those promptly.

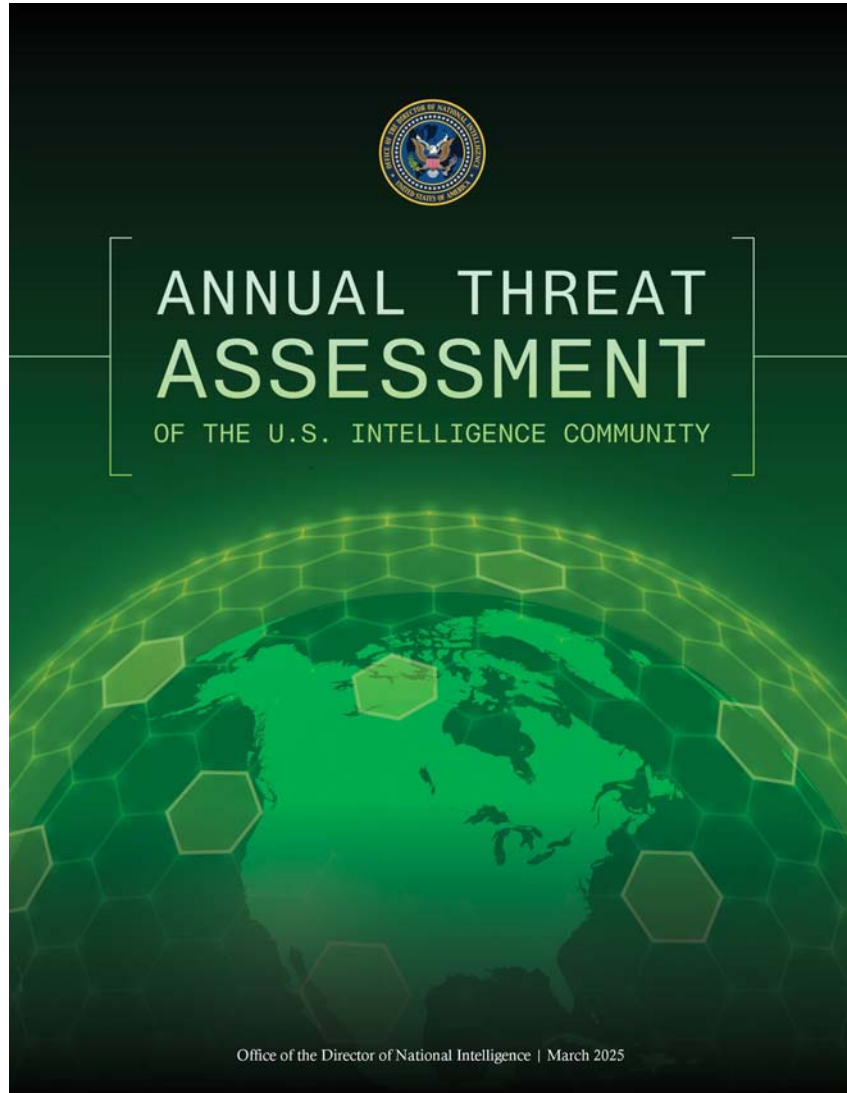
Now, the audience will remain seated while our witnesses and their aides depart the hearing room. The Capitol Police will ensure this occurs.

I want to commend the Capitol Police and our Committee security staff for running an orderly hearing today.

For the benefit of Members, the vote on the floor has been called. We will adjourn this open hearing, and we will reconvene in closed setting at 12:40 p.m.

The hearing is adjourned.

(Whereupon, the proceedings adjourned at 12:10 p.m.)



ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

March 2025

INTRODUCTION

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 *Intelligence Authorization Act* (Pub. L. No. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States primarily during the next year. All these threats require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future.

Information available as of 18 March was used in the preparation of this assessment.

CONTENTS

INTRODUCTION	2
FOREWORD	4
NONSTATE TRANSNATIONAL CRIMINALS AND TERRORISTS	5
Foreign Illicit Drug Actors	5
Transnational Islamic Extremists.....	6
Other Transnational Criminals	7
MAJOR STATE ACTORS	10
China.....	10
Russia.....	18
Iran	24
North Korea.....	30
Adversarial Cooperation.....	32

FOREWORD

The 2025 Annual Threat Assessment (ATA) is the Intelligence Community's (IC) official, coordinated evaluation of an array of threats to U.S. citizens, the Homeland, and U.S. interests in the world. A diverse set of foreign actors are targeting U.S. health and safety, critical infrastructure, industries, wealth, and government. State adversaries and their proxies are also trying to weaken and displace U.S. economic and military power in their regions and across the globe.

Both state and nonstate actors pose multiple immediate threats to the Homeland and U.S. national interests. Terrorist and transnational criminal organizations are directly threatening our citizens. Cartels are largely responsible for the more than 55,000 U.S. deaths from synthetic opioids in the 12 months ending in September 2024 and helped facilitate the nearly three million illegal migrant arrivals at the Southwest Border in 2024, straining resources and putting U.S. communities at risk. A range of cyber and intelligence actors are targeting our wealth, critical infrastructure, telecom, and media. These groups are often enabled, both directly and indirectly, by state actors, such as China and India, as sources of precursors and equipment for drug traffickers. State adversaries have weapons that can strike U.S. territory, or disable vital U.S. systems in space, for coercive aims or actual war. These threats reinforce each other, creating a vastly more complex and dangerous security environment.

Russia, China, Iran and North Korea—individually and collectively—are challenging U.S. interests in the world by attacking or threatening others in their regions, with both asymmetric and conventional hard power tactics, and promoting alternative systems to compete with the United States, primarily in trade, finance, and security. They seek to challenge the United States and other countries through deliberate campaigns to gain an advantage, while also trying to avoid direct war. Growing cooperation between and among these adversaries is increasing their fortitude against the United States, the potential for hostilities with any one of them to draw in another, and pressure on other global actors to choose sides.

This 2025 ATA report supports the Office of the Director of National Intelligence's commitment to keeping the U.S. Congress and American people informed of threats to the nation's security, representing the IC's dedication to monitoring, evaluating, and warning of threats of all types. In preparing this assessment, the National Intelligence Council worked closely with all IC components, the wider U.S. Government, and foreign and external partners and experts to provide the most timely, objective, and useful insights for strategic warning and U.S. decision advantage.

This 2025 Annual Threat Assessment details these myriad threats by actor or perpetrator, starting with nonstate actors and then presenting threats posed by major state actors. The National Intelligence Council stands ready to support policymakers with additional information in a classified setting.

NONSTATE TRANSNATIONAL CRIMINALS AND TERRORISTS

Transnational criminals, terrorists, and other nonstate actors are threatening and impacting the lives of U.S. citizens, the security and prosperity of the Homeland, and U.S. strength at home and abroad. Some transnational criminal organizations (TCOs) are producing and trafficking large amounts of illicit drugs that are imperiling American lives and livelihoods. They are conducting other illegal activities that challenge U.S. security, such as human trafficking, cyber operations, money laundering, and inciting violence. U.S. citizens—at home and abroad—are also facing more diverse, complex, and decentralized terrorist threats. Actors, ranging from designated Foreign Terrorist Organizations—including the Islamic State of Iraq and ash-Sham (ISIS), al-Qa'ida, other Islamist terrorist groups, and some drug cartels—to terrorists acting alone or in small cells, are likely to pursue, enable, or inspire attacks. Finally, large-scale illegal immigration has strained local and national infrastructure and resources and enabled known or suspected terrorists to cross into the United States.

Foreign Illicit Drug Actors

Western Hemisphere-based TCOs and terrorists involved in illicit drug production and trafficking bound for the United States endanger the health and safety of millions of Americans and contribute to regional instability. Fentanyl and other synthetic opioids remain the most lethal drugs trafficked into the United States, causing more than 52,000 U.S. deaths in a 12-month period ending in October 2024. This represents a nearly 33 percent decrease in synthetic opioid-related overdose deaths compared to the same reporting time frame the previous year, according to CDC provisional data, and may be because of the availability and accessibility of naloxone.

- Mexico-based TCOs—including the Sinaloa Cartel and the New Generation Jalisco Cartel—remain the dominant producers and suppliers of illicit drugs, including fentanyl, heroin, methamphetamine, and South American-sourced cocaine, for the U.S. market. Last year, official points of entry along the U.S.-Mexico border were the main entry point for illicit drugs, often concealed in passenger vehicles and tractor trailers. However, some TCOs likely will at least temporarily change their smuggling techniques and routes in response to increased U.S. security force presence at the border.
- Since at least 2020, the growth of Mexico-based independent fentanyl producers—actors who are autonomous or semiautonomous from Mexican cartel control—has increasingly fragmented Mexico's fentanyl trade. Independent fentanyl producers are attracted to the drug's profitability and the low barriers to market entry, including the ease of synthesizing it using basic lab equipment and few personnel.
- Colombia-based TCOs and illegal armed groups are responsible for producing and exporting the vast majority of cocaine that reaches the United States, some of which is transshipped through Ecuador, contributing to an uptick in violent criminal conflicts that spurs regional migration.

- Mexico-based TCOs are ramping up lethal attacks in Mexico against rivals and Mexican security forces using IEDs, including landmines, mortars, and grenades. In 2024, there were nearly 1,600 attacks on Mexican security forces using IEDs, surging from only three reported attacks between 2020-2021. The sophistication of TCO tactics is reshaping Mexico's security landscape and has heightened the risk to security forces.

China remains the primary source country for illicit fentanyl precursor chemicals and pill pressing equipment, followed by India. Mexico-based chemical brokers circumvent international controls through mislabeled shipments and the purchase of unregulated dual-use chemicals.

Transnational Islamic Extremists

ISIS's most aggressive branches, including ISIS-Khorasan (ISIS-K), and its entrepreneurial plotters will continue to seek to attack the West, including the United States, via online outreach and propaganda aimed at directing, enabling, or inspiring attacks, and could exploit vulnerable travel routes. ISIS has suffered major setbacks and is incapable of holding ground in Iraq and Syria. In recent years, ISIS saw the U.S. defeat of its physical caliphate in 2019, the loss of three overall leaders in 2022, 2023, and 2025, and renewed counterterrorism efforts this year removing leaders driving global operations. Nevertheless, ISIS remains the world's largest Islamic terrorist organization, has sought to gain momentum from high-profile attacks, and continues to rely on its most capable branches and globally dispersed leadership to weather degradation.

The New Year's Day attacker in New Orleans was influenced by ISIS propaganda, and separately, an Afghan national was arrested in October for planning an election day attack in the name of ISIS, highlighting ISIS's ability to reach into the Homeland to both inspire and enable attacks.

- ISIS-K in South Asia is the group's branch most capable of carrying out external terrorist attacks and maintains the intent to conduct attacks in South and Central Asia, and globally, although its capabilities vary. ISIS-K's mass casualty attacks in Russia and Iran in 2024, as well as arrests of ISIS-K supporters in Europe and the United States, highlight the group's expanding capability beyond South Asia and ability to inspire individuals to conduct attacks abroad.
- ISIS will seek to exploit the end of the Asad regime in Syria to reconstitute its attack capabilities, including external plotting, and to free prisoners to rebuild their ranks.
- In 2024, the ISIS spokesman publicly hailed the group's Africa expansion, highlighting the growing importance of the continent to the group. ISIS-Somalia has doubled in size during the past year, ISIS-West Africa remains the largest branch and leads in numbers of claimed attacks, and ISIS-Sahel is expanding into coastal West Africa.

Al-Qa'ida maintains its intent to target the United States and U.S. citizens across its global affiliates. Its leaders, some of whom remain in Iran, have tried to exploit anti-Israeli sentiment over the war in Gaza to unite Muslims and encourage attacks against Israel and the United States. Al-Qa'ida's media apparatus issued statements from leaders and the group's affiliates supporting HAMAS and encouraging attacks against Israeli and U.S. targets.

- Al-Qa'ida in the Arabian Peninsula (AQAP) relaunched its *Inspire* guide with videos and tweets that encouraged attacks against Jewish targets, the United States, and Europe. *Inspire* provided instructions for making bombs and placing explosive devices on civilian airliners and gave religious, ideological, historical, and moral justification for such attacks. In addition to trying to inspire attacks worldwide and in the United States, AQAP has the intent to conduct operations in the region and beyond.
- Al-Shabaab—al-Qa'ida's largest and wealthiest affiliate—remains focused on attacks in Somalia that further its regional objectives, provides funding to al-Qa'ida efforts outside of Somalia, and has a burgeoning relationship with the Huthis that could provide access to a new source of more sophisticated weapons, increasing the threat to U.S. interests in the region.
- In West Africa, al-Qa'ida is expanding its territorial control by gaining inroads with civilians through the provision of services and intimidation, and is threatening urban centers in Burkina Faso and Mali, where U.S. personnel are located.
- Al-Qa'ida's affiliate in Syria, Hurras al-Din, probably is exploiting the end of the Asad regime in Syria to strengthen its position. Despite its public announcement that the group was ordered dissolved by al-Qa'ida's senior leaders in Iran, Hurras al-Din members were advised not to disarm and instead to prepare for a future conflict, noting their continued fight against the Jews and their supporters.

Other Islamic terrorist groups—including some with historical ties to al-Qa'ida—continue to pose a threat to the United States primarily in the regions where they operate. Most of these groups generally have targeted local governments in recent years, while Lebanese Hizballah has continued to pursue limited targeting of primarily Israeli and Jewish individuals in and outside of the Middle East. The U.S. Government works with partners worldwide to prevent attacks against U.S. citizens, while watching for indications that these groups may shift intent and build capabilities to pursue transnational attacks.

- In South Asia, Tehrik-e-Taliban (TTP) operations in recent years have focused exclusively on targeting the Government of Pakistan, probably to avoid drawing more counterterrorism pressure. However, TTP's capabilities, historical ties to al-Qa'ida, and previous support to operations targeting the United States keep us concerned about the potential future threat. Anti-India groups, including Lashkar-e Tayyiba, similarly concern us in part because of their historical links with al-Qa'ida.

Other Transnational Criminals

Profit-motivated transnational criminals are using corruption, intimidation, and enabling technologies to expand their illegal activities into new markets and to diversify their sources of income, which increase their resiliency to U.S. and international law enforcement and financial regulatory efforts. TCOs are defrauding U.S. citizens, businesses, and government programs, while laundering billions of dollars of illicit proceeds through U.S. and international financial institutions. TCOs sometimes outsource money laundering operations and investments to individuals and networks with legal and banking expertise to circumvent financial regulations.

- TCOs and their financial facilitators use a myriad of methods to launder and repatriate illicit proceeds and to evade law enforcement and regulatory pressures. Some TCOs use digital currencies for money laundering and sanctions evasion activities because of its perceived anonymity and weaker international regulations compared to fiat currencies.

Financially motivated cyber criminals continue to prey on inadequately defended U.S. targets, such as healthcare systems and municipal governments, that could have broad impact on the U.S. populace and economy. Others have conducted attacks on critical infrastructure, disrupting utility company business networks or manipulating poorly secured control systems.

- Ransomware actors in mid-2024 attacked the largest payment processor for U.S. healthcare transactions, hampering prescriptions and causing extended delays in accessing electronic health records, patient communications, and medication ordering systems, and forcing some ambulances to divert patients to other hospitals.
- U.S. water infrastructure has become a more common target. In October 2024, criminal actors conducted cyber attacks against both large and small water utilities in the United States, possibly inspired by attacks against water infrastructure by Russian hacktivists and Iranian cyber actors in 2023 that had little effect but drew substantial publicity.

Foreign and U.S.-based human traffickers exploit vulnerable individuals and groups by promising well-paying jobs, confiscating identification documents, coercing victims to engage in risky behaviors and to work in inhumane conditions. TCOs that engage in human trafficking may also engage in other criminal activity threatening the United States, including fraud scams, drug trafficking, and weapons and human smuggling.

- Criminal actors, including Mexico-based TCOs, exploit migrants transiting the Western Hemisphere to the United States through kidnapping for ransom, forced labor, and sex trafficking operations. For example, some victims are forced to repay their smuggling fees through debt bondage once they arrive in the United States. These migrants are typically forced to become domestic servants, to work in the fishing, agriculture, and meat processing industries for low wages, or to work in illegal marijuana grow houses.

The total number of migrants trying to reach the United States has dropped significantly since January 2025 due to a surge in border security enforcement. While key drivers of migration in the Western Hemisphere, such as crime, poverty, and political repression, are likely to continue, heightened border security and mass deportation policies probably serve as a deterrent for migrants seeking to illegally cross U.S. borders.

- Law enforcement encounters with migrants at the U.S.-Mexico border were 14 percent lower in 2024 when compared to the previous year, and U.S. Border Patrol apprehensions along the Southwest border in January 2025 dropped 85 percent from the same period in 2024. Guatemalan, Mexican, and Venezuelan nationals were the most frequently encountered nationals at the U.S.-Mexico border.
- Real or perceived changes to immigration laws or travel policies in transit countries can trigger unexpected spikes. Since 2021, for instance, Nicaragua has removed visa requirements for air

travelers from third countries, triggering a surge in U.S.-bound migration from those countries through Nicaragua.

FOR SSCI USE

MAJOR STATE ACTORS

Several major state actors present proximate and enduring threats to the United States and its interests in the world, challenging U.S. military and economic strength, regionally and globally. China stands out as the actor most capable of threatening U.S. interests globally, though it is also more cautious than Russia, Iran, and North Korea about risking its economic and diplomatic image in the world by being too aggressive and disruptive. Growing cooperation among these actors expands the threat, increasing the risk that should hostilities with one occur, it may draw in others.

CHINA

Strategic Overview

President Xi Jinping and the People's Republic of China (PRC) want to achieve "the great rejuvenation of the Chinese nation" by 2049. The PRC will seek to increase its power and influence to shape world events to create an environment favorable to PRC interests, obtain greater U.S. deference to China's interests, and fend off challenges to its reputation, legitimacy, and capabilities at home and abroad.

- Beijing is deeply suspicious of U.S. intentions and views Washington's measures against China as part of a concerted, whole-of-government effort, working with U.S. allies and partners, to contain China's development and rise, undermine CCP rule, and prevent the PRC from achieving its aims. PRC leaders are most concerned about strong unified opposition from the United States and its allies, and are responding, in part, by strengthening ties with partners like Russia and North Korea.
- At the same time, China's leaders will seek opportunities to reduce tension with Washington when they believe it benefits Beijing, protects its core interests, and buys time to strengthen its position.

The PRC will likely continue posturing to be in a position of advantage in a potential conflict with the United States. The PRC will continue trying to press Taiwan on unification and will continue conducting wide-ranging cyber operations against U.S. targets for both espionage and strategic advantage. China will likely struggle to sufficiently constrain the activities of PRC companies and criminal elements that enable the supply and trafficking of fentanyl precursors and synthetic opioids to the United States, absent greater law enforcement actions.

- China's military operations to project power over Taiwan and its efforts to assert sovereignty claims in the South and East China Seas occur routinely with confrontations that increase concern of miscalculations potentially leading to conflict.
- China has demonstrated the ability to compromise U.S. infrastructure through formidable cyber capabilities that it could employ during a conflict with the United States.

Beijing will continue to strengthen its conventional military capabilities and strategic forces, intensify competition in space, and sustain its industrial- and technology-intensive economic strategy to compete with U.S. economic power and global leadership.

Military

China presents the most comprehensive and robust military threat to U.S. national security. The People's Liberation Army (PLA) is fielding a joint force that is capable of full-spectrum warfare, challenging intervention by the United States in a regional contingency, projecting power globally, and securing what Beijing claims is its sovereign territory. A major portion of China's military modernization efforts is focused on developing counter-intervention capabilities tailored against all aspects of U.S. and allied military operations in the Pacific. Beijing will focus on meeting key modernization milestones by 2027 and 2035, aimed at making the PLA a world-class military by 2049.

- Examples of PLA advances in 2024 include the PLA Navy's third carrier (CV-18 Fujian) beginning sea trials and likely being ready to enter operational service in 2025. The PLA Rocket Force probably is fielding the DF-27 ballistic missile, with a hypersonic glide vehicle payload option and an estimated range of between 5,000 and 8,000 kilometers. The PLA ground forces are also fielding its most advanced multiple rocket launcher, the PCH191, increasing its long-range, precision strike capability.
- The PLA has improved its force structure, readiness, and training. The PLA probably has made particular progress in critical areas, such as modernizing key ground forces, expanding its navy with more modern combatants, and fielding a wide variety of new missile systems; it has also improved its electronic warfare (EW) capabilities.

The PLA has the capability to conduct long-range precision-strikes with conventional weapons against the Homeland's periphery in the Western Pacific, including Guam, Hawaii, and Alaska. China has developed a range of ballistic and cruise missiles with conventional payloads that can be delivered from its mainland as well as by air and sea, including by nuclear-powered submarines. China may be exploring development of conventionally-armed intercontinental range missile systems, which, if developed and fielded, would allow China to threaten conventional strikes against targets in the continental United States.

The PLA will continue to pursue the establishment of overseas military installations and access agreements to project power and protect China's interests abroad. Beijing may also pursue a mixture of military logistics models, including preferred access to commercial infrastructure abroad, exclusive PLA logistics facilities with pre-positioned supplies co-located with commercial infrastructure, and bases with stationed forces, to meet its overseas military logistics needs.

China is using complex, whole-of-government campaigns featuring coercive military, economic, and influence operations short of war to assert its positions and strength against others, reserving more destructive tools for full-scale conflict. Beijing will likely expand these campaigns to advance unification with Taiwan, project power in East Asia, and reverse perceived U.S. hegemony.

- Beijing has pushed back against U.S. military operations, such as reconnaissance and bomber flights, freedom of navigation operations, and exercises around PRC borders and maritime

claims. The PLA regularly intercepts and shadows U.S. forces and sometimes conducts unsafe maneuvers in their vicinity.

Taiwan and Maritime Flashpoints

In 2025, Beijing will likely apply stronger coercive pressure against Taiwan and perceived increases in U.S. support to the island to further its goal of eventual unification. The PRC calls for a peaceful unification with Taiwan to resolve the Civil War that drove Taiwan's separation, even as it threatens to use force to compel unification if necessary and counter what it sees as a U.S. attempt to use Taiwan to undermine China's rise.

A conflict between China and Taiwan would disrupt U.S. access to trade and semiconductor technology critical to the global economy. Even without U.S. involvement in such a conflict, there would likely be significant and costly consequences to U.S. and global economic and security interests.

Beijing is working to isolate Taipei by pressuring states to downgrade diplomatic ties and support China's unification goal. Since 2016, Taiwan's official diplomatic relationships have dropped from 22 to only 12, and several of the remaining ones are vulnerable to Chinese pressure.

China is advancing military capabilities for a cross-Strait campaign while also using its armed forces to exert steady state pressure on Taiwan. The PLA probably is making steady but uneven progress on capabilities it would use in an attempt to seize Taiwan and deter—and if necessary, defeat—U.S. military intervention, and it is intensifying the scope, size, and pace of operations around Taiwan.

Beijing will continue to pressure Taipei with economic coercion and probably will increase it if it sees Taiwan taking steps toward formal independence. It could suspend preferential tariff terms, selectively ban Taiwan imports to China, and arbitrarily enforce regulations.

Beijing's aggressive efforts to assert sovereignty claims in the South and East China Seas are heightening tensions that could trigger a broader conflict.

- In 2024, PRC tactics in the South China Sea led to the loss of the Philippines' unilateral access to some disputed areas, and forced talks between Beijing and Manila in which the Philippines agreed to concessions in exchange for access. However, Manila is unlikely to relinquish its claims, creating potential for escalation by either side.
- Tension between China and Japan over the Senkaku Islands last flared up a decade ago. Since then, Chinese ships have remained in proximity of the disputed islands, occasionally entering the territorial zone, and driving responses from Japan's Self-Defense Force to monitor the activity.

Cyber

The PRC remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks. The PRC's campaign to preposition access on critical infrastructure for attacks during crisis or conflict, tracked publicly as Volt Typhoon, and its more recently identified compromise of U.S. telecommunications infrastructure, also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure.

- If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.

Economics

The PRC seeks to compete with the United States as the leading economic power in the world. To do so, the strategy calls for a centralized, state-directed, and nationally resourced approach to dominating global markets and strategic supply chains, limiting foreign competitors, and making other nations dependent on China. PRC leaders are applying the same strategy to bolster China's position and become more globally dominant in critical supply chains, both in upstream inputs it can provide more cheaply than others and in downstream production at wider scale.

- China's weak domestic demand, coupled with its industrial policies, such as manufacturing subsidies, have enabled a surge in cheap Chinese exports in sectors such as steel, harming U.S. competitors and fueling a record PRC trade surplus.
- China's dominance in key supply chains enables its use of economic coercion against countries that adopt policies Beijing opposes. Beijing is developing an institutionalized framework enabling more assertive and centrally controlled trade retaliation. PRC leaders are using ostensibly unofficial or technical trade and investment barriers, administrative regulations, logistics, and symbolic sanctions in a targeted way against individuals, firms, and sectors, in parallel with messages to warn and deter.
- PRC leaders appear to be preparing for more economic friction with the United States, and probably are weighing options with the new U.S. administration while looking for leverage and other ways to prevent a major escalation and decoupling.

China's dominance in the mining and processing of several critical materials is a particular threat, providing it with the ability to restrict quantities and affect global prices. Beijing has shown a willingness to restrict global access to its mineral resources—sometimes in response to geopolitical disputes—as with its banning of exports to the United States of metals used in semiconductor manufacturing, such as gallium, germanium, and antimony in December 2024 in response to U.S. export controls on advanced semiconductors and chip-making equipment. Other examples include when the PRC temporarily stopped rare earth element exports to Japan in 2010, and Beijing's creation of new laws codifying its authority to restrict mineral exports. A prolonged cessation in supplies controlled by China could disrupt critical inputs needed for U.S. industry and technological advancements.

China has similar aims in global shipping and resource access, including in the Arctic, where melting sea ice is creating opportunities for expanded maritime transport and energy exploitation, especially along the Northern Sea Route (NSR) off Russia's coast. China seeks access to the Arctic's potentially vast natural resources, including oil, gas, and minerals, even though China is not among the eight Arctic countries that control territory in the region. Beijing seeks to normalize more direct and efficient maritime shipping routes to Russia and other Northern Hemisphere areas, as a way to fuel its economic growth and energy security and reduce its dependence on Middle East energy. China has gradually increased engagement with Greenland mainly through mining projects, infrastructure development, and scientific research projects. Despite less active engagement right now, China's long-term goal is to expand access to Greenland's natural resources, as well as to use the same access as a key strategic foothold for advancing China's broader and economic aims in the Arctic.

Technology

China is using an aggressive, whole-of-government approach, combined with state direction of the private sector, to become a global S&T superpower, surpass the United States, promote self-reliance, and achieve further economic, political, and military gain. Beijing has prioritized technology sectors such as advanced power and energy, AI, biotechnology, quantum information science, and semiconductors, further challenging U.S. efforts to protect critical technologies by tailoring restrictions narrowly to address national security concerns. China is accelerating its S&T progress through a range of licit and illicit means, to include investments, intellectual property acquisition and theft, cyber operations, talent recruitment, international collaborations, and sanctions evasion.

- Some forecasts indicate China's technology sectors will account for as much as 23 percent of its gross domestic product by 2026, more than doubling since 2018. In addition to private funding, the PRC government is investing hundreds of billions of dollars in priority technologies, such as AI, microelectronics, and biotechnologies, in pursuit of its self-reliance goals.

China almost certainly has a multifaceted, national-level strategy designed to displace the United States as the world's most influential AI power by 2030. China is experiencing a boom in generative AI with the rapid emergence of a large number of PRC-developed models, and is broadly pursuing AI for smart cities, mass surveillance, healthcare, S&T innovation, and intelligent weapons. Chinese AI firms are already world leaders in voice and image recognition, video analytics, and mass surveillance technologies. The PLA probably plans to use large language models (LLMs) to generate information deception attacks, create fake news, imitate personas, and enable attack networks. China has also announced initiatives to bolster international support for its vision of AI governance.

- China has stolen hundreds of gigabytes of intellectual property from companies in Asia, Europe, and North America in an effort to leapfrog over technological hurdles, with as much as 80 percent of U.S. economic espionage cases as of 2021 involving PRC entities.

China also sees biotechnology as critical to becoming a dominant economic power and intends to grow its domestic bioeconomy to \$3.3 trillion by 2025. Beijing is investing heavily in collecting health and genetic data both at home and abroad in pursuit of these goals, and has shown it can be globally competitive in certain low-cost, high-volume commodities, such as biomanufacturing and genetic

sequencing. Beijing has identified genetic data as a national strategic resource, and is expanding state control over the country's gene banks and other genetic repositories, positioning it to potentially lead in precision medicine and agricultural biotechnology applications.

China has made progress in producing advanced 7-nanometer (nm) semiconductor chips for cryptocurrency mining and cellular devices using previously acquired deep ultraviolet (DUV) lithography equipment, but will face challenges achieving high-quality, high-volume production of these chips without access to extreme ultraviolet lithography tools. PRC researchers also continue to explore applying advanced patterning techniques to DUV machines to produce semiconductor chips as small as 3nm. China leads the world in legacy logic semiconductor (28nm and up) production, accounting for 39.3 percent of global capacity, and is expected to add more capacity than the rest of the world combined through 2028. These legacy chips are vital to producing automobiles, consumer electronics, home appliances, factory automation, broadband, and many military and medical systems.

WMD

China remains intent on modernizing, diversifying, and expanding its nuclear posture. China's robust nuclear weapons' and delivery systems' inventory poses a direct threat to the Homeland, capable of delivering catastrophic damage to the United States, and threatening U.S. military forces here and abroad.

China most likely possesses capabilities relevant to chemical and biological warfare (CBW) that pose a threat to U.S., allied, and partner forces as well as civilian populations.

Biosecurity

China's approach to and role in global biological, medical, and other health-related global priorities present unique challenges to the United States and the world. The COVID-19 pandemic that ultimately led to the death of more than one million Americans—and multiples more worldwide—began in China, which Beijing still refuses to acknowledge. China's strict censorship and repression of free speech prevented doctors treating the earliest of patients in Wuhan from warning the world of a far more serious contagion than Beijing wanted told, slowing the world's preparedness and response. To this day, Beijing refuses to fully cooperate with the rest of the international community trying to definitively pinpoint the precise cause of the disease so it can head off and prepare for any new disease.

Regarding COVID-19 origins, IC agencies have continued to evaluate new information from classified and open sources, revisit previous reporting, and consult with diverse technical experts to increase our understanding of the cause of the pandemic. These efforts have led CIA to assess that a research-related hypothesis is more likely than a natural origin hypothesis.

The other hypothesis for COVID-19—natural origin—includes many scenarios in which humans could have been infected with SARS-CoV-2—the virus that causes COVID-19—or a close progenitor through exposure to wild or domestic animals. China is home to a diverse body of naturally occurring coronaviruses found in a wide geographic area, and there is precedence for these viruses to emerge within human populations far from reservoir locations. For example, the coronavirus that is the closest known relative to SARS-CoV—the virus that causes severe acute

respiratory syndrome (SARS)—probably originated in Yunnan Province, according to scientific studies, even though the first SARS outbreak detected in humans in 2003 occurred in Guangdong Province, hundreds of miles away.

- The research-related incident hypothesis also considers a broad range of potential initial human-infection scenarios from events in research facilities, such as government or university laboratories, to research-related activities in the field, such as collecting samples from wild animals.

The PRC's dominance in pharmaceutical and medical supply production combined with lower quality safety and environmental standards than those of the United States positions Beijing to potentially restrict such exports for leverage over Washington and others in trade or security disputes. The PRC plays an increasingly important role in supplying pharmaceuticals and related medical supplies to the United States, as well as the rest of the world.

- U.S. imports of Chinese pharmaceuticals—defined as medicines, vaccines, blood, organic cultures, bandages, and organs—grew almost five-fold between 2020 and 2022 alone, from \$2.1 billion to \$10.3 billion.
- The PRC also might look to uniquely provide such supplies and medical aid to countries, more cheaply and at scales competitors cannot match, as a way to boost its global influence at the expense of the United States. The PRC's "vaccine diplomacy" during the COVID-19 pandemic—it provided vaccines to 83 countries—was driven at least in part by geopolitical considerations, such as currying favor for a new port in Burma.

Space

China has eclipsed Russia as a space leader and is poised to compete with the United States as the world's leader in space by deploying increasingly capable interconnected multi-sensor systems and working toward ambitious scientific and strategic goals. China has achieved global coverage in some of its intelligence, surveillance, and reconnaissance (ISR) constellations and world-class status in all but a few space technologies.

- China's Beidou constellation is a world-class position, navigation, and timing capability that competes with U.S. GPS and Europe's Galileo service. The PLA ISR architecture and satellite communications are areas the PLA continues to improve upon to close the perceived gap between itself and the U.S. military.
- China's successful lunar sample return mission in June 2024 contributes to Beijing's technological prowess and national prestige while supporting its effort to land astronauts on the Moon by 2030 and establish the first lunar base by 2035.
- China's commercial space sector is growing quickly with aspiration to be a major global competitor to U.S. and European space companies. For example, China launched the first set of satellites in its low Earth orbit (LEO) proliferated constellation last year for its own satellite Internet service to compete with Western commercial satellite Internet services.

Counterspace operations will be integral to PLA military campaigns, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites. China already has fielded ground-based counterspace capabilities, including EW systems, directed energy weapons (DEWs), and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites.

- China also has conducted orbital technology demonstrations, which, while not counterspace weapons tests, prove its ability to operate future space-based counterspace weapons. China has also conducted on-orbit satellite inspections of other satellites, which probably would be representative of the tactics required for some counterspace attacks.

Malign Influence Activities

Beijing will continue to expand its coercive and subversive malign influence activities to weaken the United States internally and globally, as well as counter what Beijing sees as a U.S.-led campaign to tarnish China's global relations and overthrow the CCP. Through these efforts, the PRC seeks to suppress critical views and critics of China within the United States and worldwide, and sow doubts in U.S. leadership and strength. Beijing is likely to feel emboldened to use malign influence more regularly in coming years, particularly as it fields AI to improve its capabilities and avoid detection.

- PRC actors have increased their capabilities to conduct covert influence operations and disseminate disinformation. For example, pro-China online actors in 2024 used AI-generated news anchors and fake social media accounts with AI-generated profile pictures to sow divisions on issues such as drug use, immigration, and abortion.

China's Challenges

China faces daunting challenges that will impair CCP leaders' strategic and political achievements. China's leaders probably are most concerned about corruption, demographic imbalances, and fiscal and economic struggles because they threaten the country's economic performance and quality of life, two key factors underpinning CCP legitimacy. Despite an acute economic slowdown, China's leaders probably will resist making needed structural reforms and instead maintain statist economic policies to steer capital toward priority sectors, reduce dependence on foreign technologies, and enable military modernization.

- China's growth probably will continue to slow because of low consumer and investor confidence. China's birth and marriage rates continue to decline, reinforcing negative population trends and a shrinking labor force.

Xi's focus on security and stability for the CCP and securing other leaders' personal loyalty to him is undermining China's ability to solve complex domestic problems and will impede Beijing's global leverage. Xi's blending of domestic and foreign security threats is undermining China's position and standing abroad, reducing Beijing's ability to shape global perceptions and compete with U.S. leadership.

RUSSIA

Strategic Overview

Russia views its ongoing war in Ukraine as a proxy conflict with the West, and its objective to restore Russian strength and security in its near-abroad against perceived U.S. and Western encroachment has increased the risks of unintended escalation between Russia and NATO. The resulting heightened and prolonged political-military tensions between Moscow and Washington, coupled with Russia's growing confidence in its battlefield superiority and defense industrial base, and increased risk of nuclear war, create both urgency and complications for U.S. efforts to bring the war to an acceptable close.

Regardless of how and when the war in Ukraine ends, Russia's current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to U.S. power, presence, and global interests. Despite having paid enormous military and economic costs in its war with Ukraine, Russia has proven adaptable and resilient, in part because of the expanded backing of China, Iran, and North Korea. President Vladimir Putin appears resolved and prepared to pay a very high price to prevail in what he sees as a defining time in Russia's strategic competition with the United States, world history, and his personal legacy. Most Russian people continue to passively accept the war, and the emergence of an alternative to Putin probably is less likely now than at any point in his quarter-century rule.

- Western efforts to isolate and sanction Russia have accelerated its investments in alternative partnerships and use of various tools of statecraft to offset U.S. power, with China's backing and reinforcement. Russia's relationship with China has helped Moscow circumvent sanctions and export controls to continue the war effort, maintain a strong market for energy products, and promote a global counterweight to the United States, even if at the cost of greater vulnerability to Chinese influence. Russia is also increasing military cooperation with Iran and North Korea, which will continue to help its war effort and enhance U.S. adversary cooperation and collective capacity. Finally, Moscow is increasingly willing to play spoiler in Western-centric forums such as the UN as well as use non-Western organizations like the Brazil, Russia, India, China, and South Africa (BRICS) group to press policies such as de-dollarization.
- Russia has shown it can navigate substantial economic challenges resulting from the ongoing drains of the war, Western cost imposition, and high inflation and interest rates, for at least the near term by using financial and import substitution workarounds, maintaining low debt, and continuing investments in the defense-industrial base. Russia's economy remains the fourth largest in the world (based on GDP at purchasing power parity).
- Russia's sizable ground force losses in the war have done little to undermine the strategic pillars of its military power, to include its diverse and robust nuclear deterrent and asymmetric capabilities, particularly in counterspace and undersea warfare. Russia's air and naval forces remain intact, with the former being more modern and capable than at the start of the invasion. Russia is developing a growing arsenal of conventional capabilities, such as theater strike weapons, to target the Homeland and deployed forces and assets abroad—and to hold

U.S. allies at risk—during crisis and wartime. Russia's advanced WMD and space programs threaten the Homeland, U.S. forces, and key warfighting advantages.

- Russia will continue to be able to deploy anti-U.S. diplomacy, coercive energy tactics, disinformation, espionage, influence operations, military intimidation, cyberattacks, and gray zone tools to try to compete below the level of armed conflict and fashion opportunities to advance Russian interests.
- The war in Ukraine has afforded Moscow a wealth of lessons regarding combat against Western weapons and intelligence in a large-scale war. This experience probably will challenge future U.S. defense planning, including against other adversaries with whom Moscow is sharing those lessons learned.

Russia and the Arctic

Russia controls about half of all Arctic coastline and views the region as essential to its economic well-being and national security. Moscow wants to further develop its Arctic oil and gas reserves and position itself to reap benefits from expected increases in maritime trade. Russia has concerns about increasing economic and military competition with Western countries in the region, which compounded last year when NATO enlarged to include the last two previously nonaligned Arctic states, Finland and Sweden.

- The war in Ukraine has sapped Russia's finances and available military resources to fulfill its Arctic ambitions, prompting Russia to seek a closer partnership with China in the Arctic, and welcoming other non-Western countries' increasing involvement, to offset NATO countries' perceived advantages.
- Russia's interest in Greenland is focused mainly on its proximity to strategically important naval routes between the Arctic and Atlantic Oceans—including for nuclear-armed submarines—and the fact that Greenland hosts a key U.S. military base.

Military

Moscow's massive investments in its defense sector will render the Russian military a continued threat to U.S. national security, despite Russia's significant personnel and equipment losses—primarily in the ground forces—during the war with Ukraine. Russia's air and naval forces, despite suffering some losses and expending substantial quantities of precision-guided munitions, remain capable of providing Moscow with regional and global power projection forces, while Russia's nuclear and counterspace forces continue to provide it with strategic deterrence capability.

- The Ukraine conflict has led to improvements in some Russian military capabilities. For example, Russia's initial use of EW and unmanned systems was lacking but it adapted and innovated using EW to more effectively interfere with Ukrainian use of radar and GPS and unmanned aerial vehicles (UAVs).

- Russia possesses long-range precision strike capability, most notably submarines and bombers equipped with LACMs and antiship cruise missiles, that can hold the Homeland at risk.
- Moscow has increased its defense budget to its heaviest burden level during Putin's more than two decades in power and taken measures to reduce the impact of sanctions on its military and defense industry.
- Russia has imported munitions such as UAVs from Iran and artillery shells from North Korea to mitigate to the impact of international sanctions, thereby sustaining its ability to wage war in Ukraine and enhancing the threat its military poses.

Moscow will contend with long-term challenges such as troop quality and corruption, and a fertility rate below what is needed for replacements, but its investments in personnel recruitment and procurement should allow it to steadily reconstitute reserves and expand ground forces in particular during the next decade. Nevertheless, the war in Ukraine will be a drag on those efforts as long as it persists. Moscow will have to continually balance resource allocation between large-scale production of equipment to sustain the war with modernization and recapitalization efforts.

Russia and Ukraine

Russia in the past year has seized the upper hand in its full-scale invasion of Ukraine and is on a path to accrue greater leverage to press Kyiv and its Western backers to negotiate an end to the war that grants Moscow concessions it seeks. Continuing the Russia-Ukraine war perpetuates strategic risks to the United States of unintended escalation to large-scale war, the potential use of nuclear weapons, heightened insecurity among NATO Allies, particularly in Central, Eastern, and Northern Europe, and a more emboldened China and North Korea.

Even though Russian President Putin will be unable to achieve the total victory he envisioned when initiating the large-scale invasion in February 2022, Russia retains momentum as a grinding war of attrition plays to Russia's military advantages. This grinding war of attrition will lead to a gradual but steady erosion of Kyiv's position on the battlefield, regardless of any U.S. or allied attempts to impose new and greater costs on Moscow.

- Despite recruitment challenges, Russia has regularly generated sufficient personnel to replenish losses and create new units to sustain attacks on multiple frontline axes. While Ukraine has increased its overall personnel intake since new legislation on mobilization was passed in spring 2024, Kyiv has stretched its resources trying to launch new offensives—such as in Kursk, Russia—and build more brigades while defending on all fronts.
- Moscow's rising defense spending and investments in defense-industrial capacity will continue to enable a high level of production of critical capabilities—such as artillery, long-range missiles, one-way attack UAVs, and glide bombs—and ensure Russia retains a firepower advantage over Ukraine.
- Both Putin and Ukrainian President Volodymyr Zelenskyy are interested in continuing discussions with the United States on how to end the war and have shown a willingness to test partial ceasefires. Nonetheless, Putin probably is attuned to the potential for protracted conflict to drag down the Russian economy and prompt undesired escalation with the West, and Zelenskyy probably understands that his position is weakening, the future of Western assistance is uncertain, and a ceasefire may ultimately become a necessary recourse. However, both leaders for now probably still see the risks of a longer war as less than those of an unsatisfying settlement. For Russia, positive battlefield trends allow for some strategic patience, and for Ukraine, conceding territory or neutrality to Russia without substantial security guarantees from the West could prompt domestic backlash and future insecurity.

Cyber

Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat. Moscow's unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on U.S. targets in time of conflict.

- Russia has demonstrated real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware.

Malign Influence Activities

Moscow uses influence activities to counter threats, including by stoking political discord in the West, sowing doubt in democratic processes and U.S. global leadership, degrading Western support for Ukraine, and amplifying preferred Russian narratives. Moscow's malign influence activities will continue for the foreseeable future and will almost certainly increase in sophistication and volume.

- Moscow probably believes information operations efforts to influence U.S. elections are advantageous, regardless of whether they affect election outcomes, because reinforcing doubt in the integrity of the U.S. electoral system achieves one of its core objectives.
- Russia uses a variety of entities such as the U.S.-sanctioned influence organizations Social Design Agency (SDA) and ANO Dialog and the state media outlet RT in its efforts to covertly shape public opinion in the United States, amplify and stoke domestic divisions, and discreetly engage Americans, while hiding Russia's hand.

WMD

Russia has the largest and most diverse nuclear weapons stockpile that, along with its deployed ground-, air-, and sea-based delivery systems, could inflict catastrophic damage to the Homeland. Russia has developed a more modernized, mobile, and survivable strategic nuclear force that is intended to circumvent or neutralize future augmented U.S. missile defense and ensure deterrence through reliable retaliatory strike potential. In addition, Russia's vast arsenal of non-strategic nuclear weapons helps it to offset Western conventional superiority and provide formidable escalation management options in theater war scenarios.

Russia continues efforts to modernize its nuclear weapons capabilities in the face of multiple failed tests of new systems.

Russia's CBW threat is expanding. Russian scientific institutes continue to research and develop CBW capabilities, including technologies to deliver CBW agents. Russia retains an undeclared chemical weapons program and has used chemical weapons at least twice during recent years in assassination attempts with Novichok nerve agents, also known as fourth-generation agents, against Russian opposition leader Aleksey Navalny in 2020, and against U.K. citizen Sergey Skripal and his

daughter Yuliya Skripal on U.K. soil in 2018. Russian forces almost certainly continue using chemicals against Ukrainian forces, with hundreds of reported attacks occurring since late 2022.

Space

Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities. It is expanding its arsenal of jamming systems, DEWs, on-orbit counterspace capabilities, and ASAT missiles designed to target U.S. and allied satellites.

- Russia is using EW to counter Western on-orbit assets and continues to develop ASAT missiles capable of destroying space targets in LEO.

Despite its Soviet legacy, the war in Ukraine has revealed glaring deficiencies in Russia's space-based architecture, which will continue to face difficulties from the effects of sanctions and export controls, domestic space-sector problems, and increasingly strained competition for program resources within Russia. However, Russia will remain a space competitor, probably by prioritizing assets critical to its national security and integrating military space services over civil space projects.

- Moscow uses its and others' civil and commercial remote-sensing satellites to supplement military-dedicated capabilities and has warned that other countries' commercial infrastructure in outer space used for military purposes can become a legitimate target.

Russian Antisatellite Capability

Russia is developing a new satellite meant to carry a nuclear weapon as an antisatellite capability. A nuclear detonation in outer space could cause devastating consequences for the United States, the global economy, and the world in general. It would harm all countries' national security and commercial satellites and infrastructure, as well as impair U.S. use of space as a driver for economic development.

- In February 2022, Russia launched a satellite, which its Ministry of Defense claimed at the time was for testing on-board instruments and systems under the influence of radiation and heavy charged particles.

Technology

While Russia's S&T ecosystem has been constrained in the wake of its invasion of Ukraine, Moscow continues to deploy nascent AI applications on and off the battlefield and has deepened technical cooperation with partners such as China in support of long-term R&D goals. Moscow's use of AI to augment military operations probably will further hone Russian tactics and capabilities in the event of future conflicts with the United States or NATO allies.

- Russia is using AI to create highly-capable deepfakes to spread misinformation, conduct malign influence operations, and stoke further fear. Russia has also demonstrated the use of AI-enabled antidrone equipment during its ongoing conflict with Ukraine.
- Russia's few domestic microelectronics manufacturers have only mastered production of chips down to the 65nm level and has goals of mass producing 28nm chips by 2030, significantly behind global leaders.
- While largely cut-off from Western supply chains, Russia has significantly expanded and deepened cooperation in several technical sectors with international partners. Russia seeks to further align its S&T efforts with China and BRICS allies in areas such as AI development and governance and semiconductor production to advance its own capabilities as well as broadly decrease Western influence.

Russia's Challenges

Even as Russia has proven resilient, it faces a myriad of challenges to remaining an indispensable global player, maintaining a sphere of influence, and upholding stability at home—its highest strategic aims—suggesting limits on its confidence dealing with the United States and the international community. Russia has paid a heavy price in blood, treasure, and loss of international reputation and foreign policy options because of its large-scale invasion of Ukraine. President Putin upended two decades of Russia's geopolitical resurgence, created new threats to its external and internal security, and strained its economic and military potential, making it more reliant on China and other like-minded partners like North Korea.

- Russia's military has suffered more casualties in Ukraine than in all of its other wars since World War II (750,000-plus dead and wounded), and its economy faces significant long-term macroeconomic headwinds and is increasingly dependent on China.
- Russia's aggression has strengthened European unity and prompted Finland and Sweden to join NATO. Efforts by Armenia, Moldova, and some Central Asian states to seek alternative partners highlight how the war has hurt Moscow's influence, even in the post-Soviet space, and derailed Putin's vision of a greater Eurasian union.

IRAN

Strategic Overview

Tehran will try to leverage its robust missile capability and expanded nuclear program, and its diplomatic outreach to regional states and U.S. rivals to bolster its regional influence and ensure regime survival.

However, regional and domestic challenges, most immediately tensions with Israel, are seriously testing Iran's ambitions and capabilities. A degraded Hizballah, the demise of the Asad regime in Syria, and Iran's own failure to deter Israel have led leaders in Tehran to raise fundamental questions regarding Iran's approach. Iran's consistently underperforming economy and societal grievances will also continue to test the regime domestically.

Tehran will continue its efforts to counter Israel and press the United States to leave the region by aiding and arming its loose consortium of like-minded terrorist and militant actors, known as the "Axis of Resistance." Although the demise of the Asad regime, a key ally of Tehran, is a blow to the Axis, these actors still represent a wide range of threats. These threats include some continued Israeli vulnerability to HAMAS and Hizballah; militia attacks against U.S. forces in Iraq and Syria; and the threat of Huthi missile and UAV attacks targeting Israel and maritime traffic transiting near Yemen. Supreme Leader Ali Khamenei continues to desire to avoid embroiling Iran in an expanded, direct conflict with the United States and its allies.

Iranian investment in its military has been a key plank of its efforts to confront diverse threats and try to deter and defend against an attack by the United States or Israel. Iran continues to bolster the lethality and precision of its domestically produced missile and UAV systems, and it has the largest stockpiles of these systems in the region. It considers them as critical to its deterrence strategy and power projection capability, and Iran uses their sales to deepen global military partnerships. Iran's growing expertise and willingness to conduct aggressive cyber operations also make it a major threat to the security of U.S. and allied and partner networks and data.

Iran also will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States. Iran seeks to target former and current U.S. officials it believes were involved in the killing of Islamic Revolutionary Guard Corps (IRGC)-Qods Force Commander Qasem Soleimani in January 2020 and previously has tried to conduct lethal operations in the United States.

Tehran intends for its expanding relationships with other key U.S. adversaries and the Global South to mitigate U.S. efforts to isolate the regime and blunt the impact of Western sanctions. Tehran's diplomatic efforts—including at times outreach to Europe—are likely to continue with varying degrees of success. In the past year, Iran has focused extensively on deepening ties with Russia—including through military cooperation for its war in Ukraine—and has relied on China as a key political and economic partner to help it mitigate economic and diplomatic pressure. Iran is also making progress developing closer diplomatic and defense ties to African states and other actors in the Global South and is trying to build on nascent improvements in its ties with other regional actors, such as Saudi Arabia, despite continued mutual suspicion over each other's ultimate visions for the region.

The economic, political, and societal seeds of popular discontent could threaten further domestic strife akin to the widescale and prolonged protests inside Iran during late 2022 and early 2023. The economy is beset by low growth, exchange rate volatility, and high inflation. Absent sanctions relief, these trends probably will continue for the foreseeable future.

Syria

The fall of President Bashar al-Asad's regime at the hands of opposition forces led by Hay'at Tahrir al-Sham (HTS)—a group formerly associated with al-Qa'ida—has created conditions for extended instability in Syria and could contribute to a resurgence of ISIS and other Islamist terror groups. Even if the HTS-led interim government can bridge divergent objectives, governing Syria will remain a daunting challenge amid the country's economic problems, humanitarian needs driven in part by millions of internally displaced Syrians, rampant insecurity, as well as ethnic, sectarian, and religious cleavages.

- The HTS-led interim government forces, along with elements of Hurras al-Din and other jihadist groups, engaged in violence and extrajudicial killings in northwestern Syria in early March 2025 primarily targeting religious minorities that resulted in the death of more than 1,000 people, including Alawi and Christian civilians.
- The leader of HTS claims to be willing to work with Syria's array of ethnosectarian groups to develop an inclusive governance model. Many of these groups remain skeptical of HTS's intentions, especially considering the leader's past al-Qa'ida association, suggesting protracted negotiations could devolve into violence. Israeli government officials are skeptical of HTS claims and intentions, expressing concern that historical HTS objectives against Israel persist.
- Some remaining jihadist groups refuse to merge into the HTS Ministry of Defense, and ISIS has already signaled opposition to HTS's call for democracy and is plotting attacks to undermine its governance.

Military

Iran's conventional and unconventional capabilities will pose a threat to U.S. forces and partners in the region for the foreseeable future, despite the degradation to its proxies and air defenses during the Gaza conflict. Iran's large conventional forces are capable of inflicting substantial damage to an attacker, executing regional strikes, and disrupting shipping, particularly energy supplies, through the Strait of Hormuz. Iran's unconventional warfare operations and militant partners and proxies, such as Hizballah, have traditionally enabled Tehran to pursue its interests throughout the region and maintain strategic depth with a modicum of deniability. However, Iranian officials are grappling with how to slow and eventually reverse their and their proxies' recent military losses from the Israeli campaign against Iran and its regional allies, including strikes on Iranian military targets such as air defense systems in April and October 2024. The IC assesses Iran's prospects for reconstituting force losses and posing a credible deterrent, particularly to Israeli actions, are dim in the near-term.

Iran has fielded a large quantity of ballistic and cruise missiles as well as UAVs that can strike throughout the region and continues efforts to improve their accuracy, lethality, and reliability.

Iran's defense industry has a robust development and manufacturing capacity, especially for low-cost weapons such as small UAVs. However, the limited damage Iran's strikes in April and October 2024 inflicted on Israel highlights the shortcomings of Iran's conventional military options.

Iran has also deployed small boats and submarines capable of disrupting shipping traffic through the Strait of Hormuz. Its ground and air forces, while among the largest in the region, suffer from outdated equipment and limited training.

FOR SSCI USE

Middle East Conflict

The Israel-HAMAS conflict sparked by the HAMAS October 7 attack against Israel derailed the unprecedented diplomacy and cooperation generated by the Abraham Accords and trajectory of growing stability in the Middle East. We expect the situation in Gaza, as well as Israel-Hizballah and Israel-Iran dynamics, to remain volatile.

Even in degraded form, HAMAS continues to pose a threat to Israeli security. The group retains thousands of fighters and much of its underground infrastructure, and it is probably using the ceasefire to reinforce and resupply its military and munitions stock so that it can fight again. HAMAS is capable of resuming a low-level guerilla resistance and to remain the dominant political action in Gaza for the foreseeable future. Low expectations on all sides that a ceasefire will endure and the absence of a credible post-fighting political and reconstruction plan, portend years of instability.

- While HAMAS's popularity has declined among Gazans, its popularity remains high among West Bank Palestinians, especially relative to the Palestinian Authority (PA).

The long-term Israeli-Palestinian relationship also hinges on the trajectory of an increasingly unstable West Bank. The PA's weak and declining ability to provide security and other services in the West Bank, Israeli operations in the West Bank, violence from Israeli settlers and Palestinian militant groups including HAMAS, and a potential leadership transition in the PA are likely to exacerbate governance challenges in Ramallah. Much also will depend on how Israel deals with post-conflict Gaza and its operations in the West Bank that may weaken or undermine the PA.

During the Gaza conflict, Iran encouraged and enabled its various proxies and partners to conduct strikes against Israeli and at times U.S. forces and interests in the region.

- The Huthis have emerged as the most aggressive actor, attacking commercial shipping in the Red Sea and Indian Ocean, U.S. and European forces, and Israel. In addition to receiving Iranian assistance, the Huthis have expanded their reach by broadening partnerships with other actors, such as Russia and Russian arms brokers, PRC commercial defense companies, al-Shabaab, and Iraqi Shia militants.
- Iraqi Shia militias continue to try to compel a U.S. withdrawal from Iraq through political pressure on the Iraqi government and attacks on U.S. forces in Iraq and Syria.

Further fighting between Hizballah and Israel would threaten Lebanon's fragile stability and any political progress begun by the election of a president in January after years of trying. A resumption of protracted Israeli operations in Lebanon could trigger a sharp rise in sectarian tension, undermine Lebanese security forces, and dramatically worsen humanitarian conditions. Although weakened, Hizballah maintains the capability to target U.S. persons and interests in the region, worldwide, and—to a lesser extent—in the United States.

Cyber

Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. networks and data. Guidance from Iranian leaders has incentivized cyber actors to become more aggressive in developing capabilities to conduct cyber attacks.

Malign Influence Activities

Iran often amplifies its influence operations with offensive cyber activities. During the Israel-HAMAS conflict, U.S. private industry tracked Iranian influence campaigns and cyber attacks.

- In June 2024, an IRGC actor compromised an email account associated with an individual with informal ties to then-former President Trump's campaign and used that account to send a targeted spear-phishing email to individuals inside the campaign itself. The IRGC subsequently tried to manipulate U.S. journalists into leaking information illicitly acquired from the campaign.

WMD

We continue to assess Iran is not building a nuclear weapon and that Khamenei has not reauthorized the nuclear weapons program he suspended in 2003, though pressure has probably built on him to do so. In the past year, there has been an erosion of a decades-long taboo on discussing nuclear weapons in public that has emboldened nuclear weapons advocates within Iran's decisionmaking apparatus. Khamenei remains the final decisionmaker over Iran's nuclear program, to include any decision to develop nuclear weapons.

Iran very likely aims to continue R&D of chemical and biological agents for offensive purposes. Iranian military scientists have researched chemicals that have a wide range of sedation, dissociation, and amnesic incapacitating effects, and can also be lethal.

Iran's Challenges

Iranian leaders recognize the country is at one of its most fragile points since the Iran-Iraq war, which probably weighs on their strategic calculus and confidence in their approach toward the region, the United States, and U.S. partners. They face growing political, social, economic, and regional pressures, leaving Iran increasingly vulnerable to regime-threatening instability and external interference.

NORTH KOREA

Strategic Overview

North Korean leader Kim Jong Un will continue to pursue strategic and conventional military capabilities that target the Homeland, threaten U.S. and allied armed forces and citizens, and enable Kim to undermine U.S. power and reshape the regional security environment in his favor. Kim's newly cemented strategic partnership with Russia is yielding financial benefit, diplomatic support, and defense cooperation. The partnership with Moscow also helps reduce Pyongyang's reliance on Beijing. North Korea's advancing strategic weapons capabilities and increasing access to revenue are enabling Kim's longstanding goals of securing international acceptance as a nuclear power, reducing U.S. military presence on the Korean Peninsula, expanding state control over the North's economy, and blocking foreign influence.

- In June 2024, Kim and Putin signed a comprehensive strategic agreement for sweeping economic and technology partnerships. Kim also is using the agreement's mutual defense clause, which commits each country to provide military assistance if either is invaded by a foreign power, to justify deploying combat troops to fight against Ukraine.
- Kim has no intention of negotiating away his strategic weapons programs, which he perceives as a guarantor of regime security and national pride, because they threaten the Homeland, U.S. forces in the region, and U.S. allies like South Korea and Japan. He is increasing North Korea's nuclear warhead stockpile and improving its ballistic missile technology; for example, North Korea conducted three launches in 2024 of what it claimed were IRBMs equipped with maneuverable, hypersonic payloads.
- Kim seeks to intimidate the United States and its allies into abandoning opposition to North Korea's nuclear weapons and its aggression toward South Korea. For example, he responds to U.S. military planning with South Korea and trilateral cooperation with South Korea and Japan by ordering missile launches and threatening nuclear retaliation.
- North Korea will continue to defy international sanctions and engage in illicit activities, including stealing cryptocurrency, sending labor overseas, and trading UN-proscribed goods to resource and fund Kim's priorities, including ballistic missiles and WMD.

Kim will act aggressively to counter activities he views as undermining the regime and threaten to use force when he perceives U.S. and allied actions as challenging North Korea's sovereignty, undermining his power, or aiming to curb his nuclear and missile ambitions. Pyongyang is expanding its capacity for coercive operations and using new tactics as it becomes more confident in its nuclear deterrent. Since coming to power, Kim generally has relied on non-lethal coercive activities, including missile demonstrations and cross-border balloon launches of refuse, to win concessions and counter U.S. and South Korean military, diplomatic, and civilian activities.

- North Korea uses threats to try to stop South Korean efforts to disseminate information in the North, which he views as destabilizing his control. Kim in the past has challenged South Korea's de facto maritime boundary claims and may do so again, raising the prospects of renewed clashes along the Northern Limit Line.

- Kim could escalate to more lethal asymmetric activities if he judged North Korea's efforts at deterrence were not working and he needed to send a stronger message. He also could resort to these lethal activities if he believed doing so would intimidate South Korea or the United States into changing its policies to be more favorable to the North while minimizing the risk of retaliation.

WMD

Kim remains committed to increasing the number of North Korea's nuclear warheads and improving its missile capabilities to threaten the Homeland and U.S. forces, citizens, and allies, and to weaken U.S. power in the Asia-Pacific region, as evidenced by the pace of the North's missile flight tests and the regime's public touting of its uranium enrichment capabilities. North Korea is probably prepared conduct a nuclear test and continues to flight test ICBMs so Kim can threaten the Homeland. Russia is increasingly supporting North Korea's nuclear status in exchange for Pyongyang's support to Moscow's war against Ukraine.

North Korea maintains its CBW capabilities and may use such weapons in a conflict or in an unconventional or clandestine attack against the United States or its allies.

Military

North Korea's military poses a lethal threat to U.S. forces and citizens in South Korea and the region by its ability to launch massive conventional strikes across the DMZ and continued investment in niche capabilities designed to deter outside intervention and offset enduring deficiencies in the country's conventional forces. The North's conventional military capabilities also provide Kim with options to advance his political objectives through coercion.

- The North Korean military would struggle to execute combined-arms maneuver warfare because its ground, air, and navy forces remain heavily reliant on Soviet-era equipment and lack adequate training, despite the investments to improve conventional capabilities.
- Kim will continue to prioritize efforts to build a more capable missile force—from cruise missiles to ICBMs and hypersonic glide vehicles—designed to evade U.S. and regional missile defenses, improve its precision strike capabilities, and put U.S. and allied forces at risk.

Pyongyang is positioned to gain technical expertise for its weapons developments in exchange for its munitions sales to Moscow, which could accelerate North Korea's testing and deployment efforts. Combat experience in the Russia-Ukraine war also could help Pyongyang strengthen its training and become more tactically proficient.

Cyber

North Korea is funding its military development—allowing it to pose greater risks to the United States—and economic initiatives by stealing hundreds of millions of dollars per year in cryptocurrency from the United States and other victims. Looking forward, the North may also expand its ongoing cyber

espionage to fill gaps in the regime's weapons programs, potentially targeting defense industrial base companies involved in aerospace, submarine, or hypersonic glide technologies.

North Korea's Challenges

North Korea will continue to struggle overcoming the damage Kim's need for absolute control and aggressive policies—and the isolation these create—does to the country's economic strength and viability. Kim has so far been able to advance his WMD and missile programs and continue to threaten his neighbors and the United States, but this has come at the expense of his people and the country's overall health. The regime's recentralization campaign is meant to ensure the long-term survival of Kim family rule, but its periodic crackdowns restrict economic activity, threaten livelihoods, and promote inefficient state controls, contributing to food shortages and eroding civil order because of the violent crime they increasingly encourage.

Kim will struggle to reduce North Korea's dependence on China—in particular, for access to international banking and imports of critical raw materials, consumer goods, food, and the regime's crude oil supply—and withstand the influence this gives Beijing.

ADVERSARIAL COOPERATION

Cooperation among China, Russia, Iran, and North Korea has been growing more rapidly in recent years, reinforcing threats from each of them individually while also posing new challenges to U.S. strength and power globally. These primarily bilateral relationships, largely in security and defense fields, have strengthened their individual and collective capabilities to threaten and harm the United States, as well as improved their resilience against U.S. and Western efforts to constrain or deter their activities. Russia's war in Ukraine has accelerated these ties, but the trend is likely to continue regardless of the war's outcome. *This alignment increases the chances of U.S. tensions or conflict with any one of these adversaries drawing in another. China is critical to this alignment and its global significance, given the PRC's particularly ambitious goals, and powerful capabilities and influence in the world.*

U.S. adversaries' cooperation has nevertheless been uneven and driven mostly by a shared interest in circumventing or undermining U.S. power, whether it be economic, diplomatic, or military. Concerns over escalation control and directly confronting the United States, as well as some divergent political interests, have tempered the pace and scope of these relationships. The leaders, though, are likely to continue to look for opportunities to collaborate, especially in areas in which there are mutual advantages and they lack other ways of achieving their aims toward or resisting the United States alone.

Russia has been a catalyst for the evolving ties, especially as it grows more reliant on other countries for its objectives and requirements including in but not limited to Ukraine. Moscow has strengthened its military cooperation with other states, especially Pyongyang and Tehran. Russia also has expanded

its trade and financial ties, particularly with China and Iran, to mitigate the impact of sanctions and export controls.

- The PRC is providing economic and security assistance to Russia's war in Ukraine through support to Moscow's defense industrial base, including by providing dual-use material and components for weapons. China's support has improved Russia's ability to overcome material losses in the war and launch strikes into Ukraine. Trade between China and Russia has been increasing since the start of the war in Ukraine, helping Moscow to withstand U.S. sanctions.
- Iran has become a key military supplier to Russia, especially of UAVs, and in exchange, Moscow has offered Tehran military and technical support to advance Iranian weapons, intelligence, and cyber capabilities.
- North Korea has sent munitions, missiles, and thousands of combat troops to Russia to support the latter's war against Ukraine, justified its deployment as fulfilling commitments made in the Treaty on Comprehensive Strategic Partnership that Pyongyang and Moscow announced in June 2024.

Cooperation between China and Russia has the greatest potential to pose enduring risks to U.S. interests. Their leaders probably believe they are more capable of countering perceived U.S. aggression together than alone, given a shared belief that the United States is seeking to constrain each adversary.

- For at least a decade, Beijing and Moscow have used high-profile, combined military activities primarily to signal the strength of the China–Russia defense ties. This relationship has deepened during the Russia-Ukraine war, with China providing Russia dual-use equipment and weapons components to sustain combat operations.
- Russia has increased its oil and liquefied natural gas (LNG) exports to China in an effort to maintain revenues in the face of sanctions by Western states.
- China is using its increased cooperation with Russia to attain a stronger presence in the Arctic and legitimize its influence there. One area of cooperation is China's production of icebreaker ships that enable safe passage through Arctic waters.
- The two countries probably will expand combined bomber patrols and naval operations in the Arctic theater to signal their cooperation and make it more concrete. In November, they also agreed to expand their cooperation on developing the NSR for its economic potential and as an alternative to Western dominated routes.

