AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 117–81

OPEN HEARING: 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

FIRST SESSION

WEDNESDAY, APRIL 14, 2021

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
45–487 PDF WASHINGTON : 2021

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
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
MICHAEL F. BENNET, Colorado
BOB CASEY, Pennsylvania
KIRSTEN E. GILLIBRAND, New York

RICHARD BURR, North Carolina
JAMES E. RISCH, Idaho
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
TOM COTTON, Arkansas
JOHN CORNYN, Texas
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

APRIL 14, 2021

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

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

WEDNESDAY, APRIL 14, 2021

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

The Committee met, pursuant to notice, at 10:06 a.m., in Room SH–216, Hart Senate Office Building, Hon. Mark R. Warner (Chairman of the Committee) presiding.

Present: Senators Warner, Rubio, Feinstein, Wyden, Heinrich, King (via WebEx), Bennet, Casey, Gillibrand (via WebEx), 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, and a welcome to our witnesses:

Director of National Intelligence, Avril Haines; Director of the Central Intelligence Agency, Bill Burns; Director of the Federal Bureau of Investigation, Chris Wray; Director of National Security Agency, General Paul Nakasone; and Director of Defense Intelligence Agency, Lieutenant General Scott Berrier.

Thank you for being here this morning and for representing the thousands of dedicated men and women of America's Intelligence Community.

Every year since 1994, the Senate Intelligence Committee has held an open, unclassified worldwide threats hearing, so that the American people can hear directly from the heads of the intelligence agencies about the various threats to our peace and prosperity. It is important that this hearing be conducted publicly and openly to ensure that Americans have a good understanding from a trusted, objective source of the challenges and also the opportunities we face as a Nation.

I was dismayed last year when the Director of National Intelligence refused to appear in public before our Committee for this hearing. And I am pleased that we are resuming this tradition, and look forward to continuing on an annual basis.

We look to our intelligence agencies to provide their best and most objective analytic judgments to our policymakers, regardless of which party happens to be in power. Intelligence is the eyes and ears we rely upon to provide warnings of both immediate and longer-range threats. And we must be sure that the intelligence and analysis is free of bias and not shaded in any way to fit a particular policy or agenda.

We are still in the grips of a global pandemic, though increasingly rapid deployment of effective vaccines is bringing it to bay. In addition to addressing the challenges to national security you see from the pandemic, I'd also like for each of you to address how your agencies and the IC as a whole have dealt with this challenge.

While some agencies have been able to exercise the flexibility of a remote workforce, intelligence is often a profession that relies on in-person attendance due to its classified nature. Some agencies have done very well in vaccinating their personnel. Others have lagged, frankly, far behind, and I'd like to hear how each of your agencies plans to speed up these vital vaccinations to keep the workforce healthy and safe.

As this hearing will no doubt illustrate, the work of the IC is more important than ever. The threat assessment goes into wide detail on a variety of challenges that we face, but I have some issues in particular I'd like to address: cybersecurity, election security, the rise in domestic violent extremism, and obviously the rise of China and particularly the Chinese Communist Party.

On that final point, I want to be extremely clear about something. As we grapple with the challenges posed by a rising China, our problem is with the Chinese Communist Party, not with the Chinese people or the Chinese Diaspora globally. And certainly not with Asian-Americans here in the United States. I want to caution our fellow Americans that false equivalence only breeds submission, division, and hate, and plays right into Beijing's hands.

As China grows in power and stature, the CCP has sought to undercut the United States as the world's leading technological power. We see this in the reliance on both strategic investments and traditional espionage to acquire intellectual property; their use and export of surveillance technology to authoritarian regimes; and their modernization of traditional and asymmetric military capabilities, including in the space and cyber domains.

When we look at development, for example, of 5G technology, we've seen the CCP act aggressively to influence international standard-setting bodies and invest in a national champion, Huawei, that threatens to dominate the worldwide telecommunications market. I fear that the CCP will develop a similar strategy to dominate the development of other emerging technologies, including AI, quantum computing, and BAU technology. In many ways, the IC is the only part of our overall enterprise that sees across all domains in this field, and I think we must be clear-eyed in assessing the threats posed by the CCP.

In the cyber domain, Russia was responsible for an incredibly sophisticated hack of government and private-sector systems, using software updates from what appeared to be a trusted provider in SolarWinds. Other adversaries also have the capability to undertake destructive attacks of critical infrastructure. We've also seen major hacks, such as the Hafnium attack on Microsoft Exchange users, producing serious consequences for United States networks.

In order to deter these intrusions, we will need to accurately and quickly attribute them and hold our adversaries accountable. The SolarWinds hack offered a stark reminder that if there is no requirement to report breaches of critical infrastructure—if FireEye, for example, had not come forward—we might still be in the dark today. And I think when we had our hearing on the subject, there was uniform, bipartisan agreement that we needed to move forward.

And we also want to develop new international norms where certain types of attacks, whether it be on updates or other areas, or frankly viewed on an international basis or prohibited or banned, just as use of chemical or bioweapons is banned in other domains.

Also related is the ongoing threat of misinformation and disinformation, especially when it targets America's free and democratic elections. As the IC noted in its recent assessment, Russia undertook a sophisticated disinformation campaign in 2020 to undercut our current President and to bolster the candidacy of the former one. We need to make clear that those who perpetrated this hostile interference will again pay a price.

The technologies that have made misinformation and disinformation so effective have also been used to great effect by the types of people and groups who attempted an insurrection against our country. But domestic violent extremists were around long before January 6, and they'll continue to pose a significant threat long after we put that incident to rest.

Many of our allies have also identified anti-government extremists as an increasing challenge in their countries. I'd like your thoughts on how the Intelligence Community can or should play a greater role in providing warning of attacks by violent domestic groups, and especially if any of these groups have ties or support for our adversaries overseas.

Lastly, we know the President is going to make an announcement today. We're going to need to discuss the situation in Afghanistan. We went to Afghanistan 20 years ago after the deadly attacks on 9/11 to take away the Taliban's safe haven, and we've worked with our Afghan partners and NATO allies toward that end. As you note in your statement for the record, the Al-Qaeda senior leadership has suffered severe losses in the past few years.

I know on the Committee, we'll have a variety of views about the steps forward. But, speaking at least as Chair, I think any withdrawal that takes place in that country must be conducted in a manner that is coordinated among our military, diplomatic, and intelligence partners, and in close consultation with our NATO allies. We should continue to support the Afghan government, and we must ensure the safety of those dedicated Afghans who have worked closely with the United States over the last 20 years.

I know there are a multitude of other threats that I haven't addressed, but I don't want to steal your thunder, and I look forward to today's very important discussion.

And I'll turn it over to my friend, the Vice Chairman, to make a statement.

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

Vice Chairman RUBIO. Thank you, Mr. Chairman. And I, too, want to welcome all of you for being a part of this hearing this morning to hear of the threats—the assessment of the threats—

that confront our country and our interests around the world. You know, what makes this hearing very unique, it's the one time of year when we've had it—and we haven't had them in a couple years—but it's the one time of year where the American public and the Members of Congress here in the Senate get an unvarnished presentation by an apolitical Intelligence Community of the real national security threats that our country faces.

But I think it's also a good opportunity to remind the men and women of our Nation who we work for and everyone watching what intelligence is. There's a lot of TV shows about intelligence. There's a lot of movies. You may have seen a miniseries and everything else. And there's a lot of media reports, some accurate, some not, about the work that occurs in the Intelligence Community.

At its core, the Intelligence Community and our intelligence functions are about three things: gathering information, especially information that adversaries are producing that they don't want us to have—foreign adversaries; analyzing that information to understand what it means, what it could mean, why they're doing it; and then third, using all of that to help inform policymakers in making policy decisions and inform the actions that we take. Those are the three cores of what intelligence work is all about.

It sounds simplistic, but it is incredibly important when it works. When it's working well, our country is spared all kinds of horribles that people never learn about. When it doesn't work, we face sometimes catastrophe and terrible outcomes, and everyone knows about it, and we spend a long time analyzing it.

Our job here on this side of the room is to provide oversight into how you're doing that job, how well you're doing these things, and also to provide you the resources and the authorities and otherwise other things that you might need in order to do those things well. And it's that view that I hope we can hear about what it is we can do to be helpful in that endeavor. Obviously, in the closed session especially, but here in the open one as well.

As far as the threats are concerned, again, not to be overly simplistic, but I would venture to guess that 90-something percent, if not more, of our threats can be tracked to one of five things: China, Russia, Iran, North Korea, or global terrorism. Those five sources comprise a substantial percentage of all the challenges we face in our foreign policy, sometimes in our domestic policy, and certainly in our economics and geopolitics.

A rapidly-evolving technology has helped our country tremendously. It's helped the work you do; it's helped the work we do in public policy. But it's also advantaged our adversaries, none of whom, by the way, are constrained by laws or the sorts of commitments we've made to things like the rule of law or a moral compass and principles when it comes to utilizing things like deepfakes, advanced data analytics, disinformation, misinformation, artificial intelligence, and more. They are completely unrestrained from any of the things that we are restrained by, both in law and morality.

The cyber threat that the Chairman spoke about a moment ago is real, both in our government networks and U.S. critical infrastructure. As a government, we need to, I believe, have a more explicit cyber-deterrence policy that will clearly set expectations for accepted cyber behavior and delineate very clear responses when those lines are crossed.

Today's technology environment allows adversaries to wreak havoc, and they often do so at a minimal cost. The SolarWinds hack illustrates how easily U.S. infrastructure can be compromised. It's not hard to imagine how much destruction could be levied if our adversaries were determine to conduct such an attack beyond espionage on things like the power grid or our water supply. These are 21st-century threats, unimaginable just two decades ago.

The theft of our innovation, often funded innovation that was funded at its basic level by the U.S. taxpayer. That threatens our economic competitiveness. It comes at the expense of our economy, American jobs, American industrial capability. China, for example, as part of its military-civil fusion strategy, has proven itself adept at finding ways for its agents to extract that sort of information from private corporations. It takes full advantage of the robust U.N. scientific research and development industry that capitalism has fostered by sending their agents and, frankly, by threatening and forcing students who study at our laboratories and universities to steal the research and give it to them to benefit the Communist Party. So I look forward to hearing from the FBI in particular as to the work that we're doing to confront the massive threat that this poses.

The insights of the Intelligence Community on the top threats confronting us this year are also critical to better shape our foreign policy, helping us to execute it and understanding whether or not we are achieving our national goals and furthering our national interest. In that regard, as the Chairman already pointed to, is the situation in Afghanistan. It was a decision that was begun under the previous administration and is being brought to its conclusion under the current one. And irrespective of how anyone may feel about it, no one can deny it's going to have serious security implications for our country for years to come.

There's no doubt the Nation is weary of over 20 years of war and certainly the counterterrorism fight. I think it's important to acknowledge two things. The first is that there's a very real possibility that in the very near future, sadly, tragically, in a heartbreaking way, the Taliban will regain control of all or substantial portions of Afghanistan. And that means terrible things for all those people living in that country, but particularly for women and girls.

But the second thing we need to acknowledge is that if they do, there's also a very high likelihood that—in fact, if they do, I think it's almost certain that Al-Qaeda will return to Afghanistan, will use it as a safe haven, and will use it as a launchpad for terrorist attacks against our country, our people—even potentially here in the homeland. And so, I think it's important for us to say, if you look at this year's annual threat assessment, you collectively say, despite leadership losses, terrorist groups have shown great resiliency and are taking advantage of ungoverned areas to rebuild. And that is now, given the status quo today. Imagine when that sustained pressure is no longer in place.

You go on to assess that ISIS and Al-Qaeda remain the greatest Sunni terrorist threats to U.S. interests overseas, that they also seek to conduct attacks inside the United States, although sustained U.S. and allied counterterrorism pressure has broadly degraded their capability to do so. I think it's important, obviously, in the closed session, but here in the public session to the extent possible, to hear not just about the risk that the lack of sustained pressure now poses to our future, but what it would mean in particular to potential attacks on the homeland.

The Intelligence Community can't afford to be complacent for even one minute, which, of course, makes your jobs collectively and individually, and the jobs of the men and women who work for you under you and who you represent here today, a very difficult job. The stakes—this is not an exaggeration—are often literally life and death. And it's not often that you get to appear in public so the American people can get a sense of how important your work is, even though because of the nature of their work, most people will never fully understand how dangerous and important that work can be.

As I said at the outset, the Intelligence Community and the work of our intelligence agencies is depicted in all kinds of ways in the popular culture, in the media, in the darkest recesses of the Internet. But the Intelligence Community that I have come to know through my now ten and a half years on the Committee is one that's made up of patriotic, dedicated professionals, some of the finest men and women who serve in our government and who measure their success and their failure in terms of how many Americans they've kept safe. Many of those Americans who are kept safe do not even know they've been kept safe and what they've been kept safe from because of the nature of the work that you do. And I hope we will all remember that. I know everyone on the Committee does.

So again, I thank you. I know we have a lot of ground to cover today. And I thank you for your time and your willingness to come here today. It's good to do these hearings once again.

Chairman WARNER. Thank you, Mr. Vice Chairman.

I'd remind Members that after the open hearing, we will have a closed hearing. So any of the questions that stray into the classified sector, I'd urge you to reserve those for the closed hearing. And to remind Members today, we will do five-minute rounds based on seniority.

And will that, Director Haines, the floor's yours.

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

Director HAINES. Thank you so much.

Chairman Warner, Vice Chairman Rubio, Members of the Committee. Thank you very much for the opportunity to offer the Intelligence Community's 2021 assessment of worldwide threats to U.S. national security.

On behalf of the entire Intelligence Community, I want to express how much we appreciate your support and your partnership.

I would also like to thank the men and women of the Intelligence Community. Their efforts rarely receive public accolades because of the nature of their work. But they help to keep us safe, often at a great personal sacrifice. And we remain committed to providing them with the resources our mission requires and the support we owe them. It's my honor to serve alongside these dedicated officers, including the extraordinary leaders seated next to me, and to represent their work to you.

Our goal today is to convey to you and the public we serve and protect the threat environment as we perceive it and to do our best to answer questions about the challenges that we face. I'll only highlight a few points and provide some context in my opening statement. For a more detailed threat picture, I refer you to the annual threat assessment we issued yesterday, which is a reflection of the collective insights of the Intelligence Community.

Broadly speaking, the Intelligence Community is focused on traditional categories of issues that we've been discussing for years: adversaries and competitors, critical transnational threats, and conflicts and instability. And I'll summarize our views on these.

But first, I want to take note of the shifting landscape that we're facing today and its implications for our work.

The trends underlying and intersecting these issues are increasing the pace, the complexity, and the impact of these threats in ways that require us to evolve. During the past year, the COVID–19 pandemic demonstrated the inherent risks of high levels of interdependence. And in coming years, as reflected in our recently issued Global Trends report, we assess the world will face more intense and cascading global challenges, ranging from disease to climate change to disruptions from new technologies and financial crises. And as we note in that report, these challenges will repeatedly test the resilience and adaptability of communities, states, and the international system, often exceeding the capacity of existing systems and models.

This looming disequilibrium between existing and future challenges, and the ability of institutions and systems to respond, is likely to grow and produce greater contestation at every level. And for the Intelligence Community, this insight compels us to broaden our definition of national security, develop and integrate new and emerging expertise into our work, deepen and strengthen our partnerships, and learn to focus on the long-term strategic threats while simultaneously addressing urgent crises. In short, at no point has it been more important to invest in our norms and institutions, our workforce, and the integration of our work.

Doing so provides us with the opportunity to meet the challenges we face, to pull together as a society, and to promote resilience and innovation. And as we evolve, you will see our efforts to more effectively integrate longer-term destabilizing trends into our daily work, thereby promoting strategic foresight and a deeper understanding of the threats we face, which we hope will help the policy community effectively prioritize their work to address the issues that we seek to present.

Against this backdrop, the annual threat assessment describes an array of threats we are facing in the coming year, beginning with those emanating from key state actors and starting with

China, which is an unparalleled priority for the Intelligence Community. But we also look at Russia, Iran, and North Korea in that context.

China increasingly is a near-peer competitor, challenging the United States in multiple areas while pushing to revise global norms in ways that favor the authoritarian Chinese system. China is employing a comprehensive approach to demonstrate its growing strength and compel regional neighbors to acquiesce to Beijing's preferences, including its claims over disputed territory and assertions of sovereignty over Taiwan. It also has substantial cyber-capabilities that, if deployed at a minimum, can cause localized temporary disruptions to critical infrastructure inside the United States. And while China poses an increasingly formidable challenge to the U.S. role in global affairs, it is worth noting that its economic, environmental, and demographic vulnerabilities all threaten to complicate its ability to manage the transition to the dominant role it aspires in the decades ahead.

And next, with respect to Russia, we assess that Moscow will continue to employ a variety of tactics to undermine U.S. influence and erode Western alliances. While Russia does not want to conflict with the United States, Russian officials have long believed that Washington is seeking to weaken Russia. And Moscow will use a range of tools to pursue its objectives, including mercenary operations, assassinations, and arms sales.

It will also employ, as we've reported publicly, new weapons and cyber-capabilities to threaten the United States and its allies and seeks to use malign influence campaigns, including in the context of U.S. elections, to undermine our global standing, sow discord, and influence U.S. decision-making. Russia is becoming increasingly adept at leveraging its technical prowess to develop asymmetric options in both the military and cyber spheres in order to give itself the ability to push back and force the United States to accommodate its interests.

And turning to Iran, Tehran is seeking to project power in neighboring states, deflect international pressure, minimize threats to regional stability. Iraq will be a key battleground for Iranian influence in the coming year. But Tehran will also continue to pursue a permanent military presence in Syria, destabilize Yemen, and threaten Israel.

And for its part, North Korea may take aggressive and potentially destabilizing actions to reshape its security environment and will seek to drive wedges between the United States and its allies. These efforts could include the resumption of nuclear weapons and intercontinental ballistic missile testing.

When it comes to transnational threats, the assessment focuses on key issues that really intersect with the state-actor threats that I've just outlined, starting with COVID–19. The effect of the current pandemic will obviously continue to strain governments and societies over the coming year, fueling humanitarian and economic crises, political unrest, and geopolitical competition as countries build influence—sorry, as countries such as China and Russia seek advantage through vaccine diplomacy to build influence and, in some cases, demand accessions from other governments.

Countries with high debts or that depend on oil exports, tourism, or remittances face particularly challenging recoveries, while others will turn inward or be distracted by other challenges. And the critical impact of this pandemic has also served to highlight the importance of public health to national security. And ecological degradation and a changing climate will continue to fuel disease outbreaks, threaten food and water security, exacerbate political instability and humanitarian crises. And although much of the effect of a changing climate on U.S. security will play out indirectly in a broader political and economic context, warmer weather can generate direct, immediate impacts, for example, through more intense, frequent, and variable extreme weather events, in addition to driving conflicts over scarce natural resources. And the changing climate conflict and economic deprivation will drive vulnerable populations from their homes, heightening humanitarian needs, and increasing the risk of political upheaval.

The scourge of illicit drugs and transnational organized crime will continue to take its toll on American lives, prosperity, and safety. And major narcotics trafficking groups and other transnational criminal organizations will continue to drive threats while also being used by adversaries employing cyber-tools to steal from U.S. and foreign businesses and use complex financial schemes to launder illicit proceeds, undermining confidence in financial institutions.

Emerging and disrupting technologies, as well as the proliferation and permeation of technology in all aspects of our lives, pose unique challenges. Cyber-capabilities to illustrate are demonstrably intertwined with threats from our infrastructure and to foreign malign influence threats against our democracy. And we need, as you have all stressed to us, to focus on the competition in critical technical areas such as high-performance computing, microelectronics, biotechnology, artificial intelligence, quantum computing, fiber optics, and metamaterials.

So with regard to global terrorism, ISIS and Al-Qaeda remain the most pressing threats to U.S. interests overseas, as was noted. These groups seek to conduct attacks inside the United States, but sustained counterterrorism pressure has broadly degraded their capabilities. Domestically, lone actors and small cells with a broad range of ideological motivations pose a greater immediate threat. We see this threat manifest itself in individuals who are inspired by Al-Qaeda and ISIS, often called “homegrown violent extremism” and those who commit terrorist acts for ideological goals stemming from other influences, such as racial bias and anti-governmental sentiment, which we refer to as Domestic Violent Extremism, or DVE.

And DVE is an increasingly complex threat that is growing in the United States. These extremists often see themselves as part of a broader global environment and movement. And in fact, a number of other countries are experiencing a rise in DVE. For example, Australia, Germany, Norway, and the United Kingdom consider white, racially- or ethnically-motivated violent extremists, including neo-Nazi groups, to be the fastest-growing terrorist threat they face.

And, of course, regional conflicts continue to fuel humanitarian crises, undermine stability, and threaten U.S. persons and interests. The fighting in Afghanistan, Iraq, and Syria has a direct implication for U.S. forces, while tensions between nuclear-armed India and Pakistan remain a concern for the world. The iterate of violence between Israel and Iran, the activity of foreign powers in Libya, and conflicts in other areas, including Africa and the Middle East, have the potential to escalate or spread. Asia has periodic upheavals, such as the Burmese military seizure of power in February. Latin America has contested elections. Violent popular protests are likely to continue to produce volatility. And Africa will continue to see ongoing marginalization of some communities, ethnic conflict, and contentious elections.

In closing, we face a broad array of longstanding and emerging threats, whose intersection is raising the potential for cascading crises. Our increasingly interconnected and mobile world offers enormous opportunities, but at the same time it multiplies our challenges, calling us to even greater vigilance as we seek to protect our vital national interests, promote resilience, and invest in our institutions and our people, who will be the only and best answer to addressing these challenges. We have to take care of our people.

And so, I would be remiss not to note a final threat we are tracking: anomalous health incidents that have affected a number of our personnel. The Intelligence Community is taking these incidents very seriously, and it is committed to investigating the source of these incidents, preventing them from continuing, and caring for those affected. We appreciate the support that many of you have shown for our personnel on this issue, as with everything else we work on around the globe. And we look forward to answering your questions about these and other worldwide threats today.

Thank you.

[The prepared statement of Director Haines follows:]

DNI's Final ATA Oral Remarks to SSCI– April 14, 2021

Chairman Warner, Vice Chairman Rubio, and Members of the Committee, thank you for the opportunity to offer the Intelligence Community's 2021 assessment of worldwide threats to U.S. national security. On behalf of the entire Intelligence Community, I want to express how much we appreciate your support and your partnership.

I would also like to thank the men and women of the Intelligence Community. Their efforts rarely receive public accolades because of the nature of their work but they help to keep us safe, often at personal sacrifice. We remain committed to providing them with the resources our mission requires and the support we owe them. It is my honor to serve alongside these dedicated officers, including the extraordinary leaders seated next to me, and to represent their work to you.

Our goal today is to convey to you and the public we serve and protect, the threat environment as we perceive it and to do our best to answer questions about the challenges we face. I will only highlight a few points and provide some context in my opening statement -- for a more detailed threat picture, I refer you to the Annual Threat Assessment we issued yesterday, which is a reflection of the collective insights of the Intelligence Community.

Broadly speaking, the Intelligence Community is focused on traditional categories of issues we have been discussing for years: adversaries and competitors, critical transnational threats, and conflicts and instability. I will summarize our views on these but first I want to take note of the shifting landscape we see today and its implications for our work. The trends underlying and intersecting these issues are increasing the pace, complexity, and impact of these threats in ways that require us to evolve.

During the past year, the COVID-19 Pandemic demonstrated the inherent risks of high levels of interdependence and in coming years, as reflected in our recently issued Global Trends Report, we assess that the world will face more intense and cascading global challenges ranging from disease to climate change, to disruptions from new technologies and financial crises. As we note in that report "[t]hese challenges will repeatedly test the resilience and adaptability of communities, states, and the international system, often exceeding the capacity of existing systems and models. This looming disequilibrium between existing and future challenges and the ability of institutions and systems to respond is likely to grow and produce greater contestation at every level."

For the Intelligence community, this insight compels us to broaden our definition of national security, develop and integrate new and emerging expertise into our work, deepen and strengthen our partnerships, and learn to focus on the long-term strategic threats while simultaneously addressing urgent crises. In short, at no point has it been more important to invest in our norms and institutions, our workforce, and the integration of our work. Doing so, provides us with the opportunity to meet the challenges we face, to pull together as a society, and to promote resilience and innovation.

And as we evolve, you will see our efforts to more effectively integrate longer-term destabilizing trends into our daily work, thereby promoting strategic foresight and a deeper understanding of the threats we face, which we hope will help the policy community effectively prioritize their work to address the issues we seek to present.

Against this backdrop, the Annual Threat Assessment describes an array of threats we are facing in the coming year, beginning with those emanating from key state actors. Given that China is an unparalleled priority for the Intelligence Community, I will start with highlighting certain aspects of the threat from Beijing.

China increasingly is a near-peer competitor challenging the United States in multiple arenas, while pushing to revise global norms in ways that favor the authoritarian Chinese system. China is employing a comprehensive approach to demonstrate its growing strength and compel regional neighbors to acquiesce to Beijing's preferences, including its claims over disputed territory and assertions of sovereignty over Taiwan. It also has substantial cyber capabilities that if deployed, at a minimum, can cause localized, temporary disruptions to critical infrastructure inside the United States. While China poses an increasingly formidable challenge to the U.S. role in global affairs, it is worth noting that its economic, environmental and demographic vulnerabilities all threaten to complicate its ability to manage the transition to the dominant role it aspires to in the decades ahead.

Moscow will continue to employ a variety of tactics to undermine U.S. influence and erode Western alliances. While Russia does not want a conflict with the United States, Russian officials have long believed that Washington is seeking to weaken Russia and Moscow will use a range of tools to pursue its objectives, including mercenary operations, assassinations, and arms sales. It will also employ, as we have reported, new weapons and cyber capabilities to threaten the United States and its allies, and seeks to use malign influence campaigns, including in the context of U.S. elections, to undermine our global standing, sow discord, and influence U.S. decision-making. Russia is becoming increasingly adept at leveraging its technological prowess to develop asymmetric options in both the military and cyber spheres in order to give itself the ability to push back and force the United States to accommodate Russia's interests.

Turning to Iran, Tehran is seeking to project power in neighboring states, deflect international pressure, and minimize threats to regime stability. Iraq will be a key battleground for Iranian influence in the coming year, but Tehran will also continue to pursue a permanent military presence in Syria, destabilize Yemen, and threaten Israel. For its part, North Korea may take aggressive and potentially destabilizing actions to reshape its security environment and will seek to drive wedges between the United States and its allies. These efforts could include the resumption of nuclear weapons and intercontinental ballistic missile testing.

When it comes to transnational threats, the assessment focuses on key issues that intersect with the state-actor threats I just outlined, starting with COVID-19.

The effects of the current pandemic will obviously continue to strain governments and societies over the coming year, fueling humanitarian and economic crises, political unrest, and geopolitical competition as countries, such as China and Russia, seek advantage through "vaccine diplomacy" to build influence and in some cases demand accessions from other governments. Countries with high debts or that depend on oil exports, tourism, or remittances face particularly challenging recoveries, while others will turn inward or be distracted by other challenges. The critical impact of the pandemic has also served to highlight the importance of public health to national security.

Ecological degradation and a changing climate will continue to fuel disease outbreaks, threaten food and water security, and exacerbate political instability and humanitarian crises. Although much of the effect of a changing climate on U.S. security will play out indirectly in a broader political and economic context, warmer weather can generate direct, immediate impacts—for example, through more intense, frequent, and variable extreme weather events, in addition to driving conflicts over scarce natural resources. The changing climate, conflict, and economic deprivation will drive vulnerable populations from their homes, heightening humanitarian needs and increasing the risk of political upheaval.

The scourge of illicit drugs and transnational organized crime will continue to take its toll on American lives, prosperity, and safety. Major narcotics trafficking groups and other transnational criminal organizations will continue to drive threat streams, while also being used by adversaries, employing cyber tools to steal from U.S. and foreign businesses and use complex financial schemes to launder illicit proceeds, undermining confidence in financial institutions.

Emerging and disruptive technologies, as well as the proliferation and permeation of technology in all aspects of our lives, pose unique challenges. Cyber capabilities, to illustrate, are demonstrably intertwined with threats from our infrastructure and to foreign malign influence threats against our democracy. And we need, as you all have stressed to us, to focus on the competition in critical technical areas such as high performance computing, microelectronics, biotechnology, artificial intelligence, quantum computing, fiber optics, and metamaterials.

With regard to global terrorism, ISIS and al-Qa'ida remain the most pressing threats to US interests overseas. These groups seek to conduct attacks inside the United States, but sustained CT pressure has broadly degraded their capabilities. Domestically, lone actors and small cells with a broad range of ideological motivations pose a greater immediate threat. We see this threat manifest itself in individuals who are inspired by al-Qa'ida and ISIS, often called Homegrown Violent Extremism and those who commit terrorist acts for ideological goals stemming from other influences, such as racial bias and antigovernment sentiment, which we refer to as Domestic Violent Extremism or DVE. DVE is an increasingly complex threat that is growing in the United States. These extremists often see themselves as part of a broader global movement and in fact, a number of other countries are experiencing a rise in DVE. For example, Australia, Germany, Norway, and the United Kingdom consider white racially or ethnically motivated violent extremists, including Neo-Nazi groups, to be the fastest growing terrorist threat they face.

And of course, regional conflicts continue to fuel humanitarian crises, undermine stability and threaten U.S. persons and interests. The fighting in Afghanistan, Iraq, and Syria has a direct implication for U.S. forces while tensions between nuclear-armed India and Pakistan remain a concern for the world. The iterative violence between Israel and Iran, the activity of foreign powers in Libya, and conflicts in other areas, including Africa and the Middle East, have the potential to escalate or spread. Asia has periodic upheavals such as the Burmese military's seizure of power in February; Latin America has contested elections and violent popular protests are likely to continue to produce volatility; while Africa will continue to see ongoing marginalization of some communities, ethnic conflict, and contentious elections.

In closing, we face a broad array of longstanding and emerging threats, whose intersection is raising the potential for cascading crises. Our increasingly interconnected and mobile world offers enormous opportunities. At the same time, it multiplies our challenges, calling us to even greater vigilance as we seek to protect our vital national interests, promote resilience, and invest in our institutions and our people, who will be the only and best answer to addressing these challenges. We have to take care of our people and so I would be remiss not to note, before ending, a final threat we are tracking – anomalous health incidents that have affected a number of our personnel. The Intelligence Community is taking these incidents very seriously, and is committed to investigating the source of these incidents, preventing them from continuing, and caring for those affected. We appreciate the support that many of you have shown for our personnel on this issue, as with everything else we work on around the globe.

We look forward to answering your questions about these and other worldwide threats.

Chairman WARNER. Well, Director Haines, that was a list of about as many awful things in 10 minutes as I may have heard in recent times. Enormous, enormous set of challenges.

I want to drill down on a couple of issues. One, I think in many ways, this Committee, particularly under the leadership of Senator Burr, was one of the first to really raise the flag around the challenges on 5G, where I believe—my personal belief is—that the United States and the west writ large was a little bit asleep at the switch, where suddenly we have a rise in China, not only having a national champion in the case of Huawei, but literally being involved at the standard setting, rule setting, protocol setting in a way that I think, again, we had not seen in the past.

My question is this: the idea that the IC has to become kind of that ability to look into where China is rising in a series of areas of technology development. How do we have that kind of appropriate oversight? I'd like you and maybe Director Burns to address this question. In many ways, this Committee, by default, has become a little bit of the technology committee for the Senate. And again, I want to commend folks like Senator Cornyn, and Senator Sasse, and Senator Rubio on things like semiconductors, where we're taking a lead. We're also trying to look into AI. We're looking into quantum. We're looking into all this list of rising technology areas. But how does the IC buildup that expertise of being able to monitor China's rise in a variety of technology areas?

If both you and Director Burns—if anybody else—wants to jump in as well, I'd appreciate it.

Director HAINES. Absolutely. So, thank you, Chairman. I think I'll start, and hand it over, obviously. This is an area, obviously, that you've had a lot of interest in, and I know the Committee has really helped us think through, in a sense. But it is absolutely true that we are focused on this issue. We think it's incredibly important, as you've indicated. And as you note, it's not just about 5G, which obviously is one piece of the puzzle, but it's across a whole series of technology sectors where China is increasingly catching up to us, in effect, and where we see that they're contesting our leadership, in effect, in these areas.

And the implications are the things that I think we can help to supply to the policy community, both the pace at which they are moving, but also, what are the implications for national security, and what should they be focused on and prioritizing, as well as understanding, in a sense, what the implications are for supply chain and for resilience, and how we can actually address these issues satisfactorily.

But I think as your question implies, it means that we need to be as smart about technology as any other part of the U.S. Government and our society. And I think that is something that we have been working on, and bringing in the expertise that we need to the Intelligence Community. It's a workforce issue. It's also retaining that expertise and making sure that we have expertise to do that. But it's also exchanging and deepening our partnership with the private sector and with other parts of the government. And in many respects, that's a major push that we're involved in, where we now have legislation, thanks to you, about public-private partnerships, other mechanisms that we can use to try to ensure that we're doing exchanges that are deeper than just having a meeting and a discussion, but actually having people go in and out. And I think that's going to be a big part of us ensuring that we understand the implications of this, as well as sharing information with the private sector in appropriate ways, and obviously lawful and respectful of privacy and civil liberties. But nevertheless, critical for us to understand their perspective and for us to share our own perspective in certain ways, so that we can actually manage this and help the public and the policy community in particular understand those issues.

Chairman WARNER. Director Burns, do you want to—?

Director BURNS. Yes, Sir. I would just add very briefly that I absolutely agree with you that competition in technology is right at the core of our rivalry with an increasingly adversarial Chinese Communist Party and Chinese leadership in the coming years. That requires us at CIA working with our partners across the Intelligence Community to do two things, at least, strengthen our own abilities, which we've worked very hard on in recent years. Two of the five CIA directorates on Digital Innovation and Science and Technology are focused primarily on tech and cyber issues right now. Nearly one-third of our officers of our entire workforce are focused primarily on the technology and cyber mission today. So, that's a reflection of the priority that we need to continue to attach. Partnerships are equally important, not just across the Intelligence Community, and with the private sector, as Director Haines stressed, but also with foreign partners as well. And as you know, we've had some success over the last few years in working with foreign partners to help highlight the risk on 5G technology that critical dependencies on Huawei can provide, working with them to try to highlight ways in which we can become more resilient, including on semiconductors as well.

Chairman WARNER. I think we're going to need to make sure we draw upon all parts of the government: the Commerce Department, OSTP, others, our friends on the DOD side of the house. I don't feel like we have that one centralized place to make those assessments about China. And the vast majority of Members of the Committee have joined in bipartisan legislation to try to create, in a sense, technology alliances amongst democracies around the world. I think we're going to need that coordinated effort to take on this extraordinarily challenging issue with China.

Senator Rubio.

Vice Chairman RUBIO. Thank you. So, about a year and a half ago, a bat virus infected human beings, and transferred into something that infected human beings. I don't need to tell everybody what's happened since then. The official answer for why it's happened, when it is a possible answer, is that this was a new zoonotic transmission—that it crossed over from an animal into a human. But there's another hypothesis, which is plausible. And that is one that there was an accident in a laboratory, that ended up impacting the world the way we've seen.

And there's reason to believe that's plausible.

Number one, researchers at the Wuhan Institute of Virology have demonstrated from their publication record that they were skilled at techniques in which they genetically modified bat coronaviruses in order to create new man-made viruses that were highly capable of creating disease in human beings. Second, there have been several lab leaks documented that have occurred in China, including ones involving the original SARS virus. And third, U.S. diplomats who visited the Wuhan Institute of Virology in 2018 warned of the risks of the subpar safety standards that they observed.

I think this is really a two-part question, and I'll start with you, Director Haines, but I think Director Burns or General Nakasone can weigh in. We can't conclude definitively that the virus that causes COVID–19 emerged naturally until there's a transmission chain that's been identified—how the virus evolved and transmitted between species. And to date, no such path of zoonotic transmission has been definitively identified.

Are those two things accurate?

Director HAINES. Thank you, Vice Chairman.

So, it is absolutely accurate. The Intelligence Community does not know exactly where, when, or how COVID–19 virus was transmitted initially. And basically, components have coalesced around two alternative theories. These scenarios are: it emerged naturally from human contact with infected animals; or it was a laboratory accident, as you identified. And that is where we are right now, but we're continuing to work on this issue and collect information, and to the best we can, essentially, to give you greater confidence in what the scenario is. But I'll leave it to my colleagues, if there's anything that they want to add.

Director BURNS. No, Sir, Mr. Vice Chairman. I agree with what Avril said. I mean, the one thing that's clear to us and to our analysts is that the Chinese leadership has not been fully forthcoming or fully transparent in working with the WHO, or in providing the kind of original complete data that would help answer those questions. So we're doing everything we can, using all the sources available to all of us on this panel, to try to get to the bottom of it.

General NAKASONE. I would just add, Vice Chairman, that to your parlance, we continue to gather and to analyze and form series of pieces that we're looking at, working very, very closely—partnered with obviously the IC here—but also with a number of other partners in the interagency and in academia as well.

Vice Chairman RUBIO. The second topic I wanted to touch with you is, it's really based on your assessment. This is a quote from it:

"Beijing has been intensifying efforts to shape the political environment in the United States to promote its policy preferences, to mold public discourse, to pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China on such issues as religious freedom and the suppression of democracy in Hong Kong."

We're all at this point, I think, well aware of Chinese—of Russian influence and disinformation efforts. But I think we make a mistake to not focus on both China's capabilities and on its growing and intensifying efforts to involve and engage itself in our political environment here in the United States. Different aims perhaps, different tactics in some ways, but certainly they have every capability that the Russians do, and more in many cases. And they are certainly interested in molding public discourse and creating pressure on political figures who they don't like here in the United States.

I was hoping you could further elaborate on that for the benefit of the American public.

Director HAINES. Thank you, Vice Chairman.

I'll start, and I have a feeling that others will have things to say on this, in particular Director Wray. He obviously spends time on this issue a lot.

I couldn't agree with you more that this is an issue with both China and Russia that we are working to try to ensure, frankly, that we can educate the American public on these issues.

We have, within the ODNI, I'll just speak to that for a moment, a National Counterintelligence and Security Center that focuses on this issue, and has done enormous amounts of outreach to the private sector. I know we have worked, obviously, with your Committee to try to have engagements that help to bring this to various sectors, to help them understand the degree to which China is trying to influence, and also, the degree to which they are engaging in counterintelligence activities. It's a top priority for the Intelligence Community, but let me hand it over to Director Wray.

Director WRAY. So, I've testified previously that I don't think there is any country that presents a more severe threat to our innovation, our economic security, and our democratic ideas. And the tools in their toolbox to influence our businesses, our academic institutions, our governments at all levels are deep and wide and persistent. In addition to some of the things that have mentioned in the threat assessment, I'll just highlight one, which illustrates the diversity of their tactics.

We had an indictment that we announced I think last fall, that relates to the Chinese Operation Fox Hunt, which is essentially them conducting uncoordinated, illegal law enforcement activity here on U.S. soil as a means to threaten, intimidate, harass, blackmail members of the same Diaspora that Chairman Warner mentioned in his opening comments. And it's an indication and illustration of just how challenging and diverse this particular threat is. We have now over 2,000 investigations that tie back to the Chinese government. And on the economic espionage investigation side alone, it's about a 1,300 percent increase over the last several years. We're opening a new investigation into China every ten hours. And I can assure the Committee, that's not because our folks don't have anything to do with their time.

Chairman WARNER. Senator Feinstein.

Senator FEINSTEIN. Thank you very much.

You note in your statement for the record that China, Russia, Iran, and North Korea have the ability, right now, to conduct cyberattacks on critical infrastructure and cause temporary disruptions. Additionally, in 2019 you provided examples, including China's ability to disrupt natural gas pipelines for a day to weeks, and Russia's ability to disrupt our electrical distribution networks for hours.

So here's the question: is this problem getting better or worse? Are our adversaries more capable of threatening our critical infrastructure today than they were two years ago?

General NAKASONE. Senator, thank you very much.

In terms of our critical infrastructure, our 17 sectors of critical infrastructure, to bluntly answer your question, our adversaries continue to get better at what they're doing. I would also tell you, though, that we are also working very, very holistically across our government to improve two things: our ability to have resilience in that infrastructure, and our ability to respond. And we have made progress there. But there is, as we've seen over the past two intrusions, the scope, scale, and sophistication of our adversaries today. That makes us take notice. And we, as a Nation, must take notice of what our adversaries are doing.

And so cybersecurity for us is national, and we continue to work at it every single day.

Senator FEINSTEIN. Thank you.

What would you tell the chief executive officers and chief security officers at our critical infrastructure companies? What actions should they take? What type of investments do they need to make now?

General NAKASONE. Senator, I think the first thing is the threat is real. And I don't think I have to say that very often because the chief executive officers and the CISOs know that today.

But I think the second piece is that there is no one industry nor one sector of our government that's going to be able to provide us the defense that's necessary for our Nation. This is a team sport, and so this has to be done public and private. This has to be done between the Intelligence Community, obviously, DHS, DOJ, DEA, FBI, and Justice. This is really the key piece of our way forward, which is teamwork.

And I would say that we've learned that from our elections as well. And I would offer, Director Wray, your thoughts on it.

Director WRAY. So I think you've put your finger, Senator, on the key element of the challenge. The private sector is central to this. Ninety percent of the country's critical infrastructure is in the hands of the private sector. And it's important to think of cybersecurity, not as a single event, but as a campaign. These are no longer a question of if an institution is going to be compromised, but when. And so the more important question if I were talking—and I often am talking—to CEOs and CISOs, is to focus their cybersecurity more than they have in the past inwardly. The key is how fast you detect the compromise and how fast you remediate it.

And then secondly, the importance of reaching out and coordinating with government. Public-private partnership is at a premium because we often use, in the threat context, the expression "left of boom." You know, we know we all want to get left of boom. Well, in the cyber arena, one company's right of boom is left of everybody else in the same industry's boom.

And so we need that first company—and someday you're going to be the first company if you're a CEO, someday you're going to be the second or third or fourth company—we need in every instance those companies to be stepping forward, promptly reaching out to government so that we can prevent the threat from metastasizing across the rest of the industry.

Senator FEINSTEIN. Well, let me ask this follow-up: what investments does the IC need to make, what steps do you need to take, in order to change this status quo?

Director WRAY. Well, I think we're working more and more closely than ever across the IC on the issue and so that level of partnership and integration is going well and continues to improve and is important. But I think the bigger piece is more and more public-private engagement between the IC and the private sector.

And I know that there has been discussion about different ways to incentivize the private sector to come forward more quickly and promptly and fulsomely. And I think those are our key to our future on this issue.

Senator FEINSTEIN. Thank you.

Chairman WARNER. And I would simply add, very briefly, that one of the things I think you both made, General Nakasone and Director Wray, very clear: that while some of these attacks have only exfiltrated information they could have turned into denial of service and really wreaked enormous havoc with our whole economy.

Senator Burr.

Senator BURR. Thank you, Mr. Chairman, and welcome to all of our witnesses. I think of all the partnerships that exist in Washington, the one between the Committee and these agencies is the single most important one that we have.

A couple of observations. The U.S. Government's technology policy, whether development or deployment, if it exists at all, it's stupid. I'm not speaking to the five agencies that you represent, because you internally do process new technologies in a totally different way than the whole of government. But that doesn't work when it's limited just to the Intelligence Community, which has to do it for their job.

And dovetailing on Senator Warner's 5G comment, just a personal observation. I've never seen an issue that came before this Congress or this country that deserved a response from Five Eye partners more than 5G. And I think we've always looked through a tunnel and said: Five Eyes is an intelligence-sharing structure and it's limited to that.

When we talk about things that are outside of the norm, and the future is going to be all outside the norm, why don't we leverage the relationships that we have and realize that all smart people don't exist here? If they did, we wouldn't have a problem with China. So it's not just the cost, it's the power of the intellectual capacity that's out there that Five Eyes brings to a solution for the 5G problem.

Having said that, I'm going to start with to the right, my right, with Director Wray. Just give me an approximate percentage of your workforce, both domestically and internationally, that are vaccinated today.

Director WRAY. I'm not sure that I can give you an approximate percentage, because with us, unlike some of the other agencies, our folks are vaccinated in individual states based heavily on those states' pace of roll-out of the vaccination. So we have some field offices where we're close to 100 percent and we have some field offices where we're quite a bit lower. So it's uneven, but it's on a good trajectory.

Senator BURR. Director Burns.

Director BURNS. Senator Burr, about 80 percent of our workforce across the world is fully vaccinated today; and another 10 percent has received the first shot, the first vaccine shot. But what I've been most focused on is: are my colleagues in the field, and 100 percent of them today have the vaccine available to them.

Senator BURR. Director Haines?

Director HAINES. Senator Burr, 86 percent, I believe, of our workforce has received the first shot at least, and a fair percentage of that has been vaccinated twice.

Senator BURR. General, Nakasone.

General NAKASONE. Senator, I don't know if I can give you an exact percentage, based upon the fact that outside of Fort Meade we have, obviously, had a focus with the Department of Defense and Department of State to vaccinate our personnel. Within Fort Meade, we have focused on setting up our own vaccination site, and so both being a military and civilian community, we have an opportunity to not only get the vaccine off reservation but also at Fort Meade.

Senator BURR. General Berrier.

General BERRIER. Senator, approximately 40 to 50 percent of the DIA workforce has had at least one of the two shots, and that's exponentially increasing. Starting from last week to this week on Andrews Air Force Base and Joint Base Anacostia Bolling, thousands of vaccinations have come in and we're taking advantage of that.

Senator BURR. Thank you for that, General.

Observation, there are only three members of the U.S. Congress that served on the Intelligence Committee on 9/11. All three of them sit on this Committee: Senator Wyden, Senator Feinstein, and myself.

The foreword to the Worldwide Threat Report says, "ISIS, Al-Qaeda and its militant allies continue to plot terrorist attacks against U.S. persons and interests."

Director Haines, were you at the table when the decision was made to exit Afghanistan?

Director HAINES. I was at the table for a number of discussions leading up to the decision. I'm not sure that the decision was made in a specific meeting.

Senator BURR. I'll explore additional questions in the closed session as it relates to Afghanistan.

General Nakasone, we are all focused on this cyber hack. Do you believe that new authorities are needed for you or other agencies to address the defensive mechanisms we need today and in the future? And Director Wray, do you believe that there are legal changes that need to be made that facilitate either government or the private sector being able to get ahead of what we've seen with SolarWinds and with Microsoft?

General Nakasone.

General NAKASONE. Senator, I'm not seeking legal authorities either for NSA or for U.S. Cyber Command. My intent in my discussions has always been, though, is to state that with an adversary that has increased its scope, scale, and sophistication, we have to understand that there are blind spots in our Nation today.

And one of the blind spots that our adversaries are using is the fact that they are utilizing U.S. infrastructure in a means upon which we cannot surveil that, whether or not in the Intelligence Community or in the law enforcement community, to be able to react quick enough to what they're doing.

The second piece is to what the Chairman had mentioned in his opening statement. We are troubled in terms of being able to understand the depth and breadth of an intrusion based upon the fact that for a number of good reasons, some of them, obviously, legal, that much of the private sector does not share this information readily. And so, while there is no one solution to what's going on, I think we have to understand the program in totality.

Director WRAY. I agree with General Nakasone, and I would just add a few points.

I've referenced before the importance of the private sector piece of this. And I think to the extent that there's a need for a significant change, that's one of the places where the most significant progress could be achieved.

The reality is that adversaries try to use U.S. infrastructure for a variety of reasons, and one of them is to try to blend in with legitimate traffic that exists there. And the private sector, which controls 90 percent of critical infrastructure and an even higher percentage of our PII and our innovation, has the key dots as part of the overall connecting-of-the-dots phenomenon.

So I know, for example, the Cyber Solarium Commission took a hard look and recommended a mandatory breach notification law. That's a possibility. Things like that which further strengthen the glue between the private sector and the Intelligence Community and the rest of the government, I think, have ultimately got to be the key ingredient to any long-term solution.

Thank you.

Chairman WARNER. Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman, and thank you all for being here.

A couple of quick questions. We told you, Director Haines and Director Burns, I'd be touching on these this morning. And I'm asking, really, because I was very encouraged by some of your initial comments with respect to transparency. And I think there's an opportunity now to usher in a new set of rules that give Americans information about the basic rules under which the government conducts its operations.

So two quick yes or no answers.

For you, Ms. Haines. Senator Heinrich and I sent you a letter explaining why information related to a CIA program needs to be declassified. The information is contained in a report from the Privacy and Civil Liberties Oversight Board, and those reports are required to be made public to the greatest extent possible.

Will you get back to us within 30 days about whether you intend to declassify the information, Director Haines?

Director HAINES. Thank you, Senator Wyden.

We just received the letter and absolutely intend to look at it. I'm happy to get back to you within 30 days to let you know our views on that. I defer to Director Burns, if he has anything further.

Director BURNS. No, I agree, we'll get back to you very quickly.

Senator WYDEN. Very good.

And along the same lines, Director Haines. I sent you all a letter explaining why certain information about FISA needs to be declassified. Again, my request would be to get an answer within 30 days.

Director HAINES. Understood. Thank you, Senator.

Senator WYDEN. Great.

Director HAINES. Absolutely.

Senator WYDEN. I appreciate that.

Now, I do want to turn to this question of SolarWinds, and I want to start with you, General Nakasone, if I might.

My concern is that the government's response to this extraordinary hack is just going to be to throw a bunch more money at the same companies that sold the government insecure products that the hackers exploited. And, really, what we're talking about with that approach is cyber-pork.

Now, I also believe that security and liberty aren't mutually exclusive—we can have both. And so, I was concerned about a recent suggestion you made that the government's ability to detect and stop the SolarWinds campaign was hampered by the need to get a warrant before conducting surveillance of the domestic Internet. Now, my understanding is that the government has the ability now to watch every bit of data going in and out of a Federal network, including the SolarWinds malware. And yet, the hacking of nine Federal agencies somehow went unnoticed.

So what I'd like to see is if we can all agree before seeking new powers to surveil the domestic Internet, we all ought to be working together—you, DHS, all of the agencies—so that more can be done to detect hacking that's going on in our own networks.

What is your thinking on that?

General NAKASONE. Senator, I think you point out really the important piece here, is that there is no one answer to this question. And so as I've talked about, we need the Intelligence Community being able to see what's going on outside of our borders. We need, obviously, our law enforcement capabilities to be able to understand what's going on, obviously, within the United States. We need government to be resilient upon which these intrusions are taking place.

The challenge we have right now, though, Senator, is what our adversaries are doing is not spear phishing. It's not guessing passwords. It's utilizing supply chain operations. It's using zero-day vulnerabilities—those vulnerabilities that a provider doesn't even know about. We call that "above best practices." And when they do that, we need this total entire capability to bring to that.

So again, I think as we take a look at our capabilities—as adversaries move into U.S. infrastructure—to make sure that we can identify them and be able to alert what's going on is going to have to be looked at, Sir.

Senator WYDEN. My point is only, General, let's look at ways to shore up our own house first before we start talking about approaches that could unravel some of these sacred Constitutional rights that Americans feel so strongly about. And I'll follow-up with you on this when we're offline.

Director Wray, a question for you.

In July, I sent you a number of questions related to FBI operations in Portland last summer. I asked for responses that I could share with my fellow Oregonians who want to know what happened in our State. I'd like to ask you now, can I have those responses within two weeks?

Director WRAY. We'd be happy to try to get a response back to you in two weeks. I'll have to take a closer look at the specific items.

Senator WYDEN. Great. One last question if I might, and I think this would be appropriate for Director Haines.

You and I have been talking about this question of privacy being at the mercy of unscrupulous data brokers. One of part of the solution is making sure that when the government wants Americans' records, it goes through a legal process. The other is making sure our adversaries can't buy up this data, which includes the private records of U.S. Government officials.

During your confirmation process, you agreed that this could harm national security. Would you support legislation, work with us, to keep all of this data out of the hands of our adversaries?

Director HAINES. Thank you, Senator.

So I think we had a conversation, absolutely correct, on commercially-acquired information and how it is that the Intelligence Community deals with it. And I think I absolutely agree with you that we need to establish a framework that is clear and that has privacy and civil liberties at its heart, and also addresses the functionality of it for the Intelligence Community.

So I think that is one issue. And I believe in trying to produce that framework in a way that allows the American public to see what the framework is, essentially, even if they don't have visibility into the particular transactions or what we are doing to push for that. And so that's one piece.

I think on the second piece, I agree with you that there's a concern about foreign adversaries getting commercially-acquired information as well, and am absolutely committed to trying to do everything we can to reduce that possibility in the national security arena.

Senator WYDEN. I'll follow-up with you promptly. Thank you, Mr. Chairman.

Chairman WARNER. Senator Risch.

Senator RISCH. Thank you, Chairman Warner.

My first question is for Director Burns, based on your long history of dealing with issues in the Middle East. One of the things I found missing from this report, and obviously, it's always easy to criticize something—a product you didn't help produce. But there's an absolute dearth of reference here to the Abraham Accords, which seems to me to change dramatically what's going on in the Middle East.

And obviously, it's a threat assessment, but it seems to me whether a threat is increased or decreased ought to be mentioned in here.

Could you give me your thoughts on what effect the Abraham Accords are having? I think most of us know, but I'd like to get on the record your thoughts of what affect the Abraham Accords is having, inasmuch as it's not included in the assessment?

Director BURNS. Yes, Sir.

Well, I believe the Abraham Accords, as I mentioned I think in my confirmation hearing, were a very positive step for the United States, for Israel, and for the wider interest of stability and security in a region in which stability and security are often in short supply.

I know it's the intention of this Administration to try to build on the Abraham Accords and expand the number of countries who are willing to engage and normalize with Israel. It's never an easy task, but I think it's a very important one.

Senator RISCH. Thank you. I appreciate your thoughts on that.

Next one is for Director Haines. Your office is prominently on the front page. So again, I'm going to talk about something I think that needs more than what—for consumption by the American public. On page 20, you talk about the cyber threat. Back in the day when this annual threat assessment was done every year, it was a lot easier when we were talking about symmetric kind of threats that we face.

Today, we live in an asymmetric world. And with all due respect, I really think that the cyber provision here should have been expanded. And I think the threat should have been underscored more than it was, particularly in light of the fact that in my judgment, I think our most urgent threats are asymmetric rather than symmetric. And cyber is obviously right in the heart of that.

Could you give me your thoughts on that, please?

Director HAINES. Absolutely.

Senator, I think there's nobody that would disagree with you in my experience in the Intelligence Community that cyber is a major threat and that our asymmetric threats are critical. The debate really centered on whether or not, in a sense, to emphasize it more in this section or to do so as we have done in the state actor threat piece, where you'll see that we've identified the cyber threats that are associated with many of the state actors that are our greatest adversaries in this space.

And so it is not intended to reflect a lack of prioritization or emphasis on it, but rather the fact that it really imbues the entire threat assessment in many respects. Sort of pulling on it in different categories is critical.

Senator RISCH. I appreciate that. And we know that over the years, the threat when it comes to cyber was mainly non-state actors. But a worrisome trend is more and more we're seeing state actors involved in cyber activity that threatens us. And I think probably the reason is, is there doesn't seem to be that much of a price that they pay for this. And it seems to me that that should be underscored more in the report. Your thoughts?

Director HAINES. Thank you, Senator. I mean, I think you're right to indicate that we have as a country—and I think from a policy perspective—we've seen policymakers struggle with how to effectively deter these types of attacks, whether from non-state actors or state actors and how to address that issue. And a lot of time and effort has been spent on that, and I know you're well aware of it.

I think in the context of transnational organized crime, in effect, there is work that is being done to try to deter it through a variety of means. But whether it's effective, I think it's fair to say that it's not as effective as we'd like it to be. I think General Nakasone may have more views on this, and defer to him as well if you're willing.

Senator RISCH. My time is almost up, but glad to hear your thoughts.

General NAKASONE. Senator, I think as the Director pointed out, this is an instrument of national power now by many countries. And so, one of the things that I think our Nation has done over the past years is really realize that we must be continually involved in this domain in cyberspace. This is what we've learned over the past two elections. We will continually be involved well into the future as we take a look at what our adversaries want to do.

Senator RISCH. I appreciate that. I have other questions, but will save it for the closed session. Thank you.

Chairman WARNER. I think Senator Risch makes a good point, and I think it raises the issue again of attribution and doing that in a timely manner.

Senator HEINRICH.

Senator HEINRICH. Thank you, Chairman. As we witnessed on January 6, the most serious threat to our democracy sometimes comes from within. Last December, over four months ago now, I wrote a letter to FBI Director Wray and the acting director of the DHS Intelligence and Analysis Office, asking for a public written assessment of the threat that QAnon poses to our country.

Director Haines, I want to thank you for following up on your commitment to ensure that we received a response to that letter. On February 11, I did receive a response, but unfortunately it was designated for official use only. That means it's not classified, but it still cannot be made public. And so I've spent the last two months working with the FBI to get this assessment downgraded into the public realm, with no success.

Now, the Constitution protects the advocacy of all kinds of beliefs and views, even those that philosophically embrace violent tactics. But the public deserves to know how the government assesses the threat to our country from those who would act violently on such beliefs. And that's the public assessment that I asked for.

So Director Wray, why is it that you cannot or won't tell the American people directly about the threat that adherents to the QAnon conspiracy theory presents?

Director WRAY. So, Senator, I appreciate your question.

First, let me say that I think in our effort to get you information about what is in many cases ongoing law enforcement investigations, we were trying to give you as much information as we could in an unclassified way. I recognize the FOUO dimension complicated things. And my understanding is that my staff is working with yours, and we should be able to get you a fully unclassified version very shortly.

In the meantime, let me say this. You know, we focus on the violence and the Federal criminal activity, regardless of the inspiration. We understand QAnon to be more of a reference to a complex conspiracy theory or set of complex conspiracy theories largely promoted online, which has morphed into more of a movement. And like a lot of other conspiracy theories, the effects of COVID—anxiety, social insulation, social isolation, financial hardship, et cetera—all exacerbate people's vulnerability to those theories. And we are concerned about the potential that those things can lead to violence.

And where it is an inspiration for a Federal crime, we're going to aggressively pursue it. And in fact, we have arrested at least five self-identified QAnon adherents related to the January 6 attack specifically.

Senator HEINRICH. Director, let me follow-up a little bit on that. You're no doubt familiar with some of the public speculation that Q is really Ron Watkins, the administrator of the Internet image board 8kun, formerly known as 8chan. Whether or not Watkins is Q, he and his father clearly are responsible for hosting these sites and co-opting further in the QAnon conspiracy phenomenon.

Given the prominent role that QAnon did play in the January 6 attack on the Capitol, what are the potential legal repercussions for those who might be primarily responsible for propagating these sorts of dangerous and in some cases violent messages in these forums?

Director WRAY. Well, I think your question starts to raise different legal theories. We obviously, again, have to be careful to be focused on violence, threats of violence, and things that violate Federal criminal law. That doesn't mean that rhetoric isn't a societal problem that doesn't need to be addressed. But from the FBI's perspective, from a law enforcement perspective, we try to be very careful to focus on violence, threats of violence, and associated Federal criminal activity.

There may be certain instances where language becomes part of a conspiracy, for example. And there are instances where there are other Federal statutes which may be violated. But again, those are complicated questions which I would refer to the lawyers over at the Justice Department.

Senator HEINRICH. So for any of you, as a follow-up, I think a few years ago as a Nation, we really put enormous effort into understanding the mechanisms by which violent extremists and groups like the Islamic state, for example, became radicalized in chat rooms and online forums.

Are we applying that rigor to the DVE radicalization problem?

Director WRAY. So we are using our joint terrorism task forces, of which we have over 200 all around the country, to investigate not just the homegrown violent extremists, the Jihadist-inspired terrorists, but also the domestic violent extremists. And certainly in both cases, there are a lot of parallels. You have individuals largely able to connect online. It provides a greater decentralized connectivity. And as I have said before, terrorism today—and that includes domestic violent extremism—moves at the speed of social media. And so that means recruitment. That means planning, training, dissemination of propaganda, et cetera. All those things that apply and that happen on the Jihadist-inspired side in many cases are also happening on the domestic violent extremist side. Obviously, there are on the domestic extremist side, Constitutional protections, and chronic and legal challenges that we have to be mindful of, especially given some of the history in this country clearly.

Senator HEINRICH. Yes, clearly.

Thank you.

Chairman WARNER. Senator Collins.

Senator COLLINS. Thank you.

Director Burns, let me take this opportunity to thank you publicly for your focus on the medical injuries suffered by CIA and other personnel that are commonly referred to as the "Havana Syndrome." I'm going to have a question for you on that when we're in closed session, but I did want to publicly thank you and acknowledge your efforts.

I want to turn to Afghanistan, Director Burns. Our country has already sharply reduce its footprint in this country. There's no doubt that Americans are tired of our endless wars in Afghanistan. But there are many experts who are warning of the adverse consequences of President Biden completely withdrawing our troops and our presence in Afghanistan. If, as many experts predict, the Taliban will make significant territorial gains once U.S. forces are gone. What would be the implications for U.S. interests both regionally, here at home, and globally?

And if I've directed it to the wrong person, feel free to—.

Director BURNS. Well, Senator Collins, thank you very much for the question and thank you for your earlier kind comments.

I promised in my confirmation hearing that I take very seriously ensuring that our colleagues at the CIA, but also working with my partners on this panel, receive the care that they deserve, and that we get to the bottom of the question of what caused these incidents and who might have been responsible. And I look forward to staying in close touch with you on that. I know my colleagues at CIA deeply appreciate your personal commitment on this issue.

With regard to Afghanistan, I'll begin and then turn to Director Haines.

I guess what I would say at the start is that I think we have to be clear-eyed about the reality, looking at the potential terrorism challenge, that both Al-Qaeda and ISIS in Afghanistan remain intent on recovering the ability to attack U.S. targets, whether it's in the region, in the West, or ultimately in the homeland. After years of sustained counterterrorism pressure, the reality is that neither of them have that capacity today and that there are terrorist groups, whether it's Al-Qaeda in the Arabian Peninsula or in other parts of the world, who represent much more serious threats today.

I think it is also clear that our ability to keep that threat in Afghanistan in check from either Al-Qaeda or ISIS in Afghanistan has benefited greatly from the presence of U.S. and coalition militaries on the ground and in the air, fueled by intelligence provided by the CIA and our other intelligence partners. When the time comes for the U.S. military to withdraw, the U.S. Government's ability to collect and act on threats will diminish. That's simply a fact.

It is also a fact, however, that after withdrawal, whenever that time comes, the CIA and all of our partners in the U.S. Government will retain a suite of capabilities, some of them remaining in place, some of them that will generate, that can help us to anticipate and contest any rebuilding effort. And further, it's a fact that there are a number of other variables, I think, involved on that question of rebuilding. It's the role the Taliban themselves play. They've been fighting against ISIS in Afghanistan for many years, whom they view as a very potent ideological rival. They have an obligation to ensure that Al-Qaeda is never again able to use Afghanistan as a platform for external plotting.

There's the question of the continuing capacity of the government of Afghanistan with our support to fight terrorists. And there's the question of whether or not Al-Qaeda or ISIS in Afghanistan or ISIS, in general, seeks to relocate fighters and leaders to Afghanistan as well. There's the question of the role that neighbors play who also have a concern about spillover from Afghanistan.

So all of that, to be honest, means that there is a significant risk once the U.S. military and the coalition militaries withdraw. But we will work very hard at CIA and with all of our partners to try to provide the kind of strategic warning to others in the U.S. Government that enables them and us to address that threat if it starts to materialize.

But, over to you.

Director HAINES. No, Senator, I think I fully agree with Director Burns' analysis, and that is the Intelligence Community's perspective on this issue.

Senator COLLINS. Thank you.

Chairman WARNER. Senator King, I believe, online on WebEx.

Senator KING. Thank you, Mr. Chairman.

I want to start with an issue that has been touched upon, and that is the gap in intelligence coverage between our foreign-facing agencies and domestic agencies. I think Director Wray referred to it as a blind spot. How do we deal with this? Director Haines, this SolarWinds is a perfect example. It was Russian motivated, Russian instituted. They did the work, but it was implemented through servers and infrastructure within the United States. So they went through this blind spot, if you will.

What are your suggestions of how we deal with this, bearing in mind the obligations of the Fourth Amendment and the protection of privacy of American citizens?

Director HAINES. Thank you, Senator King.

I think it's an excellent question, and it's one obviously that we're struggling within a series of areas in our discussion of DVE, in our discussion of cyber, in areas like malign influence, and so on. And I think, from at least my perspective, we are working through each of these issues very carefully to ensure that we're complying with the law; that we're within our authorities; that we're doing what we should be doing. And taking into account privacy and civil liberties and the questions that are so critical to anytime that we are collecting intelligence along these lines and trying to combine, in effect, domestic and intelligence sources.

And in that space, trying to then also provide analysis that gives people the full picture. But I think, as General Nakasone noted, there are some real challenges that we're facing in this area. And I think—.

Senator KING. Well, let me ask a specific follow-up, perhaps to General Nakasone.

If you see activity of this kind in your work overseas, are you allowed to tip the FBI and say, we think this is happening, you should follow-up?

General NAKASONE. Certainly, we are allowed to do that. We do that quite frequently, regularly with Director Wray's folks, and they do a very good job.

Senator, if I can just lay this out just a bit, because I think it's important to understand the whole spectrum of it. So it does begin overseas, understanding what our adversaries are doing outside the United States. To Director Wray's point, in the United States, it is the public-private partnership. We need to be able to understand that when adversaries come into the United States and use our infrastructure, whether or not as servers or Cloud providers, that there is coverage on that.

It's also this idea that we understand what an intrusion may have taken place. So this idea of being able to understand the data that may be lost and be shared is really important.

And then the last point is, is that we need, obviously, the public and the private industry to have the most resilience possible. And so there is a complete responsibility there. But I would offer—.

Senator KING. I've got limited time, Director, so let me follow-up on a different question. But I think this is something that bears a lot of discussion. And I hope you all will share with us your thinking of whether we need to change authorities or how we fill in this blind spot, maintaining our protection of privacy in our country.

General Nakasone, four or five years ago, I asked one of your predecessors a simple question. Do our adversaries fear our response in cyberspace? Are they deterred to the point of changing their calculus as to whether or not to launch a cyber-intrusion or an attack against us? I want to ask you the same question.

Is there an adequate deterrent or is this something we still need to establish more clearly as a matter of policy?

General NAKASONE. So Senator, I'm not sure in terms of whether or not our adversaries fell that or are necessary, but here's what I know that our adversaries understand that's different today than it was several years ago: that we are not going to be standing by the sidelines, not being involved in terms of what's going on with cyberspace and cybersecurity. Over the past several years, whether or not it's been defending our elections or being able to provide quicker attribution, this is our focus. And this has been the focus of the Agency in the IC and across our government.

Senator KING. Thank you.

And I know that I'm out of time. Director Burns, one question for the record, please. If you could provide an estimate of climate refugees over the next decade or 15 years or so, I think that's going to be a very significant national security challenge. How many refugees does your agency estimate will be on the move because of the inhospitable climate in their region? That's something you can give me for the record. I'd appreciate it.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you.

Senator BLUNT.

Senator BLUNT. Thank you, Chairman.

And Director Haines, Director Burns, and General Berrier, I think this is the first time the three of you have appeared at this particular hearing. And certainly, we're glad and grateful to have all of you here.

Director Haines, let's talk a little bit. You and I have talked about the overhead architecture issues. Part of the development of how you use AI is how much information you have to continually train on. We may talk about that later this afternoon. But for right now, the Chinese have announced public plans for 138 satellite commercial constellations that can image around the globe every ten minutes. How big a risk is that for us? And what can we do to enhance our own diversity by expanding the number and the diversity of the satellites we have up there, providing constant information, commercial and non-commercial?

Director HAINES. Thank you, Senator.

I think it may be useful to have a further discussion about this in closed session, but I think there's just no question as a general matter, that China is focused on achieving leadership in space, in effect, as compared to the United States and has been working hard on a variety of different efforts in this area to try to contest what has been presumed our leadership in these areas. And I think for the details, let's discuss in closed session.

Senator BLUNT. Well, I think we'd want to do that and look at both the diversity of what we have up there and how it competes with what they'll have.

On a really different question, Director Burns, you have extensive personal knowledge and experience with Putin. How do you assess what he's doing right now near and in the eastern Ukraine and the impact that that may have? Is this an actual movement? Do we think it's a bluff to try to get concessions? A little of both? What do you think about the Putin actions right now as it relates to Ukraine?

Director BURNS. Well, Senator, thanks for the question.

I think, as I said in my confirmation hearing, most of my white hair came from serving in Russia and dealing with Putin's Russia over the years. So, one thing I've learned is not to underestimate the ways in which President Putin and the Russian leadership can throw its weight around.

I think—and I'll turn to General Berrier about this in a moment—but I think, obviously, the Russian military buildup in Crimea and alongside the border of the Donbas is a serious concern. I think it could be a combination of the things that you mentioned, signaling a way of trying to intimidate the Ukrainian leadership. Signals to the United States. But also that buildup has reached the point where it also could provide the basis for limited military incursions as well.

And so it's something not only the United States, but also our allies have to take very seriously. And I know Director Haines and I and others have been involved and a number of briefings and conversations with our allies as well, so that we're sharing information and they share that same concern. I think, that we have as well. And that was part of the purpose of the President's call yesterday to President Putin was to register very clearly the seriousness of our concern.

Senator BLUNT. Good. We could probably talk about that more later, too.

General Berrier, what's your sense of what's happening there and the concerns we should have about it?

General BERRIER. Senator, working with our partners in Joint Staff J2, European Command, NATO, and our key Five Eyes partners, the Russians have positioned themselves to give themselves options. So as we've watched that buildup of forces, they could actually be going into a series of exercises starting any time, or they could, if they chose to perhaps do a limited objective attack. They may take that option. We don't know what the intent is right now. I agree with Director Burns and his assessment of that. And we can go into more detail in the close session, Sir.

Senator BLUNT. OK. Let me see if I can get one more question in, General Berrier. We know that our adversaries, and no matter what level of involvement they had in the pandemic, we can see now the impact that has on a big open free society like ours. But they also can see the impact it has on the military, like what happened on the "USS Theodore Roosevelt" and in other places.

What are we thinking about as a potential way we'd respond to similar circumstances from a defense point of view?

General BERRIER. Senator, the pandemic has given us insights on how we can do our jobs better, should this happen again. In terms of readiness of our key adversaries that we watch, I think initially it did have an impact on the readiness of those forces, although they seem to have overcome that. As an example is what we're seeing with the Russians in the Ukraine and the Crimea right now does not appear to be impacted by COVID, and so, we continue to watch that very carefully across the spectrum of foreign military intelligence.

Senator BLUNT. Thank you. Thank you, Chairman.

Chairman WARNER. I think a number of us are very interested in Senator Blunt's questions about Ukraine. We look forward to that this afternoon.

Senator BENNET.

Senator BENNET. Thank you, Mr. Chairman, and thank you all for being here today. I really appreciate it. In the annual threat assessment, Director Haines, you wrote that, "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." You also wrote that, "China has counter-space weapons capabilities intended to target U.S. and allied satellites."

In December 2020, U.S. Space Command said that Russia conducted a test of a direct descent anti-satellite missile, which if tested on actual satellite or used operationally would cause a large debris field that could endanger commercial satellites and pollute the space domain.

Could you tell the American people what we are doing to maintain our superiority in space, and what the role of the private sector is in doing that?

Director HAINES. Thank you, Senator.

I would say that—well, obviously, we'll have a further discussion in close session. But the private sector has just become increasingly important in our efforts to contest and to work, essentially, against contestations to our leadership in space. But what I can say is that we have been working very hard to ensure that the policy community understands, and that obviously we support Space Force in its work to promote, in effect, U.S. leadership in space. And it's been an area where we benefit, as we've indicated, economically, from a security perspective, from a communications perspective, and from the perspective of just understanding and intelligence perspective. And all of those things are areas where we want to ensure that we continue U.S. leadership in this area, and we'll get into further details after—.

Senator BENNET. I look forward to our conversation later.

Director Burns, according to Freedom House, democracy around the world has been in retreat for 15 years against authoritarianism. And we know that countries like China and Russia want nothing more to continue that for another 15 years, or maybe another 50 years. How do you assess the primary threats to democracy around the world, and which regions have we seen the most significant democratic retreats? Which regions do you consider most at risk, and how are our adversaries thinking about this?

Director BURNS. Thanks, Senator.

Senator BENNET. I probably should have called you Secretary Burns when I asked you this question, but I couldn't resist.

Director BURNS. No, thanks, Senator, very much. Well, I think the problem of erosion of democracies, as Freedom House points out, is a very real one in many parts of the world, those that have established democracies and those where democratic governance is quite fragile. That has partly to do, I think, across the board with questions about the ability of democratic governance to deliver. I think you've seen some of that in our own country in recent years. We haven't been immune from that at all.

So, the challenge, and I think President Biden has emphasized this, is working with other democracies, and I say this as an analytical judgment, to help restore that faith in the ability of democratic governance to deliver for people. That deprives authoritarian leaderships, whether it's the Chinese Communist Party or Vladimir Putin's Russia, of an argument that they use that somehow authoritarian systems are better able to deliver. The reality is that there's a great deal of resilience in democratic systems. But it's important for all of us that have democratic governments to demonstrate that, to renew ourselves. I think that's always found in—in many years in my previous incarnation serving overseas, that we get a lot further through the power of our example than we do through the power of our preaching. And I think that's true for any democratic government around the world.

The last thing I'd say is we've talked earlier in this discussion about the role of technology. And I think that's also something to be very mindful of, because the proliferation of surveillance technologies, for example, are one tool that authoritarians use to strengthen their grip and make it more difficult for democratic governance to emerge in lots of fragile societies around the world.

Senator BENNET. And in that context, Director Wray, of fragile societies and the risk that's posed to democracy, I wonder if you could share with the American people what you have learned about the intersection of social media platforms and domestic violent extremists, and what the American people can do to be more canny users of those platforms. What should they be on the lookout for?

Director WRAY. So, certainly, social media has become in many ways the key amplifier to domestic violent extremism, just as it has for malign foreign influence, which we've discussed at great length with the Committee as well. It proves a level of the same things that attract people to it for good reasons, are also capable of causing all kinds of harms that we're entrusted with trying to protect the American people against.

So, it creates speed dissemination, efficiency, accessibility—I referred to before, a level of decentralized connectivity. I think I would say that both, with respect to malign foreign influence and with respect to domestic violent extremism, people need to understand better what the information is that they are reading. A greater level of discerning skepticism is a crucial ingredient not just to protect from foreign misinformation, but also of violent extremism.

There is all sorts of stuff out there on the Internet that poses as fact, which just isn't. And there's all kinds of connectivity between like-minded individuals, which blocks out other voices, which creates a sort of echo chamber effect. And then especially with the isolation caused by COVID, increases our public susceptibility to some of the same kinds of ills that we've talked about at great length.

So, social media can bring great good to society, but it is also a platform for all kinds of security challenges that we're trying to counter.

Senator BENNET. Thank you, Mr. Chairman.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. General Nakasone, in the recent hearing we had on the SolarWinds hack, the issue of notification by victims of hacking was raised. And indeed, I believe Senator Collins has advocated for a long time in a piece of legislation that victims of cyberattacks notify the Federal Government in some manner to provide context and complete knowledge of what's out there. It seems to me that otherwise, we're looking through a soda straw at some of the threats. Do you think requiring victims of cyberattacks in the United States, requiring them to notify the Federal Government in some way, maybe confidentially, is a good idea?

General NAKASONE. Senator, as we were discussing this morning, I think to understand the depth and breadth of any intrusion in the United States, we're going to have to have some means upon which we understand what has taken place. And so, obviously the policymakers and yourselves, the legislators, will determine that, but I think that's a key component of it as well.

Senator CORNYN. That would help you and the Cyber Command in NSA do a better job?

General NAKASONE. Well, certainly, within the United States, responsibility obviously rests with the Federal Bureau of Investigation.

Senator CORNYN. Right. I beg your pardon. Director Wray, what do you say?

Director WRAY. So, we were very, I think, enthusiastic about the recommendation from the Cyber Solarium Commission that speaks to this issue. As I mentioned before, the private sector controls so many of the dots on all manner of cyber threats. And it's important to think of the private sector not just in one broad category. There's two big groups that are relevant to this issue, and why they go straight to the heart of your question. I put them in two buckets. One, there's the providers; so, the cybersecurity industry, the IT industry, et cetera. They have unique visibility into how adversaries traverse U.S. networks. And so, making sure the glue is there is critical.

But then there's also the victims. The reality is that most offenders are going to come back to victims again. So most cyber actors are coming back, and most victims are going to be popping up again. You've got repeat offenders and repeat victims. And so, their hard drives, their logs, their servers provide key technical dots to who's compromising them; how they're being compromised; and then, this is the key, who might be targeted next. And that gets back to my point from before, about why the private sector outreach is so important.

One company reaching out to us promptly after they've been compromised means that all the rest of the companies that are likely to be the next ones hit, we might be able to get in front of it. And so, if you think about the scale of the dots that are in the private sector, that's why I think that's the piece of this—. It doesn't mean that there aren't other tweaks here and there in terms of authorities, administrative subpoena authority and things like that. But ultimately, for the United States, which doesn't have state-owned enterprises all over the place to protect against this problem, we really have to solve this public-private partnership issue.

Senator CORNYN. Director Haines, the issue of supply chain vulnerability is high on Congress' agenda, and certainly on everybody's mind. But I don't really have a clear understanding of how good a handle the Intelligence Community has on what those supply chains that are critical to our national security look like. And we clearly need the help of the Intelligence Community, to help Congress, the policymakers, rack and stack what are the most urgent priorities. Semiconductors is certainly one that's on everybody's mind. But do you think the Intelligence Community has a good handle on those, so you could help Congress prioritize those so we could attack them from a policy perspective?

Director HAINES. Yes. I think, frankly, this is an area where we're doing a lot of work. And as you indicate, semiconductors are the obvious one, but there are a lot of others. And as we've been working through, for example, rare earth elements or other key areas where there may be a contestation in particular from other countries such as China, to our ability to get access to things that are critical to our national security, and where we need to promote an effort, in a sense, from the policy community to pay attention to it and to recognize where there are the vulnerabilities and how to address them over time.

The piece that I find particularly interesting is, to your point, how do you prioritize? Because there's just an enormous amount of things that you could look at to say we need to have a resilient supply chain on, and take action in order to promote. And we have been working to try to provide the policy community with as much information as possible about what the possibilities are, in a sense. But ultimately, there are some decisions to be made from the policy community about, what are you prioritizing? Where do you want to focus, in a sense? And we have been building up an infrastructure that allows us to then focus to make sure that we can both track it but also provide options for where you might be able to pull, essentially, supplies from—that are not the ones that you are pulling—in order to have that kind of resilience built-in.

Senator CORNYN. Thank you.

Chairman WARNER. Senator Casey.

Senator CASEY. Thank you, Mr. Chairman. I want to thank all three directors and the two generals who are with us today, and to commend you for your public service.

I wanted to start with Director Haines, and probably most of my question or two would be directed at Director Haines. But certainly, others may have a view on the issues I'm raising.

I want to talk in particular about supply chains, which we've heard a lot about this year, and this idea of outbound versus inbound investment by U.S. companies in that context.

We know that on March 19th, the U.S.-China Economic and Security Review Commission held a hearing to examine how U.S. capital investment props up the Chinese government's military-civil fusion strategy, and ultimately compromises U.S. national security. Some witnesses made reference to the Committee known by the acronym CFIUS, the Committee on Foreign Investment in the United States, which for decades now has reviewed inbound investment but there's nothing comparable for outbound investment in terms of review as to the national security implications of foreign investments that are made overseas. So because we don't have that parallel mechanism in place to assess outsourcing by U.S. companies to countries of concern. We could have national security implications.

I've been engaging with Senator Cornyn on this issue on developing a similar interagency committee to review outbound investment of what we call in the legislation I'm working on, critical capabilities to foreign adversaries or non-market economies like China.

So Director Haines, maybe two initial questions. Currently, how does the IC work with its partners to assess and mitigate the activities of foreign intelligence services and other adversaries attempting to compromise U.S. supply chains?

Director HAINES. Thank you, Senator.

So it's a really important and interesting question and I think just to maybe take them in part.

So on the issue of outbound and outsourcing how are we positioned? I think, from my perspective, I've had a number of calls now with my counterparts and kind of coming into the job. I think you would be surprised by how many of them in allies and partnership countries are interested in talking about this issue.

And one of the things that we are doing throughout the Intelligence Community, and I think Director Burns may have some thoughts on this as well, is promoting conversations between our intelligence services in order to understand what they're seeing in this space as well and being able to provide that, therefore, to our policymakers as, "Here is what we are seeing with respect to these particular issues that we know are critical for supply chain issues and here's where we're seeing outsourcing and outbound investments," and so on.

The second thing that I think is interesting, and you may already know this, but we're certainly lifting it up in a sense, is how many other countries are starting to do CFIUS-like processes. You'll see Canada has now got a law that effectively allows them to review investments or a variety of other countries that are starting to do this. And it's another reason for why I think our counterparts are talking to us about this issue because they're looking to figure out how does the Intelligence Community support our CFIUS process? Are there ways in which they can do the same?

And I think that exchange of information can get to many of the issues that you're describing in the supply chain area, both on the inbound and outbound side of things. And let me see if Director Burns has anything.

Director BURNS. No, no, I absolutely agree. And I think there are plenty of models on the outbound side that have worked in decades past as well, where we can deepen our partnerships with other governments, who not only have insights, but also have a real stake in taking a very careful look at some of those outbound matters.

Senator CASEY. Thank you. That's helpful.

And just, finally, the last question on this would be does the IC view the Chinese government, the Chinese Communist Party's civil-military fusion agenda, as a risk currently to U.S. supply chains?

Director HAINES. Senator, I think there is no question that the Chinese have an advantage in some respects through their civil-military fusion approach to things. They are capable, as a consequence of directing, in effect, their private sector in ways that we simply do not do. And I think that provides a short-term advantage, but I think it might be not a long-term advantage in the sense that I think that the way we structure ourselves actually makes us capable of having some flexibility that, over time, sustains our private market in ways that the Chinese don't have.

Senator CASEY. Thank you.

Chairman WARNER. The vote has started, but we are going to try to get Senator Sasse and Senator Gillibrand on WebEx in before the end of the first vote. Senator Sasse.

Senator SASSE. Thank you, Chairman.

Thanks to the five of you for being here as well. The American people are blessed to have an IC that's as serious as ours is. We have a lot of—a gazillion patriots and some actual heroes in the community and the five of you care deeply about the mission and about leading those folks and celebrating them. So I just want to say, since most of our time in the Committee is spent in an oversight capacity, which is in private, we don't get the chance to say in front of the American people enough, thank you to the entire intelligence community, and particularly the five of you who are leaders.

Director Haines, I also want to praise your statement. I think that your opening statement on behalf of the whole community today was incredibly strong. I want to highlight a couple of pieces. But I want to admit that in a way I'm just riffing on where Chairman Warner opened, that when you do an around-the-world threat assessment of what the challenges are that we face—and I think Marco, the Vice Chairman, said something very similar—I think his riff was more than 90 percent of all the intelligence and national security challenges the American people and our troops face around the world, more than 90 percent of them originate in the five bad guy category of: long-term tech race with the Chinese Communist Party, Russia sowing disinformation and corruption and cyberattacks abroad, Iranian nukes and sponsorship of terrorism abroad, North Korean nukes, and a grab-bag of Jihadis. Those five things are the five big threats we face. There aren't two and there aren't really 20 that need to be on that top tier list. There are five.

But one of the things that's new, I think, in the last four to six years, is a real consensus in your community and on this Committee in a bipartisan way that there is an unparalleled number one threat. The five things are not equal. The long-term technology race we face with China is the biggest existential national security threat we face.

And I think Chairman Warner did a great job of distinguishing between Chairman Xi's command and control tyrannical system and his party. But that's not the same as the Chinese people. That's not the same as Chinese expats. That's not the same as Asian-Americans abroad. And we have to, together, the IC and the Committee in a bipartisan way, have to make sure we communicate again and again to the American people that there is one overarching national security threat we face. And it is not race-based, it is not Chinese Americans. It is Chairman Xi and his cronies and what they want to do to try to dominate the world and oppress people, most acutely the Uighurs, but lots and lots of people in their own country and abroad.

And so I think it's important just to underscore some of the things, Director Haines, you said on behalf of the entire community. You said that, "The threat we face from China is unparalleled. It's not the same as North Korea, as big a deal as that is. It's not the same as Russian and nefarious actions abroad. China is increasingly a near-peer competitor. China will maintain its major innovation in industrial policies because Chinese leaders see this strategy as necessary to reduce dependence on foreign technologies, enable military advances, and sustain economic growth, and thus ensure the CCP survival."

Chairman Xi is not about the good of his people. He's not about the good of 1.4 billion Chinese people. He's about the good of his party and the way they oppress their people. You also said that China is trying to promote new international norms for technology and human rights, emphasizing state sovereignty and political stability over individual rights. You said that China will remain the top threat to U.S. technological competitiveness as the CCP continues to target technology sectors, et cetera.

So I think it was a very strong statement. And as a part of what happens, the majority of not just our Committee's work, but the majority of this hearing is in private today. But as far as something we put before the American people, that's an incredibly strong opening statement so I want to commend you and the whole interagency process that got it there.

I'd like to follow-up on your response, though, to Senator Casey's comment about the fact that in—I'm putting a finer point on it—but in 2018, Congress passed a new law about export controls. And the goal is to be sure that we update what emerging and foundational technologies we regard as needing to be restricted to the CCP. Obviously, the CCP is also involved in a massive technology theft—IP theft—project.

But just at the level of export controls, a law was passed in 2018 and it's largely unimplemented. And I think former Chairman Burr made the good point that in 5G we should view the Five Eyes as allies that we would use to build the technology base, whether it's a D10 or a D12, or whatever the strategy is, we need something like the TPP again that says freedom-loving Nations that believe in open navigation of the seaways, free trade, the rule of law, transparent contracts, human rights, et cetera—we need an alliance of freedom-loving peoples against the CCP's nefarious sponsorship of stuff like surveillance-state tyranny abroad. But to do that, we have to have clarity about what those critical technologies are. So I would love to hear some public explanation for the American people of when will we have the 2018 law implemented, and probably more a 30,000 foot view. More importantly, if we're going to build an alliance of freedom-loving Nations in this technology race, how can we do it? How can we lead allies if we don't have clarity for ourselves about what those critical technologies are?

Director HAINES. Thank you, Senator. Maybe I'll just start and welcome my colleagues joining on this.

I think just to focus in on the intelligence relationships in particular and the Five Eye point that you and Senator Burr are making, I think it will not surprise you that technology is one of the things that we intend to talk to them about, that we are already talking to them about at different levels. And I think it is entirely right to be focused on the idea that among the Five Eyes we can actually do some good work together, in effect, in addressing this issue that none of us can do alone in a way. And that that's a place where we do need to focus.

I think also it is true that the policy community is working, and I know the Administration is working, on a strategy on these issues that would include partners and would effectively focus on the kind of issues that you're describing. In addition, they are also looking at the technology sectors and how it is that you approach each of these to deal with whether or not de-linking in all of these different spaces is the right thing to do and how to do it, so that you don't actually have collateral impact that sometimes can have negative consequences in those areas.

But why don't I leave it to others to comment?

General BERRIER. Senator, I would just say from a DIA perspective and the Department of Defense, our closest partners are Five Eyes teammates. I have deep personal relationships with every one of my counterparts. We talk on a weekly basis. And from a strategic competition perspective or an intelligence support aspect to strategic competition, they're all in. And so this conversation about identifying the technology and how we can collectively get after this threat with the CCP, I think they are ready for that conversation.

Senator SASSE. Okay.

General NAKASONE. Yeah, I think Senator, I would just add from our competitive advantages think about what our competitive advantages for the Nation and for the Intelligence Community, whether that's artificial intelligence, big data, machine learning, space, all of these are critical capabilities that have far reaching implications, not only for our economy, but obviously, for the security of our Nation as we take a look at where we're going in the future as well.

Chairman WARNER. I mean, I'll just say the Chair and the Vice Chair want to complement Senator Sasse for agreeing with the Chair and the Vice Chair.

[Laughter]

Senator SASSE. It's always helpful. Yes.

Chairman WARNER. Anybody else want to—because we have—we're kind of clocking down.

Senator SASSE. Fair enough. In the classified session I want to follow-up on particularly some of the Taiwanese pieces.

Chairman WARNER. We're going to go to Senator Gillibrand on WebEx and then Senator Cotton.

Senator GILLIBRAND. Thank you, Mr. Chairman.

Director Wray, as you are familiar, the families of the victims of the September 11th attacks have requested a number of FBI documents to be declassified. As we approach the 20th anniversary of the attacks, I'm trying to understand what information in those reports could still be so sensitive that it cannot be shared with the American people.

For several months, I have been trying to get FBI to provide a classified copy of the documents to the Committee so that I can read them myself, but so far the FBI has refused. From an oversight perspective, this is deeply concerning. Why hasn't the FBI provided the requested documents to the Committee and will you commit to providing those documents to the Committee now?

Director WRAY. Well, Senator, I understand how important this issue is to you personally, and of course, also to the victims' families. And as somebody who grew up in New York and whose family still lives in New York that's personal to me as well. And meeting and engaging with the 9/11 victim families was a big part of my own inspiration from my last time in law enforcement to come back into service.

We do have to be a little bit careful here because of certain sorts of method issues and grand jury issues. But I have instructed our subject matter experts to review to see if there's more that we can share and I'm happy to report that we have identified some additional documents that we will be able to make available for review very shortly. And my staff will work with the Committee's staff to facilitate review.

Senator GILLIBRAND. Okay. Will you have those documents within the next two weeks?

Director WRAY. I'll have to get back with my staff on the exact timing but my definition of "shortly" is consistent with that rough timeframe.

Senator GILLIBRAND. Okay, and if you're not going to provide the particular document that I have requested, I need a reason in writing to the Committee since I, as a member of the Committee, have every right to review that document.

Director WRAY. Certainly, Senator. I agree that an important part of our collaboration with the Committee is that even in those rare instances where we can't provide information we ought to be able to and have an obligation, I think, to explain to you why.

Senator GILLIBRAND. Thank you.

To Director Haines and to General Nakasone, I'm very concerned about these blind spots, as we've already heard in testimony today, that our opponents are using the U.S. infrastructure and loopholes to penetrate our infrastructure, our companies, our data, in a way that really prohibits us from following through on our investigations in terrorist groups and other international risks.

I understand there are legal reasons, and I've heard the testimony that we want to talk about how we can ask the private sector to perhaps consider having a required reporting law passed, and I think that's a reasonable approach. But I'd like a little more context and information from both of you on how you see these gaps and these blind spots.

And, in fact, when we do have foreign terrorist attacks and undermining of our democracy, such as what Russia tried to do with the election, and undermined public confidence in our electoral process and exacerbated sociopolitical divisions in the U.S., these are serious, serious issues. And I don't like hearing that we have blind spots.

So I'd like a little more analysis about if there are other authorities that are needed. And I've heard you all say you don't need other authorities, but I guess I'm not willing to accept that we are going to have blind spots. I think there has to be an appropriate way to give the tools that our Intelligence Community needs to be able to constantly protect against cyber threat, cyber terrorism, and cyberattack.

Director HAINES. Thank you, Senator.

I'll just start, and obviously I'll leave the bulk of the answer to General Nakasone, who will have more views on the specifics in this area. But I would say that—I think, really support the law that is currently being considered, which is basically something that would create, as I understand it, an obligation on companies to provide information when there are attacks, much like FireEye did in the context of SolarWinds. And that is something that I think would be useful.

It is obviously one piece of the puzzle, and I think General Nakasone can speak with greater authority on what specifically the other issues are, and answering your further questions.

General NAKASONE. Senator, I share your concern with these blind spots, and this is something we shouldn't accept. Let me be a little bit more specific in terms of the blind spots. When an adversary decides that they're going to conduct an intrusion into a U.S. company, a U.S. Government agency, one of the things that they realize is the fact if they can come into the United States and use an Internet service provider in a period of time, they can quickly do that and conduct their operations and virtually not have any coverage in a timely manner from our ability to do surveillance in the United States. And that's obviously through a warrant, most likely done by the Federal Bureau of Investigation.

They understand the timeline that it takes for a warrant to be done, and so they are being able to expose this gap. This is one of the areas that we have to understand our adversaries are using today. It's the way that they have structured their activities, and it's in a way that we as we go forward need to be able to address. Again, it's not that we are looking for authorities for the National Security Agency. It's let's make sure that we identify what's taking place, so the appropriate measures can be undertaken.

Chairman WARNER. Senator Cotton.

Senator COTTON. Thank you all for your appearance here today. These hearings are always a welcome opportunity to highlight the work that you and all of the men and women do in your agencies and organizations to help keep our country safe. Most of the Committee's work, like most of your work, happens behind closed doors in a classified setting, so the American people don't appreciate the great work that you and the men and women you lead do for our country. So I'm glad that we have a chance to highlight this once a year or so.

I also want to stress the importance of protecting all the information that your people collect. And Director Wray, part of the FBI's responsibility is to ensure that classified information is handled correctly, that it's not disclosed in a way that could pose a risk toward Americans' national security or intelligence or military operations. Is that correct?

Director WRAY. Yes, that's correct.

Senator COTTON. And that applies to all persons, to include persons especially who are cleared to handle classified information as well.

Director WRAY. Well, it's a responsibility that we share with other agencies in that respect, but yes.

Senator COTTON. And so you do investigate instances of alleged disclosure of classified information that was done wrongly?

Director WRAY. Absolutely. We have quite a number of such investigations.

Senator COTTON. So I just want to take this opportunity to call your attention to a letter that Senator Hagerty and I and 16 other Republican Senators sent to you yesterday, about what appears to have been a potentially serious breach of handling of classified information by Dr. Colin Kahl, the nominee to be the Undersecretary of Defense for Policy. Could I get your commitment to provide a prompt response to that letter to the United States Senate, since this nomination could be pending just anytime now?

Director WRAY. Senator, I'm aware of the letter. I haven't had a chance to review it yet, but I'm happy to take it—.

Senator COTTON. Thank you. I don't expect you to be fully apprised of the facts or have a conclusion about whether you should or should not, or will or will not, start an investigation. But I think it's very worrisome, and there are people sitting in Federal prison today for mishandling classified information. And if a GS employee is going to be sitting in Federal prison because they mishandled classified information, we should always insist that everyone handle it correctly, no matter how powerful they are or who they're connected to. So thank you for that commitment, Director Wray.

Ms. Haines, I want to turn to a line from the annual threat assessment about the migration crisis we see on our southern border. It lists several potential factors, in terms of seasonal employment opportunities or the pandemic or what have you. One factor was perceived changes in U.S. immigration policy. Is it possible that a factor could also be actual changes to U.S. immigration policy?

Director HAINES. Thank you, Senator.

I think we were looking at the degree of folks coming, and so I don't think that there were, in fact, changes at the time that would've accounted for. In other words, it was perceived changes that they were looking at.

Senator COTTON. So I know that you are not in charge of immigration policy and I don't expect you to be, but I'll give you three changes that actually have been made by the Biden administration since the first day.

One, they created an exception to the pandemic exclusionary order for minors. Not shockingly, we have a surge of minors at the border.

Two, they eliminated the Safe Third Country agreements with Central American countries, most notably Guatemala, the geographic chokepoint from Central America. And three, they eliminated the Remain in Mexico policy as well. So those are three actual policies on which word is out in Central America.

And finally, I'll just give you this bit of open source intelligence that you can go back, Director Burns and Director Haines, and tell your analysts about. I was at the border a couple weeks ago. I had a chance to see the heartbreaking scenes of young mothers and fathers with their young kids under the bridge outside McAllen where they were being processed in, after having just crossed the river with the help of smugglers and traffickers.

I grabbed a border patrol officer who spoke Spanish so he could interpret for me. I asked a couple dozen of them why they made the journey now, where they had come from, how long they'd been there. Not a single one of them made a comment about asylum, in terms of persecution based on race, ethnicity, sex, religion, political views, or anything else. The most common answers were: Joe Biden, I can get in now, and I want a job.

I have some other issues I want to discuss, but as I said earlier, most of that we have to do in a classified setting, so I'll look forward to talking with you all again in a few minutes. Thank you.

Chairman WARNER. Thank you, Senator Cotton. Senator Rubio, any closing comments?

Vice Chairman RUBIO. No, I want to thank you guys. I think it's been important to get a lot of these things on the record. It's a rare opportunity for the American public to hear from each of you individually, and I'm glad we were able to do it again this year. And I look forward to our session this afternoon.

Thank you all for being here.

Chairman WARNER. Well, let me before I just close, three quick things.

One, I think you've heard this from virtually every member. A hearty thanks to not just you, but to literally thousands of men and women that work for you, and I hope you will take that message back to the workforce. I think Senator Burr mentioned we value very much this relationship we have with the IC and want to keep it open, and we always want to have your back.

Two, I think, Director Haines, you've made mention of this. I think almost the majority of Members on the Committee are actively working on bipartisan legislation that would encourage around this idea of tech alliances; that we do this not only in a greater way with the private sector, but we also do it with—even beyond our Five Eye partners.

And three, as we have discussed again in a broadly bipartisan way, we've taken some of the lessons from our SolarWinds hearing, and I think we may have at least a partial response where, with appropriate liability protections, there would be some level of mid-incident reporting to an enterprise that would include public and private together. So that we could potentially close some of these gaps that Senator Gillibrand and others have raised in their questioning.

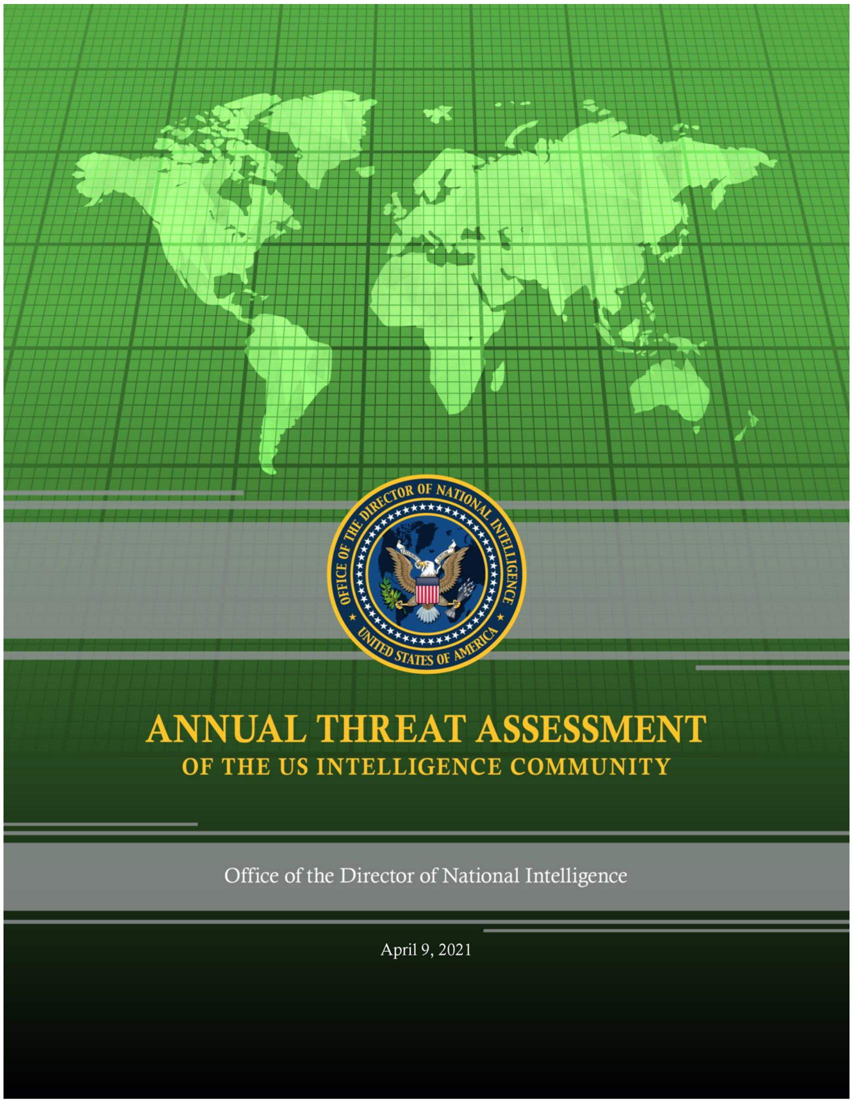
Again, we thank you all. We've got a couple of votes.

We will still reconvene in room SVC–217 at one o'clock. Have an enjoyable lunch.

Thank you.

[Whereupon at 12:15 p.m. the hearing was recessed, subject to the call of the Chairman.]

Supplemental Material



ANNUAL THREAT ASSESSMENT
OF THE US INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence

April 9, 2021

April 9, 2021

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 9 April 2021 was used in the preparation of this assessment.

CONTENTS

FOREWORD

In the coming year, the United States and its allies will face a diverse array of threats that are playing out amidst the global disruption resulting from the COVID-19 pandemic and against the backdrop of great power competition, the disruptive effects of ecological degradation and a changing climate, an increasing number of empowered non-state actors, and rapidly evolving technology. The complexity of the threats, their intersections, and the potential for cascading events in an increasingly interconnected and mobile world create new challenges for the IC. Ecological and climate changes, for example, are connected to public health risks, humanitarian concerns, social and political instability, and geopolitical rivalry. The 2021 Annual Threat Assessment highlights some of those connections as it provides the IC's baseline assessments of the most pressing threats to US 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 US adversaries' vulnerabilities. It accounts for functional concerns, such as weapons of mass destruction and technology, primarily in the sections on threat actors, such as China and Russia.

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, despite the pandemic. 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. Russia is pushing back against Washington where it can globally, employing techniques up to and including the use of force. Iran will remain a regional menace with broader malign influence activities, and North Korea will be 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 US and allied forces, weakening our conventional deterrence, and worsening the longstanding threat from weapons of mass destruction.

The 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. Countries with high debts or that depend on oil exports, tourism, or remittances face particularly challenging recoveries, while others will turn inward or be distracted by other challenges.

Ecological degradation and a changing climate will continue to fuel disease outbreaks, threaten food and water security, and exacerbate political instability and humanitarian crises. Although much of the effect of a changing climate on US security will play out indirectly in a broader political and economic context, warmer weather can generate direct, immediate impacts—for example, through more intense storms, flooding, and permafrost melting. This year we will see increasing potential for surges in migration by Central American populations, which are reeling from the economic fallout of the COVID-19 pandemic and extreme weather, including multiple hurricanes in 2020 and several years of recurring droughts and storms.

The scourge of illicit drugs and transnational organized crime will continue to take its toll on American lives, prosperity, and safety. Major narcotics trafficking groups have adapted to the pandemic's challenges to maintain their deadly trade, as have other transnational criminal organizations.

Emerging and disruptive technologies, as well as the proliferation and permeation of technology in all aspects of our lives, pose unique challenges. Cyber capabilities, to illustrate, are demonstrably intertwined with threats to our infrastructure and to the foreign malign influence threats against our democracy.

ISIS, al-Qa‘ida, and Iran and its militant allies continue to plot terrorist attacks against US persons and interests, including to varying degrees in the United States. Despite leadership losses, terrorist groups have shown great resiliency and are taking advantage of ungoverned areas to rebuild.

Regional conflicts continue to fuel humanitarian crises, undermine stability, and threaten US persons and interests. Some have direct implications for US security. For example, the fighting in Afghanistan, Iraq, and Syria has direct bearing on US forces, while tensions between nuclear-armed India and Pakistan remain a concern for the world. The iterative violence between Israel and Iran, the activity of foreign powers in Libya, and conflicts in other areas—including Africa, Asia, and the Middle East—have the potential to escalate or spread.

The 2021 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 US 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/or impactful near-term risks in the context of the longer-term, overarching threat environment.

CHINA’S PUSH FOR GLOBAL POWER

The Chinese Communist Party (CCP) will continue its whole-of-government efforts to spread China’s influence, undercut that of the United States, drive wedges between Washington and its allies and partners, and foster new international norms that favor the authoritarian Chinese system. Chinese leaders probably will, however, seek tactical opportunities to reduce tensions with Washington when such opportunities suit their interests. China will maintain its major innovation and industrial policies because Chinese leaders see this strategy as necessary to reduce dependence on foreign technologies, enable military advances, and sustain economic growth and thus ensure the CCP’s survival.

- Beijing sees increasingly competitive US-China relations as part of an epochal geopolitical shift and views Washington’s economic measures against Beijing since 2018 as part of a broader US effort to contain China’s rise.

- China is touting its success containing the COVID-19 pandemic as evidence of the superiority of its system.

- Beijing is increasingly combining its growing military power with its economic, technological, and diplomatic clout to preserve the CCP, secure what it views as its territory and regional preeminence, and pursue international cooperation at Washington’s expense.

Regional and Global Activities

China seeks to use coordinated, whole-of-government tools to demonstrate its growing strength and compel regional neighbors to acquiesce to Beijing’s preferences, including its claims over disputed territory and assertions of sovereignty over Taiwan.

- China-India border tensions remain high, despite some force pullbacks this year. China’s occupation since May 2020 of contested border areas is the most serious escalation in decades and led to the first lethal border clash between the two countries since 1975. As of mid-February, after multiple rounds of talks, both sides were pulling back forces and equipment from some sites along the disputed border.

- In the South China Sea, Beijing will continue to intimidate rival claimants and will use growing numbers of air, naval, and maritime law enforcement platforms to signal to Southeast Asian countries that China has effective control over contested areas. China is similarly pressuring Japan over contested areas in the East China Sea.

- Beijing will press Taiwan authorities to move toward unification and will condemn what it views as increased US-Taiwan engagement. We expect that friction will grow as Beijing steps up attempts to portray Taipei as internationally isolated and dependent on the mainland for economic prosperity, and as China continues to increase military activity around the island.

- China’s increasing cooperation with Russia on areas of complementary interest includes defense and economic cooperation.

Beijing will continue to promote the Belt and Road Initiative (BRI) to expand China's economic, political, and military presence abroad, while trying to reduce waste and exploitative practices, which have led to international criticism. China will try to increase its influence using "vaccine diplomacy," giving countries favored access to the COVID-19 vaccines it is developing. China also will promote new international norms for technology and human rights, emphasizing state sovereignty and political stability over individual rights.

China will remain the top threat to US technological competitiveness as the CCP targets key technology sectors and proprietary commercial and military technology from US and allied companies and research institutions associated with defense, energy, finance, and other sectors. Beijing uses a variety of tools, from public investment to espionage and theft, to advance its technological capabilities.

Military Capabilities

China will continue pursuing its goals of becoming a great power, securing what it views as its territory, and establishing its preeminence in regional affairs by building a world-class military, potentially destabilizing international norms and relationships. China's military commitment includes a multiyear agenda of comprehensive military reform initiatives.

- We expect the PLA to continue pursuing overseas military installations and access agreements to enhance its ability to project power and protect Chinese interests abroad.

- The PLA Navy and PLA Air Force are the largest in the region and continue to field advanced long-range platforms that improve China's ability to project power. The PLA Rocket Force's highly accurate short-, medium-, and intermediate-range conventional systems are capable of holding US and allied bases in the region at risk.

WMD

Beijing will continue the most rapid expansion and platform diversification of its nuclear arsenal in its history, intending to at least double the size of its nuclear stockpile during the next decade and to field a nuclear triad. Beijing is not interested in arms control agreements that restrict its modernization plans and will not agree to substantive negotiations that lock in US or Russian nuclear advantages.

- China is building a larger and increasingly capable nuclear missile 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 second-strike capability.

Space

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

- We expect a Chinese space station in low Earth orbit (LEO) to be operational between 2022 and 2024. China also has conducted and 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 (PNT)—and satellite communications into its weapons and command-and-control systems to erode the US 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 US and allied satellites.

- Beijing continues to train its military space elements and field new destructive and nondestructive ground- and space-based antisatellite (ASAT) weapons.

- China has already fielded ground-based ASAT missiles intended to destroy satellites in LEO and ground-based ASAT lasers probably intended to blind or damage sensitive space-based optical sensors on LEO satellites.

Cyber

We assess that China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat. China's cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US homeland, suppression of US web content that Beijing views as threatening to its internal ideological control, and the expansion of technology-driven authoritarianism around the world.

- We continue to assess that China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States.

- China leads the world in applying surveillance systems and censorship to monitor its population and repress dissent, particularly among ethnic minorities, such as the Uyghurs. Beijing conducts cyber intrusions that affect US and non-US citizens beyond its borders—such as hacking journalists, stealing personal information, or attacking tools that allow free speech online—as part of its efforts to surveil perceived threats to CCP power and tailor influence efforts. Beijing is also using its assistance to global efforts to combat COVID-19 to export its surveillance tools and technologies.

- 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.

Intelligence, Influence Operations, and Elections Influence and Interference

China will continue expanding its global intelligence footprint to better support its growing political, economic, and security interests around the world, increasingly challenging the United States' alliances and partnerships. Across East Asia and the western Pacific, which Beijing views as its natural sphere of influence, China is attempting to exploit doubts about the US commitment to the region, undermine Taiwan's democracy, and extend Beijing's influence.

- Beijing has been intensifying efforts to shape the political environment in the United States to promote its policy preferences, mold public discourse, pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China on such issues as religious freedom and the suppression of democracy in Hong Kong.

RUSSIAN PROVOCATIVE ACTIONS

***Moscow will continue to employ a variety of tactics this year meant to undermine US influence, develop new international norms and partnerships, divide Western countries and weaken Western alliances, and demonstrate Russia's ability to shape global events as a major player in a new multipolar international order*.** Russia will continue to develop its military, nuclear, space, cyber, and intelligence capabilities, while actively engaging abroad and leveraging its energy resources, to advance its agenda and undermine the United States.

We expect Moscow to seek opportunities for pragmatic cooperation with Washington on its own terms, and we assess that Russia does not want a direct conflict with US forces.

- Russian officials have long believed that the United States is conducting its own "influence campaigns" to undermine Russia, weaken President Vladimir Putin, and install Western-friendly regimes in the states of the former Soviet Union and elsewhere.

- Russia seeks an accommodation with the United States on mutual noninterference in both countries' domestic affairs and US recognition of Russia's claimed sphere of influence over much of the former Soviet Union.

Regional and Global Activities

We assess that Moscow will employ an array of tools—especially influence campaigns, intelligence and counterterrorism cooperation, military aid and combined exercises, mercenary operations, assassinations, and arms sales—to advance its interests or undermine the interests of the United States and its allies. We expect Moscow to insert itself into crises when Russian interests are at stake, it can turn a power vacuum into an opportunity, or the anticipated costs of action are low. Russia probably will continue to expand its global military, intelligence, security, commercial, and energy footprint and build partnerships with US allies and adversaries alike—most notably Russia's growing strategic cooperation with China—to achieve its objectives.

- We assess that Russia's Federal Security Service (FSB) organized the assassination of a Chechen separatist in a Berlin park in 2019 and tried to kill opposition activist Aleksey Navalnyy inside Russia in 2020 with a fourth-generation chemical agent.

- In the Middle East and North Africa, Moscow is using its involvement in Syria and Libya to increase its clout, undercut US 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 Union, Moscow is well positioned to increase its role in the Caucasus, intervene in Belarus if it deems necessary, and continue destabilization efforts against Ukraine while settlement talks remain stalled and low-level fighting continues.

- Since 2006, Russia has used energy as a foreign policy tool to coerce cooperation and force states to the negotiating table. After a price dispute between Moscow and Kyiv, for example, Russia cut off gas flows to Ukraine, including transit gas, in 2009, affecting some parts of Europe for a 13-day period. Russia also uses its capabilities in civilian nuclear reactor construction as a soft-power tool in its foreign policy.

Military Capabilities

We expect Moscow's military posture and behavior—including military modernization, use of military force, and the integration of information warfare—to challenge the interests of the United States and its allies. Despite flat or even declining defense spending, Russia will emphasize 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 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.

- Private military and security companies managed by Russian oligarchs close to the Kremlin extend Moscow's military reach at low cost, allowing Russia to disavow its involvement and distance itself from battlefield casualties. These proxy forces, however, often fail to achieve Moscow's strategic goals because of their limited tactical proficiency.

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 physical security at Russian nuclear sites since the 1990s.

- Moscow views its nuclear capabilities as necessary to maintain deterrence and achieve 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.

- Russia is building a 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 US 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.

- Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis.

- A Russian software supply chain operation in 2020, described in the cyber section of this report, demonstrates Moscow's capability and intent to target and potentially disrupt public and private organizations in the United States.

- Russia is also using cyber operations to defend against what it sees as threats to the stability of the Russian Government. In 2019, Russia attempted to hack journalists and organizations that were investigating Russian Government activity and in at least one instance leaked their information.

- Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.

Intelligence, Influence Operations, and Elections Influence and Interference

Russia presents one of the most serious intelligence threats to the United States, using its intelligence services and influence tools to try to divide Western alliances, preserve its influence in the post-Soviet area, and increase its sway around the world, while undermining US global standing, sowing discord inside the United States, and influencing US voters and decisionmaking. Russia will continue to advance its technical collection and surveillance capabilities and probably will share its technology and expertise with other countries, including US adversaries.

- Moscow almost certainly views US elections as an opportunity to try to undermine US global standing, sow discord inside the United States, influence US decisionmaking, and sway US voters. Moscow conducted influence operations against US elections in 2016, 2018, and 2020.

Space

Russia will remain a key space competitor, maintaining a large network of reconnaissance, communications, and navigation satellites. It will focus on integrating space services—such as communications; positioning, navigation, and timing (PNT); geolocation; and intelligence, surveillance, and reconnaissance—into its weapons and command-and-control systems.

- Russia continues to train its military space elements and field new antisatellite (ASAT) weapons to disrupt and degrade US 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 US and allied satellites.

IRANIAN PROVOCATIVE ACTIONS

Iran will present a continuing threat to US and allied interests in the region as it tries to erode US influence and support Shia populations abroad, entrench its influence and project power in neighboring states, deflect international pressure, and minimize threats to regime stability. Although Iran's deteriorating economy and poor regional reputation present obstacles to its goals, Tehran will try a range of tools—diplomacy, expanding its nuclear program, military sales and acquisitions, and proxy and partner attacks—to advance its goals. We expect that Iran will take risks that could escalate tensions and threaten US and allied interests in the coming year.

- Iran sees itself as locked in a struggle with the United States and its regional allies, whom they perceive to be focused on curtailing Iran's geopolitical influence and pursuing regime change.

- Tehran's actions will reflect its perceptions of US, Israeli, and Gulf state hostility; its ability to project force through conventional arms and proxy forces; and its desire to extract diplomatic and economic concessions from the international community.

- With regards to US interests in particular, Iran's willingness to conduct attacks probably will hinge on its perception of the United States' willingness to respond, its ability to conduct attacks without triggering direct conflict, and the prospect of jeopardizing potential US sanctions relief.

- Regime leaders probably will be reluctant to engage diplomatically in talks with the United States in the near term without sanctions or humanitarian relief or the United States rejoining the Joint Comprehensive Plan of Action (JCPOA). Iran remains committed to countering US pressure, although Tehran is also wary of becoming involved in a full-blown conflict.

Regional Involvement and Destabilizing Activities

Iran will remain a problematic actor in Iraq, which will be the key battleground for Iran's influence this year and during the next several years, and Iranian-supported Iraqi Shia militias will continue to pose the primary threat to US personnel in Iraq.

- The rise in indirect-fire and other attacks against US installations or US-associated convoys in Iraq in 2020 is largely attributed to Iran-backed Iraqi Shia militias.

- Iran will rely on its Shia militia allies and their associated political parties to work toward Iran's goals of challenging the US presence and maintaining influence in Iraqi political and security issues. Tehran continues to leverage ties to Iraqi Shia groups and leaders to circumvent US sanctions and try to force the United States to withdraw through political pressure and kinetic strikes.

- Although Tehran remains an influential external actor in Iraq, Iraqi politicians, such as Prime Minister Mustafa al-Kadhimi, will attempt to balance Baghdad's relations with Iran and the United States in an effort to avoid Iraq becoming an arena for conflict between the two countries.

Iran is determined to maintain influence in Syria.

- Iran is pursuing a permanent military presence and economic deals in Syria as the conflict winds down there. Tehran almost certainly wants these things to build its regional influence, support Hizballah, and threaten Israel.

Iran will remain a destabilizing force in Yemen, as Tehran's support to the Huthis—including supplying ballistic and cruise missiles as well as unmanned systems—poses a threat to US partners and interests, notably through strikes on Saudi Arabia.

Tehran remains a threat to Israel, both directly through its missile forces and indirectly through its support of Hizballah and other terrorist groups.

Iran will hedge its bets in Afghanistan, and its actions may threaten instability. Iran publicly backs Afghan peace talks, but it is worried about a long-term US presence in Afghanistan. As a result, Iran is building ties with both the government in Kabul and the Taliban so it can take advantage of any political outcome.

Military Capabilities

Iran's diverse military capabilities and its hybrid approach to warfare—using both conventional and unconventional capabilities—will continue to pose a threat to US and allied interests in the region for the foreseeable future.

- Iran demonstrated its conventional military strategy, which is primarily based on deterrence and the ability to retaliate against an attacker, with its launch of multiple ballistic missiles against a base housing US forces in Iraq in response to the January 2020 killing of Iranian Islamic Revolutionary Guard Corps Qods Force (IRGC-QF) Commander Qasem Soleimani. Iran has the largest ballistic missile force in the region, and 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, maintain strategic depth, and provide asymmetric retaliatory options.

- The IRGC-QF and its proxies will remain central to Iran's military power.

Attacks on US Interests and the Homeland

We assess that Iran remains interested in developing networks inside the United States—an objective it has pursued for more than a decade—but the greatest risk to US persons exists outside the Homeland, particularly in the Middle East and South Asia.

- Iran has threatened to retaliate against US officials for the Soleimani killing in January 2020 and attempted to conduct lethal operations in the United States previously.

- During the past several years, US law enforcement has arrested numerous individuals with connections to Iran as agents of influence or for collecting information on Iranian dissidents in the United States, and Iran's security forces have been linked to attempted assassination and kidnapping plots in Europe, the Middle East, and South Asia.

- Iran probably can most readily target US interests in the Middle East and South Asia because it has assets and proxies in the region with access to weapons and explosives.

Nuclear Breakout

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. However, following the US withdrawal from the JCPOA agreement in May 2018, Iranian officials have abandoned some of Iran's commitments and resumed some nuclear activities that exceed the JCPOA limits. If Tehran does not receive sanctions relief, Iranian officials probably will consider options ranging from further enriching uranium up to 60 percent to designing and building a new 40 Megawatt Heavy Water reactor.

- Iran has consistently cast its resumption of nuclear activities as a reversible response to the US withdrawal from the JCPOA and messaged that it would return to full compliance if the United States also fulfilled its JCPOA commitments.

Since June 2019, Iran has increased the size and enrichment level of its uranium stockpile beyond JCPOA limits. Since September 2019, Iran has ignored restrictions on advanced centrifuge research and development and restarted uranium enrichment operations at the deeply buried Fordow facility. In January, Iran began to enrich uranium up to 20 percent and started R&D with the stated intent to produce uranium metal for research reactor fuel, and in February, it produced a gram quantities of natural uranium metal in a laboratory experiment.

Cyber, Intelligence, Influence, and Election Interference

Iran's expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US and allied networks and data. Iran has the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities.

- Iran was responsible for multiple cyber attacks between April and July 2020 against Israeli water facilities that caused unspecified short-term effects, according to press reporting.

Iran is increasingly active in using cyberspace to enable influence operations—including aggressive influence operations targeting the US 2020 presidential election—and ***we expect Tehran to focus on online covert influence, such as spreading disinformation about fake threats or compromised election infrastructure and recirculating anti-US content.***

- Iran attempted to influence dynamics around the 2020 US presidential election by sending threatening messages to US voters, and Iranian cyber actors in December 2020 disseminated information about US election officials to try to undermine confidence in the US election.

NORTH KOREAN PROVOCATIVE ACTIONS

North Korean leader Kim Jong Un may take a number of aggressive and potentially destabilizing actions to reshape the regional security environment and drive wedges between the United States and its allies—up to and including the resumption of nuclear weapons and intercontinental ballistic missile (ICBM) testing.

- We assess that Kim views nuclear weapons as the ultimate deterrent against foreign intervention and believes that over time he will gain international acceptance and respect as a nuclear power. He probably does not view the current level of pressure on his regime as enough to require a fundamental change in its approach.

- Kim also aims to achieve his goals of gaining prestige, security, and acceptance as a nuclear power through conventional military modernization efforts, nuclear weapon and missile development, foreign engagement, sanctions-evasion, and cyber capabilities.

Military Capabilities

North Korea will pose an increasing threat to the United States, South Korea, and Japan as it continues to improve its conventional military capabilities, providing Kim with diverse tools to advance his political objectives or inflict heavy losses if North Korea were attacked.

- Pyongyang portrayed a growing and more diverse strategic and tactical ballistic missile force during its January 2021 and October 2020 military parades.

WMD

North Korea will be a WMD threat for the foreseeable future, because Kim remains strongly committed to the country's nuclear weapons, the country is actively engaged in ballistic missile research and development, and Pyongyang's CBW efforts persist.

- Despite announcing an end to North Korea's self-imposed moratorium on nuclear weapons and ICBM testing in December 2019, Kim thus far has not conducted long-range missile testing and has left the door open to future denuclearization talks with the United States. Kim may be considering whether to resume long-range missile or nuclear testing this year to try to force the United States to deal with him on Pyongyang's terms.

Cyber

North Korea's cyber program poses a growing espionage, theft, and attack threat.

- Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States, judging from its operations during the past decade, and it may be able to conduct operations that compromise software supply chains.

- North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs.

TRANSNATIONAL ISSUES

COVID-19 PANDEMIC AND DISEASES

The COVID-19 pandemic has disrupted life worldwide, with far-reaching effects that extend well beyond global health to the economic, political, and security spheres. We expect COVID-19 to remain a threat to populations worldwide until vaccines and therapeutics are widely distributed. The economic and political implications of the pandemic will ripple through the world for years.

The pandemic is raising geopolitical tensions, and great powers are jockeying for advantage and influence. States are struggling to cooperate—and in some cases are undermining cooperation—to respond to the pandemic and its economic fallout, particularly as some governments turn inward and question the merits of globalization and interdependence. Some governments, such as China and Russia, are using offers of medical supplies and vaccines to try to boost their geopolitical standing.

The economic fallout from the pandemic is likely to create or worsen instability in at least a few—and perhaps many—countries, as people grow more desperate in the face of interlocking pressures that include sustained economic downturns, job losses, and disrupted supply chains. Some hard-hit developing countries are experiencing financial and humanitarian crises, increasing the risk of surges in migration, collapsed governments, or internal conflict.

- 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. In April, the International Monetary Fund estimated that the global economy would grow 6 percent this year and 4.4 percent in 2022. This year's forecast is revised up 0.5 percentage points relative to the previous forecast, reflecting expectations of vaccine-powered strengthening of activity later in the year and additional policy support in a few large economies. The global growth contraction for 2020 is estimated at 3.3 percent.

- The resurgence in COVID-19 infections early this year may have an even greater economic impact as struggling businesses in hard-hit sectors such as tourism and restaurants fold and governments face increasing budget strains.

- The effects on developing countries—especially those that rely heavily on remittances, tourism, or oil exports—may be severe and longer lasting; many developing countries already have sought debt relief.

- The economic fallout from the COVID-19 pandemic, along with conflict and weather extremes, has driven food insecurity worldwide to its highest point in more than a decade, which increases the risk of instability. The number of people experiencing high levels of acute food insecurity doubled from 135 million in 2019 to about 270 million last year, and is projected to rise to 330 million by yearend.

The COVID-19 pandemic is prompting shifts in security priorities for countries around the world. As militaries face growing calls to cut budgets, gaps are emerging in UN peacekeeping operations; military training and preparedness; counterterrorism operations; and arms control monitoring, verification, and compliance. These gaps are likely to grow without a quick end to the pandemic and a rapid recovery, making managing conflict more difficult—particularly because the pandemic has not caused any diminution in the number or intensity of conflicts.

COVID-19-related disruptions to essential health services—such as vaccinations, aid delivery, and maternal and child health programs—will increase the likelihood of additional health emergencies, especially among vulnerable populations in low-income countries. As examples, the pandemic has disrupted HIV/AIDS treatments and preventative measures in Sub-Saharan Africa, as well as measles and polio vaccination campaigns in dozens of countries. World populations, including Americans, will remain vulnerable to new outbreaks of infectious diseases as risk factors persist, such as rapid and unplanned urbanization, protracted conflict and humanitarian crises, human incursions into previously unsettled land, expansion of international travel and trade, and public mistrust of government and health care workers.

CLIMATE CHANGE AND ENVIRONMENTAL DEGRADATION

We assess that the effects of a changing climate and environmental degradation will create a mix of direct and indirect threats, including risks to the economy, heightened political volatility, human displacement, and new venues for geopolitical competition that will play out during the next decade and beyond. Scientists also warn that warming air, land, and sea temperatures create more frequent and variable extreme weather events, including heat waves, droughts, and floods that directly threaten the United States and US interests, although adaptation measures could help manage the impact of these threats. The degradation and depletion of soil, water, and biodiversity resources almost certainly will threaten infrastructure, health, water, food, and security, especially in many developing countries that lack the capacity to adapt quickly to change, and increase the potential for conflict over competition for scarce natural resources.

- 2020 tied for the hottest year on record, following a decade of rising temperatures from 2010 to 2019. Arctic Sea ice minimum coverage reached its second lowest level on record in 2020, highlighting the increasing accessibility of resources and sea lanes in a region where competition is ratcheting up among the United States, China, and Russia.

- In 2020, six Atlantic storms passed a "rapid intensification threshold" because of warming temperatures, representing more damaging storms that offer less time for populations—as well as US military installations on the Gulf Coast—to evacuate or prepare.

- The 2020 storm season hit Central America particularly hard. The region already was suffering from several years of alternating drought and storms, increasing the potential for large-scale migration from the region as pandemic-related restrictions on movement ease.

- Environmental degradation from pollution and poor land management practices will continue to threaten human health and risk social unrest. Air pollution was the fourth leading risk factor for premature death globally in 2019, resulting in approximately 7 million deaths, and has been found to increase the susceptibility to and severity of COVID-19 infections. Despite temporary improvements in air quality globally in 2020 resulting from COVID-19 lockdowns, by September 2020 air pollution had returned to pre-pandemic levels.

- The threat from climate change will intensify because global energy usage and related emissions continue to increase, putting the Paris Agreement goals at risk. Even in the midst of a global pandemic that shuttered countries and significantly reduced travel, global CO2 emissions only decreased by less than 6-percent in 2020. By December 2020, they had rebounded to previous monthly levels as countries began to reopen, an indication of how strongly emissions are coupled to economic growth.

EMERGING TECHNOLOGY

Following decades of investments and efforts by multiple countries that have increased their technological capability, US leadership in emerging technologies is increasingly challenged, primarily by China. We anticipate that with a more level playing field, new technological developments will increasingly emerge from multiple countries and with less warning.

- New technologies, rapidly diffusing around the world, put increasingly sophisticated capabilities in the hands of small groups and individuals as well as enhancing the capabilities of nation states. **While democratization of technology can be beneficial, it can also be economically, militarily, and socially destabilizing.** For this reason, advances in technologies such as computing, biotechnology, artificial intelligence, and manufacturing warrant extra attention to anticipate the trajectories of emerging technologies and understand their implications for security.

China has a goal of achieving leadership in various emerging technology fields by 2030. China stands out as the primary strategic competitor to the U.S. because it has a well-resourced and comprehensive strategy to acquire and use technology to advance its national goals, including technology transfers and intelligence gathering through a Military-Civil Fusion Policy and a National Intelligence Law requiring all Chinese entities to share technology and information with military, intelligence and security services.

- Beijing is focused on technologies it sees as critical to its military and economic future, including broad enabling technologies such as biotechnology, advanced computing, and artificial intelligence, as well as niche technical needs such as secure communications.

Moscow also views the development of advanced S&T as a national security priority and seeks to preserve its technological sovereignty. Russia is increasingly looking to talent recruitment and international scientific collaborations to advance domestic R&D efforts but resource constraints have forced it to focus indigenous R&D efforts on a few key technologies, such as military applications of AI.

CYBER

Cyber threats from nation states and their surrogates will remain acute. Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure. Although an increasing number of countries and nonstate actors have these capabilities, we remain most concerned about Russia, China, Iran, and North Korea. Many skilled foreign cybercriminals targeting the United States maintain mutually beneficial relationships with these and other countries that offer them safe haven or benefit from their activity.

States' increasing use of cyber operations as a tool of national power, including increasing use by militaries around the world, raises the prospect of more destructive and disruptive cyber activity. As states attempt more aggressive cyber operations, they are more likely to affect civilian populations and to embolden other states that seek similar outcomes.

Authoritarian and illiberal regimes around the world will increasingly exploit digital tools to surveil their citizens, control free expression, and censor and manipulate information to maintain control over their populations. Such regimes are increasingly conducting cyber intrusions that affect citizens beyond their borders—such as hacking journalists and religious minorities or attacking tools that allow free speech online—as part of their broader efforts to surveil and influence foreign populations.

Democracies will continue to debate how to protect privacy and civil liberties as they confront domestic security threats and contend with the perception that free speech may be constrained by major technology companies. Authoritarian and illiberal regimes, meanwhile, probably will point to democracies' embrace of these tools to justify their own repressive programs at home and malign influence abroad.

During the last decade, state sponsored hackers have compromised software and IT service supply chains, helping them conduct operations—espionage, sabotage, and potentially prepositioning for warfighting.

- A Russian software supply chain operation against a US-based IT firm exposed approximately 18,000 customers worldwide, including enterprise networks across US Federal, state, and local governments; critical infrastructure entities; and other private sector organizations. The actors proceeded with follow-on activities to compromise the systems of some customers, including some US Government agencies.

FOREIGN ILLICIT DRUGS AND ORGANIZED CRIME

We expect the threat from transnational organized crime networks supplying potent illicit drugs, which annually kill tens of thousands of Americans, to remain at a critical level. The pandemic has created some challenges for traffickers, mainly due to restrictions on movement, but they have proven highly adaptable, and lethal overdoses have increased.

- Mexican traffickers dominate the smuggling of cocaine, fentanyl, heroin, marijuana, and methamphetamine into the United States. They produce heroin, marijuana, and methamphetamine in Mexico, and they obtain cocaine from South American suppliers. They almost certainly will make progress producing high-quality fentanyl through this year, using chemical precursors from Asia.

- The total number of overdose deaths increased from 2018 to 2019, and opioids—particularly fentanyl—are involved in more than half those deaths, according to the Centers for Disease Control. As of July 2020, provisional data suggests that the total number of overdose deaths have continued to rise.

- Traffickers temporarily slowed drug smuggling because of stricter controls along the US southwest border associated with the pandemic but have since resumed operations.

Transnational criminal organizations will continue to employ cyber tools to steal from US and foreign businesses and use complex financial schemes to launder illicit proceeds, undermining confidence in financial institutions.

MIGRATION

The forces driving global migration and displacement—including economic disparities and the effects of extreme weather and conflict—almost certainly will encourage migration and refugee flows, but pandemic restrictions will remain a check on cross-border movements. Migration and displacement will heighten humanitarian needs, increase the risk of political upheaval, exacerbate other health crisis risks, and aid recruitment and radicalization by militant groups—particularly as COVID-19 strains global humanitarian response mechanisms and funding.

Many refugees and internally displaced persons are unlikely to return to their homes.

The number of people being displaced within their own national borders continues to increase, further straining governments' abilities to care for their domestic populations and mitigate public discontent.

Transnational organized criminal groups exploit migrants through extortion, kidnapping, and forced labor, and facilitate migration to divert attention from their other illicit activities.

In the Western Hemisphere, the combined effects of the pandemic and hurricanes, as well as perceived changes in US immigration policy and seasonal employment opportunities in the United States, are creating the economic and physical conditions for a resurgence in US-bound migration—especially if COVID-19 infection rates in the United States decline.

Last year, mobility restrictions tied to COVID-19 initially suppressed migration from Central America to the US southwest border, but the number of migrants started to rise again in mid-2020.

High crime rates and weak job markets remain primary push factors for US-bound migration from Central America because origin countries lack the capacity to address these challenges.

Migration from the Middle East and North Africa to Europe has continued to decline since its peak in 2015, and COVID-19 travel restrictions are likely to further suppress migrant flows this year, but renewed conflicts in the Middle East could trigger more migration, and previous waves fanned nationalist sentiments in many European countries. Countries are witnessing the rise of populist politicians and parties campaigning on loss of sovereignty and identity. Some European countries are trying to balance migration and COVID-19 concerns with the need for workers to supplement their aging workforces.

GLOBAL TERRORISM

We assess that ISIS and al-Qa'ida remain the greatest Sunni terrorist threats to US interests overseas; they also seek to conduct attacks inside the United States, although sustained US and allied CT pressure has broadly degraded their capability to do so. US-based lone actors and small cells with a broad range of ideological motivations pose a greater immediate domestic threat. We see this lone-actor threat manifested both within homegrown violent extremists (HVEs), who are inspired by al-Qa'ida and ISIS, and within domestic violent extremists (DVEs), who commit terrorist acts for ideological goals stemming from domestic influences, such as racial bias and antigovernment sentiment. DVEs also are inspired by like-minded individuals and groups abroad. Lebanese Hizballah might conduct attacks against US and allied interests in response to rising tensions in the Middle East and as part of its effort to push the United States out of the region. The diffusion of the terrorist threat globally, competing priorities for many countries, and in some cases decreased Western CT assistance probably will expand opportunities for terrorists and provide them space to recover from recent setbacks.

ISIS

ISIS remains capable of waging a prolonged insurgency in Iraq and Syria and leading its global organization, despite compounding senior leadership losses. Although we have seen a decline in the number of ISIS-inspired attacks in the West since they peaked in 2017, such attacks remain a high priority for the group. ISIS-inspired attacks very likely will remain the primary ISIS threat to the US homeland this year, rather than plots operationally supported or directed by ISIS, given the logistical and security challenges the group would need to overcome to deploy and support attackers in the United States.

- ISIS will attempt to expand its insurgency in Iraq and Syria, where it has been attacking prominent local leaders, security elements, infrastructure, and reconstruction efforts.
- The appeal of ISIS's ideology almost certainly will endure, even if it appeals to a narrower audience. The group will continue to use its media to encourage global supporters to conduct attacks without direction from ISIS leadership, but ISIS's degraded media capabilities probably will hamper its ability to inspire its previous high pace of attacks and attract recruits and new supporters.

Al-Qa'ida

Al-Qa'ida's senior leadership cadre has suffered severe losses in the past few years, but remaining leaders will encourage cooperation among regional elements, continue calls for attacks against the United States and other international targets, and seek to advance plotting around the world. Al Qa'ida's regional affiliates will exploit local conflicts and ungoverned spaces to threaten US and Western interests, as well as local governments and populations abroad.

- Al-Qa'ida's affiliates in the Sahel and Somalia have made gains during the past two years, but the group experienced setbacks elsewhere, including losing key leaders or managing only limited operations in North Africa, South Asia, Syria, and Yemen.

Hizballah

We expect Hizballah, in coordination with Iran and other Iran-aligned Shia militants, to continue developing terrorist capabilities as a deterrent, as retaliatory options, and as instruments of coercion against its adversaries.

Hizballah's focus on reducing US influence in Lebanon and the Middle East has intensified following the killing of IRGC-QF Commander Qasem Soleimani. Hizballah maintains the capability to target, both directly and indirectly, US interests inside Lebanon, in the region, overseas, and—to a lesser extent—in the United States.

Racially or Ethnically Motivated Violent Extremists

DVEs motivated by a range of ideologies that are not connected to or inspired by jihadi terrorist organizations like al-Qa'ida and ISIS pose an elevated threat to the United States. This diverse set of extremists reflects an increasingly complex threat landscape, including racially or ethnically motivated threats and antigovernment or antiauthority threats.

Of these, violent extremists who espouse an often overlapping mix of white supremacist, neo-Nazi, and exclusionary cultural-nationalist beliefs have the most persistent transnational connections via often loose online communities to like-minded individuals and groups in the West. The threat from this diffuse movement has ebbed and flowed for decades but has increased since 2015.

- Violent extremists who promote the superiority of the white race have been responsible for at least 26 lethal attacks that killed more than 141 people and for dozens of disrupted plots in the West since 2015. While these extremists often see themselves as part of a broader global movement, most attacks have been carried out by individuals or small, independent cells.

- Australia, Germany, Norway, and the United Kingdom consider white racially or ethnically motivated violent extremists, including Neo-Nazi groups, to be the fastest growing terrorist threat they face.

- Both these and other DVEs, such as antigovernment or antiauthority extremists, are motivated and inspired by a mix of ideological, sociopolitical, and personal grievances against their targets, which have increasingly included large public gatherings, houses of worship, law enforcement and government facilities, and retail locations. Lone actors, who by definition are not likely to conspire with others regarding their plans, are increasingly choosing soft, familiar targets for their attacks, limiting law enforcement opportunities for detection and disruption.

CBRN

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

CONFLICTS AND INSTABILITY

Internal and interstate conflict and instability will continue to pose direct and indirect threats to US persons and interests during the next year. Competition for power and resources, ethnic strife, and ideology will drive insurgency and civil war in many countries. Interstate conflicts will also flare, ranging from border sparring, such as that between China and India, to potentially more sustained violent confrontations.

AFGHANISTAN

We assess that prospects for a peace deal will remain low during the next year. The Taliban is likely to make gains on the battlefield, and the Afghan Government will struggle to hold the Taliban at bay if the coalition withdraws support.

- Kabul continues to face setbacks on the battlefield, and the Taliban is confident it can achieve military victory.
- Afghan forces continue to secure major cities and other government strongholds, but they remain tied down in defensive missions and have struggled to hold recaptured territory or reestablish a presence in areas abandoned in 2020.

INDIA-PAKISTAN

Although a general war between India and Pakistan is unlikely, crises between the two are likely to become more intense, risking an escalatory cycle. 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 heightened tensions raise the risk of conflict between the two nuclear-armed neighbors, with violent unrest in Kashmir or a militant attack in India being potential flashpoints.

MIDDLE EAST

The Middle East will remain a region characterized by pervasive conflicts, with active insurgencies in several countries, sparring between Iran and other countries, and persistent 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 and its leaders struggle to meet public expectations for political and economic reform. As a result, some states are likely to experience destabilizing conditions that may push them close to collapse. Conflicts that have simmered may flare, particularly if Russia, Turkey, and other countries intervene, increasing the risk of escalations and miscalculations.

Iraq

The Iraqi Government almost certainly will continue to struggle to fight ISIS and control Iranian-backed Shia militias. Baghdad relies on US and other external support to target ISIS leaders and cells; the group nonetheless has shown resilience as an insurgency. Iranian-backed Shia militias are likely to continue attacks against US targets, such as the February rocket attack on Irbil International Airport, to press US forces to leave if the Iraqi Government does not reach an agreement with Washington on a timetable for withdrawal. US personnel would also face danger if popular protests against government corruption and a declining economy took a more violent turn or if Baghdad became embroiled in a broader regional conflict.

Libya

The interim Government of National Unity will face enduring political, economic, and security challenges that have prevented previous governments from advancing reconciliation. Instability and the risk of renewed fighting in Libya's civil war will persist this year—despite limited political, economic, and security progress—and might spill over into broader conflict, as Libyan rivals struggle to resolve their differences and foreign actors exert influence. Egypt, Russia, the UAE, and Turkey are likely to continue financial and military support to their respective proxies. A potential flashpoint will be whether Russia and Turkey abide by the cease-fire, brokered by the UN in October 2020, which calls for the departure of foreign forces.

Syria

Conflict, economic decline, and humanitarian crises will plague Syria during the next few years, and threats to US forces will increase. President Bashar al-Asad is firmly in control of the core of Syria, but he will struggle to reestablish control over the entire country against residual insurgency, including reinforced Turkish forces, Islamic extremists, and opposition in Idlib Province. Asad will stall meaningful negotiations and rely on the support of Russia and Iran. The Kurds will face increasing Syrian regime, Russian, and Turkish pressure, especially as Kurdish economic and humanitarian conditions decline and if the United States withdraws forces. US forces in eastern Syria will face threats from Iranian and Syrian-regime-aligned groups, mostly through deniable attacks. Terrorists will try to launch attacks on the West from their safe havens in the country, and increased fighting or an economic collapse might spur another wave of migration.

ASIA

The Burmese military's February seizure of power, detention of State Counselor Aung San Suu Kyi, and declaration of a one-year state of emergency marked a break in that country's democratic transition and ushered in new societal instability and widespread popular protests amidst COVID-19-related economic strains.

LATIN AMERICA

The Western Hemisphere almost certainly will see hotspots of volatility in the coming year, to include contested elections and violent popular protests. Latin America will hold several presidential and legislative elections this year, some of which—such as Honduras and Nicaragua—are occurring amidst heavily polarized environments in which allegations of fraud probably will arise.

- Public frustration is mounting over deep economic recessions following the COVID-19 pandemic, which is also compounding public concerns about crime and widespread official corruption. Colombia, Guatemala, and Peru have witnessed protests during the pandemic.

- Already-high rates of crime and narcotics trafficking probably will increase as poverty worsens and resources for police and judiciaries shrink, potentially fueling migration attempts to the United States.

- The political and economic crisis in Venezuela will continue, sustaining the outflow of Venezuelans into the rest of the region and adding strain to governments contending with some of the highest COVID-19 infection and death rates in the world.

AFRICA

East Africa will struggle with ethnic conflict in Ethiopia, power struggles within the transitional government in Sudan, and continued instability in Somalia, while a volatile mixture of intercommunal violence and terrorism will threaten West Africa's stability. Conflicts, undergoverned spaces, the marginalization of some communities, and persistent communications connectivity are likely to fuel terrorism during the next year, particularly in the Sahel and parts of eastern and southern Africa. Throughout Sub-Saharan Africa, a string of contentious elections will elevate the risk of political instability and violence.