

**OPEN HEARING:
2022 ANNUAL WORLDWIDE THREAT ASSESSMENT
OF THE U.S. INTELLIGENCE COMMUNITY**

HEARING
BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
OF THE
UNITED STATES SENATE
ONE HUNDRED SEVENTEENTH CONGRESS
SECOND SESSION

—————
MARCH 10, 2022
—————

Printed for the use of the Select Committee on Intelligence



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

—————
U.S. GOVERNMENT PUBLISHING OFFICE

SELECT COMMITTEE ON INTELLIGENCE

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

MARK R. WARNER, Virginia, *Chairman*

MARCO RUBIO, Florida, *Vice Chairman*

DIANNE FEINSTEIN, California	RICHARD BARR, North Carolina
RON WYDEN, Oregon	JAMES E. RISCH, Idaho
MARTIN HEINRICH, New Mexico	SUSAN COLLINS, Maine
ANGUS KING, Maine	ROY BLUNT, Missouri
MICHAEL F. BENNET, Colorado	TOM COTTON, Arkansas
BOB CASEY, Pennsylvania	JOHN CORNYN, Texas
KIRSTEN E. GILLIBRAND, New York	BEN SASSE, Nebraska

CHUCK SCHUMER, New York, *Ex Officio*

MITCH McCONNELL, Kentucky, *Ex Officio*

JACK REED, Rhode Island, *Ex Officio*

JAMES INHOFE, Oklahoma, *Ex Officio*

MICHAEL CASEY, *Staff Director*

BRIAN WALSH, *Minority Staff Director*

KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

MARCH 10, 2022

OPENING STATEMENTS

	Page
Warner, Hon. Mark R., a U.S. Senator from Virginia	1
Rubio, Hon. Marco, a U.S. Senator from Florida	4

WITNESSES

Haines, Avril, Director of National Intelligence, accompanied by: William J. Burns, Director, Central Intelligence Agency; Lieutenant General Scott D. Berrier, Director, Defense Intelligence Agency; General Paul Nakasone, Director, National Security Agency; and Christopher Wray, Director, Federal Bureau of Investigation	6
---	---

SUPPLEMENTAL MATERIAL

Report titled “Annual Threat Assessment of the U.S. Intelligence Community”	43
---	----

**OPEN HEARING: 2022 ANNUAL WORLDWIDE
THREAT ASSESSMENT OF THE U.S. INTEL-
LIGENCE COMMUNITY**

THURSDAY, MARCH 10, 2022

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, Hon. Mark R. Warner, Chairman of the Committee, presiding.

Present: Senators Warner, Rubio, Feinstein, Wyden, Heinrich, King, Bennet, Casey, Gillibrand, Burr, Risch, Collins, Blunt, Cotton, Cornyn, and Sasse.

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

Chairman WARNER. Good morning. I call this hearing to order. I want to welcome our witnesses: Director of National Intelligence, Avril Haines; the CIA Director, Bill Burns; the FBI Director, Chris Wray; Director of the National Security Agency and the Commander of U.S. Cyber Command, General Paul Nakasone; and DIA Director, Lieutenant General Scott Berrier.

Thank you all for being here today, and thank you also to the literally thousands of dedicated IC professionals who help do the good work that allows you to appear before this Committee.

The annual worldwide threats hearing is critically important. It is not only an opportunity for the intelligence agencies to inform our Members of the many threats and opportunities facing the United States, it's also really one of the only times when the combined leadership of the IC comes together to actually inform the American public

It's why last year, after there was no worldwide threats hearing in 2020, Congress codified this briefing requirement in law. This dialog and transparency is a fundamental pillar of democracy. It allows the American people to appreciate the IC's usually secret mission and also to hold our Nation's security agencies accountable.

In that light, I want to first express, though, my enormous, enormous gratitude for the accuracy with which the IC predicted Putin's plans to invade Ukraine. Those warnings made plain for all to see that the lies of the Kremlin, which was attempting to put together false flag operations to somehow legitimize Putin's actions, were totally false. And your forward-leaningness—and, candidly, I know for some of you, probably outside your traditional comfort

zone—I think was critically, critically important in throwing Putin off guard, but also showing to our allies, and not just our traditional allies but people across the world, the nefarious intent of Vladimir Putin.

Right now, Putin is waging an illegal and disastrous war in Ukraine. And as we saw yesterday, the bombing of the Children's and Maternal Hospital, with horrific humanitarian consequences. We all know that Putin had this aspiration to restore Russia's greatness, but what he got is that now Russia is even further viewed as a pariah state and his invasion has been virtually unanimously condemned. Truth is, right now, NATO is more unified than ever.

Russia's economy suffers under crippling sanctions from a global coalition, not only Five Eyes or NATO, but the E.U., Japan, Sweden, Finland. And as we've all indicated a number of times, it's a pretty remarkable action when even Switzerland gets out of its traditional neutral position.

Truth is, businesses are fleeing Russia. We've seen international energy companies and others, the pictures in the last couple of days of McDonald's. And I still remember the very first McDonald's going into Moscow. What an event that was. But the fact is that, at least on a short-term basis, McDonald's is closing down all its stores.

All the while, the people of Ukraine demonstrate a bravery and a commitment to defend their country against the madness of Putin's attempt at authoritarian subjugation. We've also been, I think, all inspired by President Zelensky's courage and his willingness to stand up against Putin's efforts. I also want to take a moment, and I've shared this with my colleagues, you know, democracy is sometimes messy.

The way we sometimes go about passing our laws is messy. In the last few years in our country, whether it was grappling with the January 6th intervention, whether it was COVID, whether it was the ability of social media to pit us against each other on a tribal basis, I think it sometimes made us question whether traditional liberal democracy and its values can be successful against an authoritarian regime.

And I believe with all my heart that the people of Ukraine are literally voting with their lives, embracing the values that we take for granted every day. And maybe we all want to take a deep breath at some point and recognize, with all our flaws, our system is still the best in the world, and people are willing to die to try to touch some of the freedoms that we take on a daily basis.

And as we focus on this enormous crisis and as Russia axed up in the relative stability of the post-World War II order in Europe, I don't think we can take our eyes off one of the other great challenges our country and the world face, and that is the strategic competitor that the Chinese Communist Party of President Xi presents. And I think it is always important—I know I say this always—to make the point that our beef, particularly when it comes to China, is not with the Chinese people or the Chinese diaspora, but is with the Communist Party, because the failure to do so simply plays into Xi's efforts that are broadcasted on all of the Chinese social media platforms that somehow this is an anti-Asian, anti-

China effort. We see this not only here; I had a conversation with our Australian counterpart just recently on this same topic. And the truth is, China is unlike any adversary that we've faced, I believe, since the Second World War. It's demonstrated not only its ability to try to compete with us on a military basis, but compete with us on an economic basis. Russia, the Soviet Union, was a military threat an ideological threat but was never truly an economic threat.

And one area that is of enormous concern to me is China's competition with us in the technology realm. I got my start in telecom about 40 years ago, and I could never have imagined all the innovations that have come about from technology. Social media, satellites, high performance computing, semiconductors—the list goes on and on. Technology has become so incredibly integral to our lives and our national security. I truly believe that whoever wins the technology race in the 21st century will lead to economic and other levels of dominance.

I think that ability to compete against China—and it will require, frankly, not only the United States, but it will require great working with our allies around the world—is critically important in a clear intelligence and national security threat. One of the things I think that the Administration has done quite well is in terms of rallying forces against Russia. We see China on a daily basis continue to compete in those domains. Truth is, China is relying on strategic investments, cyber, and traditional espionage. I think the FBI Director has indicated close to \$500 billion a year of intellectual property theft. The truth is, China is not trying to have a dual-win circumstance. They intend to win and dominate in technology domain after technology domain.

Unlike the United States, I believe China will use that power to spread its authoritarian ideas, whether through economic coercion like the Belt and Road Initiative, or in an area that, again, we've talked with many of you about, in terms of China infiltrating those critically-important, technology-setting bodies that sometimes have been not viewed with appropriate focus.

And that's, again, why I want to thank the ODNI, the CIA, and all of you for refocusing your agencies on this critical competition in the technology domain. A rising China and a ruthless Russia, both headed by authoritarian regimes seeking to undermine the cause of democratic governments worldwide again, are a stark reminder that what we take for granted here in this country, freedom of the press, freedom to vote, democracy—as messy as it is—that order is not guaranteed. It requires conviction, leadership, and sometimes sacrifice, again, as we see that sacrifice play out on a daily basis with the people of Ukraine.

Now, while I focus today on China and Russia, I know there are a multitude of other threats that I haven't addressed from rogue states like Iran and North Korea, the persistent threat of terrorism, the ongoing global pandemic and future emerging global health threats, and the obviously continued and pressing threat of global warming, which looms closer and closer. We see the floods playing out right now in Australia. Suffice it to say, I can't think of a time when the worldwide threats were more voluminously complex. I can't think of a better group of people, though, to come

forward to present the Intelligence Community's view on these issues. I look forward to the day's very important discussion, and I appreciate you being here.

I'll turn now to my friend, the Vice Chairman.

**OPENING STATEMENT OF HON. MARCO RUBIO,
A U.S. SENATOR FROM FLORIDA**

Vice Chairman RUBIO. Thank you, Mr. Chairman. Thank you all for being here.

This is, I imagine, probably the most important and most watched worldwide threats hearing in my time in the U.S. Senate. I was raised in the final decade of a long Cold War, in which the struggle between the two global superpowers and two ideologies really threatened to end life on the Earth. I came into adulthood and I witnessed the collapse of an evil empire, a vision and an image unimaginable to anyone just a few short years before it happened. And it seemed at that time that the world had reached the end of history, that liberal democracy had won and was destined to spread to every corner of the globe, and the connections of a globalized economy would, from here on out, prevent war between great powers forever.

The truth is that, in every era, leaders, nations, and civilizations have struggled with the same feature of our fallen nature, and that is the desire of the powerful to conquer, to enslave, to rule over those that are weaker than themselves. Western civilization in general—our Nation, the United States of America, in particular—embraced moral principles that stigmatized this part of our nature. And we created rules and institutions both at home and around the world to control it. But it's now clear that the last 30 years were but a brief respite from the rhythms of human history because, while much has changed about humanity and our species, there is one thing that will never change: human nature.

Putin's invasion of Ukraine has especially horrified the Western world because we had grown accustomed to war and brutality being what happens in other regions, troubled regions, far away, or the stuff of grainy black and white videos. But now the victims are people who are familiar to us. They're people who just a month ago had jobs. They had lives. They had trips planned. They had weddings on the books. They lived much like we do on this very day. And then overnight, they have no home to return to, no job to resume. And we see the images of wives and children boarding busses and trains and unsure that they will ever see their husband or father alive again.

This man's barbarism is a shocking opening chapter in the return of history, and now we must prepare ourselves for this new era, for frankly, greater dangers lie ahead. Vladimir Putin's claim is both meritless but familiar: that his is a powerful country and therefore he has the right to make vassals of his neighbors. But it is not his claim alone. In the Middle East, Iran considers its Ayatollah to be the leader of the entire Muslim world, Shia and Sunni alike, and it seeks an arc of power extending to Lebanon to Syria to Iraq and eventually to Bahrain. It seeks the weapons to gain them immunity from the world doing anything about it.

And in the Far East, we find the most audacious and consequential claim of all: an assertive China which believes that all roads must one day lead to Beijing, and that their smaller neighbors must accept their place in the world as tributary states. Standing in the way of this axis of totalitarianism is an imperfect yet very powerful living rejection of their claims. The United States of America—we face no shortages of challenges here at home. We're divided over issues that range from the consequential to, frankly, the trivial, but we cannot avoid the fork in the road before us now. We will either awaken from complacency, build our national strength, and confront this century's version of authoritarianism, or it will one day come for us and the world will enter a new Dark Age.

In this new conflict, the agencies each of you have been entrusted to lead will play a role more pivotal than ever. Conflict now between competing powers and worldviews is no longer just a domain of soldiers and sailors. In this new era, our adversaries engage us daily on the battlefield of information and cyberspace and technology and in the heavens.

They infiltrate our schools to steal our research and our laboratories to steal our science. They enter our computers to take our data and our companies to take our industries. And they embed themselves in our social media to divide us against one another and to confuse us and in our critical infrastructure to one day hold us hostage.

There is not a single American soldier on the ground in Ukraine; not a single American airman patrols the skies. We may not be at war with Russia, but we are most certainly in conflict with Putin. When Putin was denying any intention of invading Ukraine, it was your work—the work of our Intelligence Community—that prepared a skeptical world to get ready and immunized it from the virus of disinformation. When it came time to inflict damage on his economy, it was our intelligence that identified the ones that would have the greatest impact.

And all of us, as the Chairman has pointed out, have been inspired by the bravery of President Zelensky. But every American deserves and needs to know that neither his people nor the world would have been able to witness this bravery on a daily, real-time basis had it not been for the hard work of the men and women of our Intelligence Community, often days and weeks before the storm.

And so today, even as we hear about the conflict before us now, I hope we will hear about how our intelligence agencies are evolving to meet the new challenges of a new era and specifically how twenty-first century intelligence was applied to the crisis in Ukraine.

Today, we discuss the various threats confronting our Nation. But in all of this, let's not lose sight of the central threat before us now, because the spirit of totalitarianism has never left us. But it now possesses and lives inside great powers. And it's not looking for an off-ramp, it's not looking for a face-saving exit, it's not looking for its security interest to be respected or their rightful place in the world to be recognized. It is looking to fulfill the darkest impulse of our fallen nature: to conquer, to dominate, and to enslave.

This is no time to forget the lessons of history, for this is a monster you cannot make a deal with. This is a monster that has to be defeated.

Thank you.

Chairman WARNER. Thank you, Senator Rubio. And before I go to the Director, I just want to remind Members that we will have a classified briefing after this. So I would ask everyone to please respect that in terms of the form of your questions.

And unlike the traditional way we approach this, order of arrival at the gavel, today we're going to go on a strict seniority basis down the dais, and I am going to ask Members to respect the five-minute rule.

With that, Director Haines the floor is yours.

STATEMENT OF AVRIL HAINES, DIRECTOR OF NATIONAL INTELLIGENCE, ACCOMPANIED BY: WILLIAM J. BURNS, DIRECTOR, CENTRAL INTELLIGENCE AGENCY; LIEUTENANT GENERAL SCOTT D. BERRIER, DIRECTOR, DEFENSE INTELLIGENCE AGENCY; GENERAL PAUL NAKASONE, DIRECTOR, NATIONAL SECURITY AGENCY; AND CHRISTOPHER WRAY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Director HAINES. Thank you very much, Chairman Warner, Vice Chairman Rubio, for your kind words. And Members of the Committee, thank you for the opportunity to speak with you today and provide testimony alongside my wonderful colleagues and on behalf of the Intelligence Community on the IC's 2022 Annual Assessment of Worldwide Threats to U.S. national security.

Before I start, I just want to take a moment to express to you how much I've appreciated your thoughtful support and partnership this last year and to publicly thank the men and women of the Intelligence Community for their extraordinary work to keep us safe. I know how privileged I am to be part of this community, truly, of talented people and to be given a chance to do something useful in service to my country, and I thank you for the opportunity.

Broadly speaking, this year's assessment focuses on adversaries and competitors, critical transnational threats, and conflicts and instability. And these categories often overlap, and one of the key challenges of this era is assessing how various threats and trends are likely to intersect so as to identify where their interactions may result in fundamentally greater risk to our interests than one might otherwise expect or where they introduce new opportunities.

The 2022 Annual Threat Assessment highlights some of these connections as it provides the IC's baseline of the most pressing threats to U.S. national interests. I'll try to do so today as I provide a summary of our work. The assessment starts with threats from key state actors, beginning with the People's Republic of China, which remains an unparalleled priority for the Intelligence Community, and then turns to Russia, Iran, and North Korea.

All four governments have demonstrated the capability and intent to promote their interests in ways that cut against U.S. and allied interests. The PRC is coming ever closer to being a pure competitor in areas of relevance to national security, is pushing to revise global norms and institutions to its advantage, and is chal-

lenging the United States in multiple arenas, but particularly economically, militarily, and technologically. China is especially effective at bringing together a coordinated whole-of-government approach to demonstrate its strength and to compel neighbors to acquiesce in its preferences, including its territorial and maritime claims and assertions of sovereignty over Taiwan.

President Xi Jinping is determined to force unification with Taiwan on Beijing's terms, and China would prefer coerced unification that avoids armed conflict. And it has been stepping up diplomatic, economic, and military pressure on the island for years to isolate it and weaken confidence in its leaders. At the same time, Beijing is preparing to use military force if it decides that that is necessary. PRC is also engaged in the largest ever nuclear force expansion and arsenal diversification in its history, and is working to match or exceed U.S. capabilities in space, presenting the broadest, most active and persistent cyber espionage threat to U.S. government and private sector networks.

Russia, of course, also remains a critical priority and is a significant focus right now. In light of President Putin's recent and tragic invasion of Ukraine, which has produced a shock to the geopolitical order with implications for the future that we are only beginning to understand and are sure to be consequential.

And the IC, as you know, provided warning of President Putin's plans, but this is a case where I think all of us wish we had been wrong. Nevertheless, the invasion has proceeded consistent with the plan we assessed the Russian military would follow, only they are facing significantly more resistance from heroic Ukrainians than they expected and encountering serious military shortcomings.

Russia's failure to rapidly seize Kyiv and overwhelm Ukrainian forces has deprived Moscow of the quick military victory that it probably had originally expected would prevent the United States and NATO from being able to provide meaningful military aid to Ukraine. Moreover, we assess Moscow underestimated the strength of Ukraine's resistance and the degree of internal military challenges we are observing in the Russian military, which include an ill-constructed plan, morale issues, and considerable logistical challenges.

What is unclear at this stage is whether Russia will continue to pursue a maximalist plan to capture all or most of Ukraine, which we assess would require more resources even as the Russian military has begun to loosen its rules of engagement to achieve their military objectives. If they pursue the maximalist approach, we judge it will be especially challenging for the Russians to hold and control Ukrainian territory and install a sustainable pro-Russian regime to Kyiv in the face of what we assess is likely to be a persistent and significant insurgency. And of course, the human toll of the conflict is already considerable and only increasing.

Thus far, the Russian and Ukrainian militaries have probably suffered thousands of casualties along with numerous civilian deaths, and of course, well more than a million people have fled Ukraine since Russia invaded. Moreover, Russian forces are at the very least operating with reckless disregard for the safety of civilians as Russian units launch artillery and airstrikes into urban

areas as they have done in cities across Ukraine, including the Chairman's mention of the hospital and near critical infrastructure such as the Enerhodar nuclear plant. The IC is engaged across the interagency to document and hold Russia and Russian actors accountable for their actions.

The reaction to the invasion from countries around the world has been extraordinarily severe. Western unity in imposing far-reaching sanctions, and export controls as well as foreign commercial decisions are having cascading effects on the Russian economy. The economic crisis that Russia is experiencing is also exacerbating the domestic political opposition to Putin's decision to invade.

NATO's unified response, the significant resistance that the Ukrainians have demonstrated on the battlefield, Europe's rapid response to Russia's invasion—not just in terms of economic measures but also actions long thought to be off the table, such as the provision of lethal aid to Ukraine and shutting down EU airspace to Russian planes—all almost certainly surprised Moscow. In particular, while Putin probably anticipated many of the current sanctions to be imposed when he weighed the cost of the invasion, we judge that he did not anticipate either the degree to which the United States and its allies and partners would take steps to undermine his capacity to mitigate western sanctions or the pull-back from Russia initiated by the private sector.

Nevertheless, our analysts assessed that Russia, that Putin, is unlikely to be deterred by such setbacks and instead may escalate the conflict, essentially doubling down to achieve Ukrainian disarmament and neutrality to prevent it from further integrating with the United States and NATO. We assess Putin feels aggrieved the West does not give him proper deference and perceives this as a war he cannot afford to lose. But what he might be willing to accept as a victory may change over time, given the significant costs he is incurring. Putin's nuclear saber-rattling is very much in line with this assessment. Putin's public announcement that he ordered Russia's strategic nuclear forces to go on special alert in response to aggressive statements from NATO leaders was extremely unusual. We have not seen a public announcement from the Russians regarding a heightened nuclear alert status since the 1960s; But we have also not observed force-wide nuclear posture changes that go beyond what we have seen in prior moments of heightened tensions during the last few decades. Our analysts assess that Putin's current posturing in this arena is probably intended to deter the West from providing additional support to Ukraine as he weighs an escalation of the conflict. And Putin probably still remains confident that Russia can militarily defeat Ukraine and wants to prevent Western support from tipping the balance and forcing a conflict with NATO.

Regardless, our number one intelligence priority is defense of the homeland, and we will remain vigilant in monitoring every aspect of Russia's strategic nuclear forces. With tensions this high, there is always an enhanced potential for miscalculation, unintended escalation, and we hope that our intelligence can help to mitigate those concerns.

Beyond its invasion of Ukraine, Moscow presents a serious cyber threat, a key space competitor, and one of the most serious foreign

influence threats to the United States. Using its intelligence services, proxies, and wide-ranging influence tools, the Russian government seeks to not only pursue its own interests, but also to divide Western alliances, undermine U.S. global standing, amplify discord inside the United States, and influence U.S. voters and decision making.

And to finish with our state actors, Iran continues to threaten U.S. interests. It tries to erode U.S. influence in the Middle East, entrench its influence and project power in neighboring states, minimize threats to regime stability.

Meanwhile, Kim Jong-un continues to steadily expand and enhance Pyongyang's nuclear conventional capabilities, targeting the United States and its allies, periodically using aggressive and potentially destabilizing actions to reshape the regional security environment in his favor, and to reinforce his status as a de facto nuclear power.

The assessment focuses next on a number of key global and transnational threats, including global health security, transnational organized crime, the rapid development of destabilizing technologies, climate migration, terrorism. I raise these because they pose challenges of a fundamentally different nature to our national security than those posed by the actions of nation-states, even powerful ones like China. We look at the Russia-Ukraine war and can imagine outcomes to resolve the crisis and the steps needed to get there, even though unpalatable and difficult. And similarly, we view the array of challenges China actions pose and can discuss what is required, how to think about tradeoffs involved. And transnational issues are more complex, requiring significant and sustained multilateral effort, and that we can discuss ways of managing them. All of them pose a set of choices that will be more difficult to untangle and perhaps require more sacrifice to bring about meaningful change.

This reflects not just the interconnected nature of the problems, but also the significant impact increasingly-empowered non-state actors have on the outcomes and the reality that some of the countries who are key to mitigating threats posed by nation-states are also the ones we will be asking to do more in the transnational space. For example, the lingering effects of the COVID-19 pandemic is putting a strain on governments and societies, fueling humanitarian and economic crises, political unrest, and geopolitical competition as countries such as China and Russia seek to exploit the crisis to their own advantage.

And no country has been completely spared. Even when a vaccine is widely distributed globally, the economic and political aftershocks will be felt for years. Low income countries with high debts face particularly challenging recoveries, and the potential for cascading crises that lead to regional instability whereas others turn inward or will be distracted by other challenges. These shifts will spur migration around the world, including on our southern border. The economic impact has set many poor and middle income countries back years in terms of economic development, and is encouraging some in Latin America, Africa, and Asia to look to China and Russia for quick economic and security assistance to manage their new reality.

We see the same complex mix of interlocking challenges stemming from climate change, which is exacerbating risk to U.S. national security interests across the board, but particularly as it intersects with environmental degradation and global health challenges.

And terrorism of course remains a persistent threat to U.S. persons and interests at home and abroad, but the implications of the problem are evolving. In Africa, for example, where terrorist groups are clearly gaining strength, the growing overlap between terrorism, criminal activity, smuggling networks has undermined stability, contributed to coups and an erosion of democracy, and resulted in countries turning to Russian entities to help manage these problems.

And global transnational criminal organizations continue to pose a direct threat to the United States through the production and trafficking of lethal illicit drugs, massive theft including cyber-crime, human trafficking, and financial crimes and money laundering schemes. In particular, the threat from illicit drugs is at historic levels, with more than 100,000 American drug overdose deaths for the first time annually, driven mainly by a robust supply of synthetic opioids from Mexican transnational criminal organizations.

In short, the interconnected global security environment is marked by the growing specter of great power competition and conflict, while transnational threats to all nations and actors compete for our attention and also our finite resources.

And finally, the assessment turns to conflicts and instability, highlighting a series of regional challenges of importance to the United States: iterative violence between Israel and Iran. Conflicts in other areas, including Africa, Asia, and the Middle East, have the potential to escalate or spread, fueling humanitarian crises and threatening U.S. persons. Africa, for example, has seen six irregular transfers of power since 2020 and probably will see new bouts of conflict in the coming year as the region becomes increasingly strained by a volatile mixture of democratic backsliding, inter-communal violence, and the continued threat of cross-border terrorism.

Of course, we are also focused on our workforce and their families. The IC continues to contribute to the government-wide effort to better understand potential causal mechanisms of anomalous health incidents and remains committed to ensuring afflicted individuals receive the quality care they need. The safety and well-being of our workforce is our highest priority, and we are grateful to Members of your Committee for your continued support on these efforts.

In closing, I just want to note how much effort has gone into improving our capability to share intelligence and analysis with our partners and allies across the Intelligence Community. As we have seen in our approach to the threat to Ukraine, as you've noted, the sharing of intelligence and analysis has paid real dividends in helping facilitate collective action against the renewed threat of nation-state aggression. And while such efforts must be done with care to ensure we are able to protect our sources and methods, we are laying the groundwork to broaden our work where doing so creates

the conditions for a more united focus on other emerging challenges. We appreciate your support in these efforts.

Thank you. I look forward to your questions.

Chairman WARNER. Thank you, Director Haines, and thank you on behalf of the other members of the panel on deferring to only have you do the opening statement.

My first question is on the cyber domain and I want to ask Director Haines and General Nakasone. And I want to just again compliment the Members of this Committee. When we saw the Russians launch the SolarWinds attack, it was this Committee that first focused on that issue. And in a broadly bipartisan way, we recognized that only about 30 percent of our cyber-attacks are actually being reported to the government. I'm proud to say that in the budget bill that hopefully we'll take up the next day or two—it's already passed the House—we finally have put in place a cyber-notification process, something that I would recognize that Senator Collins has been working on literally for years and years and years. We are this close to the finish line. Since only about 30 percent of our cyber incidents are reported, we need to make sure that information gets to the FBI, gets to CISA, gets to our private-sector partners in a real-time way.

One of the things I've been surprised at is that the Russian cyber capabilities, while we've not seen a very efficient military so far, I don't think any of us think that Russia does not have extraordinarily critical and first-rate cyber tools. The fact that they have not launched much beyond traditional malware—they've not launched the kind of worm-driven NotPetya attacks that we saw in 2017—my concern has been that that type of attack could literally go beyond the geographic boundaries of Ukraine, bleed into Poland where it could affect American troops or shut down Polish hospitals, and result in the death of Polish citizens, which could potentially move us into Article 5 territory.

General Nakasone, I'd like to start with you. You're the best expert on this topic. Have you been a bit surprised that they haven't launched their full array of attacks? And how concerned are you, as Russia gets more and more stymied on the military front, that they may unleash some of their additional cyber tools?

General NAKASONE. Chairman, thank you very much for the question. I begin by saying that we remain vigilant. We're 15 days into this conflict. By no means are we sitting back and taking this casually. We are watching every single day for any type of unusual activity. And I would just build on the scenario that you talked about. This idea of malware spreading is one scenario that we look at. But there are three other scenarios that also come into our thinking.

One might be the use of ransomware, broad use of ransomware that our adversaries might use.

The next would be scenario proxies, those that necessarily may not be part of the Russian government but are functioning as a proxy or as a non-nation-state actor due to this type of activity to perhaps launch malware.

And the final one is this idea of a disruptive or destructive attack on a country in Eastern Europe that could take place.

As I said, we're 15 days into this. We've seen three to four attacks. The reasons in terms of why there haven't been more, I think—obviously, this is part of Russia's own strategic calculus. But secondly, a tremendous amount of work was done prior to the actual invasion, work that was done by my agency, work that was done by Cyber Command, by the interagency, by a series of private sector partners that harden the infrastructure of Ukraine. I think that that was part of it. And the final thing is there have been actions since then that I think that have contributed to the Russians in terms of the way that they approach the future.

I would just conclude by saying not only are we vigilant, we're prepared, and most importantly, we're sharing information and sharing our expertise with our partners.

Chairman WARNER. Let me get to my second question. I want to honor my own commitment to try to keep within five minutes. One of the things that my friend, Senator Burr, often mentioned is we don't have a technology committee in the Senate. In many ways, the Intelligence Committee has become the technology committee.

I think a lot of the competition going forward, particularly vis-à-vis China, will be around technology. I think we were all surprised at their enormous success in the 5G domain. Again, many of us are working on making sure we make the kind of investments that China is making on semiconductors. Candidly, shutting off semiconductors to Russia will be as effective as any tool in shutting down their military industrial complex.

Director Burns, you have made this a priority. How do we make sure that across the IC, we both monitor and incent policymakers and the balance of the government to make the necessary investments in technology?

Director BURNS. Well, thanks, Mr. Chairman.

Nothing is going to matter more to the future of CIA and, I think, the U.S. Intelligence Community more broadly than our ability to compete technologically. It's the main arena, as you said before, Mr. Chairman, for competition with China.

So just in the last couple of months, we've established a new mission center at the CIA alongside a new mission center on China, and equally important, a mission center focused on technology issues to make sure that we're anticipating, keeping pace, getting out ahead of the pace of innovation to deepen partnerships with the private sector, because that's absolutely essential, I think, to our future as we look at competition and technology.

We've just created the position of Chief Technology Officer for the first time at CIA. So all of that, I think, reflects the enormously high priority that we will continue to attest to that set of issues.

Chairman WARNER. Thank you. Senator Rubio.

Vice Chairman RUBIO. Thank you all for being here.

I'll direct this to you, Director Haines. But anybody who wants to answer it can do so. I think we've learned from all this, the best way to combat disinformation is through transparency. So I want to walk through some component pieces of a particular topic involving labs and Ukraine and then allow you or anyone to expand who could provide greater insight.

As you're all well aware, Russia has been laying out this argument for a number of months now about how there are these labs

in Ukraine that are developing chemical and biological weapons, that the U.S. is involved, that they've discovered it. And they've been making that argument for a period of time. And it's the argument they usually make before they use that kind of stuff themselves against someone.

So let me just start with a question on the component pieces, and then allow you to expand more on the important parts of it. There is a difference between a biological research facility and a biological weapons research facility, correct?

Director HAINES. Correct.

Vice Chairman RUBIO. Okay. Does Ukraine have any biological weapons research facilities?

Director HAINES. No, but let me be clear, we do not assess that Ukraine is pursuing either biological weapons or nuclear weapons, which has been some of the propaganda that Russia is putting out.

Vice Chairman RUBIO. Okay. So they do have the biological research facilities. What is our government's role in their biological research programs?

Director HAINES. So as I understand it, Ukraine operates about a little over a dozen essentially bio labs. And what they are involved in is Ukraine's biodefense and their public health response. And that's essentially what they're intended to do. And I think that the U.S. government provides assistance, or at least has in the past provided assistance, really in the context of biosafety, which is something that we've done globally with a variety of different countries.

So I would defer, obviously, the details of that assistance to the agencies involved.

Vice Chairman RUBIO. Well, I guess that's the important component. How do we define biosafety or biodefense? Is it the ability to have antidotes or responses if someone were to use an agent against you if you were having an outbreak? What exactly is that?

Director HAINES. I will quickly get out of my area of expertise. But I'll give you a generic answer that I understand.

So it is essentially for biodefense. You can think about things like medical countermeasures, for example, things that will help you to address a pandemic that is an outbreak in your country, things along those lines; things that prevent spreading of pandemics and other health issues, things along those lines. And the kinds of biosafety pieces that you would be providing assistance for are things like making sure that, as you're producing medical countermeasures, that you're taking appropriate precautions, that you're letting the medical community internationally know, notifying when appropriate.

So that's the kind of assistance. But again, I just want to be absolutely clear that we do not believe that Ukraine is pursuing biological or nuclear weapons, that we've seen no evidence of that. And frankly, this influence campaign is completely consistent with longstanding Russian efforts to accuse the United States of sponsoring bio-weapons work in the former Soviet Union.

So this is a classic move by the Russians.

Vice Chairman RUBIO. So, I think the one thing that's piqued a lot of people's interest, and I hope we can address, is that Assistant Secretary Nuland said a couple of days ago, in response to my

question in another hearing—this is a quote: “The U.S. government is concerned about preventing any of these research materials from falling into the hands of Russian forces should they approach.”

So people will hear that and say, well, that means that there must be something in these labs that’s very dangerous. They possess pathogens or something that must be very dangerous. Look, we’re all coming off the trauma of COVID–19, the possibility that there might have been an accident or a leak out of a lab there that we still don’t know the answer to. And so it’s in that context that people read that statement or hear it and say, okay, it sounds to me like they have labs, these labs are working on dangerous things, and if the Russian were worried that it’s going to get out of the laboratory, how should people assess that statement? Why are we so concerned? And again, I know I’m asking you some questions regarding medicine and biology and research and so forth. But it’s really important for this effort to understand what exactly is in these labs that we’re so worried about them getting their hands on.

Director HAINES. Medical facilities that I’ve certainly been in, done research in high school type of thing, in college—all have equipment for pathogens or other things that you have to have restrictions around, because you want to make sure that they’re being treated and handled appropriately.

And I think that’s the kind of thing that probably Victoria Nuland was describing and thinking about in the context of that. We have to be concerned in the same way that we have to be concerned about in the Enerhodar nuclear power plant or other facilities that, when they’re seized and if they’re seized, that there may be damage done or theft. And they may in fact misuse some of the material that’s there that’s not intended for weapons purposes but, nevertheless, can be used in dangerous ways or that can create challenges for the local populations.

Vice Chairman RUBIO. All right. Thanks.

Chairman WARNER. Senator Rubio, thank you for raising this. I think we’ve seen some of these reports, that this may be another area where Russia is trying to offer a false flag signal, and really appreciate your line of questioning.

I want to turn to Senator Feinstein. But I do want to acknowledge that Dianne has served the longest on this Committee. And we appreciate very much the challenges, the personal challenges you’ve been going through, and your attendance here always.

I remember one time you literally had come, I think, from a medical procedure. You were still here showing up at one of these hearings, and we’re grateful for your leadership. And I call on you now for five minutes.

Senator FEINSTEIN. Well, thank you very much, Mr. Chairman.

In an unclassified annual threat assessment you state that, quote, “Individuals and small cells inspired by a variety of ideologies and personal motivation include Sunni violent extremism, racially or ethnically motivated violent extremism, and militia violent extremism probably represent the greatest terrorist threat to the United States.”

Now, while we have no interest in giving Al-Qaeda or ISIS an opportunity to recover, you’re making the clear point that individ-

uals and small cells represent the greatest threat to the United States.

So here's the question. How are you allocating your resources for counterterrorism? It appears that most of the funding for counterterrorism goes into efforts focused against specific groups instead of attempting to locate individuals.

How do you justify that allocation compared against the assessed threat?

Director HAINES. I'm happy to start, but I suspect Director Wray and others may have some thoughts on this.

I think from at least the Intelligence Community perspective, it's true that we focus in on groups that are critical to our national security, groups such as al-Shabab and ISIS and Al-Qaeda Khor in these contexts, as examples. But it is also true that we are looking at, consistently across the board, how it is that the ideologies that they propagate and that others propagate that are of concern and reflected in our assessment are creating violent extremism in a variety of places including in small groups and even for individuals.

And our system is set up in such a way as to identify not simply the networking that we see with respect to such groups, but also to essentially create the opportunity for us to try to provide as much warning as we can with respect to individuals and others that—

Senator FEINSTEIN. Could the military respond as well?

Director HAINES. Absolutely. Yes. And it's challenging obviously when you have somebody that's disconnected from a system. Yes.

Director WRAY. I would just add that from the FBI's end, of course, the types of terrorist threats that you referenced, Senator, are at the top of our priority list. And through our Joint Terrorism Task Forces in every Field Office, we're prioritizing those. And the reason why the Jihadist-inspired homegrown violent extremists, and then the domestic violent extremists, are such a high priority is because unlike the more classic, post-9/11 sleeper cells where you have a large group of people plotting, planning, preparing, fundraising, training, there are a lot of dots to connect in a plot like that. With the kind of terrorist threat we're talking about here, you're talking about an individual going after an easily-accessible target with a very crude weapon, which means there's a lot fewer dots to connect. And so the key is getting the eyes and ears out in the community.

And that's why the growth in the Joint Terrorism Task Forces with task force officers from state and local police departments all over the country has been such an important development.

Senator FEINSTEIN. Anyone, please. I'd like other comments.

Director BURNS. All I would add, Senator, is even at CIA, even as we focus more and more attention and resources on major power adversaries like China and Russia for all the obvious reasons, we remain sharply focused on the counterterrorism challenge, as well. I think it's notable that in the same month—last month in February—when all of us had to deal with renewed Russian aggression in Ukraine, we played a central role along with our partners in the U.S. military in finding the former Emir of ISIS, Hajji Abdullah, locating him, and then cooperating with our military partners in a

successful operation against him. So we'll remain very sharply focused.

Senator FEINSTEIN. So if I understand what you're saying, you're changing the allocation of resources to individuals from groups. Is that correct or not?

Director BURNS. No. What I was suggesting, Senator, is that even as we focus more attention and resources on major power adversaries like China and Russia at CIA, where we're focused on external terrorist threats, we remain sharply focused on the threats posed to the homeland by everyone from ISIS—and I mentioned the successful operation against the former ISIS Emir—as well as Al-Qaeda and its affiliates like al-Shabab, like Al-Qaeda in the Arabian Peninsula

That was my only point.

Senator FEINSTEIN. Thank you. I will hear from the military, please.

General BERRIER. Senator, DIA's Defense Counterterrorism Center, DCTC, is focused on foreign terrorist threats. They continue to operate as they have for the last 20 years, focused on organizations' foreign transnational terrorist threats. Thank you.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator.

Senator Burr.

Senator BURR. Thank you, Mr. Chairman.

I want to take this opportunity to highlight what's already been pointed out: the success of our intelligence and the analysis of that intelligence product. Your thousands of employees deserve the thanks of this Committee, of this Congress, and of the American people. Likewise, President Zelensky and the Ukrainian people have reminded us that democracy does not come without a cost.

It has to be protected. This democracy, the independence of Ukraine, demands that democracies around the world respond with everything needed to preserve Ukraine's independence and democracies that are threatened. Likewise, leaders like Putin don't want their people to have the freedoms that we cherish and that we strive to protect.

This would not be possible without the men and women who work for you on behalf of not just this country, but democracies around the world. We are eternally grateful for all the work that they do, but more importantly, the response that they've had to this current challenge.

Mr. Chairman, I have no questions in open session.

Chairman WARNER. Thank you, Senator Burr, for once again acknowledging the great work of this community. I appreciate it.

Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman. I share Senator Burr's view. And let me thank you particularly, Director, for your professionalism and dedication. We've talked on a number of subjects and I have appreciated it.

Now let me turn to cybersecurity. In a recent unclassified briefing from my office, government cybersecurity experts reconfirmed that a technology known as SS7, which allows phones to roam from one network to another, could also allow foreign actors to get into

our networks and intercept American's calls and texts. These experts also identified Russia as one of the top threats for this kind of surveillance.

Now, fortunately, there's a way to prevent this that doesn't get in the way of communications between our country and Russia. U.S. carriers could simply block roaming requests from Russian phone networks. The only inconvenience would be that anyone with the U.S. phone in Russia would need to buy a local phone card.

Director Haines, my question would be: would this policy make it harder for the Russian government to spy on Americans?

Director HAINES. Thank you so much, Senator Wyden. And I think it's an excellent question, obviously. I asked my folks what they thought about this. And basically, I think we want to explore it, if you're willing to give us a little bit of time. I gather it really would require a little bit of research to understand what the consequences would be of doing that exact kind of blocking.

So I'd like to be able to come back to you. I think it's a really worthy question and appreciate the interest.

Senator WYDEN. Good.

And you inherited this problem because I've been asking you about it for some time. But you're new on the beat and you've been responsive and I appreciate it.

Director Burns, the public knows far less about intelligence activities conducted under Executive Order 12333 than under the FISA law. So I want to express my appreciation to you and to the Director for being more forthcoming and transparent about this subject than your predecessors.

Here's my question. The CIA released a portion of a report from the Privacy Board that raised the concern that when CIA analysts searched their records for information on Americans. There was no requirement to justify it. No requirement, for example, to write down the justification for a search.

My question—and we've been talking with your folks—is: will you commit this morning to requiring CIA analysts to write down their requests for conducting searches on Americans so those searches can be reviewed?

Director BURNS. The short answer, Senator, is yes. I can assure you that CIA will comply with our Attorney General guidelines on documentation requirements for conducting queries. In fact, I met last Friday with the new Chair of the Privacy and Civil Liberties Oversight Board to talk about this issue. And I stressed my personal commitment to working with her and the rest of the Board very effectively in the years ahead.

Senator WYDEN. So when could we expect that this reform would actually be implemented?

Director BURNS. Well, as I said, you have my commitment that we'll review our current procedures and ensure that all our systems are compliant, and I'd be glad to report back to you in six months on that.

Senator WYDEN. Okay, let's see if we can speed it up, because we've been waiting a long time for this one as well. We'll talk further about it. You've been responsive as well.

Let me go to you, Director Wray, if I might. You testified on Tuesday that the FBI bought a license for the NSO hacking tools to evaluate them and determine what security concerns they raise.

Did the FBI inform anybody else in the government about what it learned from that evaluation?

Director WRAY. I think I'd have to defer to closed session about anything on the—. I think what you're getting at is the so-called VEP, the vulnerabilities process that's interagency. And while we participate in that, whether or not it applied here is a different question. But we could maybe talk a little bit more about that in closed session.

Senator WYDEN. I'm glad to do that. Here's what I'm interested in. I'm just asking whether the government believes that the FBI's operational use of these tools would be legal and whether that's still on the table. The public deserves to know that. Even if the FBI decided against using NSO's hacking tools, the Department of Justice Inspector General has confirmed that the FBI does use hacking in investigations.

I do think the public deserves some information on this. Let's continue the discussion.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Wyden.

And I just want to again acknowledge if Congress had just followed Senator Collins ten or eleven years ago, we might be further along on the cyber issue.

Senator COLLINS.

Senator COLLINS. Thank you.

Director HAINES, following up on the Chairman's leadership here. Before I begin my questioning, I just want to personally thank you for working with the Chairman and me and other Members of this Committee on the Cyber Security Bill. We very much valued and appreciated your support, which was critical.

Director BURNS, you have always shown extraordinary insight into Putin's thinking. We all read about the Russian Defense Ministry publicly accusing Ukraine of possibly planning a false-flag chemical weapon attack. What do you make of that? Does that signal that Putin intends to launch a chemical or biological weapon attack on the Ukrainians?

Director BURNS. Well, thanks very much, Senator. I think it underscores the concern that all of us need to focus on those kind of issues, whether it's the potential for a use of chemical weapons, either as a false flag operation or against Ukrainians. This is something, as all of you know very well, is very much a part of Russia's playbook.

They've used those weapons against their own citizens. They've at least encouraged the use in Syria and elsewhere. So it's something we take very seriously. And it's one of the reasons, as Director Haines said earlier, that I am convinced that our efforts at selective declassification to preempt those kinds of false-flag efforts and the creation of false narratives have been so important. In all the years I spent as a career diplomat, I saw too many instances in which we lost information wars with the Russians.

In this case, I think we have had a great deal of effect in disrupting their tactics and their calculations, and demonstrating to

the entire world that this is a premeditated and unprovoked aggression built on a body of lies and false narratives. So this is one information war that I think Putin is losing.

Senator COLLINS. General Berrier, I feel very strongly that the Ukrainians should be able to defend their own airspace. But obviously, they need planes, they need manned drones. What is the current status of the battle for control of the Ukrainian airspace? And what is your assessment of what additional aircraft or manned drones would mean for Ukraine?

General BERRIER. Senator, thank you for that question.

My assessment is that the Ukrainians have been somewhat effective with the assets and resources that they have. The Russians have not achieved what I would call air dominance or air superiority over the country of Ukraine right now. That said, they are taking some losses and they do need additional assets.

Weapons like Stingers have moved in and they have been used with effect. I think the Ukrainians will continue to be able to use those in small unit tactics with great effect. Certainly, additional assets and resources with UAVs and aircraft, I'm sure they could make very good use of that.

Senator COLLINS. Thank you.

Director Berrier, I want to switch to a different issue. I believe that we have a very strong moral obligation to welcome those Afghans who have risked their lives, their families' lives, their livelihoods, to help our troops, our diplomats, and our intelligence professionals. Nevertheless, fulfilling that obligation does not require compromising a thorough, comprehensive vetting process for those Afghans who managed to get on to airplanes before the last U.S. aircraft left the runway. Unfortunately, a report from the Department of Defense IG found that Afghan evacuees have not been screened appropriately, using all available DoD databases. And as a result, at least 50 individuals with security concerns already are in the United States, and most of those cannot be located right now.

Do you know whether the NGIC, the National Ground Intelligence Center, has completed a biometric analysis as part of this vetting process?

General BERRIER. Senator, I don't know the answer to that question right now, but I will take it for the record and get back to you.

Senator COLLINS. Thank you.

Chairman WARNER. Thank you, Senator Collins. You know, we mentioned the fact that this Committee has really taken on a major focus on technology. And I want to acknowledge the fact that on some of the very sophisticated areas of technology, Senator Heinrich may be the only one that actually brings real expertise to those issues. So I appreciate that.

Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

Director Burns, I actually want to reiterate my colleague's statement of thanks to you for working with us on increasing some of the transparency around CIA's activities under 12333. I think this is all about ensuring we just understand how Americans' privacy and civil liberties are protected under those authorities, and I know that's something you care about as well.

I want to ask about the current situation in Chernobyl and how concerned we should be about that. I know there's been a lot of reporting that Ukraine's grid operator was concerned about the reserve diesel generators potentially running out of fuel once that was disconnected from the larger power grid.

How concerned should we be, and what do we know about the situation there that can be discussed in this setting?

Director HAINES. I'm happy to start. From my perspective, my understanding of it is that we should be concerned but that we haven't yet seen anything that brings us from concern to it's a complete crisis. And I think if you want further details, what I should do is come back to you in writing on it and give you our best sense of it. But I don't know if others have anything to add.

Senator HEINRICH. I look forward to that.

Director, you talked a little bit about Russia's strategic nuclear posture. And I want to pivot from that for just a moment and ask about tactical—some people have even referred to them as small nuclear weapons, almost as if they're something we don't need to be overly concerned about.

But folks who work with nuclear weapons today know that even tactical nuclear warheads have yields many times larger than what we used at the end of World War II. How concerned should we be about Russia's potential use of a tactical nuclear weapon in Ukraine? What would that look like? And what can we do to prevent that from happening, especially given how Putin seems to be in a posture where he needs some sort of a reset and has proven himself to be very unpredictable?

Director HAINES. I think, probably, we can have a further conversation about this in the closed session. But, as a general matter, as I indicated, we're obviously very concerned. We want to make sure that we're monitoring everything that may be going on with respect to Russia's strategic nuclear forces. But as I indicated, we have not yet seen posture changes that are beyond what we've seen previously during moments of tension such as in relation to Crimea or in 2016 vis-à-vis Syria, and so on. They have made certain posture changes and they're consistent with what we are seeing now. It's nothing unprecedented in a sense.

Senator HEINRICH. The international community's sanctions and economic work with respect to Russia have resulted in quite impressive outcomes. Obviously, Putin is trying to find workarounds for these sanctions, to include relying on energy sales, on the country's reserves and gold, and Chinese currency as well as cryptocurrency. I've read that while there are mitigating actions the Russian government can take to try to get around the worst of the sanctions, they can't really recreate their financial system.

Director Wray, do you agree with that assessment? And also, what avenues do we have to combat Russia's misuse of cryptocurrency to evade the current sanctions regime?

Director WRAY. I think Director Haines may want to weigh in a little bit on this as well, but I think the top line takeaway is that the Russians' ability to circumvent the sanctions with cryptocurrency is probably highly overestimated on the part of maybe them and others. We are, as a community and with our

partners overseas, far more effective on that than I think sometimes they appreciate.

And there's a lot of expertise in terms of tools and strategies to help block that kind of effort. Ultimately, what they really need to do is get access to some form of fiat currency, which becomes more challenging. I don't know, Director Haines, if you want to—

Senator HEINRICH. And you are utilizing those tools?

Director WRAY. Absolutely. We have built up significant expertise both at the FBI and with some of our partners. And there have been some very significant seizures and other efforts that I think have exposed the vulnerability of cryptocurrency as a way to get around sanctions.

Director HAINES. The only thing I'd add to what Director Wray said is just with respect to the first part of your question, which is the enormous economic impact that's been had as a consequence of the sanctions. In that part of what we've seen is, as I indicated in my opening statement, we expected President Putin anticipated to some extent what the sanctions would be and how we would approach this given our past practice in these areas. He built up a reserve fund that was really intended to help him defend his currency in the context of sanctions. But through the actions of our Treasury Department and others in Europe and the West, what they've done is actually make it very hard for him to access that money in order to defend his currency. And we've seen it in freefall. I believe it's lost about 40 percent of its value. It is extraordinary to watch the stock markets—the fact that they've had to close down so much of their economy, industry. Also the private sector impact has been extraordinary and I think really exacerbates the challenge for them in a pretty extraordinary way.

Director BURNS. The only thing I would add very briefly, Senator, is that I think among the many profoundly-flawed assumptions that President Putin made in launching this invasion was his assumption that he had built a sanctions-proof economy. That by building, as Director Haines said, a very large war chest of foreign currency reserves and gold reserves, and by not anticipating there'd be sanctions against the Russian Central Bank, by not anticipating that the German leadership would show such resolve, in particular, I think he deeply underestimated the economic consequences. And I think they're just now being felt in Russia and that's going to intensify.

Chairman WARNER. Senator Heinrich, I think some of your crypto issues are really important. I've got some questions on that in the closed session.

Senator Blunt this is going to be your last Worldwide Threat Assessment briefing and we really thank you for your service on this Committee.

Senator BLUNT. Well, there are things I'll miss about the Senate next year, but one of them will probably not be the worldwide threat discussions that we have publicly and every week on this fine Committee, Chairman, and thanks for your leadership.

I just want to say that I'm working on NGS issues, and we'll address some of that in the classified briefing.

Chairman WARNER. Thank you, Senator Blunt.

Senator BLUNT. Thank you.

Let's follow up, Director Burns, on your other idea about the economy. Do you think Putin overestimated what the Chinese might be able to do to offset the sanctions and other economic activities? Or, do you think the Chinese will step in in a way that he might have anticipated?

Director BURNS. Thanks very much for the question, Senator.

I think he may be overestimating the extent to which the Chinese leadership will be able or willing to help him deal with quite severe economic consequences of his invasion of Ukraine. It remains to be seen how this will play out. But, you know, I recall after the sanctions that were levied against Russia after his prior aggression in Crimea, the Chinese drove a very hard bargain over pipelines that the Russians were trying to negotiate.

So they weren't particularly flexible or sympathetic, in a way, during that period as well. So I suspect there's not going to be any easy out for President Putin as he looks at trying to deal with those economic consequences—not from the Chinese, not from anyone else.

Senator BLUNT. Do we have any sense of how the Chinese have reacted to recent locking arms with the Russians right before all of these events happened?

Director BURNS. I think, Senator, that the Chinese leadership, first, has invested a lot in partnership with Russia, and I don't expect that to change anytime soon. I do, however, believe that the Chinese leadership, President Xi in particular, is unsettled by what he's seen, partly, because his own intelligence doesn't appear to have told him what was going to happen.

Second, because of the reputational damage that China suffers by association with the ugliness of Russia's aggression in Ukraine.

Third, by the economic consequences at a time when growth rates in China, as you look over the rest of this year, are lower than they've been in 30 years.

And fourth, I think because President Xi is probably a little bit unsettled as he watches the way in which President Putin has driven Americans and Europeans more closely together and strengthened the transatlantic alliance in ways that would have been a little bit hard to imagine before the invasion began.

I think the Chinese leadership looks at Europe, not just as a market, but as a kind of player with whom they can have an independent relationship and try to look for ways in which they can drive wedges between us and our European allies. And what President Putin has so successfully done is to make that much less likely.

Senator BLUNT. I didn't intend to dwell in this public session on China as much as I'm going to wind up doing in my five minutes, but you know the Chinese have also announced their plans, their intention, their capability devoted to biotech. Underlying those activities, I think, is something, Director Wray, we should be really focused on: how much that may impact Americans as Chinese try to get more information about Americans in various ways, as they develop their own biotech potential to impact populations.

I'll let you start, and then, Director Haines, I'll come to you.

Director WRAY. So certainly, the Chinese have shown that they are willing to pursue our personal data at a scale unlike anything

anywhere else in the world. They have stolen more of our personal and corporate data than every other nation combined. And one of the other lessons we saw from the COVID period is their aggressive targeting of COVID research, whether it was vaccines or other forms of medical treatment. And you could almost clock any company's announcement that they were making progress on something. Almost within days, you could then see Chinese targeting or trying to steal that research.

Senator BLUNT. Right. We certainly know they've done that with personal data, financial data. I'm wondering about their biotech focus, Director Haines. Do we need to be now concerned about genetic data in ways that we might not have been at an earlier time?

Director HAINES. Yes, we do have concerns with bio data across the board and I think not just genetic data, as you point out. But that's a critical aspect of it. The collection of that by China, in particular, but by other countries as well, and how that can be used in the future, particularly as the technology develops. So, absolutely.

Senator BLUNT. I've noticed some of the reporting here and the studies here. You could take a biotechnology look at populations here or Africa or other places, and decide to do things that specifically have impact on just a segment of the population that has the genetic code that may be susceptible to that, where their surrounding neighbors and others in the country don't have. I think it's an area we'll be talking more about, and I look forward to discussing that further.

Thank you, Chairman.

Chairman WARNER. Thank you, Senator Blunt.

Senator Bennett, again, I just want to publicly thank you for what were able to do last week in looking at some of our overhead assets. You're up.

Senator BENNET. Thank you, Mr. Chairman, and thank you very much for coming to Colorado.

I want to start by lending my thanks to all of you and to the people that work for you. While Putin was lying to us and to the Ukrainians and his own people, your people were ascertaining the truth, and we were warning the world.

And that could not have happened without the work that you've done. So I deeply, deeply appreciate it. We were on the phone on Saturday, most of us, I guess, with President Zelensky. He started the call by saying, we're just fighting to be able to live our lives like you. And he ended the call by saying, the world should live in peace, the world should live in a pluralistic way, by which he meant with freedom of speech, freedom of religion, self-determination—and that's what's at stake here. And I think we've got a chance to win this fight, in part, because of the people that work for all of you. So I want to say thank you.

Director Haines, Putin's aggression against Ukraine and against international rules and norms demonstrates the urgency of maintaining American superiority in emerging domains, including space and cyber, two domains that really I think the American people have not heard enough about.

Last week, as the Chairman mentioned, he joined me in Colorado for a series of briefings with Space Command, the National Space

Defense Center, and NRO leadership. Our conversation reinforced for me that our military and Intelligence Community missions are inextricably linked. And we are concerned that the decision to relocate Space Command does not fully account for the Intelligence Community missions that are in Colorado, the depth of the private sector which is so critical to building resilience in space.

It's my view that we should be spending money on the mission in space, not on moving Space Command and starting from scratch. Could you explain how strengthening the integration of our military and intelligence missions is critical to maintaining our superiority in space?

Director HAINES. Yes, absolutely. I couldn't agree more with the overall sentiment, which is that we have to integrate these areas. I do think that it's a domain in which obviously the Defense Department, but also other parts of the government such as NASA and so on are occupying, and it's increasingly crowded with commercial satellites as well.

And all of us have to be able to integrate together in order to effectively manage things. But no two entities more than, I suppose, the Department of Defense and the IC in order for us to do our jobs. And as we've been doing—we have a number of mechanisms that we use for that kind of coordination.

There's obviously the Joint Space Warfighter Forum which has the USSPACECOM Commander and the NRO Director as co-chairs and leading that. And that's an example of DoD and the IC coming together on these issues. And we have a number of other things: SPACECOM, the National Space Defense Center, an integrated protection strategy, that are intended to do this.

I would just say that, as I know you already know, but just to acknowledge it, we have work to do in this area to make sure that, frankly, as compartmented as some aspects of our work is, that we integrate that as well, effectively, so that we can actually work across this domain in a sensible and strategic way. I really appreciate your support and others for this area because I think it's obviously critically important to our future.

Senator BENNET. We heard some unbelievable things while we were there, which obviously we can't talk about in open session. But it is very clear—I think the Chairman would agree with this assessment—that we do not have a moment to lose here in space.

I just have a minute left.

Director Burns, could I just ask you to talk a little bit while we're in public session? Just give the American people a sense of how Russia is using disinformation across the world. How it's using it in its own country, but also how it's using it across the democracies to try to pit us against one another and divide us from one another?

These are things that appear to the American people sometimes to look like just another person's Twitter feed when, in fact, the Russians can be behind it. So could you spend a minute on that?

Director BURNS. Sure. Thanks, Senator, and I'll focus on the ways in which I think President Putin has worked methodically over the last two decades to turn Russian society into a kind of propaganda bubble. He's used financial pressures, he's used lethal actions. I remember vividly when I was Ambassador in Russia

some years ago, going to the funeral of a very courageous independent Russian journalist named Politkovskaya in the fall of 2006. And that's just one part of the pressure that he's brought against open information in Russia. He's intensified his domination of the state-run media and in his strangulation of independent media, especially in recent years, and particularly since the invasion of Ukraine began.

But I guess the last thing I'd say is I don't believe that he's going to be able to seal Russians off entirely from the truth. There are lots of Russians who have VPN accounts, who have access to YouTube to this day, who have access to information. And I don't believe he can wall off indefinitely Russians from the truth, especially as realities began to puncture that bubble. The realities of killed and wounded coming home, an increasing number. The realities of the economic consequences for ordinary Russians as I was discussing before. The realities of the horrific scenes of hospitals and schools being bombed next door in Ukraine and of civilian casualties there as well.

I don't think he can bottle up the truth indefinitely. Thank you. Thank you, Mr. Chairman.

Chairman WARNER. Senator Cotton, thank you as well, also, for your constant willingness to press this Committee and frankly the IC leadership both on the unclassified and classified sections of collaboration between the DoD projects and the IC projects. Senator Cotton.

Senator COTTON. Thank you.

Director Haines, I want to address the Administration's fiasco of failing to help Poland transfer its aircraft to Ukraine. The Pentagon spokesman yesterday cited your Intelligence Community, quote, "the Intelligence Community has assessed the transfer of MiG-29s to Ukraine may be mistaken as escalatory and could result in significant Russian reaction that might increase the prospects of a military escalation with NATO."

The State Department spokesman said essentially the same thing earlier today. Since Administration policymakers are justifying their hesitancy to help Poland transfer these aircraft by pointing to your Intelligence Community, could you tell us what is the basis for this alleged assessment that the transfer of these aircrafts would be viewed as escalatory?

Director HAINES. Thank you, Senator Cotton.

So, it is our analysts' assessment that the transfer of these airplanes could be perceived as a significant escalation by the Russians. They are obviously an advanced and considerable weapon.

Senator COTTON. I'm sorry. Director, I'm sorry. So I appreciate your analysts and their deep expertise and knowledge about this. I'm asking what specific evidence, information, intelligence do they have that the transfer of these aircrafts, as opposed to anti-aircraft missiles that shoot Russian jets out of the sky, is going to be viewed as escalatory?

Director HAINES. Why don't I provide to you a written product that will give you the basis for that?

Senator COTTON. So the Pentagon spokesman also said that this is the same intelligence that they had last year that delayed the transfer of many of those missiles as well; that there's no new in-

telligence. He said it was the same intelligence he's had last year. Was that the case?

Director HAINES. No, Senator, I'm not aware of what it is that he was referencing, but this is a recent assessment that was done by the Intelligence Community. I'm very happy to provide that—

Senator COTTON. I understand you didn't do assessments. I'm saying, do you have new intelligence?

Director HAINES. So when analysts—I know you know this—but obviously, they're looking at a body of intelligence and then they're also providing their own knowledge and experience. And I don't know whether or not there is—

Senator COTTON. So we can address this in a closed setting. But here's my opinion. You don't have new intelligence. This is opinion. And in many cases, this is policymakers who are looking to the Intelligence Community to provide them cover for their hesitancy.

General Berrier, could you explain, as an intelligence officer, how Vladimir Putin might be A-OK with us transferring missiles that turned their tanks into burning piles of rubbish or shoot their jets out of the sky, yet transferring tactical aircraft is going to be unacceptable? Why is the latter escalatory and the former not escalatory?

General BERRIER. Senator Cotton, thank you. I will take a stab at that in open session here. I think when you look at anti-tank weapons and air defense, Sir, shoulder fired kinds of weapons, there is a range of escalation. And I think in our view that escalation ladder doesn't get checked higher with those weapons versus something like combat aircraft.

Senator COTTON. I've got to say, I don't think there's a lot of common sense between this distinction. And a lot of farmers in Arkansas wouldn't understand it either. I mean your own written assessment, Ms. Haines, says that Russia, quote, "doesn't want a direct conflict with the United States," end quote. That was from January 21st. That assessment said Russia doesn't want a conflict with the United States.

You think they're more likely to want a conflict now after Vladimir Putin has seen the performance of his army? Not just against the Ukrainian army, but with moms with Molotov cocktails and grandmas with AK-47s. You think they're more likely to want a piece of us now than they were two months ago?

Director HAINES. I don't think it's an issue of whether or not they're more likely to want to conflict. It's whether or not they perceive us as being in that conflict with them. I think we're in a very challenging position, where we are obviously providing enormous amounts of support to the Ukrainians, as we should and need to do, but at the same time trying not to escalate the conflict into a full-on NATO or U.S. war with Russia.

And that's a challenging space to manage. And the analysts, I think, are just trying to provide their best assessment of what is likely to be perceived as that kind of escalation in this circumstance.

Senator COTTON. I mean, I've got to say, it seems to me that Vladimir Putin simply deterred the U.S. government from providing these aircraft by saying they would view this as escalatory. And if that's going to be our position, we might as well call the

commanding general at Fort Lewis, outside Seattle, and tell him to take the flag down and surrender our position because he's not going to stop in Ukraine. He's not going stop in Europe. Is going to go all the way to the West Coast. And every time he raises a threat, we immediately back off.

One other question I want to ask in this area as well about intelligence sharing. Last Thursday, the House Armed Services Committee Chairman Adam Smith said, quote, "we are providing some intelligence. We're not providing the kind of real-time targeting because that, you know, steps over the line that makes us participate in the war," end quote. Just a few hours later, the White House press secretary contradicted him saying, we have consistently been sharing intelligence that includes information the Ukrainians can use to inform and develop their military response to Russia's invasion. That has been ongoing and reports that suggest otherwise are inaccurate.

So who is correct? The Democratic Chairman of the House Armed Service Committee or the White House press secretary? Are we not providing that kind of real-time targeting intelligence to Ukraine?

Director HAINES. We are providing an enormous amount of intelligence to Ukraine. I'd be happy to get into in closed sessions the details of what we're providing. Maybe if there's anything else that people would like to add?

Senator COTTON Can you at least tell me who is correct between the Chairman of the House Armed Services Committee and the White House press secretary?

Director HAINES. Honestly, Senator, I think getting into this in closed session would be easier so that we can actually explain to you what it is that we're providing. But I'm happy to defer to my colleagues who may have additional—

Senator COTTON. I'm sure we'll address it in closed session.

Chairman WARNER. Thank you, Senator Cotton.

Senator Blunt, last worldwide threat. Senator Casey, your first worldwide hearing. Senator Casey.

Senator CASEY. Mr. Chairman, thanks very much. I think I join a chorus of gratitude and commendation for the work of the Intelligence Community, not only with respect to what's happening in Ukraine, but I think more generally. And so I want to thank both Director Haines and Director Burns for the work they and their teams have done, not just most recently, but in many cases for years and even decades. So many dedicated professionals.

I think that gratitude, though, is extended to every member of this panel: Director Wray, General Nakasone, General Berrier. It might be that you're the collective public service of the people that work in each of your areas of responsibility—that that public service might be more consequential today than it's ever been. So I want to extend that thank you more broadly.

I want to try to get maybe to two issues. One is on food security, or I should say food insecurity, across the world at this time and how it's exacerbated by what's playing out in Ukraine. But also to get to a question on China. We're told that in 2019, the number of people across the world who were on the edge of famine was about 27 million.

That was in 2019. It's a hell of a lot worse right now: 45 million people across the world on the edge of famine. So in just two or three years, two years really, from '19 to '21, up from 27 million to 45 million. We know that Ukraine itself, its farmlands, provide food for the whole world, especially to places like the Middle East and South Asia and North Africa.

Here's the data on wheat, corn, and barley: 12 percent of the wheat of the world provided by Ukraine, 16 percent of corn, 18 percent of barley. So you have both an exacerbating problem on food insecurity and Ukraine providing all that support. So with this state of food insecurity in mind, how does the IC incorporate food insecurity into its various analyses of threats in the United States and beyond.

Director Haines, if you could start. Or anyone else.

Director HAINES. Of course, Senator. Thank you very much for the question. And I agree with you. This is a really incredibly important issue and one that we are following.

We assess that Russia's invasion, which as you point out has caused energy prices to rise, which also has a dynamic relationship to the food security issue and has put upward pressure on global food prices. And this is what poses essentially the additional risk to food security globally. It could disrupt food supplies, particularly wheat for the reasons that you identified, because Ukraine, having been known as the breadbasket of Europe in many respects, is critical to that. And both Russia and Ukraine are important food suppliers to the global market. This is part of what I think we're going to be seeing as a challenge moving forward.

And as a consequence, we perceive that there is an increasing challenge through 2022, particularly with developing countries that rely on many of the food supplies at particular prices for them to manage those, so we are doing work on this. If you're interested in additional material, I'll definitely get that to you from the real experts, as opposed to me. But others may have more to add on this.

Senator CASEY. Thanks very much. I wanted to get to a question on China.

The China section of the threat assessment says, and I'm quoting in pertinent part, quote, "Beijing's willingness to use espionage subsidies, trade policy to give its firms a competitive advantage, represents not just an ongoing challenge for the U.S. economy and its workers, but also advances Beijing's ability to assume leadership of the world's technological advancement and standards," unquote.

As many of you know, Senator Cornyn and I have worked for a good while now on a piece of legislation which would institute as a matter of law, a committee to review outbound investment, especially the offshoring of critical U.S. supply chains.

How's the IC working to better understand both the Chinese government's surreptitious efforts to gain an unfair competitive advantage over U.S. firms and workers?

Director HAINES. I'll start and others should weigh in. I think we are obviously following this very closely, and we recognize that Beijing targets U.S. private sector companies in a variety of ways. Cyber is one aspect of it but it's not the only way in which they do it. And we've observed China targeting company insiders, not

just for their access to computer networks, but also because of the opportunity for essentially economic and other espionage in these spaces. And really other individuals that have access to critical technologies, to your point.

We've also observed China engage in theft of trade secrets, U.S. export-control violations, hacking ransomware, cyber pieces. All of this leads to grave concerns, obviously, with respect to their capacity to steal from American companies and innovation, and to ultimately use that to bolster their capabilities to promote their own technological advancement in areas that are of critical national security interest to us. And we've also seen how they've created an essential legal framework that provides them with access to companies that invest or that move to Beijing in order to allow for that information to be used by the Chinese government and to advance their technological innovation.

So let me leave it to others who probably have more to add.

Chairman WARNER. Director Wray.

Director WRAY. I would just add that some of the reforms that have taken place thanks to this Committee's leadership on the CFIUS process, for example, have been extremely important. And we've dedicated now, collectively, significantly more resources to trying to be more proactive, which is what some of the new authorities enable us to do. Certainly at the FBI, we now have about a 1,300 percent increase in economic espionage investigations tying back to the Chinese government from, say, a decade ago. And we are finding that more and more, much as Director Haines referenced more broadly in her opening statement, that sharing information through a variety of ways with private sector partners often enables them to make responsible decisions that maybe in the past, in a shortsighted way, they would not have made. I think that's ultimately going to have to be a key part of this as we go forward. We can't just investigate or disrupt our way out of it. We need the private sector engaged too.

Chairman WARNER. Senator Casey, thank you for your and Senator Cornyn's leadership on this. And I also want to acknowledge Senator Cornyn's leadership on the CFIUS reform a few years back that really has given Director Wray and others the tools they need.

Senator Cornyn.

Senator CORNYN. Thank you. I want to join my colleagues in thanking you and the people you represent for your service to our country.

I want to talk about Russian propaganda. We all know that in 2016, there had been extensive work of this Committee and the Director of National Intelligence, the Intelligence Community writ large, on Russian propaganda. I want to talk not about their role in our elections, but now, when it comes to energy. John McCain, our former colleague, used to say that Russia was a gas station masquerading as a country, which is a humorous way of talking about how Russia is economically dependent on energy exports and is doing everything it can to keep Europe and the rest of the world dependent on Russian energy exports.

Many of us have pointed out that the high price of oil that Putin is reaping today is being used to fund this horrific invasion in Ukraine. I just want to point out, I think it's the Energy Informa-

tion Administration predicts that by 2050 that the world will still continue to need fossil fuels and its role in providing energy will, to the world, will be four times what renewables can provide. And this is not meant to denigrate the role of renewables. It plays an important part in our portfolio. But I do worry that Russia's ability to provide a monopoly and to weaponize energy when it comes to Europe could well undermine the sanctions that we are trying to impose. It would certainly seem to make the other countries in Europe who are reliant on Russia for their oil and gas more pliable or compliant with Russia's wishes.

Back in 2017, Director Haines, the Office of the Director of National Intelligence, the office you now hold, reported on page 8 in annex A to a document called "Assessing Russian Activities and Intentions in Recent Elections." But there's a piece about how "Russia Today," which I believe now is a registered foreign agent of the Russian Federation, was conducting anti-fracking messages with the intended impact of weakening political support for U.S. production of our natural resources and diminishing any challenge to Russia's preeminent role when it comes to providing oil and gas and energy to Europe and the rest of the world.

So it seems to me that Russia has been, for some time, trying to discredit any energy initiatives which threaten its preeminent position, whether it's attacking American or European fossil fuels or funding green groups to spread disinformation.

Can you elaborate, Director Haines, on how extensive Russia's propaganda campaign has been in this area?

Director HAINES. Not with precision, and I'm not familiar with the specific report that you're referencing. But it certainly is consistent with what we've seen, and therefore, don't doubt it. And we could definitely provide you a further assessment that gives you a sense of what scale we've seen and whether there are any particular trends in that area.

But I think your overall conclusions are ones that we share, which is to say that they would use their information campaign and influence in order to promote their own energy industry and in order to divide us on these issues as well.

General NAKASONE. The only thing I would add, Director, is that this is the methodology we've seen when the Russians find the divisive issue, find the two groups that you can both feed this, use social media as an influence, and then be able to continually pursue that message.

Senator CORNYN. Director Burns, isn't Putin's monopoly on providing energy to Europe a boot on the neck of the Europeans? And doesn't this threaten their willingness to cooperate when it comes to these economic sanctions? Because he can just turn the gas off, right?

Director BURNS. Senator, one of the most striking, unintended consequences from Putin's point of view is the extent to which a number of leading European governments seem to be belatedly realizing what you just described: the threat that they face by overdependence on Russian energy resources. You have not just the demise of Nord Stream 2, but also the fact the Germans just announced the construction of an LNG facility clearly aimed at diversifying, beyond Russia, their sources of energy. And so I think

that's something that President Putin certainly did not anticipate when he began this invasion. But it could have a quite significant, long-term, strategic effect as well.

Chairman WARNER. Senator King, I just want to also acknowledge the great work that you and Senator Sasse have done on the Cyber Symposium. A number of us have raised some of those questions, but thank you for your good work.

Senator KING. Thank you very much. I apologize for being late. If we could apply AI to the Senate schedule, we might not have three hearings scheduled at exactly the same time.

Thank you very much for your testimony here today. I think one of my first questions in a large strategic sense for you, Director Haines, is China-Russia cooperation. It seems to me in the last couple of years, really in the last year, we've seen a closer cooperation and communication between those two countries. How do we assess that? It seems to me if you're talking worldwide threats, that's one of them.

Director HAINES. Yes, absolutely, Senator King. I think your assessment is our assessment, which is to say that we are seeing them cooperate more. And we anticipate that it will strengthen over the coming years. And it's across a variety of sectors: economic, political, military. In fact, the announcements that were made during the Olympics are an indication of how close they're becoming.

At the same time, we do see it as not yet at the point where we are, for example, with allies. They have not achieved that kind of level of cooperation. And we anticipate it is unlikely in the next five years that they will, in fact, become the way we are an ally with our other NATO members in that context. But others may have things to add to this.

Senator KING. Director Burns.

Director BURNS. The only thing to add, Senator, is as Director Haines said, the joint statement that President Xi and President Putin issued on the 4th of February, at the beginning of the Winter Olympics, was the most sweeping expression of their commitment to partnership we've seen.

But I would only add that I think what's unfolded in Ukraine, the ugliness of it, the flawed assumptions that underpinned it from the point of view of President Putin have unsettled the Chinese leadership a little bit. They're unsettled by the reputational damage that could come from that.

Senator KING. And the Chinese seem more concerned about reputational damage than Russia just generally?

Director BURNS. Russia, President Putin, has a low bar in terms of concern about reputational damage, I think. But I do think they're concerned about that. I think they're concerned about economic consequences at a time when their own projected growth rates are lower than they've been in quite some time.

And I think as I mentioned earlier, they're concerned about the way in which President Putin is driving Europeans and Americans closer together at a moment when I think the Chinese have always valued their independent relationships with the Germans and other leading Europeans as offering opportunities to drive wedges between them and the United States, which, I think, President

Putin's actions have helped to deprive them. So I think they're concerned by all that.

Senator KING. One more unintended consequence of what Mr. Putin has done.

General Nakasone, one thing that has surprised me in Ukraine is the lack of a strong, consistent Russian cyber attack on Ukraine. I expected to see the grid go down and communications, and that hasn't happened. Do you have any assessment of why?

I thought that would be in the first couple of days.

General NAKASONE. Senator, I think that you know, as we look at this—and we're only 15 days in, and so much can still occur—we're very vigilant to make sure nothing does occur. But, with that said, I think that there are several things that are important to note. We've worked very, very hard with Ukraine over the past several years, really since the shutdown of energy in 2015. We had Hunt Forward teams from U.S. CYBERCOMMAND in Kyiv. We worked very, very closely with a series of partners at NSA and the private sector to be able to provide that information; the inter-agency. These are all impacts that I think have played out positively early on. And I think, to a degree, there's still obviously a Russian calculus that will play out here. We will be very, very vigilant to see what occurs there.

Senator KING. Finally, Director Haines, one of the learnings from the Ukraine experience, from our point of view, is the value of sharing intelligence. I don't mean sharing necessarily between allies, but I mean with the American people, with the people of the world. I've always thought that we classify too much and that we really blunt the impact that we could have on international relations by not sharing, as long as we don't compromise sources and methods.

It appears that a conscious decision was made to share more. Is that the case?

Director HAINES. Yes, we have, all of us, I think, engaged in this, and it has been an extraordinary team effort, to be honest, in trying to promote more mechanisms for sharing, finding ways to make sure that we're integrating our work across the Intelligence Community and providing that information to partners and allies in this context, and also disclosing certain things publicly, as you've indicated.

And I think it really has been, at least from my perspective, critical to the diplomatic effort. I think it has helped to galvanize the response and also, I hope, helped to prepare the Ukrainians to some extent, even though I think, honestly, it's obviously tragic that despite all of the information we put out, that we still see the Russians invade Ukraine.

And so it's a bit bittersweet in this moment, but I think we've learned a lot of lessons from it, and I think it will allow us to continue to do that in places where we see the need.

General NAKASONE. Senator, if I might, just on top of what the Director said. We share a lot of intelligence, but here's the difference. The intelligence that we're sharing is accurate, it's relevant, and it's actionable. I think when we look back at this, that's the key piece of what we've been able to do as an Intelligence Community.

Senator KING. Thank you. Thank you, Mr. Chairman

Chairman WARNER. Senator Sasse, even though you claim to be the longest serving rookie on this Committee, I want to personally thank you for your relentless focus on China and holding the IC's feet to the fire, that it's not just language but dollars that flow that.

Senator Sasse.

Senator SASSE. Thanks, Chairman, and thanks to all five of you for being here. I have a bunch of questions about self-deterrence, around the MiG U-turn, around real-time sharing of lethal targeting information, but I think I'm not going to do that here. I'm going to save it for the classified setting, because I think Senator Cotton's exchange is the most important part of this hearing so far today.

Vladimir Putin will embrace the idea that we might self-deter every time he issues a press release, and lawyerly hairsplitting about providing this kind of weaponry is not escalatory, but providing that kind of weaponry is escalatory. I don't think we really believe that. I think the Administration is pushing the Intelligence Community to give them cover for lean-forward decisions they don't want to be making.

So I applaud Senator Cotton on his line of questioning, and I suspect it'll be the heart of a lot of what we do in the classified setting.

I want to stay on the China point that the Chairman just mentioned—. And Director Burns, first of all, kudos. Kudos to all of you. It's been said many times today, but believe me, I associate myself with the praise for the pre-textual rebuttal of Putin's lies about why he was going to invade. The whole IC did great work.

Director Burns, since you arrived, standing up the China Mission Center as you pledged to do is a really important development.

So thank you. Could you explain to us how Chairman Xi views Putin and this invasion; a month ago, today, and a month from now?

Director BURNS. I think, as I said, I think the Chinese leadership, President Xi, has invested a lot in partnership with President Putin and Russia. I don't think that's going to change any time soon. It's for a lot of very cold-blooded reasons. I do, however, think that President Xi is unsettled by what he's seen transpire in the last 15 days in Ukraine. I don't think they anticipated that the Russian military was going to prove largely ineffective so far. I don't think they anticipated that the West would react with such resolve, in terms of not only military support for the Ukrainians, but also in terms of economic consequences, as well. I think they are worried about reputational damage, and I think they're worried about the wider economic consequences.

At a time when, especially in 2022, with the Chinese leadership preoccupied by the party congress in November, they're looking for relative stability and predictability in the global economy. This unsettles that as well. So I think that's raised some question marks, you know, in the minds of the Chinese leadership as they look at what is going to be an enduring partnership, but maybe with a few more concerns than they had 16 days ago.

Senator SASSE. That's helpful. I have heard from multiple foreign ministers and defense ministers and other NATO leaders over the

course of the last month that one of the—you can't say there are any silver linings to the evil of what Putin is doing in targeting women and children and civilians. There is no moral limit to what the guy will do. But if you made a list a year from now of developments that happened in the world because of this invasion, the horror list is a mile long.

But one of the only things on the good side of the ledger is that I think many European leaders are going to get more steely-eyed-realist about who Chairman Xi is, because the guy greenlit this invasion. Russia has eleven time zones and they were able to move almost all their troops back from the Far East, because Xi wants to see the West destabilized. He wants to see Europe and the U.S. humiliated and embarrassed, and there are a whole bunch of European corporate executives that lust for the 550 million middle-class consumers of the 1.4 billion Chinese. And a lot of European political leaders who are willing to provide cover for that and pretend that Xi is a sort of benign figure, and he is not. And the fact that he greenlit this by Putin, I think, is a pretty important development for our allies to get more serious about.

General Berrier, I wonder if you could help us understand what are the most important needs the Ukrainian military has to extend this fight? And how can the U.S. do more and faster?

General BERRIER. So, Senator, thanks for the question. We'll go into much more detail in the closed session. Right now, they do need support in the cities where the combat operations are going on right now, in the major cities. They need humanitarian support as well as small arms, ammunition, artillery rockets. The entire panoply, if you will, of ground forces kind of support.

The anti-tank weapons are very important. The air defense weapons, as we've talked about it, are very important. I would like to go back to the escalation ladder, though, with these types of weapons. I do believe that there is an escalation ladder, and there is a difference between an anti-tank weapon, a shoulder-fired air defense weapon, and a combat aircraft and a jet that could cross a border and actually conduct operations on Russian soil.

So in terms of analytical thinking, that's where that's at.

Senator SASSE. I know we're at time, but I just want to underscore one historical point. In World War II, there were planes dragged across the U.S.-Canadian border. So this conversation has been had before, and it's not impossible to figure out a way to solve the problem if we wanted to solve the problem.

Women and children are being bombed. Nobody on this Committee is calling for U.S. boots on the ground in Ukraine. But there's more we can do, and we should be going faster. The answers the American public hears, particularly from State Department and White House press briefings, is often process about process about a meeting. There's a war going on, and Zelensky is a hero on behalf of 44 million Ukrainians. He's asking for more help, and the Administration should be doing more faster.

Chairman WARNER. I know we're going to closed session, but I think a couple of Members want to at least ask one more question.

I want to simply reemphasize what Senator Rubio's line of questioning would be, about things that are already floating in the Internet around the possibilities of bio tools being used. And I

think Director Haines did most of this effort. I do think, in the public session, Director Burns, if you could address this. And clearly, there is a difference between bioresearch centers and bioweapons centers.

Anything you can do to help clarify some of the things that are already floating, because I'm fearful that this could be the new direction of a Russian false-flag operation.

Director BURNS. The first thing I'd say, Senator, is that unlike Russia, which does have chemical weapons and has used them and does do biological weapons research and has for years, Ukraine has neither. And second, as Director Haines said, in any public health system around the world, there's going to be work done in the interests of wider public health to ensure that we have a grip on issues like that. But that's in no way threatening.

That's not something that can be weaponized in the way that the Russians have clearly demonstrated by their own actions against their citizens and people outside their country. Their willingness to use—. And when you couple that with their demonstrated willingness to create false-flag operations and try to create the impression that somehow Ukrainians are responsible for this, that should give us all pretty serious reason for concern about their propaganda.

Chairman WARNER. Thank you. Senator Rubio.

Vice Chairman RUBIO. Just to follow up on that, trying to put it in perspective. So as Assistant Secretary Nuland said, there are these facilities there and there's something in those facilities. It's dangerous because we're afraid the Russians will get a hold of it. Now I understand that there's a difference between a bioweapons facility and one that's doing research. A bio research facility is a totally different thing from a bioweapon facility, because you could have samples of a deadly or serious pathogen. But that doesn't mean you could weaponize it or that you're working on weaponizing it. But people ask themselves if there are these facilities there and there's a lot at play here, I mean there is a lot we should have and this is none of you but a long time ago this should have been acknowledged like, yes, there are these labs. This is what they do because a lot of these fact checkers just said, don't even mention labs, because it's—they don't even exist. They do. They exist all over the world.

There's labs like that right here. So what I think got some people fired up is when she said, we're worried that the Russians will get a hold of these facilities, because that implies that there's something in those facilities that's very dangerous. So I don't know if you could shed some light on how there can be things in the lab that are dangerous, but they not be weapons labs.

Director BURNS. All I would say, Senator, is that the danger here, it seems to me, is the capacity the Russians have developed and that they've used in the past, and their interest in trying to create false narratives here, as well. You have to be careful about any of those substances you've talked about, what you see in public health or research systems around the world for civilian purposes. Why you have to be careful about that that is in no way akin to the kind of threats that would be posed by weapons research and development or weapons facilities.

Vice Chairman RUBIO. Yes. I just think that the answer is what piqued a lot of people's—. And look, the latching onto it is my point. I think there's been such a good job done at defeating them in the information space, but this is one where they seem to have latched on. I don't think anyone believes per se that if there's some very serious attack, or even a fake one, that they're going to convince the American public that the Ukrainians are behind it. But it's the confusion around it that I worry about debilitating the debate and allowing them to deflect it.

I do want to ask you in particular, Director Burns, because you have been involved with Russia issues for a very long time.

I think, as much as anyone involved today in this issue, you've had an opportunity to watch Vladimir Putin through the years. This whole thing about they're having negotiations or parent negotiations today in Turkey with the foreign ministers. It's my view that he uses negotiations as just another tool on his toolbox.

What is your view of why he continues to agree to these talks and put these talks forward if we know they're not resulting in anything and in fact he's violating whatever they even nominally agree to?

Director BURNS. Senator, yours is a fair assumption that these sometimes are just used tactically as well. I think the core issue here is that President Putin does not have a sustainable endgame in Ukraine right now. So the question is, is he simply going to continue to double down and grind down the Ukrainian military and the Ukrainian population? Or at some point, does he recognize that reality that he doesn't have a sustainable endgame and look for ways to end the bloodshed to cut his losses and to reaffirm the sovereignty and territorial integrity of Ukraine? Now, given Putin's track record, given the fact that he's someone who hates to act out of what he believes to be weakness—that he hates to concede or admit mistakes—that's probably a long shot.

But that's our hope at least that at some point he recognizes that because, absent that, off-ramps become just rhetoric.

Chairman WARNER. Thank you for raising the bio issue, Senator Rubio.

Senator King.

Senator KING. General Berrier, we see these horrendous pictures of apartment blocks being hit, hospitals being hit in Ukraine. My question is what's hitting them? The use of the term bombing is very common, but my impression is it's mostly missiles and artillery.

Is it bombing from aircraft or missiles and artillery?

General BERRIER. It a combination of mostly missiles, artillery, multiple rocket launchers. There are some precision guided munitions that are being dropped from aircraft, but that number is small.

Senator KING. So the talk about a no-fly zone wouldn't really impact what's causing the damage currently, is that correct?

General BERRIER. The Air Force is having a tough time flying in Ukraine right now. They're conducting surveillance and reconnaissance. They're using their assets to do a bunch of different things. And quite honestly, a no-fly zone is a combat operation that re-

quires manned and unmanned aircraft, ISR assets, resources, and, on the escalation ladder, that is escalatory.

Senator KING. I understand that, but my point is, a no-fly zone wouldn't inhibit missiles, rockets, and artillery.

General BERRIER. That is correct.

Senator KING. Thank you.

Chairman WARNER. Thank you.

Senator Burr.

Senator BURR. Mr. Chairman, thank you. I'm going to direct it to Director Haines. This is really precipitated by Senator Cotton's question on the transfer of aircraft.

We gave a green light to Poland to transfer MIGs. The United States. Publicly. When Poland came back and said we'd like to transfer these over to a U.S. facility and have Ukrainian pilots fly from there, all of a sudden the American line was: we think that would be a escalatory.

We're all part of the same thing called NATO, and under that agreement, when one of NATO's member's geography is challenged, the rest respond. Now, we can get into whatever we want to in closed session. I as much as anybody really respect the analytic product that comes out of the Intelligence Community. It should be questioned; that's why we have analysts in every area and outside of the Intel community. But when the U.S. publicly gives Poland a green light to transfer aircraft, and then changes their mind when the aircrafts are transferred off of our space, our geography, as a member of NATO as well. And we say that that would make it escalatory, but if Poland transferred it, we didn't consider it to be escalatory. Then I draw this conclusion. This is a policy decision. It's a policy decision made by the Administration. And I remind all of you at the table, intelligence is never supposed to influence policy. It's the reason that we tried desperately—we don't always succeed—but we try desperately not to present you with a policy question, as part of the Intelligence Community. By the same token, we expect that if intelligence is inappropriately being used to reach a policy decision, that it's the Intelligence Community that pushes back on that.

So I look forward to your explanation, but I remind you that there is a bright line that the Intelligence Community has always maintained between policy and the advice you give about what the intelligence says.

My hope is we haven't, as an Intelligence Community, put our finger on the scale of a policy decision that's been made. Because, clearly, this is confusing to the American people—how America could say, Poland, it's okay for you to transfer, but you can't transfer it off of our geography.

I thank you, Mr. Chairman.

Chairman WARNER. Senator Collins.

Director HAINES. Can I respond? Just to say Senator Burr, obviously you know this, but analytic objectivity, and for all of us here, is an absolutely core ethic for the Intelligence Community. And I do not believe that there is any issue here with respect to political or policy pressure being put on the analysts. They were asked the question of whether or not providing these airplanes would be perceived by the Russians in an escalatory way. And they answered

the question. I don't know when the timing was with respect to the policy—things that were made—

Senator BURR. Director, I'm not questioning what the analysts came to a conclusion on. But if the analyst came to a conclusion that the transfer of aircraft was escalatory, then it would apply to Poland's transfer, not just a transfer off of United States geography. And that was not used as a reason when Poland was given the green light. But it was used when it was thrown into our laps, which leads me to believe that there is a policy decision that we're not going to be involved in. I only throw it out there to you for the thought process of going through it. We can get into it in closed session.

Director HAINES. Okay.

Senator BURR. Thank you, Mr. Chairman.

Chairman WARNER. Senator Collins.

Senator COLLINS. Director Haines, I want to switch to Iran. Your predecessors at every single Worldwide Threat Hearing since 2016 have labeled Iran as the foremost state sponsor of terrorism. Is that your assessment as well?

Director HAINES. Senator Collins, there's no question that Iran continues to support terrorism.

Senator COLLINS. There's widespread speculation that, in exchange for a new nuclear agreement with Iran, that the Administration is considering lifting sanctions on Iranian organizations or individuals, including those that are tied directly to Iran's terrorist activity. And there's one speculation that the Administration may go so far as to rescind the Foreign Terrorist Organization designation of Iran's primary arm to foment terror in the region, the IRGC.

Now, I'm not going to ask you whether sanctions should be lifted or not, recognizing that is a policy decision. But I do believe that it's fair to ask you which Iranian entities are actively supporting the regime's malign activity today. So let me pull on that thread a bit. Tony Blair's Institute for Global Change said in a report last year that the IRGC acts as an institutionalized militia and uses its vast resources to spread a mission of Jihad through an ideological army of recruits and proxies.

So, with respect to the IRGC, do you agree that it continues to conduct, support, and facilitate terrorism throughout the Middle East?

Director HAINES. Thank you, Senator. The regime as a whole has supported destabilizing activities throughout the Middle East and continues to be a concern, and IRGC is among entities that do—that are part of the regime's overall strategy. But I think if you want detail on particular entities, we should provide that to you separately and in writing. But I don't know if others have anything.

Senator COLLINS. Is there any evidence that the Central Bank of Iran has stopped financing terrorist activity?

Director HAINES. I think if you mean money that goes through the Central Bank of Iran may be ultimately used by Iran—

Senator COLLINS. Yes.

Director HAINES. In the context of the things, I don't have details. But we can certainly look at whether or not it's increasing or decreasing based on our assessments.

Senator COLLINS. Is it fair to say that the assessment of the IC is that advances made by Iran related to launching missiles into space have an inherent dual-use technology as a delivery vehicle for a nuclear or a conventional ballistic missile?

Director HAINES. Absolutely. Senator, we obviously have had concerns about their ballistic missile technology and their advancements in this areas. And obviously, over the course of many bipartisan Administrations, sanctions have been enacted as a consequence of that.

Senator COLLINS. And finally, I would just note, and I commend you for this, that in your confirmation hearing we discussed the prospect of a renegotiation of the JCPOA. And one of your points was that there should be more opportunity to consult with Congress on issues related to any new agreement. And I've appreciated the IC's attentiveness to keeping a focus on Iranian activity. But I've been disappointed in the lack of transparency and outreach from the policy community regarding the status of the negotiations. And I would just ask that you take that back to the White House. Thank you.

Chairman WARNER. So, we're going to move through, and everybody obviously gets this last round. As a—maybe—incentive to limit this to one or two questions, in an unprecedented move, the Committee is providing lunch directly after this. And unfortunately, for our panel, there will be no breaks or we will go over. And if you guys answer briefly, you will also get lunch.

Senator Cotton. [Laughter.]

Senator COTTON. Senator Burr raised an excellent point. It's a second arbitrary distinction about these Polish MiGs. Apparently, the U.S.-government position was they go from Poland, okeydokey. That's A-Okay. They go from the United States, nope. Vladimir Putin views that as escalatory. I still don't think there's any intelligence to justify that distinction.

I want to return, General Berrier, to what you said to Senator Sasse. You said that you believe that there is a difference in escalation between anti-tank missiles and anti-aircraft missiles on the one hand, and aircraft on the other hand. I understand you believe that. I understand that Director Haynes believes that, and she claims that the analysts believe that. I don't believe it. I don't believe it, and I don't believe there's intelligence to support it. I bet the Russian pilot that gets shot out of the air by an anti-aircraft missile as opposed to the aircraft doesn't believe it either. But it's not really a matter of what you believe or I believe. It's a matter of what we can prove and what we can prove that Vladimir Putin believes. And I just don't think the proof is there. We'll know in a few minutes, I guess, if there is.

I want to address a bigger point, and I want to join with a lot of my colleagues to commend the Intelligence Community and especially the DIA for the outstanding work it did leading up to the invasion. In my seven years on the Committee, it's the best I've seen the Intelligence Community perform—between September until February 24th. Director Haines, you testified that you think Vladimir Putin underestimated the Ukrainians' skill and their will to fight and he overestimated his own military's ability. Is it fair to

say our Intelligence Community made the same mistakes based on the testimony we've heard here?

Director HAINES. So, we assessed, prior to the invasion, that he was underestimating the Ukrainians' resistance, likely resistance, too. So I think we did well there. We did not do as well in terms of predicting the military challenges that he has encountered with his own military.

Senator COTTON. General Berrier, could you address this?

General BERRIER. Senator, I will address that. My view was that, based on a variety of factors, that the Ukrainians were not as ready as I thought they should be. Therefore, I questioned their will to fight. That was a bad assessment on my part, because they have fought bravely and honorably and are doing the right thing. So that was an issue for me as the Director of DIA.

Senator COTTON. And I understand that. But assessing a people's will to fight is one of the hardest things an intelligence agency could do. In some ways, it's a moral or a psychological question, not an intelligence question. But in other things, like how long Kyiv would hold out or these other major cities, or how long Ukraine would still have an Air Force or air defense systems, did we make mistakes about those assessments as well?

General BERRIER. Well, we made some assumptions about his assumptions, which proved to be very, very flawed. And so, his actual activity as he got into this fight turned his operation kind of on its head. And what we've seen is a devolvement, if you will, of the operations that he has going on now. And I'd like to save the rest of this for a closed session.

Senator COTTON. To the extent we can address it here, could you say why you think we made those mistakes?

General BERRIER. I think assessing will, morale, and a will to fight is a very difficult analytical task. We had different inputs from different organizations, and we, at least from my perspective as the Director, I did not do as well as I could have.

Senator COTTON. Director Haines, could you give your opinion on why the IC made those mistakes?

Director HAINES. I don't think I have anything to add in open session. I'm trying to—we can discuss further.

Senator COTTON. Okay. I just want to say because, and I'm not—I just don't want to be critical, but these mistakes had potentially real-world policy implications about the willingness of the President or other NATO leaders to provide weapons that they thought might have fallen into the hands of Russians in a matter of hours, or to impose sanctions for something that might have been a fait accompli.

And we need to ask ourselves, if we made mistakes about the first two weeks of this war, are we making mistakes about the next two weeks or the next two months, and the policy implications those might have? And furthermore, to Richard Burr's point about the use of policy to influence intelligence, I have to say I have concerns that part of the reason the Administration went relatively soft on Russia and was hesitant in Ukraine in 2021 is they were relying on Russia to get the bad nuclear deal that Susan Collins was talking about?

I have the unavoidable conclusion that influenced part of it.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. I wanted to just ask the question, recognizing intelligence is not science—it's an art. What do we think that Putin would do if the United States or the Poles provided these MiGs to the Ukrainians?

General BERRIER. Senator, we have run through a number of scenarios as the escalation ladder continues to unfold. I'd like to answer that question in closed session.

Senator CORNYN. Thank you.

Chairman WARNER. Senator Sasse.

Senator SASSE. Thank you, Chairman.

I'll save most of my questions for classified, too. I want to make one comment and then ask General Nakasone one small question about the pre-textual work that you all did.

The comment is, at many White House briefings and a number of State Department briefings over the course of the last week and a half, the phrase has been used that the U.S. did or NATO did, or the U.S. hypothetically did or NATO hypothetically did escalatory things or aggressive things. I think we should get the language right, which is there are claims by Putin that we did escalatory or aggressive things, or are hypothesizing about aggressive things.

There's only one aggressor here, and that's the jackass who's killing women and children. There's one aggressor. There's one person targeting civilians. And us trying to figure out what our obligations are to our allies and our obligations are to the world and to humanity when civilians are being targeted, is a really important debate that we should be having more aggressively, leaning farther forward. And we shouldn't accept the idea that because Putin calls us aggressive when we figure out how we try to stop the guy, we are not the aggressor.

General Nakasone, you all have done some really great work on sharing intelligence to expose what Putin was up to. What do you think the implications will be, one or two or three years from now, from what we've learned from this more aggressive, promiscuous, healthily promiscuous sharing of intel in advance?

General NAKASONE. I think we'll redefine sharing, Senator. You talk about sharing with our partners, that that had an impact, about being able to bring our coalition together. We talk about sharing with the Ukrainians actionable intelligence that allows them to be able to take combat operations to a new level.

And then I think the other piece is being able to shine a light on disinformation. We've seen this in the elections—2018, 2020. When we take on an adversary, when we work with a series of partners being able to shine a light on these mis-stories and these false-flag operations, it suddenly isn't as big a deal. And I think that's what we'll learn from sharing.

Chairman WARNER. Let me just make two quick comments. One, you know, I remember when many of us were in Munich a few weeks back and some of the, I think, very legitimate questions that Senator Cotton's asking about what we got right or wrong post-conflict starting. I just recall all of the interactions I had, and some of us who were with us there had, with all of our European part-

ners who candidly had the same assessments, particularly around control of the skies.

I think the more global comment I'd make, and it's one of the reasons why I think it's so important that we do this in public. You've heard from both sides of the aisle that Members are pressing the leaders of the IC on their analysts' assessment, the quality of their intelligence, decision making. This is a Committee that robustly asks hard questions.

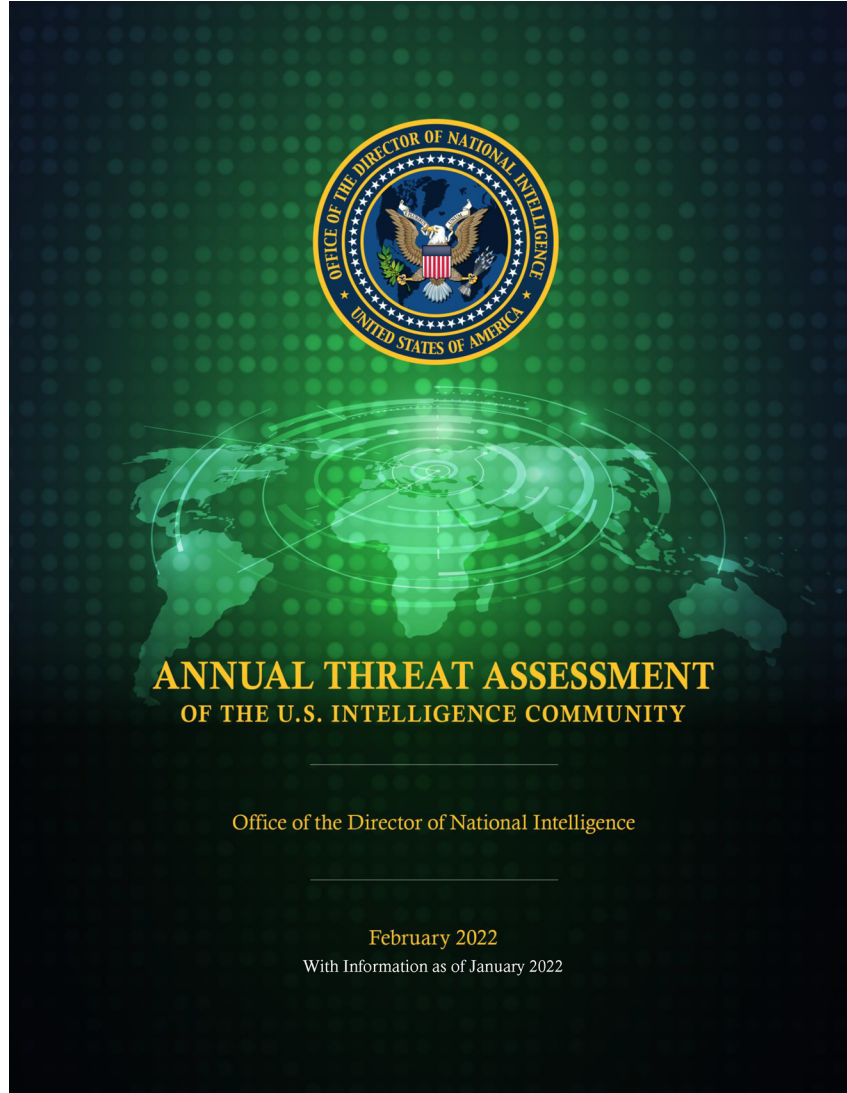
I want to assure the public, at least, that this same level of questions, if not higher, are raised in closed settings. Frankly, the fact that Senator Wyden didn't ask for those returns in his normal 30-day period as opposed to a week period—. I don't think you have a Committee here that is captured by the community. We have great respect for the community. I think virtually everyone here has commended their, I believe, excellent work, I would argue, both leading up to the invasion and continuing to keep us informed. The people should know that this Committee operates in the same way behind closed doors as it does in open session.

And I hope people will take some solace from that. And recognizing because we're moving on and I know there's a host of questions for the closed setting, we will move directly next door. And again, lunch will be served.

We stand in recess.

[Whereupon at 12:25 p.m. the hearing was recessed subject to the call of the Chairman.]

Supplemental Material



ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

February 7, 2022

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 (P.L. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed every day 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 during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC. All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future, such as climate change and environmental degradation.

As required by the law, this report will be provided to the congressional intelligence committees as well as the committees on the Armed Services of the House of Representatives and the Senate.

Information available as of 21 January was used in the preparation of this assessment.

CONTENTS

INTRODUCTION	2
FOREWORD	4
CHINA	6
RUSSIA	10
IRAN	14
NORTH KOREA	16
HEALTH SECURITY	18
Infectious Diseases and the Impact of the COVID-19 Pandemic	18
Biological Weapons	19
Anomalous Health Incidents	20
CLIMATE CHANGE AND ENVIRONMENTAL DEGRADATION	21
ADDITIONAL TRANSNATIONAL ISSUES	22
Preface	22
Innovative Use of New Technology	22
Transnational Organized Crime	23
Foreign Illicit Drugs	23
Money Laundering and Financial Crimes	24
Cyber Crime	24
Migration	24
Global Terrorism	25
CONFLICTS AND INSTABILITY	28
South Asia	28
Other Regions	29

FOREWORD

In the coming year, the United States and its allies will face an increasingly complex and interconnected global security environment marked by the growing specter of great power competition and conflict, while collective, transnational threats to all nations and actors compete for our attention and finite resources. These challenges will play out amidst the continued global disruption resulting from the COVID-19 pandemic, contention over global efforts to deal with a changing climate, increasingly powerful non-state actors, and rapidly evolving technology, all within the context of an evolving world order where the continued diffusion of power is leading actors to reassess their place and capabilities in an increasingly multipolar world. These challenges will intersect and interact in unpredictable ways, leading to mutually reinforcing effects that could challenge our ability to respond, but also introducing new opportunities to forge collective action with allies and partners against both the renewed threat of nation-state aggression and emerging threats to human security. The 2022 Annual Threat Assessment highlights some of those connections as it provides the Intelligence Community's (IC's) baseline assessments of the most pressing threats to U.S. national interests, while emphasizing the United States' key adversaries and competitors. It is not an exhaustive assessment of all global challenges and notably excludes assessments of U.S. adversaries' vulnerabilities. It accounts for functional concerns, such as weapons of mass destruction and cyber, primarily in the sections on threat actors, such as China and Russia.

Competition and potential conflict between nation-states remains a critical national security threat. Beijing, Moscow, Tehran, and Pyongyang have demonstrated the capability and intent to advance their interests at the expense of the United States and its allies. China increasingly is a near-peer competitor, challenging the United States in multiple arenas—especially economically, militarily, and technologically—and is pushing to change global norms and potentially threatening its neighbors. Russia is pushing back against Washington where it can—locally and globally—employing techniques up to and including the use of force. In Ukraine, we can see the results of Russia's increased willingness to use military threats and force to impose its will on neighbors. Iran will remain a regional menace with broader malign influence activities, and North Korea will expand its WMD capabilities while being a disruptive player on the regional and world stages. Major adversaries and competitors are enhancing and exercising their military, cyber, and other capabilities, raising the risks to U.S. and allied forces, weakening our conventional deterrence, and worsening the longstanding threat from weapons of mass destruction. As states such as China and Russia increasingly see space as a warfighting domain, multilateral space security discussions have taken on greater importance as a way to reduce the risk of a confrontation that would affect every state's ability to safely operate in space.

The lingering effects of the COVID-19 pandemic will continue to strain governments and societies, fueling humanitarian and economic crises, political unrest, and geopolitical competition as countries, such as China and Russia, seek advantage through such avenues as “vaccine diplomacy.” No country has been completely spared, and even when a vaccine is widely distributed globally, the economic and political aftershocks will be felt for years. Low-income countries with high debts face particularly challenging recoveries and the potential for cascading crises leading to regional instability, whereas others will turn inward or be distracted by other challenges. The IC continues to investigate the concerning incidences of Anomalous Health Incidents and the danger they pose to U.S. personnel.

Ecological degradation and a changing climate will continue to fuel disease outbreaks, threaten food and water security, and exacerbate political instability and humanitarian crises. Great power competition and disputes between wealthy and low-income nations will threaten progress on the collective action that will be needed to meet global goals for reduction of greenhouse gas emissions.

Other transnational challenges will pose an array of direct and indirect threats to the United States. They will interact in complex and cascading ways with each other and with threats posed by great power competition, increasingly empowered non-state actors, the pandemic, and climate change. Emerging and disruptive technologies, as well as the proliferation and permeation of technology into all aspects of our lives, pose unique challenges. The scourge of transnational organized crime, illicit drugs, violent extremism, and endemic corruption in many countries will continue to take their toll on American lives, prosperity, and safety. Both state and non-state cyber actors threaten our infrastructure and provide avenues for foreign malign influence threats against our democracy. We will see continuing potential for surges in migration from Afghanistan, Latin America, and other poor countries, which are reeling from conflict and the economic fallout of the COVID-19 pandemic. Economic and political conditions in Latin America continue to spark waves of migration that destabilize our Southern neighbors and put pressure on our Southern border. Finally, ISIS, al-Qa'ida, and Iran and its militant allies will take advantage of weak governance to continue to plot terrorist attacks against U.S. persons and interests, including to varying degrees in the United States, and exacerbate instability in regions such as Africa and the Middle East.

Regional instability and conflicts continue to threaten U.S. persons and interests. Some have direct implications for U.S. security. For example, the Taliban takeover of Afghanistan threatens U.S. interests, including the possibility of terrorist safe havens re-emerging and a humanitarian disaster. The continued fighting in Syria has a direct bearing on U.S. forces, whereas tensions between nuclear-armed India and Pakistan remain a global concern. The iterative violence between Israel and Iran, and conflicts in other areas—including Africa, Asia, and the Middle East—have the potential to escalate or spread, fueling humanitarian crises and threatening U.S. persons, as in the case of Al-Shabaab, which is leveraging continued instability in East Africa and the lack of security capacity of regional states to threaten U.S. interests and American lives.

The 2022 Annual Threat Assessment Report supports the Office of the Director of National Intelligence's transparency commitments and the tradition of providing regular threat updates to the American public and the United States Congress. The IC is vigilant in monitoring and assessing direct and indirect threats to U.S. and allied interests. As part of this ongoing effort, the IC's National Intelligence Officers work closely with analysts from across the IC to examine the spectrum of threats and highlight the most likely and impactful near-term risks in the context of the longer-term, overarching threat environment.

CHINA

REGIONAL AND GLOBAL OBJECTIVES AND ACTIVITIES

The Chinese Communist Party (CCP) will continue efforts to achieve President's Xi Jinping's vision of making China the preeminent power in East Asia and a major power on the world stage. The CCP will work to press Taiwan on unification, undercut U.S. influence, drive wedges between Washington and its partners, and foster some norms that favor its authoritarian system. China's leaders probably will, however, seek opportunities to reduce tensions with Washington when it suits their interests. China will maintain its statist economic policies because China's leaders see state direction as necessary to reduce dependence on foreign technologies, enable military modernization, and sustain growth—ensuring CCP rule and the realization of its vision for national rejuvenation.

- Beijing sees increasingly competitive U.S.–China relations as part of an epochal geopolitical shift and views Washington's diplomatic, economic, and military measures against Beijing as part of a broader U.S. effort to prevent China's rise and undermine CCP rule.
- The CCP is increasing its criticism of perceived U.S. failures and hypocrisy, including the U.S. withdrawal from Afghanistan and racial tensions in the United States.
- Beijing is increasingly combining growing military power with its economic, technological, and diplomatic clout to strengthen CCP rule, secure what it views as its sovereign territory and regional preeminence, and pursue global influence.
- However, China faces myriad—and in some cases growing—domestic and international challenges that probably will hinder CCP leaders' ambitions. These include an aging population, high levels of corporate debt, economic inequality, and growing resistance to China's heavy-handed tactics in Taiwan and other countries.

China uses coordinated, whole-of-government tools to demonstrate strength and compel neighbors to acquiesce to Beijing's preferences, including its territorial and maritime claims and assertions of sovereignty over Taiwan.

- Beijing will press Taiwan to move toward unification and will react to what it views as increased U.S.–Taiwan engagement. We expect that friction will grow as China continues to increase military activity around the island, and Taiwan's leaders resist Beijing's pressure for progress toward unification. China's control over Taiwan probably would disrupt global supply chains for semiconductor chips because Taiwan dominates production.
- In the South China Sea, Beijing will continue to use growing numbers of air, naval, and maritime law enforcement platforms to intimidate rival claimants and signal that China has effective control over contested areas. China is similarly pressuring Japan over contested areas in the East China Sea.

Beijing will continue to promote the Belt and Road Initiative (BRI) to expand China's economic, political, and military presence abroad. Beijing will adjust its approach to BRI in response to publicity and sustainability challenges, and diversify project selection in an attempt to improve the initiative's brand and minimize international criticism. China also will promote new international norms for technology and human rights,

emphasizing state sovereignty and political stability over individual rights. It will continue to erode the vestiges of freedom in Hong Kong.

China will remain the top threat to U.S. technological competitiveness as Beijing targets key sectors and proprietary commercial and military technology from U.S. and allied companies and institutions. Beijing uses a variety of tools, from public investment to espionage to advance its technological capabilities. Beijing's willingness to use espionage, subsidies, and trade policy to give its firms a competitive advantage represents not just an ongoing challenge for the U.S. economy and its workers, but also advances Beijing's ability to assume leadership of the world's technological advancement and standards.

China will continue deepening diplomatic, defense, and technology cooperation with Russia to challenge the United States.

MILITARY CAPABILITIES

China will continue pursuing its goal of building a world-class military that will enable it to secure what it views as its sovereign territory, establish its preeminence in regional affairs, and project power globally while offsetting perceived U.S. military superiority.

- Beijing is accelerating the development of key capabilities it believes the People's Liberation Army's (PLA) needs to confront the United States in a large-scale, sustained conflict.

The PLA Navy and Air Force are the largest in the region and continue to field advanced platforms that improve China's ability to establish air superiority and project power. The PLA Rocket Force's (PLARF) short-, medium-, and intermediate-range conventional systems can hold U.S. forces and bases in the region at risk. In 2020, the PLARF fielded its first operational hypersonic weapons system, the DF-17 hypersonic glide vehicle-capable medium-range ballistic missile (MRBM), which could challenge U.S. missile defense systems.

We expect the PLA to continue to pursue the establishment of overseas military installations and access agreements to enhance its ability to project power and protect China's interests abroad.

WMD

Beijing will continue the largest ever nuclear force expansion and arsenal diversification in its history. Beijing is not interested in agreements that restrict its plans and will not agree to negotiations that lock in U.S. or Russian advantages. China is building a larger and increasingly capable nuclear missile and bomber force that is more survivable, more diverse, and on higher alert than in the past, including nuclear missile systems designed to manage regional escalation and ensure an intercontinental strike capability in any scenario.

- China is building hundreds of new intercontinental ballistic missile (ICBM) silos.
- As of 2020, the People's Liberation Army Air Force (PLAAF) had operationally fielded the nuclear-capable H-6N bomber, providing a platform for the air component of the PRC's nascent nuclear triad.
- China conducted a hypersonic glide vehicle (HGV) flight test that flew completely around the world and impacted inside China.

SPACE

Beijing is working to match or exceed U.S. capabilities in space to gain the military, economic, and prestige benefits that Washington has accrued from space leadership.

- China's space station began assembly and crewed missions in 2021, with full operational capability expected between 2022 and 2024. China also plans to conduct additional lunar exploration missions, and it intends to establish a robotic research station on the Moon and later, an intermittently crewed lunar base.
- The PLA will continue to integrate space services—such as satellite reconnaissance and positioning, navigation, and timing—and satellite communications into its weapons and command-and-control systems to erode the U.S. military's information advantage.

Counterspace operations will be integral to potential military campaigns by the PLA, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites. The PLA is fielding new destructive and nondestructive ground- and space-based antisatellite (ASAT) weapons.

CYBER

We assess that China presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks. China's cyber pursuits and export of related technologies increase the threats of attacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its control, and the expansion of technology-driven authoritarianism globally.

- China almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems.

China leads the world in applying surveillance and censorship to monitor its population and repress dissent, particularly among minorities. Beijing conducts cyber intrusions that affect U.S. and non-U.S. citizens beyond its borders—such as hacking journalists—to counter perceived threats to the CCP and tailor influence efforts.

- China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

MALIGN INFLUENCE

China will continue expanding its global intelligence and covert influence posture to better support the CCP's political, economic, and security goals, increasingly challenging U.S. influence. China is attempting to exploit doubts about U.S. leadership, undermine democracy, and extend Beijing's influence, especially in East Asia and the western Pacific, which Beijing views as its traditional sphere of influence.

- China will continue spreading COVID-19 misinformation and downplaying its early failures while casting blame on the West. Its misinformation includes claims that the United States created COVID-19.

- Beijing probably is reviewing publicly disclosed Russian influence operations and gaining experience from operations that use social media and other technologies against societies in Asia and elsewhere.
- Beijing is intensifying efforts to mold U.S. public discourse, pressure perceived political opponents, and muffle criticism on such issues as religious freedom, suppression of democracy in Hong Kong, and oppression of the Uyghurs as well as other minorities.

RUSSIA

REGIONAL AND GLOBAL OBJECTIVES AND ACTIVITIES

We expect that Moscow will remain an influential power and a formidable challenge to the United States amidst the changing geopolitical landscape during the next decade. It will continue to pursue its interests in competitive and sometimes confrontational and provocative ways, including pressing to dominate Ukraine and other countries in its “near-abroad,” while exploring possibilities to achieve a more stable relationship with Washington.

- We assess that Russia does not want a direct conflict with U.S. forces. Russia seeks an accommodation with the United States on mutual noninterference in both countries’ domestic affairs and U.S. recognition of Russia’s claimed sphere of influence over much of the former Soviet Union.
- Russia’s officials have long believed that the United States is trying to undermine Russia, weaken President Vladimir Putin, and install Western-friendly regimes in the former Soviet states and elsewhere, which they conclude gives Russia leeway to retaliate.

Russia continues to prepare for a military attack against Ukraine, with well over 100,000 troops massed near the Ukraine border, including Russian military forces in Belarus, occupied-Crimea, and the separatist forces in Eastern Ukraine. Moscow is sending more forces. In mid-December 2021, Russia issued a statement demanding that NATO provide formal security guarantees, including putting an end to the possibility that Ukraine might join the Alliance.

We assess that Moscow will continue to employ an array of tools to advance its own interests or undermine the interests of the United States and its allies. These will be primarily military, security, and intelligence tools, with economic cooperation playing a smaller role. We expect Moscow to insert itself into crises when Russia’s interests are at stake, the anticipated costs of action are low, or it sees an opportunity to capitalize on a power vacuum.

Russia probably will continue to expand its global military, intelligence, security, commercial, and energy footprint and build partnerships aimed at undermining U.S. influence and boosting its own.

- In the Middle East and North Africa, Moscow is using its involvement in Syria, Libya, and Sudan to increase its clout, undercut U.S. leadership, present itself as an indispensable mediator, and gain military access rights and economic opportunities.
- In the Western Hemisphere, Russia has expanded its engagement with Venezuela, supported Cuba, and used arms sales and energy agreements to try to expand access to markets and natural resources in Latin America, in part to offset some of the effects of sanctions.
- In the former Soviet republics, Moscow is well positioned to increase its role in the Caucasus and, if it deems necessary, intervene in Belarus and Central Asia to halt instability after widespread anti-government protests, as it did in Belarus after the fraudulent 2020 election and early this year in Kazakhstan.
- We expect Russia to continue to use energy as a foreign policy tool to coerce cooperation and force states to the negotiating table, as it recently did in 2021, when Russia stopped coal and electricity

exports to Ukraine. Russia also uses its capabilities in COVID-19 vaccine development and civilian nuclear reactor construction as a soft-power tool in its foreign policy.

Russia uses corruption as an effective foreign policy tool to further its geopolitical goals and buy influence in other countries; however, it also serves as a long-term domestic vulnerability as well as a drag on Russia's economic performance and ability to attract investment.

- Russia has used corruption to help develop networks of patronage in countries, including Hungary, Bulgaria, Slovakia, and Ukraine, to influence decisionmaking, and help carry out Russia's foreign policy objectives.
- Russians regularly identify corruption as one of the country's biggest problems, which has been a recurrent cause of public protests and a key theme of imprisoned Russian opposition figure Aleksey Navalnyy's campaign against the Kremlin.
- We assess that Russia would need to reduce corruption and state control of the economy, and improve the rule of law in Russia to attract investment and expand growth beyond 1-3 percent per year.

MILITARY CAPABILITIES

We expect Moscow to sustain military modernization and enhance its armed forces, enabling it to defend Russia's national security while projecting influence globally and challenging the interests of the United States and its allies. Despite slow growth in defense spending, Russia will emphasize the development and acquisition of new weapons that present increased threats to the United States and regional actors while continuing its foreign military engagements, conducting training exercises, and incorporating lessons from its involvement in conflicts in Syria and Ukraine.

- Moscow has the wherewithal to deploy forces in strategically important regions, but the farther it deploys from Russia, the less able it probably will be to sustain intensive combat operations.
- Wagner group and other private security companies managed by Russian oligarchs close to the Kremlin extend Moscow's military reach at low cost in areas ranging from Syria to the Central African Republic and Mali, allowing Russia to disavow its involvement and distance itself from battlefield casualties.

WMD

We assess that Russia will remain the largest and most capable WMD rival to the United States for the foreseeable future as it expands and modernizes its nuclear weapons capabilities and increases the capabilities of its strategic and nonstrategic weapons. Russia also remains a nuclear-material security concern, despite improvements to material protection, control, and accounting at Russia's nuclear sites since the 1990s.

- Moscow views its nuclear capabilities as necessary for maintaining deterrence and achieving its goals in a potential conflict against the United States and NATO, and it sees a credible nuclear weapons deterrent as the ultimate guarantor of the Russian Federation.
- Moscow continues to develop long-range nuclear-capable missile and underwater delivery systems meant to penetrate or bypass U.S. missile defenses.

- Russia is expanding and modernizing its large, diverse, and modern set of nonstrategic systems, which are capable of delivering nuclear or conventional warheads, because Moscow believes such systems offer options to deter adversaries, control the escalation of potential hostilities, and counter U.S. and allied troops near its border.

CYBER

We assess that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. We assess that Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions, as well as a deterrence and military tool.

- Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.
- Russia is also using cyber operations to attack entities it sees as working to undermine its interests or threaten the stability of the Russian Government. Russia attempts to hack journalists and organizations worldwide that investigate Russian Government activity and in several instances, has leaked their information.

MALIGN INFLUENCE

Russia presents one of the most serious foreign influence threats to the United States, using its intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances, and increase its sway around the world, while attempting to undermine U.S. global standing, amplify discord inside the United States, and influence U.S. voters and decisionmaking. We assess that Moscow probably will build on these approaches to try to undermine the United States as opportunities arise—Russia and its influence actors are adept at capitalizing on current events in the United States to push Moscow-friendly positions to Western audiences.

- Moscow almost certainly views U.S. elections as opportunities for malign influence as part of its larger foreign policy strategy. Moscow has conducted influence operations against U.S. elections for decades, including as recently as the 2020 presidential election. We assess that it probably will try to strengthen ties to U.S. persons in the media and politics in hopes of developing vectors for future influence operations. Moscow almost certainly will continue these online influence operations in the United States and in countries such as Belarus, Ukraine, and other countries of key Russian interest. Moscow will also continue and seek out new methods of circumventing technology companies' anti-disinformation activities to further expand its narratives globally.

SPACE

Russia will remain a key space competitor, maintaining a large network of reconnaissance, communications, and navigation satellites. Moscow will focus on integrating space services—such as communications; positioning, navigation, and timing; geolocation; and intelligence, surveillance, and reconnaissance—into its weapons and command-and-control systems, allowing Moscow to more quickly identify, track, and target U.S. satellites during a conflict.

In recent years, Russia has focused its efforts on developing its civil and commercial space capabilities. Moscow is capable of employing its civil and commercial remote sensing satellites to supplement military-dedicated capabilities that reduce U.S. ability to perform sensitive military activities undetected. In addition to improving its launch capability, it is working to support human spaceflight for future deep space missions.

Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities, and it is developing, testing, and fielding an array of nondestructive and destructive counterspace weapons—including jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and ground-based ASAT capabilities—to target U.S. and allied satellites.

- Russia is investing in electronic warfare and directed energy weapons to counter western on-orbit assets. These systems work by disrupting or disabling adversary C4ISR capabilities and by disrupting GPS, tactical and satellite communications, and radars.
- Russia continues to develop ground-based direct ascent ASAT weapons capable of destroying space targets in low Earth orbit.

IRAN

REGIONAL AND GLOBAL OBJECTIVES AND ACTIVITIES

Iran will continue to threaten U.S. interests as it tries to erode U.S. influence in the Middle East, entrench its influence and project power in neighboring states, and minimize threats to regime stability. Tehran will try to leverage its expanding nuclear program, proxy and partner forces, diplomacy, and military sales and acquisitions to advance its goals. The Iranian regime sees itself as locked in an existential struggle with the United States and its regional allies, while it pursues its longstanding ambitions for regional leadership.

The election of President Ebrahim Raisi in 2021 has invigorated Supreme Leader Ali Khamenei to try to make progress toward his long-term vision of molding Iran into a pan-Islamic power capable of defending global Muslim causes while tightening its theocratic rule at home.

- The regime is reluctant to directly engage diplomatically with the United States on a renewal of the Joint Comprehensive Plan of Action (JCPOA), even though it still aspires to secure sanctions relief. Iran's hardline officials deeply distrust Washington and do not believe the United States can deliver or sustain any benefits a renewed JCPOA might offer.

We assess that Iran will threaten U.S. persons directly and via proxy attacks, particularly in the Middle East. Iran also remains committed to developing networks inside the United States—an objective it has pursued for more than a decade. Iranian-supported proxies will launch attacks against U.S. forces and persons in Iraq and Syria, and perhaps on other countries and regions. Iran has threatened to retaliate against former and current U.S. officials for the killing of Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) Commander Qasem Soleimani in January 2020, and has previously attempted to conduct lethal operations in the United States.

- *Iran remains a threat to Israel, both directly through its missile forces and indirectly through its support of Lebanese Hezbollah and other terrorist groups.*
- *Iran will remain a problematic actor across the region with its backing of Iraqi Shia militias, which is the primary threat to U.S. personnel in Iraq. Iran's economically and militarily propping up of a rogue Syrian regime, and spreading instability across Yemen through its support to the Huthis—including a range of advanced military systems—also pose a threat to U.S. partners and interests, including Saudi Arabia.*

MILITARY CAPABILITIES

Iran's hybrid approach to warfare—using both conventional and unconventional capabilities—will pose a threat to U.S. interests in the region for the foreseeable future. The IRGC-QF and its proxies will remain central to Iran's military power.

- Despite Iran's economic challenges, Tehran will seek to improve and acquire new conventional weaponry.
- Iran's unconventional warfare operations and network of militant partners and proxies enable Tehran to advance its interests in the region and maintain strategic depth.

Iran's ballistic missile programs, which include the largest inventory of ballistic missiles in the region, continue to pose a threat to countries across the Middle East. Iran's work on a space launch vehicle (SLV)—including its Simorgh—shortens the timeline to an ICBM because SLVs and ICBMs use similar technologies, if it decided to develop one.

NUCLEAR ISSUES

We continue to assess that Iran is not currently undertaking the key nuclear weapons-development activities that we judge would be necessary to produce a nuclear device. In July 2019, following the U.S. withdrawal from the JCPOA in May 2018, Iran began resuming some activities that exceed JCPOA limits. If Tehran does not receive sanctions relief, Iranian officials probably will consider further enriching uranium up to 90 percent.

- Iran has consistently cast its resumption of nuclear activities as a reversible response to the U.S. withdrawal from the JCPOA and messaged that it would return to full compliance if the United States lifted sanctions and also fulfilled its JCPOA commitments.
- Iran continues to increase the size and enrichment level of its uranium stockpile beyond JCPOA limits. Iran continues to ignore restrictions on advanced centrifuge research and development and continues uranium enrichment operations at the deeply buried Fordow facility. Iran has been enriching uranium hexafluoride (UF₆) up to 60 percent U-235 since April 2021, and continues to accumulate UF₆ enriched up to 20 percent. The IAEA has verified that Iran is conducting uranium metal research and development, including producing laboratory-scale quantities of uranium metal enriched up to 20 percent U-235.

CYBER AND MALIGN INFLUENCE

Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data. Iran's opportunistic approach to cyber attacks makes critical infrastructure owners in the United States susceptible to being targeted by Tehran, especially when Tehran believes it must demonstrate that it can push back against the United States in other domains. Recent attacks on Israeli and U.S. targets show that Iran is more willing than before to target countries with stronger capabilities.

- Iran was responsible for multiple cyber attacks between April and July 2020 against Israeli water facilities. Iran's successful disruption of critical infrastructure in Israel—also a superior cyber power compared with Iran—reflects its growing willingness to take risks when it believes retaliation is justified.

NORTH KOREA

REGIONAL AND GLOBAL OBJECTIVES AND ACTIVITIES

North Korean leader Kim Jong Un will continue efforts to steadily expand and enhance Pyongyang's nuclear and conventional capabilities targeting the United States and its allies, periodically using aggressive and potentially destabilizing actions to reshape the regional security environment in his favor. These actions will include developing and demonstrating capabilities up to and possibly including the resumption of nuclear weapons and ICBM testing.

- We assess that Kim views nuclear weapons and ICBMs as the ultimate guarantor of his totalitarian and autocratic rule of North Korea and believes that over time he will gain international acceptance as a nuclear power. He probably does not view the current level of pressure on his regime, the economic hardships resulting from sanctions and his domestic COVID-19 countermeasures as enough to require a fundamental change in approach.
- Kim also aims to achieve prestige as a nuclear power as well as strategic dominance over South Korea. Kim probably will continue to try to undermine the U.S.–South Korea alliance by vacillating between periods of escalatory behavior and symbolic gestures toward the South to exploit differences between Washington's and Seoul's approach to solving the Korea problem.
- We assess that North Korea continues to engage in illicit activities, including cyber theft and the export of UN-proscribed commodities to fund regime priorities, including Kim's WMD program.

MILITARY CAPABILITIES

North Korea will pose a serious threat to the United States and its allies by continuing to invest in niche capabilities that will provide Kim with a range of options to deter outside intervention, offset enduring deficiencies in the country's conventional forces, and coercively advance his political objectives.

- In early 2021, in a public report to the Eighth Party Congress, Kim identified priorities for developing new weapon systems, such as a nuclear-powered submarine, hypersonic glide vehicles, long-range solid-propellant missiles, and multiple independently targetable reentry vehicles (MIRV). Although some of these capabilities are longer-term projects, we assess that they represent Kim's commitment to expanding and diversifying his arsenal over time.

Kim is continuing to prioritize efforts to build an increasingly capable missile force designed to evade U.S. and regional missile defenses. Kim probably will continue to order missile tests—including of short-range ballistic missiles (SRBMs), cruise missiles, submarine-launched ballistic missiles (SLBMs), and HGVs—to validate technical objectives, reinforce deterrence, and normalize Pyongyang's missile testing.

- In September 2021, North Korea claimed for the first time to have tested an HGV that probably would be capable of reaching regional targets. North Korea followed with two more claimed hypersonic missile flight tests in January 2022, demonstrating its commitment to continued development of hypersonic weapons.

WMD

Kim remains strongly committed to expanding the country's nuclear weapons arsenal and continuing ballistic missile research and development. North Korea's continued development of ICBMs, IRBMs, and SLBMs demonstrates its intention to bolster its nuclear delivery capability.

- Fissile material production continues in North Korea, which maintains its plutonium program and probably is expanding its uranium enrichment program.

In January, North Korea began laying the groundwork for an increase in tensions that could include ICBM or possibly a nuclear test this year—actions that Pyongyang has not taken since 2017. Flight tests are part of North Korea's effort to expand the number and type of missile systems capable of delivering nuclear warheads to the entire United States.

- North Korea continues to seek a sea-based nuclear-strike capability. In October 2021, North Korea flight tested a new SLBM.

North Korea's chemical and biological weapons (CBW) capabilities remain a threat, and the IC is concerned that Pyongyang may use such weapons during a conflict or in an unconventional or clandestine attack.

CYBER

North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang is well positioned to conduct surprise cyber attacks given its stealth and history of bold action.

- Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States.

Cyber actors linked to North Korea have conducted espionage efforts against a range of organizations, including media, academia, defense companies, and governments, in multiple countries.

HEALTH SECURITY

INFECTIOUS DISEASES AND THE IMPACT OF THE COVID-19 PANDEMIC

The COVID-19 pandemic has killed millions of people and disrupted life worldwide, with far-reaching effects extending well beyond global health to the economic, political, and societal spheres. Although the most severe health impacts of COVID-19 are lessening as global vaccination coverage increases and natural immunity builds, countries worldwide will continue to grapple with COVID-19 during the next year. The socioeconomic and political implications of the pandemic will ripple through the world for years.

The economic fallout from the pandemic is likely to continue to challenge governments and hold back human development and wellbeing, particularly in low-income countries. Societal discontent resulting from these conditions could worsen instability in some countries and fuel surges in international migration, as people grow more desperate in the face of interlocking pressures that include sustained economic downturns.

- The COVID-19 pandemic will continue to increase debt burdens, constrain government spending by poor countries, and cause persistent job insecurity, in turn undermining economic and political stability, particularly in low-income countries. Although global trade shows signs of bouncing back from the COVID-19-induced slump, economists caution that any recovery this year could be disrupted by ongoing or expanding pandemic effects, keeping pressure on many governments to focus on internal economic stability.
- The economic fallout from COVID-19, combined with conflict and weather extremes, has driven hunger worldwide to its highest point in more than a decade, which increases the risk of instability. The number of people facing acute food insecurity doubled from 135 million in 2019 to more than 270 million in 2020, and is projected to continue rising.

COVID-19 is likely to continue to strain health systems and create conditions that could facilitate the spread of other infectious diseases globally, including to the U.S. homeland.

- The pandemic has significantly disrupted essential health services—for example, causing healthcare worker shortages, delays in non-emergency procedures, or avoidance of healthcare facilities because of fears of becoming infected with COVID-19—which are likely to worsen health outcomes and continue to hamper countries' abilities to control disease, particularly low and middle-income countries.
- Influenza and other seasonal respiratory diseases could surge to abnormally high levels in 2022 with the reduction of COVID-19 mitigation measures, which have dampened circulation of these diseases since early 2020, and in turn reduced the level of population immunity to these infections.

Countries globally remain vulnerable to the emergence of a novel pathogen that could cause a devastating new pandemic. Drivers for disease emergence persist and are on the rise, including deforestation and other human encroachment into unsettled land, wildlife harvesting and trade, livestock production, and climate change. These drivers are compounded by factors that facilitate global spread, such as international travel and trade, inadequate global disease surveillance and control, distrust of public health authorities, health disinformation, and health system strain brought on by the COVID-19 pandemic. Emerging agricultural

diseases—even those that do not harm humans directly—threaten to cause immense economic damage and disruption to food supplies if they spread globally or into new regions.

COVID-19 Origins Assessment

The IC continues to investigate how SARS-CoV-2, the virus that causes COVID-19, first infected humans. The IC assesses that the virus probably emerged and infected humans through an initial small-scale exposure that occurred no later than November 2019. All agencies assess that two hypotheses are plausible explanations for the origin of COVID-19: natural exposure to an infected animal and a laboratory-associated incident.

- Four IC elements and the National Intelligence Council assess with low confidence that the initial SARS-CoV-2 infection was most likely caused by natural exposure to an animal infected with it or a close progenitor virus—a virus that probably would be more than 99 percent similar to SARS-CoV-2. One IC element assesses with moderate confidence that the first human infection with SARS-CoV-2 most likely was the result of a laboratory-associated incident, probably involving experimentation, animal handling, or sampling by the Wuhan Institute of Virology. Analysts at three IC elements remain unable to coalesce around either explanation without additional information.
- Beijing continues to hinder the global investigation, resist sharing information, and blame other countries, including the United States.

BIOLOGICAL WEAPONS

Global shortcomings in preparedness for the pandemic and questions surrounding the origins of the COVID-19 virus and biosecurity may inspire some adversaries to consider options related to biological weapons developments.

- As China, Iran, and Russia continue to publicly tout individual or collaborative efforts to improve biosecurity, they have pushed narratives that further drive threat perceptions, including linking U.S. laboratories abroad to COVID-19 origins, breaches in biosafety, untrustworthy vaccines, and biological weapons. This messaging probably will be amplified in the lead up to the once-every-five-years Review Conference of the Biological and Toxin Weapons Convention, tentatively slated to convene in mid-2022.
- Rapid advances in dual-use technology, including bioinformatics, synthetic biology, and genomic editing, could enable development of novel biological weapons that complicate detection, attribution, and treatment.

ANOMALOUS HEALTH INCIDENTS

We continue to closely examine Anomalous Health Incidents (AHIs) and ensure appropriate care for those affected. IC agencies assess with varying levels of confidence that most reported health incidents can be explained by medical conditions, or environmental or technical factors and that it is unlikely that a foreign actor—including Russia—is conducting a sustained, worldwide campaign involving hundreds of incidents without detection. This finding does not change the fact that U.S. personnel are reporting real experiences, nor does it explain every report. The IC continues to actively investigate the AHI issue, focusing particularly on a subset of priority cases for which it has not ruled out any cause, including the possibility that one or more foreign actors were involved.

CLIMATE CHANGE AND ENVIRONMENTAL DEGRADATION

We assess that climate change will increasingly exacerbate risks to U.S. national security interests as the physical impacts increase and geopolitical tensions mount about how to respond to the challenge. Meanwhile, environmental degradation will increasingly intersect with and worsen climate change effects in many countries, particularly low-income countries.

- Geopolitical tensions are likely to grow as countries increasingly argue about how to accelerate the reductions in net greenhouse gas emissions necessary to meet the Paris Agreement goal of limiting global temperature rise to 1.5°C since pre-industrial times. The current trajectory of growing global greenhouse emissions, based on governments' current policies and pledges, would cause the global temperature rise to reach 1.5°C around 2030, and surpass 2°C by mid-century.
- Countries will debate who bears more responsibility to reduce emissions and who should pay—and countries will compete to control resources and dominate new technologies needed for the clean energy transition. Most countries will face difficult economic choices and probably will count on technological breakthroughs to rapidly reduce their net emissions later. China and India will play critical roles in determining the trajectory of temperature rise.
- The increasing physical effects of climate change are likely to exacerbate domestic and cross-border geopolitical flashpoints producing additional instability. The reduction in sea ice already is amplifying strategic competition in the Arctic over access to its natural resources and shipping routes. Elsewhere, as temperatures rise and more extreme effects manifest, there is a growing risk of conflict over water and migration, particularly after 2030, and an increasing chance that countries will unilaterally test and deploy large-scale solar geoengineering—creating a new area of disputes.
- Scientific forecasts indicate that intensifying physical effects of climate change out to 2040 and beyond will be most acutely felt in low-income countries, which we assess are also the least able to adapt to such changes. These physical effects will increase the potential for instability and possibly internal conflict in some countries, in some cases creating additional demands on U.S. diplomatic, economic, humanitarian, and military resources. Despite geographic and financial resource advantages, the United States and its partners face costly challenges that will become more difficult to manage without concerted effort to reduce emissions and cap warming.

Unsustainable land use, poor water governance, and pollution will intersect with and worsen the effects of climate change, primarily but not exclusively in low-income countries in the near term. The combination of environmental degradation, rising temperatures, changing precipitation patterns, and other climate effects is likely to lead to an array of human challenges such as food and water insecurity and threats to human health.

ADDITIONAL TRANSNATIONAL ISSUES

PREFACE

The pandemic and climate change highlight the challenges that a wide range of transnational issues pose to U.S. national security; we will now address several more priority issues. Some have a direct and immediate impact on U.S. interests, such as narcotics trafficking and terrorism. Others seem to be building for the future, or pose chronic, indirect challenges, such as corruption. These issues also vary in the scope of the threats they pose, having broad, global impact or causing local, even individual harm.

Transnational threats interact in a complex system along with more traditional threats such as great power competition, often reinforcing each other and creating compounding and cascading risks to U.S. national security. Underpinning many of the threats are weak or poor governance and geopolitical competition. During the past decade, an erosion of democracy around the world, strains in U.S. alliances, and challenges to accepted, international norms have made it more difficult to tackle transnational challenges such as climate change and the pandemic while creating greater opportunities for rogue governments and groups to operate with impunity. Increasing interconnections among countries—ranging from supply chains to social media—have also created new opportunities for transnational interference and conflict.

Corruption illustrates the complexity of the transnational issues, the relationships among them, and the range of their implications for U.S. interests. Corruption is a chronic challenge but thrives particularly in poorly governed countries. It can undermine weak governments and economies, contributing to political instability, organized crime, and disputes over migration—all of which in turn can fuel greater corruption. Corruption in international transactions can directly cost U.S. exporters billions of dollars in sales, give U.S. adversaries geopolitical openings, and prop up regimes that abuse human rights. However, corruption also can be a positive—undermining the capacity and credibility of authoritarian regimes.

Several transnational challenges stand out for the clear and direct threats they will pose to U.S. interests during the coming years. Among these are the rapid development of destabilizing technologies, including some that are transforming the battlefield, the threats posed by transnational organized crime and terrorism, and the challenge of international migration.

INNOVATIVE USE OF NEW TECHNOLOGY

Multiple trends are shaping the technology landscape of the next decades. The increasing convergence of seemingly unrelated fields and the rise of global competition to generate and lock in advantage are leading to a global diffusion of emerging technologies, shrinking timelines for development and maturation of technologies, and increasingly blurred lines between commercial and military endeavors, particularly in fields with broad impact across societies and economies, such as artificial intelligence (AI), biotechnologies, robotics and automation, and smart materials and manufacturing.

- Emerging technologies are rapidly improving a broad range of human experiences and capabilities, but at least in the short term, these same technologies are disrupting longstanding systems and societal dynamics, forcing individuals, communities, and governments to adjust and find new ways of living, working, and managing. As with any disruption, some will thrive whereas others will struggle, potentially facing increasing inequalities and imbalances.

Novel uses of both mature and new technologies are proliferating among a growing number of state and non-state actors, posing direct and growing threats to traditional pillars of U.S. military power, such as secure rear-area lines of communication and mobilization, air and space dominance, and power projection. The threats posed by new technologies will ultimately hinge on how they are operationalized by individual actors, each driven by unique goals, perceptions, strengths, and vulnerabilities.

- One of the most significant, ongoing trends in new military technology and weaponry is the growing combination of high speed, long range, greater maneuverability, and pinpoint accuracy. These advances are improving actors' ability to strike across continents as well as regionally or locally with UAVs, guided rockets, artillery shells, and mortars. Long-range precision strike inventories are likely to include increasing numbers of hypersonic and highly maneuverable systems that present a daunting challenge to those trying to develop countermeasures to detect, track, and intercept such fast-moving and maneuverable weapons. Many technologies previously available only to the advanced, industrial nations are trickling down to smaller and less expensive systems thereby becoming more available worldwide, as seen in recent battlefield use of UAVs by Azerbaijan and Ethiopia.
- Some technologies—such as hypersonic systems and nascent efforts to operationalize military AI—probably will remain within the purview of great powers and wealthier states, but relatively low cost and more widely available systems ranging from cyber tools to unmanned aerial and naval vehicles could be exploited by lesser powers and non-state actors to achieve high impact and even strategic-level effects.
- We are in the midst of a rapid expansion of state and non-state use of unmanned vehicles in both the air and sea domains, which could disrupt the status quo in part because air and naval defense often hinge on the assumption that the primary threat stems from a relatively small number of crewed platforms or ground-based missiles.

TRANSNATIONAL ORGANIZED CRIME

Global transnational criminal organizations (TCOs) pose a direct threat to the United States through human trafficking, the production and trafficking of lethal illicit drugs, cyber crime, and financial crimes and money laundering schemes eroding the integrity of the international financial system. Cyber criminals, in addition to phishing and other online fraud schemes, are also increasing their ransomware attacks. TCO activities also indirectly threaten U.S. national security by compounding and aggravating corruption, violence, and challenges to governance that undermine the rule of law in partner nations, spurring violence, driving atrocities, and contributing to migration.

- Human trafficking, including sex trafficking and forced labor, is not only a violation of human rights and freedoms but a threat to U.S. national security and economic development and is enabled by corrupt actors and networks that fuel the growth of transnational organized crime.

Foreign Illicit Drugs

Illicit drug trafficking by TCOs, particularly synthetic drugs, endangers the health and safety of millions of U.S. citizens and imposes as much as one trillion dollars in direct and indirect economic losses. The threat from illicit drugs is at historic levels, with more than 100,000 American drug-overdose deaths for the first time annually, driven mainly by a robust supply of synthetic opioids from Mexican TCOs.

- Mexican TCOs are the dominant producers and suppliers of illicit drugs for the U.S. market. They produce fentanyl, heroin, methamphetamine, and marijuana in Mexico, and obtain cocaine from South America to smuggle into the United States. Mexican TCOs probably will seek to continue expanding their capacity to produce finished fentanyl.
- Since 2019, Mexican TCOs have shifted from importing finished fentanyl from China to synthesizing fentanyl from precursor chemicals, primarily also from China, partly because of China's fentanyl class controls. Mexican TCOs are able to circumvent international controls on precursor chemicals by changing analogues and methodologies for synthesizing and producing synthetics.
- Turf battles among Mexican TCOs vying for drug routes and territory have resulted in steady, high homicide rates since 2018 that are four times the rate of homicides in the United States. In parts of Mexico, TCOs use billions of dollars of drug proceeds to intimidate politicians and influence elections, as well as recruit and arm fighters capable of directly confronting government security forces.

Money Laundering and Financial Crimes

TCOs exploit the U.S. financial, services, and manufacturing sectors by conducting complex money laundering and fraud schemes.

- TCOs generate hundreds of billions of dollars of revenue by trafficking illicit drugs and other goods and people; conducting extortion and racketeering that targets U.S. persons; producing and selling counterfeit and stolen goods in U.S. markets; and running financial fraud schemes.

Cyber Crime

Transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide. These criminals are driven by the promise of large profits, reliable safe havens from which to operate, and a decreasing technical barrier to entry for new actors.

- Many major transnational cybercrime groups have diversified business models that engage in direct wire-transfer fraud from victims, or use other forms of extortion alongside or in place of ransomware. In 2020, business-e-mail compromise, identity theft, spoofing, and other extortion schemes ranked among the top five most costly cybercriminal schemes.

U.S. Government entities, businesses, and other organizations face a diverse range of ransomware threats. Attackers are innovating their targeting strategies to focus on victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions, driving ransomware payouts up.

MIGRATION

In the Western Hemisphere, factors such as longstanding poor socioeconomic conditions, perceived changes in U.S. immigration policy, and employment opportunities in the United States will continue to drive migration to the Mexico-U.S. border; a growing number of people from around the world see transiting Mexico as a way to reach the United States. High crime rates, violence, corruption, weak job markets, and poor living conditions remain

primary push factors for U.S.-bound migration from Central America and Haiti because origin countries lack the capacity to address these challenges.

- Eased COVID-19-related travel restrictions and perceptions of greater job opportunities in a recovering U.S. economy are contributing to a rise in migration. These dynamics, along with perceptions of U.S. immigration policies, will determine the flow of migrants this year.

Economic disparities and the effects of conflict and extreme weather will encourage internal and international migration and refugee flows. Migration and displacement will heighten humanitarian needs, increase the risk of political upheaval, exacerbate the risk of other health crises, and aid recruitment and radicalization by militant groups—particularly as COVID-19 strains global humanitarian response mechanisms.

- The number of people displaced within their own national borders continues to increase, straining governments' abilities to care for their domestic populations and mitigate public discontent. Afghanistan is likely to be a growing source of global migration in 2022, as a result of reduced international support, deteriorating economic conditions, and repressive Taliban regime governance.

Transnational organized criminal groups exploit migrants through extortion, kidnapping, human trafficking, and forced labor.

Conflicts in the Middle East, Africa, and Europe, aggressive Russian actions on the periphery of Europe, a possible renewal of Belarusian efforts to fuel the migrant crisis along its border with Poland and Lithuania, and the Taliban takeover of Afghanistan could trigger more migration to Europe this year and a nationalist backlash. Countries are witnessing the rise of populist politicians and parties campaigning on loss of sovereignty and identity.

- The UNHCR estimated that 500,000 Afghan refugees could attempt to cross into surrounding countries if the situation in Afghanistan did not stabilize and is working with surrounding countries to prepare for Afghan refugee arrivals.
- Conflict in Ethiopia's Tigray region since November 2020 has worsened humanitarian conditions and resulted in at least 2.1 million internally displaced persons. The ongoing conflict has also led to refugees fleeing to neighboring countries, which could destabilize the region resulting in additional migrants seeking to travel to Europe.

GLOBAL TERRORISM

Terrorism remains a persistent threat to U.S. persons and interests at home and abroad. Individuals and small cells inspired by a variety of ideologies and personal motivations—including Sunni violent extremism, racially or ethnically motivated violent extremism, and militia violent extremism—probably present the greatest terrorist threat to the United States. ISIS, al-Qa'ida, and terrorists aligned with Iran such as Lebanese Hizballah, probably pose the greatest threat to U.S. persons and interests abroad. Consistent U.S. and allied counterterrorism pressure has degraded the external attack capabilities of ISIS and al-Qa'ida, but they still aspire to conduct attacks in the United States. Communal conflict, insurgency, and instability almost certainly will provide terrorist groups continued opportunities to recruit members, acquire funds, and establish or expand safe havens from which to plot attacks—including reviving safe havens in Afghanistan. Local insurgencies have at times bolstered their Sunni jihadist credentials to fully assimilate into ISIS and al-Qa'ida, allowing them to strengthen and resulting in increased attacks, lethality, and territorial influence and

control. Terrorists remain interested in using chemical and biological agents in attacks against U.S. interests and possibly the U.S. homeland.

ISIS

ISIS leaders remain committed to their vision of building a self-styled global caliphate headquartered in Iraq and Syria and are working to rebuild capabilities and wear down opponents until conditions are ripe for seizing and holding territory. The threat from ISIS against U.S. persons and interests probably will remain greatest in regions where the group has an operational presence; ISIS's ideology and propaganda, however, almost certainly will continue to inspire attacks in the West, including in the United States.

- In Iraq and Syria, ISIS probably will prioritize attacks on local military and civilian targets to erode its opponents' will to fight, maintain relevance among members and supporters, and stoke religious and ethnosectarian tension. ISIS has slowed its operational tempo in Iraq and Syria, probably because of logistical, financial, personnel, and leadership shortfalls. The group remains intent on freeing some of the 10,000 ISIS fighters who remain in detention in northeast Syria.
- In Afghanistan, ISIS-Khorasan is attempting to exploit an influx of funds and personnel from prison breaks to undermine the Taliban and build an external attack capability if it can withstand Taliban pressure.

Al-Qa'ida

Al-Qa'ida has increasingly devolved operational responsibility to regional affiliates as it has shifted away from centrally directed plotting. Because of leadership and battlefield setbacks, al-Qa'ida is constrained in its efforts to lead a unified global movement, but it will try to maintain its presence in Afghanistan and capitalize on permissive operating environments.

Al-Qa'ida remains intent on striking U.S. interests; it is more capable of striking U.S. interests in the regions where its affiliates operate rather than in the Homeland. The primary threat to the United States abroad from al-Qa'ida emanates from the countries where its strongest affiliates currently operate—Yemen, Somalia, and West Africa—and will vary based on local circumstances, including affiliate leadership priorities and battlefield conditions.

Al-Qa'ida senior leaders lack an operational presence in Afghanistan, and the group's affiliate, al-Qa'ida in the Indian Subcontinent (AQIS) is weak. Al-Qa'ida and AQIS praised the Taliban's return to power and are likely to maintain their ties to the Taliban regime.

- Al-Qa'ida probably will gauge its ability to operate in Afghanistan under Taliban restrictions and will focus on maintaining its safe haven before seeking to conduct or support external operations from Afghanistan.

Hizballah

Lebanese Hizballah will continue to work with Iran to develop terrorist capabilities as a complement to the group's growing conventional military capabilities.

- Hizballah seeks to reduce U.S. influence in Lebanon and the broader Middle East, and maintains the capability to target U.S. persons and interests in the region, worldwide, and—to a lesser extent—in the United States.

Foreign Racially or Ethnically Motivated Violent Extremists

Foreign Racially or Ethnically Motivated Violent Extremists (REMVE) very likely will continue to pose a threat to the United States and its allies. These actors continue to rely on transnational ties and adapt violent extremist narratives around current events, including the U.S. and coalition departure from Afghanistan last August.

Foreign REMVEs draw on a diverse range of ideologies, including white supremacy, neo-Nazism, exclusionary cultural-nationalist beliefs, and racial conspiracy theories. Foreign REMVEs organize primarily on a number of online platforms, especially podcasts, applications, and encrypted social media platforms.

- In mid-2021, foreign REMVEs in Europe sought to exploit popular fears of a potential Afghan refugee crisis similar to the influx of refugees from Syria in 2015 and 2016. Xenophobic sentiments have prompted an increasing number of individuals to engage with foreign REMVE groups in Europe.

CONFLICTS AND INSTABILITY

SOUTH ASIA

Afghanistan

The Taliban takeover is rolling back social changes of the past two decades and deepening Afghanistan's humanitarian crisis, heightening prospects for increased migration and displacement.

- The Taliban has been organizing its new regime with a bias for longtime stakeholders. Many of the people named to senior positions served in the Taliban's last government and are under international sanction. Few ethnic minorities and no women have been selected, and the Taliban is likely to keep resisting international pressure to govern more inclusively.
- Across the country, most girls' schools are closed, and all but a few women have been told to stay home from work. In some areas, public punishments have returned, along with restrictions on beard length and media controls. However, near-term prospects for regime-threatening resistance are low because large swathes of the Afghan public are weary of war and fearful of Taliban reprisals, and armed remnants lack strong leadership and external support.
- Taliban leaders lack the resource base and technical capacity to prevent a major economic contraction. They probably will rely on humanitarian aid to sustain some basic services and would rather preside over a more rudimentary economic system and tax the drug trade than accept international conditions for additional assistance.
- A majority of Afghans are suffering food insecurity because of the effects of conflict, drought, and COVID-19 disruptions, and further deterioration almost certainly will increase internal displacement, which could lead to international migration. Refugee flows could spike if the Taliban attempted to relieve pressure by allowing larger populations to leave Afghanistan or conditions sharply deteriorated.
- Regional powers will continue to narrow their interests and seek to develop transactional arrangements with the Taliban while proceeding cautiously with formal recognition. They would have preferred a more inclusive government, but they are prioritizing stability and are unlikely to intervene in ways that would significantly change Taliban behavior.

India-Pakistan

Crises between India and Pakistan are of particular concern because of the risk—however low—of an escalatory cycle between two nuclear-armed states. Pakistan has a long history of supporting anti-India militant groups; under the leadership of Prime Minister Narendra Modi, India is more likely than in the past to respond with military force to perceived or real Pakistani provocations, and each side's perception of heightened tensions raises the risk of conflict, with violent unrest in Kashmir or a militant attack in India being potential flashpoints.

India-China

Relations between New Delhi and Beijing will remain strained in the wake of the lethal clash in 2020, the most serious in decades. We assess that the expanded military postures by both India and China along the disputed border elevates the risk of armed confrontation between two nuclear powers that might involve direct threats to U.S. persons and interests and calls for U.S. intervention. Previous standoffs have demonstrated that persistent low-level friction on the Line of Actual Control (LAC) has the potential to escalate swiftly.

OTHER REGIONS

Internal and interstate conflict and instability will continue to pose direct and indirect threats to U.S. persons and interests during the next year. Several threats, which we assess to be particularly important, are discussed below.

Near East

The Middle East will remain a region characterized by persistent conflict, with active insurgencies in several countries, sparring between Iran and other countries, and terrorism and protest movements sparking occasional violence. Domestic volatility will persist as popular discontent and socioeconomic grievances continue to rise, particularly as the region contends with the economic fallout from the COVID-19 pandemic, increasing the risk of internal or international conflict that would threaten U.S. persons and national security interests.

- Iran-backed Shia militias are likely to continue attacks against U.S. targets in Iraq, and ISIS remains a persistent threat. U.S. personnel would also face danger if popular protests against government corruption, continued dysfunction in the wake of the elections in October 2021, and poor economic conditions took a more violent turn, or if Baghdad became embroiled in a broader regional conflict.
- Conflict, economic hardship, and humanitarian crises will plague Syria during the next few years, and threats to U.S. forces will increase. President Bashar al-Asad will rely on the support of Russia and Iran and the nascent progress he has made reintegrating Syria into the region to stall meaningful peace negotiations. U.S. forces in eastern Syria will face continued threats from Iran, Iran-backed militias, and Syrian regime-aligned groups. ISIS and Hurras al-Din probably will plan and could attempt to launch attacks on the West from their safe havens in the country and increased fighting or further economic decline could spur another wave of migration.

There is some prospect to reduce conflicts that threaten U.S. persons and interests in the Middle East. Countervailing factors—heightened fear of Iran, doubts about U.S. reliability, and economic imperatives—are encouraging efforts to deescalate conflicts. Relations between Israel and select Arab states continue to warm, Qatar's isolation from its neighbors is waning, some Arab states are working to normalize relations with Damascus and encourage its return to the Arab league, and key Gulf states are talking with Iran, including its key rival, Saudi Arabia.

East Asia

In addition to Beijing's provocative behavior in numerous parts of Asia, domestic developments in some East Asian countries risk exacerbating underlying tensions with the potential to produce unrest and violence.

- Burma's security and economic conditions probably will continue to deteriorate because both the regime and the opposition are relying on the use of force in an attempt to break the ongoing political stalemate and advance their respective positions. Both sides remain entrenched in their positions and neither are able to decisively prevail. Economic deterioration and ongoing violence in addition to the ongoing COVID-19-pandemic will amplify the country's deteriorating humanitarian conditions, such as population displacement, food insecurity, and a poorly functioning health care system.

Western Hemisphere

Latin America and the Caribbean almost certainly will see hotspots of volatility in the coming year, undermining or distracting reliable U.S. partners from improving living conditions, tackling illicit flows, addressing climate change, and warding off foreign influence. In many cases, the COVID-19 pandemic has intensified high levels of public discontent with worsening longstanding poor socioeconomic conditions and public services that manifested in large anti-government protests. Elevated levels of U.S.-bound migration from Latin America and the Caribbean region will persist into at least mid-2022 because the underlying economic and insecurity drivers will remain unchanged, and migrants view the U.S. labor market and immigration policies and enforcement as favorable.

Africa

Sub-Saharan African governments will exhibit clear agency in their foreign affairs as the international community recognizes the importance of the region to its economic and security interests. Large numbers of U.S. citizens will be at risk from conflict in several countries. As the region seeks to reinvigorate its upward trajectory following the social and economic effects of the COVID-19 pandemic, it will continue to face unstable commodities prices, poor service delivery and endemic corruption, stresses of extreme weather events, and insecurity because of terrorism, insurgency, sectarian violence, and political instability.

- East Africa probably will see new bouts of conflict in the coming year as the region becomes increasingly strained by the civil war in Ethiopia, power struggles within the transitional government in Sudan, continued instability in Somalia, and a potentially contentious election in Kenya. In Ethiopia, the prospects for a long-term ceasefire remain slim because the belligerents probably do not believe the other side will negotiate in good faith or have a right to be at the table, increasing the prospects for continued conflict, atrocities, and food insecurity. Sudan is almost certainly starting on a protracted and fragile path towards civilian governance that will depend on reconciliation between three opposing elements: the guarded security leadership, the fragmented political coalition, and the mercurial street. In Somalia, leaders' myopic focus on politicking has led to government paralysis, widening the opening for al-Shabaab and raising the risk of recurring outbreaks of violence in Mogadishu.
- In West Africa, a volatile mixture of democratic backsliding, intercommunal violence, and terrorism will threaten the region's stability. Recent undemocratic transfers of power in Burkina Faso, Chad, Guinea and Mali highlight the region's fragility and in some cases the belief among publics that their government are not able to effectively deliver services or managing expanding insecurity. Some of the leaders who remain in power are turning to autocratic, state-centric, and religious governance practices, with some prioritizing security in key urban centers while ceding rural territory to jihadists.

