S. HRG. 118–98

OPEN HEARING: THE 2023 ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 8, 2023

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

52–501 WASHINGTON : 2023

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 S. KING, Maine
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, Jr., Pennsylvania
KIRSTEN E. GILLIBRAND, New York
JON OSSOFF, Georgia

JAMES E. RISCH, Idaho
SUSAN M. COLLINS, Maine
TOM COTTON, Arkansas
JOHN CORNYN, Texas
JERRY MORAN, Kansas
JAMES LANKFORD, Oklahoma
MIKE ROUNDS, South Dakota

CHARLES E. SCHUMER, New York, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*
ROGER F. WICKER, Mississippi, *Ex Officio*

MICHAEL CASEY, *Staff Director*
BRIAN WALSH, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

MARCH 8, 2023

OPENING STATEMENTS

WITNESSES

OPEN HEARING: ON THE 2023 ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

WEDNESDAY, MARCH 8, 2023

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

The Committee met, pursuant to notice, at 10:11 a.m., in Room SH–216 in the Hart Senate Office Building, in open session, the Honorable Mark R. Warner, Chairman of the Committee, presiding.

Present: Senators Warner (presiding), Rubio, Wyden, Heinrich, King, Bennet, Casey, Gillibrand, Ossoff, Risch, Collins, Cotton, Cornyn, Moran, Lankford, and Rounds.

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

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

Thank you all for coming before the Committee today to discuss the Intelligence Community's annual worldwide threat assessment. This is an opportunity for agencies to brief this oversight committee, and most importantly the American public, about the numerous threats and challenges facing our country.

Our Nation's intelligence professionals are America's eyes and ears. They provide crucial intelligence assessments and warnings to policymakers so that we might address not just immediate threats but dangers on the horizon.

I'd like to thank you and, importantly, the thousands of men and women of America's Intelligence Community whom you represent, for their quiet, unsung, and often unacknowledged service.

I think we all know—and we see this on a daily basis—we live in an increasingly challenging and complex world. While the ongoing war in Ukraine has shown that conventional military capabilities are still important, I think the very nature of national security is undergoing a profound transformation. National security in 2023 is not the same as it was in 1993, or for that matter, in 2003.

We can no longer just pay attention to who has the most tanks, airplanes, or missiles. We also need to focus on technology, R&D

dollars, strategic investment flows, and supply chains, because whoever leads and wins the challenges in technology domains will have an edge in national security competition in the future.

We've already seen this with the outsized impact of cyber tools, which now give both state and non-state actors alike the power to cripple a country's critical infrastructure and entire economies from behind a keyboard without firing a single shot. And we're increasingly seeing rising competition in the technology space with the authoritarian regimes that are challenging democratic norms at home and around the world.

The People's Republic of China under President Xi and the Chinese Communist Party is now unfortunately a near-peer competitor with our country in its economy, technology, and military capabilities. I think it is more important than just political correctness to emphasize, at least in my mind, our beef is with Xi Jinping, the Communist Party, and their authoritarian tendencies. It is not with the Chinese people, it is not with the Chinese diaspora, it is not with Chinese-Americans or Asian-Americans, who oftentimes have been the strongest critics of the increasingly-authoritarian regime of the Xi government and who are often victims themselves of CCP's repression.

While America has focused for two decades on counterterrorism, China was racing to overtake the United States in a range of emerging and foundational technologies, such as advanced wireless communication semiconductors, quantum synthetic biology, and next generation energy, as well as taking not only the extraction but the processing of rare earth minerals that are so critical in so many of those technologies.

The PRC has also become an active player in the international technology standard-setting bodies and is embedding itself in global supply chains. All of this is why the United States must aggressively invest in talent, tools, and research to lead in tomorrow's technologies.

Today, you'll undoubtedly be asked about the IC's assessments on the origins of COVID–19. Let's be clear, despite China's denials, it is entirely fair for us to ask whether the virus that has killed at least 6.8 million so far might have been accidentally released from a lab in Wuhan. That these questions are even necessary is a testament to the failings of the Chinese system and stands in contrast to the openness of our own public health officials during the pandemic. The lack of transparency in China's authoritarian systems may mean that we will never be absolutely certain where COVID–19 or, God forbid, the next pandemic, could have or will next originate.

Looking towards Russia, we are now in the second year of the war in Ukraine. The IC—and I'm going to commend so many of you who did an incredible job of predicting Putin's plans and issuing warnings about the invasion, declassifying and sharing intelligence in a timely way—and I know from many of you that was totally against your grain, but making that declassification in a timely way, I really think upended Russia's plans and kept Putin off his game.

Over the last years, Ukrainians have displayed resolve bravery, resourcefulness, as they have defended their country against Rus-

sia's ruthless invasion. NATO's more united than ever and democracies around the world have rallied with unprecedented assistance to Ukraine in training, intelligence sharing, humanitarian, and modern military equipment.

I hope that we'll hear IC's assessment of the trajectory of this bloody conflict and what we think the end game will be, while at the same time, obviously maintaining Ukraine's right to exist as a sovereign nation.

I'm sure that we will discuss the multitude of other threats from rogue states like Iran and North Korea to emerging global health threats to the threat of global warming as well as the threats presented to the IC's workforce by anomalous health incidents or AHIs.

All of your agencies rely on world class talent of your workforce, and that's why this Committee will continue our efforts to ensure on federal security clearance reform. Hiring and retention is so important to make sure we maintain that world class workforce.

One last thing to note, and I think I speak for everyone on both sides of the aisle on this Committee: we still have unfinished business regarding the classified documents that we need to see in order for this Intelligence Committee to effectively oversee its job on intelligence oversight. We must resolve this issue soon.

The challenges we face are more varied and dynamic than ever and clearly you all have your hands full, but we also have, I think, in this hearing, particularly for the public part, a chance to underscore conviction in our values and our efforts to reinvigorate our allies around the world and to be clear eyed about the threats that authoritarian regimes like China and Russia pose.

So, I look forward to today's discussion. And with that, I'll turn it over to the Vice Chairman.

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

Vice Chairman RUBIO. Thank you, Mr. Chairman. Thank you all for coming in here today.

For two decades after the end of the Cold War, our country, the United States, was the world's sole superpower and that gave us the luxury to hope for a world in which Russia and China were coming into convergence with the values of the free world. And I think it also gave us the luxury of entertaining this fantasy that somehow free trade and globalizing the economy would produce peace, prosperity, and prevent nation-state rivalry.

And that brief period of time, between the end of the Cold War and very recently, was an historic anomaly. The truth is that if you look at 500 years of geopolitics, it's been defined by great power competition and that's where we find ourselves once again.

It's clear there's not going to be any convergence of values. It's clear that globalization led to the rise of China. But it also de-industrialized America, created long and vulnerable supply chains that eroded our middle class, left our society deeply divided along socioeconomic lines. And we now find ourselves in a new world, one divided between the free nations led still by America and the authoritarian and tyrannical block, led by Beijing—and then dozens and dozens of developing countries that are leveraging both sides

against each other on issue after issue to cut the best deal for themselves.

So today, we gather here, as we do once a year, to discuss the worldwide threats facing our country and those threats, there are no shortage of them, from China, Russia, Iran, North Korea, global terrorism, narco-terrorists operating just right off and across our border—and even in the homeland. All these are very serious threats, but it is my view that the greatest threat facing America is not another country. It is whether or not we have the ability and the willingness to accurately assess and appropriately adapt our foreign and domestic policies in this time of historic, revolutionary, and disruptive technological, social, economic, and geopolitical changes.

The answer to that question is not just going to determine the direction of our country. The answer to that question will define the twenty-first century. And on this matter, I believe that the Intelligence Community has a critical and vital role to play, first, because the changes we must make will have to overcome complacency, bureaucratic resistance, opposition from interest groups who benefit from the status quo, and frankly, public discomfort with the consequences of some of the changes we're going to need to make.

Complacency—because we've relied on our power advantages, and we've forgotten what it's like to live in a world where we have near-peer competitors.

Bureaucratic resistance—because our government, frankly, the commentary class, think tanks, academia, to some extent even Congress, is still filled with officials who came of age in the post-Cold War fantasy about the end of history.

Opposition from powerful interests—because multinational corporations that dominate and have consolidated some of our most important industries are deeply invested in foreign supply chains and in the current state of the global economy.

And public discomfort—frankly, because we've become a society addicted to cheap products from China and viral videos on TikTok.

Overcoming all of this will only be possible if we can motivate policymakers and convince our citizens of the need to act on at least five distinct areas of great power competition and potentially great power conflicts.

It's a military competition, one which we can no longer rely on overwhelming advantages to deliver relatively quick success.

It's a diplomatic and political competition for influence and multilateral institutions and entering into and maintaining important international alliance.

It's an economic and industrial competition over critical industries, supply chains, access to resources, the flow of capital.

It's a scientific and technological competition on areas ranging from precision medicine, artificial intelligence, cyber, the digital economy, quantum computing, control over valuable personal data, and protecting innovation and intellectual property.

And it's an informational competition involving closed and controlled societies dedicated to using our openness to divide us against each other here at home and drive disinformation to further their narrative and undermine our standing in the world.

In the twenty-first century, providing policymakers information on these areas of competition and understanding how they intersect with one another is a vital and critical national priority. And only our intelligence agencies have the resources and the broad-based insight needed to provide this.

Intelligence work today is not just about collecting state secrets and protecting our own, it is now also increasingly about the importance analysis of what all of these factors mean tied together so that we as policymakers can decide what matters and what doesn't, so that we can prioritize the urgent over the important.

Getting this wrong is the single greatest threat facing our country; and getting it right, the single most important task we have at hand. So, I hope we can hear in this open setting how each of the agencies represented here today is adjusting to this historic challenge, because we simply have no time to waste.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Rubio.

For Members and audience, we're going to have an open session now. We are going to work through the votes this morning and the Vice Chairman and I will take turns getting out to vote. We will go immediately into a closed session and bring lunch along the way. We want to make sure we take advantage of as much time as needed with our distinguished panel.

And although we've got great attendance at the gavel, we are going to go by seniority today, just because I know a lot of Members have got other committee meetings as well this morning.

With that, I think, Director Haines, are you going to start us off?

STATEMENT OF HON. AVRIL HAINES, DIRECTOR OF NATIONAL INTELLIGENCE

Director HAINES. Yes, Chairman. I'll deliver the statement for the group in a sense.

Chairman Warner, Vice Chairman Rubio, Members of the Committee, thank you for the opportunity to be here today alongside my wonderful colleagues, on behalf of the extraordinary public servants we lead in the Intelligence Community, to present the IC's annual threat assessment.

Before I start, I just want to publicly thank the men and women of the Intelligence Community whose work we're presenting today, from the collector to the analyst and everybody in between, who made it possible for us to bring you the annual threat assessment in hopes that this work will help keep our country safe and prosperous. Thank you.

This year's assessment notes that during the coming year, the United States and its allies will face an international security environment dominated by two sets of strategic challenges that intersect with each other and existing trends to intensify their national security implications.

First great powers rising, regional powers, and an evolving array of non-state actors are vying for influence and impact in the international system, including over the standards and rules that will shape the global order for decades to come. The next few years are critical as strategic competition with China and Russia intensifies, in particular how the world will evolve and whether the rise of

authoritarianism can be checked and reversed. Other threats are, of course, also individually significant, but how well we stay ahead of and manage this competition will be fundamental to our success at navigating everything else.

Second, challenges that transcend borders, including climate change, human and health security, and economic needs made worse by energy and food security as well as Russia's unprovoked and illegal invasion of Ukraine are converging as the planet emerges from the COVID–19 pandemic and all at the same time as great powers are challenging longstanding norms for transnational cooperation. And further compounding this dynamic is the impact that rapidly emerging technologies are having on governance, business, society, and intelligence around the world. And given that background, perhaps needless to say, the People's Republic of China, which is increasingly challenging the United States, economically, technologically, politically, and militarily around the world remains our unparalleled priority. Chinese Communist Party, or CCP, under President Xi Jinping will continue efforts to achieve Xi's vision of making China the preeminent power in East Asia and a major power on the world stage.

To fulfill Xi's vision, however, the CCP is increasingly convinced that it can only do so at the expense of U.S. power and influence and by using coordinated whole of government tools to demonstrate strength and compel neighbors to acquiesce to its preferences, including its land, sea, and air claims in the region and its assertions of sovereignty over Taiwan.

Last October, President Xi secured his third five-year term as China's leader at the 20th Party Congress. And as we meet today, China's national legislature is in session, formally appointing Xi and confirming his choice to lead the PRC's State Council, as well as its ministries and leaders of the military, legislature, and judicial branches. And after more than a decade of serving as China's top leader, Xi's control over key levers of power gives him significant power and influence over most issues. Xi has surrounded himself with likeminded loyalists at the apex of the Party's Standing Committee, China's highest decision-making body. And we assess that during the course of Xi's third term, they will together attempt to press Taiwan on unification, undercut U.S. influence, which they perceive as a threat, and drive wedges between Washington and its allies and partners and promote certain norms that favor China's authoritarian system.

And you may have seen Xi's recent criticism during his speech on Monday, of what he referred to as America's suppression of China, reflecting his longstanding distrust of U.S. goals and his apparent belief that the United States seeks to "contain China". And Xi's speech this week was the most public and direct criticism that we've seen from him to date and probably reflects growing pessimism in Beijing about China's relationship with the United States as well as Xi's growing worries about the trajectory of China's domestic economic development and indigenous technology innovation, challenges that he now blames on the United States.

He also wants to message his populist and regional actors that the U.S. bears the responsibility for any coming increase in tensions. And despite this more public and directly critical rhetoric

however, we assess that Beijing still believes it benefits most by preventing a spiraling of tensions and by preserving stability in its relationship with the United States. And specifically, Beijing wants to preserve stability in East Asia, avoid triggering additional economic punishments from U.S. sanctions and U.S. partners, and showcase a steady relationship with the United States to help avoid setbacks in its other relationships around the world, even while signaling opposition to claimed U.S. provocations including the shoot-down of the PRC balloon. He wants a period of relative calm to give China the time and stability it needs to address growing domestic difficulties.

And Xi's principal focus is on domestic economic development, which is not assured. In fact, the IC assesses that China's long term economic growth will continue to decelerate because China's era of rapid catchup growth is ending and structural issues such as debt, demographics, inequality, overreliance on investment, and suppressed consumption remain. And although the CCP may find ways to overcome its structural challenges over the long term, in the short term, the CCP continues to take an increasingly aggressive approach to external affairs, pursuing its goal of building a world-class military, expanding its nuclear arsenal, pursuing counter-space weapons capable of targeting U.S. and allied satellites, forcing foreign companies and coercing foreign countries to allow the transfer of technology and intellectual property in order to boost its indigenous capabilities, continuing to increase global supply chain dependencies on China with the aim of using such dependencies to threaten and cut off foreign countries during a crisis, expanding the cyber pursuits and increasing the threat of aggressive cyber operations against the U.S. homeland and foreign partners, and expanding influence operations, including through the export of digital repression technologies.

And the CCP will also seek to reshape global governance in line with his preferences and governance standards that support its monopoly of power within China. Beijing is elevating PRC candidates and policies at the U.N., attempting to gain buy-in for Xi's development and global initiatives, promotes blocks like the Shanghai Cooperation Organization as a counterweight to the West, and shape multilateral groupings such as the formerly 17+1 Forum in Eastern Europe, but with mixed success. In brief, the CCP represents both the leading and most consequential threat to U.S. national security and leadership globally. And its intelligence specific ambitions and capabilities make it for us our most serious and consequential intelligence rival.

During the past year, the threat has been additionally complicated by a deepening collaboration with Russia, which also remains an area of intense focus for the Intelligence Community. In fact, we were last here for you and for our ATA hearing last year, it was only a few weeks after Russia's unprovoked and illegal invasion of Ukraine. And now we are over a year into the war, which is reshaping not only Russia's global relationships and strategic standing, but also our own, strengthening our alliances and partnerships in ways that President Putin almost certainly did not anticipate, often precipitating the very events that he was trying to avoid, such as Sweden and Finland's petition to join NATO.

And on the battlefield, there is currently a grinding attritional war in which neither side has a definitive military advantage, and the day-to-day fighting is over hundreds of meters currently focused largely in Donetsk as Russia tries to capture the remainder of the Oblast. The Russians are making incremental progress on Bakhmut, which is not a particularly strategic objective, but are otherwise facing considerable constraints, including personnel and ammunition shortages, dysfunction within the military's leadership, exhaustion, as well as morale challenges. And even as the Russian offensive continues, they are experiencing high casualty rates. Putin is likely better at understanding the limits of what his military is capable of achieving and appears to be focused on more modest military objectives for now.

Export controls and sanctions are hampering Russia's war effort, particularly by restricting access to foreign components necessary to produce weapon systems. If Russia does not initiate a mandatory mobilization and identify substantial third-party ammunition supplies, it will be increasingly challenging for them to sustain even the current level of offensive operations in the coming months; and consequently, they may fully shift to holding and defending the territories they now occupy.

In short, we do not foresee the Russian military recovering enough this year to make major territorial gains. But Putin most likely calculates that time works in his favor and that prolonging the war, including with potential pauses in the fighting, may be his best remaining pathway to eventually securing Russia's strategic interests in Ukraine, even if it takes years.

And Ukraine, of course, also faces challenges. Ukraine's prospects for success in a major spring offensive will probably hinge on a number of factors. And at present, the Ukrainian armed forces remain locked in a struggle to defend against Russian offenses across eastern Ukraine. And while these Russian assaults are costly for Russia, the extent to which Ukrainian forces are having to draw down their reserves and equipment, as well as suffer further casualties, will all likely factor into Ukraine's ability to go on the offensive later this spring.

The IC continues to monitor Putin's reactions and his nuclear saber-rattling. Our analysts assess that his current posturing is intended to deter the West from providing additional support to Ukraine as he weighs a further escalation of the conflict. He probably will still remain confident that Russia can eventually militarily defeat Ukraine and wants to prevent western support from tipping the balance and forcing a conflict with NATO.

And of course, the already considerable human toll of the conflict is only increasing. In addition to the many tens of thousands of casualties suffered by the Russian and Ukrainian militaries, more than eight million people have been forced to flee Ukraine since Russia invaded. And there is widespread reporting of atrocities committed by Russian forces, including deliberate strikes against non-military targets such as Ukraine's civilian population and civilian infrastructure, particularly its energy facilities and electric grid.

Russia and its proxy groups almost certainly are using so called filtration operations to detain and forcibly deport tens of thousands

of Ukrainian civilians to Russia. The IC is engaged with other parts of the U.S. government to document and hold Russia and Russian actors accountable for their actions.

The reaction to the invasion from countries around the world has been resolute, hurting Russia's reputation and generating criticism at home. And Moscow has suffered losses that will require years of rebuilding and leave it less capable of posing a conventional military threat to Europe and operating assertively in Eurasia and on the global stage. And as a result, Russia will become even more reliant on asymmetric options, such as nuclear, cyber, space capabilities, and on China.

Now, our assessment also covers Iran, which continues to pursue its longstanding ambitions for regional leadership and is a threat to U.S. persons, directly and via proxy attacks. Iran also remains a threat to Israel, both directly through its missile and UAV forces and indirectly through its support of Lebanese Hezbollah and other proxies. And most concerning, Iran has accelerated the expansion of its nuclear program, stating that it is no longer constrained by JCPOA limits and has undertaken research and development activities that would bring it closer to producing the fissile material necessary for completing a nuclear device following a decision to do so.

North Korea, similarly, remains a proliferation concern as it continues its efforts to steadily expand and enhance its nuclear and conventional capabilities targeting the United States and our allies, periodically using aggressive and potentially destabilizing actions to reshape the regional security environment in its favor and to reinforce its status as a de facto nuclear power.

And in addition, regional challenges such as interstate conflicts, key cases of instability, and poor governance developments also pose growing challenges.

In Africa and in the developing world, increased poverty, hindered economic growth, and widened inequality are creating the conditions that are feeding domestic unrest, insurgencies, democratic backsliding, authoritarianism, and cross-border conflict spillover. Several parts of the Middle East will remain plagued by war over the year, insurgencies, and corruption.

In the Western Hemisphere, persistent economic weakness, insecurity, and corruption are fueling public frustration in anti-status-quo pressures that very likely will present governance challenges to leaders, while also posing sustained spillover, migration, criminal, and economic challenges for the United States. And throughout the world, countries are struggling to maintain democratic systems and prevent the rise of authoritarians, in some cases because Russia and China are helping autocrats take or hold power.

And as I noted at the outset, transnational challenges interact in this complex system along with more traditional threats and often reinforce each other, creating compounding and cascading risks to U.S. national security. For example, climate change remains an urgent threat that will increasingly exacerbate risks to U.S. national security as the physical impacts increase and geopolitical tensions mount over the global response to the challenge.

And now, entering its fourth year, the COVID–19 pandemic remains one of the most significant threats to global public health at

a cost of more than 6.5 million lives and trillions of dollars in lost economic output today. In addition to direct effects of the pandemic resulting on economic human security, political national security implications of COVID–19 continue to strain recovery efforts presenting both known and unforeseen challenges that probably will ripple through society and the global economy during the next year—and for years to come.

Russia's aggression against Ukraine has aggravated COVID–19-related fragilities in the global economy, raised commodity prices, fueled market volatility, and contributed to food insecurity and financial instability. The combination of elevated energy and food prices has increased the number of individuals facing extreme poverty and food insecurity. Affected countries will struggle to reverse those trends through 2023, even if global food prices stabilize. Russia's war in Ukraine can be blamed for these intensifying effects, something much of the world also understands and that others, including China will have to come to terms with as they consider to what extent they want to continue assisting or enabling Russia.

Climate change, the pandemic, and conflicts are exacerbating irregular migration and in the Western Hemisphere. Push and pull factors that drive migrants to the United States, such as deteriorating socioeconomic and security conditions, misperceptions of U.S. policies, and employment opportunities in the United States will almost certainly persist through 2023.

Transnational criminal organizations exploit migrants through extortion, kidnapping, and human trafficking, including sex trafficking and forced labor. These organizations also continue to pose a direct threat through the production and trafficking of lethal illicit drugs, massive theft, financial and cybercrimes, money laundering, and eroding the rule of law in partner nations. In particular, the threat from illicit drugs is at historic levels with the robust supply of synthetic opioids from Mexican TCO's continuing to play a major role in driving American overdose deaths to over 100,000 annually.

And terrorism, of course, remains a persistent threat. But the problem is evolving. Individuals and cells adhering to ideologies espoused by ISIS, Al-Qaeda, and transnational racially or ethnically motivated violent extremist movements in particular, post significant threats to U.S. persons, facilities, and interests.

And then two indirect threats that I think are worth highlighting in the report: new technologies, particularly in the field of AI and biotechnologies are being developed and proliferating faster than companies and governments are able to shape norms governing their use, protect against privacy challenges associated with them, and prevent dangerous outcomes that they can trigger. The convergence of emerging technologies is likely to create breakthroughs that are not as predictable and that risk rapid development of more interconnected, asymmetric threats to U.S. interests.

And relatedly, foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years, threatening to distort publicly available information and probably outpacing efforts to protect digital freedoms and at the same time, educate audiences on how to distinguish fact from propaganda. Au-

thoritarian governments usually are the principal offenders of digital repression and of course, democracies with open information environments are the most vulnerable to them.

In closing, I want to bring to your attention an absolutely crucial authority that will expire at the end of this year if Congress does not act—Section 702 of the Foreign Intelligence Surveillance Act. I can tell you without hesitation that Section 702 was relied upon in gathering intelligence that was relevant to putting together this assessment, and it is hard to overestimate, frankly the importance of this authority to our work across the board. FISA Section 702 provides unique intelligence on foreign intelligence targets at a speed and reliability that we cannot replicate with any other authority. Section 702 was originally enacted with the primary focus of enabling the U.S. government to quickly collect on the communication of terrorists abroad. The authority allows the IC to acquire foreign intelligence from non-US people located outside of the United States who are using U.S. electronic communication service providers.

702 is still vital to our counterterrorism mission, as evidenced by its key role in the United States government's operations against former Al-Qaeda leader Ayman al-Zawahiri. But 702 is now principally relied upon for vital insights across a range of high priority threats: malicious cyber actors targeting U.S. critical infrastructure; U.S. government efforts to stop components of weapons of mass destruction from reaching foreign actors; and even key intelligence related to threats emanating from China, Russia, North Korea, Iran.

I realize that 702 is a powerful authority and it is incumbent on all of us in the Intelligence Community to ensure that the privacy and civil liberty interests of Americans are built into its design and implemented at every level. And over the last many years, we have significantly expanded oversight, dedicated resources to compliance in order to do just that, and we welcome the opportunity to work with you on reauthorizing this critical authority.

Thank you so much for your patience. And we look forward to your questions.

[The prepared statement of the witness follows:]

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

Avril Haines, Director of National Intelligence
Congressional Testimony
Annual Threat Assessment of the US Intelligence Community
March 08, 2023

Chairman Warner, Vice Chairman Rubio, Members of the Committee, thank you for the opportunity to be here today, alongside my wonderful colleagues and on behalf of the extraordinary public servants we lead in the Intelligence Community to present the IC's annual assessment of worldwide threats to U.S. national security.

Before I start, I just want to publicly thank the men and women of the intelligence community, whose work we are presenting today. From the collector to the analyst and everyone in between who made it possible for us to bring you the annual threat assessment in hopes that this work will help keep our country safe and prosperous – **Thank you.**

This year's assessment notes that during the coming year, the United States and its allies will face a complex and pivotal international security environment, dominated by the two sets of strategic challenges that intersect with each other and existing trends to intensify their national security implications.

First, great powers, rising regional powers, and an evolving array of non-state actors are vying for influence and impact in the international system, including over the standards and rules that will shape the global order for decades to come. The next few years are critical as strategic competition with China and Russia intensifies, in particular, over how the world will evolve and whether the rise of authoritarianism can be checked and reversed. Other threats are, of course, also individually significant, but how well we stay ahead of--and manage--this competition will be fundamental to our success at navigating everything else.

Second, challenges that transcend borders, including climate change, human and health security, and economic needs made worse by energy and food insecurity, as well as Russia's unprovoked and illegal invasion of Ukraine, are converging as the planet emerges from the COVID-19 pandemic -- and all at the same time as great powers are challenging longstanding norms for transnational cooperation. Further compounding this dynamic is the impact that rapidly emerging or evolving technologies are having on governance, business, society, and intelligence around the world.

I won't try to summarize the assessment in my opening – I know you would prefer to get to questions and so I will focus instead on current events in relation to China and Russia, which may serve as a basis for further questions, while only briefly touching on the other issues covered by our report.

Perhaps needless to say, the People's Republic of China, which is increasingly challenging the United States economically, technologically, politically, and militarily around the world, remains our unparalleled priority. The Chinese Communist Party or "CCP" under President Xi Jinping, will continue efforts to achieve Xi's vision of making China the preeminent power in East Asia and a major power on the world stage.

To fulfill Xi's vision, however, the CCP is increasingly convinced that it can only do so at the expense of U.S. power and influence, and by using coordinated, whole-of-government tools to demonstrate strength and compel neighbors to acquiesce to its preferences, including its land, sea, and air claims in the region and its assertions of sovereignty over Taiwan.

Last October, President Xi secured his third five-year term as China's leader at the 20th Party Congress, and as we meet today, China's national legislature is in session, formally appointing Xi and confirming his choice to lead the PRC's State Council, as well as its ministries and the leaders of the military, legislative, and judicial branches. After more than a decade serving as China's top leader, Xi's control over key levers of power gives him significant influence over most issues.

Xi has surrounded himself with like-minded loyalists at the apex of the Party's Standing Committee, China's highest decision-making body and we assess that during the course of Xi's third term they will together attempt to press Taiwan on unification; undercut U.S. influence – which they perceive as a threat; drive wedges between Washington and its allies and partners; and promote certain norms that favor China's authoritarian system.

You may have seen Xi's recent criticism during his speech on Monday of what he referred to as America's "suppression of China" reflecting his longstanding distrust of U.S. goals and his apparent belief that the United States seeks to "contain" China.

Xi's speech this week was the most public and direct criticism that we have seen from him to date, and probably reflects growing pessimism in Beijing about China's relationship with the United States, as well as Xi's growing worries about the trajectory of China's domestic economic development and indigenous technology innovation -- challenges that he now blames on the United States. He also wants to message his populace and regional actors that the US bears the responsibility for any coming increase in tensions.

Despite this more public and directly critical rhetoric, however, we assess that Beijing still believes it benefits most by preventing a spiraling of tensions and by preserving stability in its relationship with the United States.

Specifically, Beijing wants to preserve stability in East Asia, avoid triggering additional economic punishments from U.S. sanctions and U.S. partners, and showcase a steady relationship with the United States to help avoid setbacks in its other relationships around the world, even while signaling opposition to claimed U.S. provocations, including the shoot-down of the PRC balloon. He wants a period of relative calm to give China the time and stability it needs to address growing difficulties.

Xi's principal focus is on domestic economic development, which is not assured. In fact, the IC assesses that China's long-term economic growth will continue to decelerate because China's era of rapid catch-up growth is ending and structural issues, such as debt, demographics, inequality, overreliance on investment and suppressed consumption, remain.

And although the CCP may find ways to overcome its structural challenges over the long-term, in the short-term the CCP continues to take an increasingly aggressive approach to external affairs, pursuing its goal of building a world-class military, expanding its nuclear arsenal, pursuing counter-space weapons capable of targeting U.S. and allied satellites, forcing foreign companies and coercing foreign countries to allow the transfer of technology and intellectual property in order to boost its indigenous capabilities, continuing to increase global supply chain dependencies on China with the aim of using such dependencies to threaten and cut off foreign countries during a crisis, expanding its cyber pursuits and increasing the threat of aggressive cyber operations against the U.S. homeland and foreign partners, and expanding influence operations, including through the export of digital repression technologies.

The CCP will also seek to reshape global governance in line with his preferences and governance standards that support its monopoly of power within China. Beijing is elevating PRC candidates and policies at the UN, attempting to gain buy-in for Xi's vague development and global initiatives, promote blocs like the Shanghai Cooperation Organization as a counterweight to the West, and shape multilateral groupings, such as the formerly 17+1 forum in Eastern Europe, but with mixed success.

Economically, Beijing will try to expand its influence abroad and be seen as a champion of global development by promoting China-led alternatives to existing international development forums and frameworks. And in the technology arena, U.S.-China technology competition is primarily and most consequentially centered on foundational technologies for which leadership in new breakthroughs and applications will disproportionately influence broader longer-term technological advantage, as in the case of Semiconductors, Artificial Intelligence, Advanced computing, Quantum computing, and biotechnology and biomanufacturing.

In brief, the CCP represents both the leading and most consequential threat to U.S. national security and leadership globally and its intelligence-specific ambitions and capability make it for **us** our most serious--and consequential--intelligence rival.

During the past year, the threat has been additionally complicated by a deepening collaboration with Russia, which also remains an area of intense focus for the Intelligence Community.

In fact, when we were last before you for an ATA hearing, it was only a few weeks after Russia's unprovoked and illegal invasion of Ukraine. Now, we are over a year into the war, which is reshaping not only Russia's global relationships and strategic standing but also our own, strengthening our alliances and partnerships in ways that President Putin almost certainly did not anticipate – often precipitating the very events he hoped to avoid, such as Sweden and Finland's petition to join NATO.

On the battlefield, there is currently a grinding attritional war in which neither side has a definitive military advantage and the day-to-day fighting is over hundreds of meters – currently focused in Donetsk, as Russia tries to capture the remainder of the Oblast.

The Russians are making incremental progress on Bakhmut, which is not a particularly strategic objective, but are otherwise facing considerable constraints, including personnel and ammunition shortages, dysfunction within the military's leadership, exhaustion, as well as morale challenges.

Even as the Russian offensive continues, they are experiencing high casualty rates. Putin is likely better understanding the limits of what his military is capable of achieving and appears to be focused on more modest military objectives for now.

Export controls and sanctions are hampering Russia's war effort, particularly by restricting access to foreign components necessary to produce weapons systems. These economic strictures and Moscow's resulting need to increase support to ailing civilian industries such as aviation, auto, and rail, is stressing Russia's federal budget.

If Russia does not initiate a mandatory mobilization and identify substanial third-party ammunition supplies, they will face increasing challenges to sustain even the current level of offensive operations in the coming months and may fully shift to holding and defending the territories they occupy.

This makes the coming months a pivotal period in the war. While we do not foresee the Russian military recovering enough this year to make major territorial gains, Putin most likely calculates that time works in his favor and that prolonging the war, including with potential pauses in the fighting, may be his best remaining pathway to eventually securing Russia's strategic interests in Ukraine, even if it takes several years.

Ukraine, of course, also faces challenges. Ukraine's prospects for success in a major spring offensive will probably hinge on several factors. At present, the Ukrainian Armed Forces remains locked in a struggle to defend against Russian offensives across eastern Ukraine. While these Russian assaults are almost certainly costly for Russia, the extent to which Ukrainian forces are having to draw down their reserves and equipment, as well as suffer further casualties, will all likely factor into Ukraine's ability to go on the offensive later this spring.

The IC continues to monitor Putin's reactions and his nuclear saber rattling. Our analysts assess that his current posturing is intended to deter the West from providing additional support to Ukraine as he weighs a further escalation of the conflict. He probably still remains confident that Russia can eventually militarily defeat Ukraine and wants to prevent Western support from tipping the balance and forcing a conflict with NATO.

And of course, the already considerable human toll of the conflict is only increasing. In addition to the many tens of thousands of casualties suffered by the Russian and Ukrainian militaries, more than 8 million people have been forced to flee Ukraine since Russia invaded. There is widespread evidence of atrocities committed by Russian forces, including deliberate strikes against non-military targets such as Ukraine's civilian population and civilian infrastructure, particularly its energy facilities and electrical grid. Russia and its proxy groups almost certainly are using so-called filtration operations to detain and forcibly deport tens of thousands of Ukrainian civilians to Russia. The IC is engaged with other parts of the U.S. Government to document and hold Russia and Russian actors accountable for their actions.

The reaction to the invasion from countries around the world has been resolute, hurting Russia's reputation in the world and generating criticism at home.

Moscow has suffered losses that will require years of rebuilding and leave it less capable of posing a conventional military threat to Europe and operating assertively in Eurasia and on the global stage. As a result, Russia will become even more reliant on asymmetric options, such as nuclear, cyber, and space capabilities, and on China.

Our Assessment also covers **Iran,** which continues to pursue its longstanding ambitions for regional leadership and is a threat to U.S. persons directly and via proxy attacks. Iran also remains a threat to Israel, both directly through its missile and UAV forces and indirectly through its support of Lebanese Hizballah and other proxies. Most concerning, Iran has accelerated the expansion of its nuclear program, stating that it is no longer constrained by any JCPOA limits, and has undertaken research and development activities that would bring it closer to producing the fissile material for completing a nuclear device following a decision to do so.

North Korea similarly remains a proliferation concern as it continues its efforts to steadily expand and enhance its nuclear and conventional capabilities targeting the United States and our allies, periodically using aggressive and potentially destabilizing actions to reshape the regional security environment in its favor and to reinforce its status as a *de facto* nuclear power.

In addition, **regional challenges** such as interstate conflicts, key cases of instability, and poor governance developments also pose growing challenges. In **Africa** and the developing world, increased poverty, hindered economic growth, and widened inequality are creating the conditions that are feeding domestic unrest, insurgencies, democratic backsliding, authoritarianism, and cross-border conflict spillover.

Several parts of the **Middle East** will remain plagued by war, insurgencies, and corruption. In the **Western Hemisphere**, persistent economic weakness, insecurity, and corruption are fueling public frustration and anti-status quo pressures that very likely will present governance challenges to leaders while also posing sustained spillover migration, criminal, and economic challenges for the United States.

Throughout the world, countries are struggling to maintain democratic systems and prevent the rise of authoritarians, in some cases because Russia and China are helping autocrats take or hold power.

As I noted at the outset, transnational challenges interact in this complex system along with more traditional threats and often reinforce each other, creating compounding and cascading risks to U.S. national security. For example, **climate change** remains an urgent threat that will increasingly exacerbate risks to U.S. national security as the physical impacts increase and geopolitical tensions mount over the global response to the challenge.

And, now entering its fourth year, **the COVID-19 pandemic** remains one of the most significant threats to global public health, at a cost of more than 6.5 million lives and trillions of dollars in lost economic output to date. In addition to direct effects of the pandemic, resultant economic, human security, political, and national security implications of COVID-19 continue to strain recovery efforts, presenting both known and unforeseen challenges that probably will ripple through society and the global economy during the next year and for years to come.

Russia's aggression against Ukraine has aggravated COVID-19-related fragilities in the global economy, raised commodity prices, fueled market volatility, and contributed to food insecurity and financial instability. The combination of elevated energy and food prices has increased the number of individuals facing extreme poverty and food insecurity.

Affected countries will struggle to reverse these trends through 2023, even if global food prices stabilize. Russia's war in Ukraine can be blamed for these intensifying effects, something much of the world also understands and that others—including China—will have to come to terms with as they consider to what extent they want to continue assisting or enabling Russia.

Climate change, the pandemic, and conflicts are exacerbating **irregular migration** and in the Western Hemisphere, push and pull factors that drive migrants to the United States—such as deteriorating socioeconomic and security conditions, misperceptions of U.S. policies, and employment opportunities in the United States—will almost certainly persist through 2023.

Transnational criminal organizations (TCOs) exploit migrants through extortion, kidnapping, and human trafficking, including sex trafficking and forced labor. These organizations also continue to pose a direct threat through the production and trafficking of lethal illicit drugs, massive theft, financial and cyber crimes, money laundering, and eroding the rule of law in partner nations.

In particular, the threat from illicit drugs is at historic levels, with the robust supply of synthetic opioids from Mexican TCOs continuing to play a major role in driving American overdose deaths to over 100,000 annually.

And **terrorism**, of course, remains a persistent threat, but the problem is evolving. Individuals and cells adhering to ideologies espoused by ISIS, al-Qa'ida, and transnational racially or ethnically motivated violent extremists movements, in particular, pose significant threats to U.S. persons, facilities, and interests.

And then two indirect threats that I think are worth highlighting.

New technologies—particularly in the fields of AI and biotechnology—are being developed and proliferating faster than companies and governments are able to shape norms governing their use, protect privacy challenges associated with them, and prevent dangerous outcomes they can trigger. The convergence of emerging technologies is likely to create breakthroughs that are not as predictable and that risk a rapid development of more interconnected, asymmetric threats to U.S. interests.

Relatedly, foreign states' malicious use of **digital information and communication technologies** will become more pervasive, automated, targeted, and complex during the next few years, threatening to distort publicly available information and probably outpacing efforts to protect digital freedoms and, at the same time, educate audiences on how to distinguish fact from propaganda. Authoritarian governments usually are the principal offenders of digital repression, and of course democracies with open information environments are the most vulnerable.

In closing, I want to bring to your attention an absolutely crucial authority that will expire at the end of this year if Congress does not act – Section 702 of the Foreign Intelligence Surveillance Act. I can tell you without hesitation that Section 702 was relied upon in gathering intelligence that was relevant to putting together this assessment, as it is hard to overestimate the importance of this authority to our work generally.

FISA Section 702 provides unique intelligence on foreign intelligence targets at a speed and reliability that we cannot replicate with any other authority.

Section 702 was originally enacted to enable the US government to quickly collect on the communications of terrorists located abroad. The authority allows the IC to acquire foreign intelligence from non-US people located outside of the United States who are using US electronic communications service providers.

702 is still vital to our counterterrorism mission, as evidenced by its key role in the US government's operation against former al-Qa'ida leader Ayman al-Zawahiri. But 702 is now principally relied upon for vital insights across a range of our high priority threats, including: malicious cyber actors targeting US critical infrastructure; weapons proliferators attempting to evade sanctions to deliver precursor chemicals to hostile actors; and even key intelligence related to threats emanating from Russia, North Korea, Iran, and China.

I realize that Section 702 is a powerful authority and it is incumbent on all of us in the intelligence community to ensure that the privacy and civil liberty interests of Americans are built into its design and implementation at every level. Over the last many years, we have significantly expanded oversight and dedicated resources to compliance in order to do just that – and we welcome the opportunity to work with you on reauthorizing this critical authority.

Thank you for your patience, we look forward to your questions.

Chairman WARNER. Thank you, Director Haines. And again, this is a critically important time for not only those of us on the Committee but the public at large to see the intelligence community leadership. I personally believe the value of 702, but we're going to have to lean in on being willing to have the same kind of courage of declassification that we showed in advance of Putin's invasion of Ukraine to make the case to the American public, and for that matter to skeptical Members of Congress, in terms of how this is not simply used as an anti-terrorism tool, but also in terms of our competition with Russia and China.

I'm going to take my time and come back to the question of the changing nature of national security. I made the comment that national security today is different than it was in 1993 or 2003. At that moment in time, perhaps relatively simpler times, we looked at our adversaries in terms of how many tanks and planes and guns they might have.

Increasingly, I believe, and I think the vast majority of us on this Committee believe, the competition falls into who wins various technology domains. General Nakasone and I were talking before the session today about how then-Chairman Burr and I were trying to make the case that Huawei posed a national security threat to American telecom providers and others. It took us years to make that case and we're still recovering from that activity. I think a lot more recently, Senator Cornyn and I and others on this Committee recognize that we've fallen far behind in the research, development, and fabrication—the making of semiconductor chips. And again, in a broad bipartisan way Congress reacted to that.

The vast majority of us on this Committee think that increasing Chinese use of mobile apps like TikTok—and while we have different approaches—I know the Vice Chairman and I very much believe that TikTok poses a national security threat, both in terms of data collection and in terms of a potentially enormous propaganda tool.

What I would like to hear from all of you, and maybe we'll start with Director Wray, is do you share at least my assessment that national security has to be redefined in 2023 to recognize that domination of technology domains that on the surface do not appear to have anything to do with national security—artificial intelligence, Director Haines mentioned biotechnology, quantum computing, who wins the challenge around advanced energy—these are national security issues as well and we have to do a better job of both convincing the public and quite honestly, some in the business community. We've made progress on the business community, but many are still, as Senator Rubio made mention, inexorably tied to a global supply chain that relies on cheap Chinese goods. How do we make that case? Do you start with accepting the premise that national security has to include who wins each of these technology domains?

And I'll just go right down the line.

Director WRAY. Well, certainly Mr. Chairman, I wholeheartedly agree that technology and economic security have become inextricably intertwined with national security. And the efforts this Committee has made and that a lot of us in the Intelligence Com-

munity have made to engage the private sector, I think are essential to that. And we just have to keep doubling down on that.

You could just look at, for example, on the cyber side, our critical infrastructure, 85 percent of it or something, is in the hands of the private sector. And if you look at our innovation, if you look at our PII, our personal identifiable information, the percentage is even higher. And if you look at what the Chinese are trying to steal, that's where it is. So, we need to be working more and more closely with the business community to try to build resilience. I think there has been a lot of progress that's been made, but we need to make more.

Chairman WARNER. General.

General NAKASONE. Chairman, I certainly agree on the statement with regards to the changing nature of power. I think that's where the National Security Agency has always found itself in being able to hardwire to look for what's next technology we should be chasing.

Being able to leverage a workforce that is very, very heavily inculcated with science, technology, engineering, and mathematics, but I think the big piece that at least I've learned over the past several years is the fact that it's all about partnerships. It's the partnerships that we have here in the IC. It's the partnerships with the public sector. It's the partnerships that we have to develop that will give us the competitive advantage as we look at this new changing character.

Chairman WARNER. Director Haines.

Director HAINES. Yes, absolutely agree obviously with my colleagues. One of the things that we have been learning in the Intelligence Community, exactly as General Nakasone indicated, is our work with the private sector in this space is particularly important. Over my lifetime, I have seen increasingly the innovation of critical, foundational technologies occurring in the context of the private sector and our capacity to work with them to understand essentially what those innovations are and how we can help them protect themselves in this context, is another aspect of this that has to be focused on and something we spend a lot of time on.

Chairman WARNER. Director.

Director BURNS. Mr. Chairman, I fully agree. I think the revolution in technology is not only the main arena for competition with the People's Republic of China, it's also the main determinant of our future as an intelligence service as well. As you know, we've undertaken a number of innovations over the last couple of years to strengthen our capacity on that revolution and technology: for the first time appointing a Chief Technology Officer, for the first time establishing a CIA wide technology strategy, creating a new mission center focused largely on technology. And as my colleagues emphasized, building better partnerships, stronger partnerships with the private sector as well as with academia, creating a technology fellows program, because we have to be more flexible in our employment practices as well, to attract people who are accomplished in the private sector, in the tech sector who may be interested in a couple of years of public service, as well. And we're deeply interested in trying to attract those kinds of people as well.

And then finally, I absolutely agree on the importance of partnerships, not just across the Intelligence Community but with others in the Executive Branch. So, as you know, we're working closely with the Department of Commerce and their CHIPS Implementation Act Office as well, to provide the kind of direct support that I think is essential to that effort as well.

Chairman WARNER. General.

General BERRIER. Chairman, I completely agree with the statement. You went back to 1993, I'll go back to 1984. When I came into the Army in 1984, we owned the technology; the West owned the technology. We won the Cold War and then I think we took our eye off that ball. So now, it's about how do we apply this asymmetric advantage that we have and this partnership of folks sitting at this table right now, who work so closely together to try and defend our Nation.

Like the other agencies, DIA has hired the right people at the right time to get into this, to try and understand it and make an impact for the Department of Defense.

Chairman WARNER. I'm over time but my only closing comment is that does mean we may need to redirect some of the resources. I mean the idea of China's extraction of cobalt out of the DRC and how they're going to get it back to China, becomes a national security issue. The question of China flooding the zone on standard-setting bodies to define the next technology rules from beyond 5G to ORAN, open radio access networks, next generation of wireless, is a national security concern. Who's leading the way on biotech innovation becomes a national security concern, and I think we need to make sure that we are both reporting on this and that we are engaging our private sector partners. I agree with Senator Rubio: too many of our corporate world still believes that these collaborations inside of China are benign, even though when they turn a blind eye to the literally unprecedented amounts of intellectual property theft, too often because they're making way too much money on investing in China tech. Some of that has changed, but this is an ongoing challenge.

Senator Rubio.

Vice Chairman RUBIO. Thank you.

I'll start with you, Director Wray. Let me ask you, as I know you are familiar with this. The most downloaded app in the world—one of the most downloaded apps in the world, the social media company TikTok: could the Chinese government, through its ownership of ByteDance that owns ByteDance U.S.—if they wanted to, and ByteDance U.S. were willing to cooperate or forced to cooperate, could they use TikTok to control data on millions of users?

Director WRAY. Yes.

Vice Chairman RUBIO. Could they use it to control the software on millions of devices, given the opportunity to do so?

Director WRAY. Yes.

Vice Chairman RUBIO. Could they use it to drive narratives, like to divide Americans against each other. For example, let's say China wants to invade Taiwan, to make sure that Americans are seeing videos arguing why Taiwan belongs to China and why the U.S. should not intervene?

Director WRAY. Yes, and I would make the point on that last one in particular, that we're not sure that we would see many of the outward signs of it happening if it was happening. And I think the thing, the most fundamental piece that cuts across every one of those risks and threats that you mentioned, that I think Americans need to understand is that something that's very sacred in our country, the difference between the private sector and the public sector—that's a line that is non-existent in the way the CCP operates.

Vice Chairman RUBIO. Do you think it's valuable to look at how TikTok operates in China versus the U.S.? For example, in the U.S., kids are being encouraged to choke themselves out—we've had kids die. In China they're encouraged to focus on math and science and building the country. Is that an example of how two different versions of TikTok, one feeding our society poison and the other inculcating positive values, an example of how potentially or in reality TikTok could be used to damage our country?

Director WRAY. I think those are among many telling indicators that we should be looking at in assessing the national security concerns this poses.

Vice Chairman RUBIO. So, they can collect our data, manipulate information, poison the minds, and feed garbage into the minds of millions of people and so forth. Given the threat, I imagine this is the reason why TikTok is no longer allowed on federal devices. Pretty soon, no federal devices can have TikTok on it, correct?

Director WRAY. Well, certainly at the FBI, TikTok never has been and nor will it be approved, and I think it's my understanding that that's about to be in place across the entire Federal Government.

Vice Chairman RUBIO. So, given the weight of all this, does anyone on the panel disagree that TikTok is not a good thing for America?

Well, if no one disagrees, my question is then, if TikTok is bad for America and we've talked about all of these disadvantages and potential harm that's caused by it, should the fact that it is popular among people under the age of 35 be the reason why we don't take strong action against it?

Director WRAY. Not from my perspective.

Vice Chairman RUBIO. Okay, because that's what the Secretary of Commerce said, that potentially we won't do something about this because it would upset people under the age of 35.

So, I guess my point—just to tie it all up—this is a substantial national security threat for the country, of a kind that we didn't face in the past. At the end of the day, it's not about some grown man in the middle of the day putting up videos that people that have a job shouldn't be putting up. But it's also about all these other things that we've talked about—the data, the ability to manipulate information.

I would imagine that it's probably one of the most valuable surveillance tools on the planet. I mean if we went out and decided to build something like this of our own to influence or spy on another society, I'm not sure we could build something like this. And we've invited them in and protected them by our laws.

So, I don't understand why this company is allowed to operate as long as it's owned—it's my understanding and maybe Director Haines, you can clarify this—but I think this is the case. Under Chinese law, any company, I don't care what the companies are, in China that the Chinese government says give me everything you have, they have no choice but to give it to them or someone else will be in charge. Correct? Okay.

My time is remaining here. I want to talk a little bit about COVID and the pandemic. So, here's what we know about COVID. Okay, it originated in the city of Wuhan, where the Wuhan Institute of Virology, which has a questionable safety record and conducts experiments on making viruses that are not infectious in humans infectious in humans. They do it for the purpose of then developing a vaccine. They're located in that city. The Chinese CDC is also located in the city.

Number two, unlike for example SARS, to this moment, unless it happened in the last hour, the Chinese have not been able to say here's the bat, here's the pangolin, here's the animal that the virus came from.

Number three, there is evidence, both in open source—it's been widely discussed that the Chinese, at a minimum, have not been to say the least, open about any of this. And in fact, real clear indications that they've done everything possible to obstruct any sort of international inquiry into how this began or to be sharing this information. This is a lot of circumstantial evidence that adds together. And I believe that's why the FBI has concluded what on the origins of COVID, Director Wray.

Director WRAY. So, Mr. Vice Chairman, as the Committee knows, the FBI has long assessed, going all the way back to the summer of 2021, that the origin of the pandemic was likely a lab incident in Wuhan.

Vice Chairman RUBIO. So, Director Haines, I know that there's a difference of opinion among the different agencies. I think Energy and FBI have that assessment. What is preventing the other agencies from reaching the same assessment? Is it basically the lack of a smoking gun? Will we not be able to say that we believe that the lab origin is the likeliest outcome, unless somehow we can provide a smoking gun proof that that's what happened?

Director HAINES. Thank you, Sir. You're right, basically, there's a broad consensus in the Intelligence Community that the outbreak is not the result of a bioweapon or genetic engineering. What there isn't a consensus on is whether or not it's a lab leak, as Director Wray indicated, or natural exposure to an infected animal. Those are the two operating theories. And what would change—essentially elements/perspectives—would be additional information. And we've been trying to collect additional information. I think you're absolutely right that China has not fully cooperated, and we do think that's a key critical gap that would help us to understand what exactly happened.

Vice Chairman RUBIO. My time is up.

Mr. Chairman, I would just point out it is true that the lab leak—we don't have a smoking gun. We don't have some guy calling another guy saying hey, we had a lab leak. We also don't have a smoking gun that it was a naturally occurring event, which is the

easiest one for them to prove, come out, have a press conference, show us the bat or the pangolin—whatever a pangolin is—and show us that this is the one and here's the virus that came from that animal, because it wouldn't have not just been found on one animal, it would have been pretty widespread.

That's the easiest thing for the Chinese to have done and they haven't done it. I think that's a pretty strong reason to suspect that it's not naturally occurring, because they've done it with the other pandemics.

Thank you.

Chairman WARNER. And I would just point out—before I go to Senator Wyden, when those of us raise the issue around TikTok, it is not simply an American concern. Canada, the EU, India have also taken action on this application because of this national security concern.

Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman and thank you all for your service.

Begin with you, Director Burns. Last year, you committed to me that the CIA would require written justifications that could be audited whenever CIA conducts searches of its databases for information on Americans. Has the agency done that?

Director BURNS. Yes, sir, we have. And thank you very much for your attention on this issue. In keeping with the commitment that I made to you last year, the CIA has made substantial and rapid progress developing and implementing, across all of the CIA, a capability to support written, auditable justifications for searches, as you said, designed to retrieve U.S. person information.

We've kept your staff regularly updated on this. We're ahead of the schedule that I set out for you in that letter last September. We've already begun implementing the tool we've developed in the database that the Privacy and Civil Liberties Oversight Board has been focused on, and now we're moving forward with that approach across the remaining databases.

Senator WYDEN. Thank you for doing this.

Let me turn to commercial information. Director Wray, does the FBI purchase U.S. phone geolocation information?

Director WRAY. So, to my knowledge, we do not currently purchase commercial database information that includes location data derived from internet advertising. I understand that we previously—as in the past—purchased some such information for a specific national security pilot project, but that's not been active for some time.

I could provide more information about that in closed session if you would like. But when we use so-called ad tech location data, it is through a court authorized process.

Senator WYDEN. And you do not plan to change your current practice of not buying this geolocation information?

Director WRAY. We have no plans to change that at the current time.

Senator WYDEN. I think it's a very important privacy issue that that not take place. We'll discuss it more at the closed session.

Director Haines, you convened an outside panel to study and make recommendations related to the government's purchase of

data, including sensitive data on Americans. There has been a lengthy report that has been done here. Will you agree to release this report to the public?

Director HAINES. Thank you, Senator. I'll absolutely—. We'll have our folks review it for that purpose.

Senator WYDEN. Is there any reason why it shouldn't be made available to the public?

Director HAINES. No, I think it absolutely should. As long as there's not classified information in it, we'll provide it.

Senator WYDEN. Okay. One additional question for you, if I might, Director Haines.

As you know, last May, Senator Moran and I urged the President to prioritize the rewriting of the Executive Order that governs classification, declassification—hadn't been updated in ages. In August, you wrote back on behalf of the President saying that the process was underway.

My concern is that we're not seeing the urgency that is necessary, because we all know what the challenge is, and that's foot dragging by some people who mean well, but they're just not on the program of reform. Will you push the National Security Council to get this done, because my sense is this just isn't going to happen unless you can successfully push the National Security Council to break up the status quo?

Because the classification system is now at the point where, as you correctly said and to your credit, it's not serving national security. And I think it's so broken, we're not getting classified what we need to get classified, and we surely are classifying stuff that shouldn't be classified. So, we got to break up business as usual here. And it's only going to happen in my view if you can push the National Security Council.

Can you commit to doing that?

Director HAINES. Thank you, Senator. First of all, for your and for Senator Moran's attention on this issue, I think it is incredibly important and something that, over many years, I think for all of us, we've seen the frustration of actually trying to make this better.

I know the President is committed to this issue. I absolutely will ensure that he and the National Security Council know of your concerns and relay them as such.

Senator WYDEN. I want to also ask you, Madam Director, about security clearances and past marijuana use. At the end of 2021, you issued guidance that past marijuana use was not by itself a disqualification for security clearance. I think it'd be very good if you could tell the American people why it's important that this past use not be a disqualification to serve your country. This is a national security issue, and we desperately need people. We've got new Members in this Committee talking about languages that they're going to be focused on as we try to recruit and the like. Tell the American people why past marijuana use is not disqualifying for a National Security post?

Director HAINES. Thank you, Senator.

I think we recognize, frankly, that many states have legalized or decriminalized marijuana use and wanted to be sure that we're not disqualifying people solely for that purpose in that context. We obviously believe that we want to have the talent that exists in Amer-

ica. When somebody is using experimentally in a legal state, that's something that shouldn't on its own disqualify.

We continue to approach this from a whole-of-person perspective, and we expect if anybody takes the job to comply with our policies and our laws in a trusted position.

Senator WYDEN. My time is up. I only want to say that I know we've got some big privacy issues ahead of us and I want to thank all of you for keeping your door open to discuss them with me.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Wyden. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Director Haines, I want to follow up on the Vice Chairman's questions to you and the panel about the origins of COVID. We know that 6.5 million people have died, that trillions of dollars have been lost in economic activity. We also know that had we known early the origin of COVID, we might have well been able to change the trajectory and been better prepared for future pandemics. So, this matters.

It is disturbing to me that in your written statement, you say all agencies assess that two hypotheses are plausible explanations for the origin of COVID: natural exposure to an infected animal, and a laboratory-associated incident. That's one of those statements that's technically true but misleading.

We've heard the FBI director today say that the most likely explanation is a laboratory incident. We know that the Wuhan whistleblower, who first raised alarms, was silenced by the Chinese government and later died of COVID. We know, as your statement says, that Beijing continues to hinder the global investigation, resists sharing information, and blames other countries. Those are not the actions of an innocent party. We know that the Department of Energy has changed its assessment to say that the most likely cause is a laboratory incident.

I just don't understand why you continue to maintain on behalf of the Intelligence Community, that these are two equally plausible explanations. They simply are not.

Director HAINES. Thank you, Senator.

And I think I share your frustration with the fact that China hasn't been more cooperative on this issue to provide intelligence that would be of use to the scientists and others who work on these questions. And I think you're absolutely right. This is critically important. It has been extremely challenging. Let me give you where we are in the Intelligence Community with more precision to your point.

There are four elements, plus our National Intelligence Council, that assess with low confidence that the infection was most likely caused by natural exposure to an infected animal. So, the IC remains divided on this issue. We have the FBI, as you noted, that sees it as more likely that it's a lab leak and has done that with moderate confidence. And the Department of Energy has changed its view slightly with low confidence. It says that a lab leak is most likely. But they do so for different reasons than the FBI does, and their assessments are not identical.

So, you can see how challenging this has been across the community. And not even every element of the IC has been able to put

themselves on one side of the ledger or the other. I've given you seven, but not everybody has been able to put themselves on one versus the other.

So, it is a really challenging issue, and I think our folks honestly are trying to do the best that they can to figure out what exactly happened based on the information they have available to them.

Senator COLLINS. Let me switch to a different issue. General Berrier, in the Administration's hasty withdrawal from Afghanistan by an arbitrary date, billions of dollars' worth of military assets were left behind, including munitions, 16,000 pairs of night vision goggles, 167 aircraft, communications equipment, 2,000 vehicles. The list goes on and on and on. My concern is that all of these assets could be useful in launching a terrorist attack on the United States or one of our allies.

Given the continued chaos in Afghanistan and presence of terrorist groups that want to harm the United States, that have made no secret about harming us or our allies, what is the Intelligence Community's assessment on the counterterrorism threat to the United States homeland and our allies, particularly one launched from Afghanistan?

General BERRIER. Senator Collins, thank you for that question. From our perspective, at the Defense Intelligence Agency, certainly our reach and grasp into that nation since the fall of the government has eroded over time, but we still have some access. And I would say, based on what we know right now from the threat of Al-Qaeda, they're trying to survive, basically without a real plan to at least—or intent—to attack the West anytime soon.

And I would say that ISIS–K poses a bit of a larger threat, but they are under attack from the Taliban regime right now, and it's a matter of time before they may have the ability and intent to actually attack the West at this point.

Senator COLLINS. General Nakasone, very quickly, could you give me your assessment?

General NAKASONE. Yes, that dovetails very closely with the Defense Intelligence Agency. We see the same challenges across the IC with some of our collection. But we do see a challenged ISIS–K in Afghanistan right now as they battle the Taliban.

Senator COLLINS. Thank you.

Chairman WARNER. Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

Director Burns, U.S. law states that to be designated as a foreign terrorist organization, a group must be engaged in premeditated, politically motivated violence against non-combatant targets, and the activity must threaten the national security of the United States. In my view, and in the view of a number of folks, the Wagner Group fits that definition. Wagner now openly operates as private military for Vladimir Putin, conducting terrorist operations in Ukraine and in countries across Africa.

Director, I realize that the responsibility for designating foreign terrorist organizations lies with the Secretary of State, but I'd like to get your assessment of the Wagner Group's activities, whether you would describe the atrocities its mercenaries have committed as terrorism, and if you think there is any downside to making such a designation?

Director BURNS. Well, thanks, Senator.

And as you rightly pointed out, I'll steer away from the policy question there. But certainly, our assessment is that the Wagner Group is a vicious, aggressive organization, which has posed a threat, not just to the people of Ukraine. And we see that every day, especially in the intense fighting that's going around the city of Bakhmut right now, largely conducted on the Russian side by the Wagner Group, which is suffering incredible casualties.

But I've also seen it, as we were discussing earlier, in my own travels in West Africa and the Sahel, where I think the deeply destabilizing impact of Wagner can be seen in a lot of very fragile societies right now. We work as an agency, along with our partners, to help many of those governments and many of our security service partners to resist that. We work with the French and with other countries, other allies, in that effort as well. But we take very seriously the threat posed by Wagner and do everything we can to counter it and disrupt it.

Senator HEINRICH. Great. Thank you, Director.

Director Haines, earlier I shared with you a report by the Converging Risk Lab called "The Security Threat That Binds Us," which outlined, among other things, the need to elevate ecological security in U.S. national security policymaking. And one example they really go into a great deal of detail about is China's aggressive fishing activities and how those have contributed to over-fishing more than any other nation. This has led to increasingly hostile fishing disputes between China and its neighbors, as well as along the coast of Africa and Latin America, threatening economic, food security, and sovereignty.

In the view of the report's authors, the IC needs greater capacity to analyze the negative effects of illegal fishing activities, as well as a whole host of other causes of ecological disruption. And it needs to elevate the relative importance of ecological security issues within the IC prioritization framework.

Have you had a chance to look at that, and can you commit to work with me to try to implement some of the recommendations included in that report?

Director HAINES. Yes, absolutely, Senator.

I did see the report, and I thought it was actually excellent. We've given it to our National Intelligence Manager for Climate and Global Issues, who is focused on these issues. I think one of the things that it does say very much in line with what you just indicated is it's not just about collecting more analysis. It's about prioritizing it. It's about ensuring we have access to the outside folks. And I think that is something that we are trying to do. In other words, get expertise both from the federal science community and work with them, but also with academic communities, and also with partners who have access to academic and other resources on these issues.

I absolutely commit to working with you further on this question. And I share your concern about unregulated, unlawful fishing that the Chinese have been doing in a variety of areas where we've seen them strip resources from countries.

Senator HEINRICH. Thank you, Director.

General Nakasone, I want to ask you one last quick question before my time is out, and it involves supply chains, which we are hearing a lot more about now, for appropriate reasons. The 2021 National Intelligence Estimate on Climate Change states that China is the world's leading supplier of advanced grid components for ultra-high voltage systems—things like transformers, circuit breakers, inverters—which we assess create cyber vulnerability risk.

Can you talk a little bit about your concerns about those vulnerabilities to our electric grid and what it means to currently be dependent on China for components for things like large power transformers?

General NAKASONE. Senator, you highlight the challenge of supply chains, and we know supply chains well, even from a different adversary with SolarWinds. What have we learned? I would tell you, first of all, is that as we are reliant on more and more nations to provide this type of capability, we have to have a vigilance in terms of how we look at this. Whether or not we're understanding the complete supply chain of the critical pieces that come into it, or whether or not we have sensoring on the other end that tells us something is anomalous, something is unique, something that has changed. This is the world in which we live. This is the world in which we have to operate for the future.

Senator HEINRICH. Would it be a good idea to try to produce some of those critical components here, or with trusted allies and friends instead of being so dependent?

General NAKASONE. Certainly, and I think the work of many of you on this Committee with regards to semiconductors is one great example of the importance of fabrication within the United States.

Senator HEINRICH. Thank you. Thank you, General.

[Now Presiding: Vice Chairman Rubio.]

Vice Chairman RUBIO. Senator Cotton.

Senator COTTON. I want to raise a question that Senator Warner raised in his opening statement about the classified documents that were found at the residences or offices of President Trump, President Biden, and Vice President Pence. I want to be clear. I'm not talking about who done it, about who took them there and how they handled them and what criminal standards there are and is there an investigation. I'm talking about the documents themselves and what risk, if any, they pose to our national security.

Director Haines, the last time you appeared in front of this committee, you said that you had not personally reviewed those documents. Is that still the case?

Director HAINES. I've only reviewed documents that have already gone through an initial classification review process. So, now I have reviewed some of the documents but not all of the documents myself, that is. There are others, obviously, within our institutions that have reviewed them.

Senator COTTON. Director Wray, have you reviewed these documents personally?

Director WRAY. I have reviewed some of the documents personally, and my team, of course, has reviewed the documents.

Senator COTTON. To both of you, why have you not reviewed all of these documents? It would seem this would be a matter of vital

urgency to put your eyes on these documents and make a determination if you think there actually is national security risk in the contents of those documents.

Director HAINES. Thank you, Senator. I'll start, and Director Wray can continue.

So, when we get documents that have been compromised in the context of leak, investigation, or other things like that, I don't personally review them generally, even when they have significant consequences. There are the subject matter experts within the institutions that do that. They provide their views, and then they typically will summarize or otherwise indicate issues that have to be addressed as a consequence, if there are any.

Senator COTTON. Director Wray is the same answer?

Director WRAY. It's similar, except I would just add that we have teams of people who are experienced with these mishandling of classified documents cases, of which we have any number and have had for years. And I would add that although I have not reviewed all of the documents myself, I have gone through a fairly meticulous listing of all the documents. That includes detailed information about the content, so it's not reading every page of each one.

Senator COTTON. I bet General Nakasone and General Berrier, when they were second lieutenants, were taught that they were responsible for everything their organization does and fails to do, which I think is a pretty good principle of leadership.

I just think on something of such prominence and perhaps such significance that you both should review them. More importantly, this Committee should review them. As you heard Senator Warner say, we're all very frustrated that we haven't even had these documents characterized to us, and we've patiently allowed Senator Warner and Senator Rubio to try to resolve this matter.

But I would say our patience is starting to run out, and at least some of us are prepared to start putting our foot down if we don't get better answers and the stone wall doesn't stop.

Director Haines, I want to turn to concern I've raised with you and Director Burns and others, and that's my worries about growing politicization and the analysis coming out of our intelligence agency.

This is an annual threat assessment. There is an annual threat assessment. So, let's look at it. On page 33, you write, transnational, racially, or ethnically motivated violent extremists continue to pose the most lethal threat to U.S. persons and interests. Are you serious? You seriously think that racially and ethnically motivated violent extremists are the most lethal threat that Americans face?

Director HAINES. Yes, sir. In terms of the number of people killed or wounded as a consequence.

Senator COTTON. How many people were killed by racially and ethnically motivated violent extremists in the United States last year?

Director HAINES. I don't have the exact number for you right here, but I will get it for you.

Senator COTTON. How many people were killed by fentanyl in the United States last year?

Director HAINES. As you know, it's over 100,000 for fentanyl.

Senator COTTON. So, isn't that a more lethal threat?

Director HAINES. Absolutely, but it's not being compared against fentanyl in that statement. It's in the context of terrorist threat.

Senator COTTON. Okay, so on page 38, you write about governance challenges in Europe. You talk about populist parties taking advantage of inflation and high energy prices. You worry that public discontent, potentially including increased mass protests, could undermine backing from mainstream European governments while increasing support for populist and extreme parties. You also say it could undermine the quality of democracy.

How is this foreign intelligence? And who are these populist parties in Europe that we're so concerned about?

Director HAINES. So, we can get you further information about this, but I'll just say, as a general matter, Senator, we do cover different effects on democracy throughout the world, and that is something that is typically perceived as part of our remit.

Senator COTTON. Are the Brothers of Italy, the Italian Prime Minister, Giorgia Meloni's, party, are they a populist or extreme party that are a threat to America's interests?

Director HAINES. I wouldn't want to speak for the analysts as to whether or not they consider them a populist party. I suspect that they may, but I don't know that they would say that they're a threat to us, to the United States.

Senator COTTON. All right, just one final example of this. On page 18, about nuclear issues with Iran. You write that since the assassination in November 2020 of nuclear scientist Mohsen Fakhrizadeh, Iran has accelerated the expansion of its nuclear program. Unfortunate ending for Mohsen Fakhrizadeh in November of 2020. Did anything else happen in the world in November of 2020 that might have caused Iran to accelerate its nuclear program?

Director HAINES. Senator, I'm not sure what you're referring to.

Senator COTTON. A pretty big event. A pretty big event here in America. November 2020.

Director HAINES. If you mean the election—.

Senator COTTON. I do mean the election.

Director HAINES. I don't believe that our analysts perceive that as being the key—.

Senator COTTON. Right. Because I've gone through the IEA reports. Iran took almost a year, almost a year after President Trump withdrew from the nuclear deal until the summer of 2019 to say it was going to incrementally begin to breach its limits. After we killed Qasem Soleimani in January 2020, they basically ceased all enrichment or other activity. And since November of 2020, they've reintroduced advanced centrifuges. They've began enriching uranium past the critical 3.67 percent mark. They produced uranium metal. They've moved enrichment underground. They're now enriching to almost 90 percent.

Undersecretary of Defense for Policy Colin Cole said to the House recently that they're just twelve days away from a breakout, implying that all happened on the former Administration's watch. This has all happened since November of 2020, Director Haines, and your report makes nothing, says nothing about the Biden Administration's policies.

You really don't think the Ayatollah has had any change of views once it was clear Joe Biden was going to be President?

Director HAINES. I think our analysts would look at leaving the JCPOA as one element that's relevant to the——

Chairman WARNER. Your time has expired.

Senator COTTON. Alright, so my time has expired.

I'll say, Director Burns, we've talked about this in a classified setting before, I mean, your organization produces the vast majority of the analysis for the IC. And it's not just the conclusions but also the priorities and the volume of focus on things like climate change or gay marriage bills in other countries or some of these conclusions that just cause me great pause about the priorities and the resources we're applying to the critical threats this country face. We can talk more about it in a classified setting.

Chairman WARNER. Thank you.

Senator King.

Senator KING. Thank you, Mr. Chairman.

First, Director Haines, the good news is the report is clearly written and I think establishes a lot of very valuable information. The bad news is I made the mistake of reading it Monday night just before trying to go to sleep. There are a lot of serious matters in there.

One of the things that really jumped out at me, and I want to follow up on Senator Heinrich's question, is on page 9. China now is on track to control 65 percent of lithium-ion battery market. They dominate all parts of the supply chain. Forty percent of the world's active pharmaceutical ingredients. And their global share across all manufacturing of solar panels is 80 percent now—will certainly go to 90 percent.

This is important information for us in terms of informing us about the dangerous dependency that we've developed in a whole lot of areas, and semiconductors is one that we've talked about. But it suggests to me that this issue of dependency is something that really has to have some serious policy examination. Would you concur?

Director HAINES. Yes, absolutely. I think one of the things that we're really trying to expose here is the fact that it's not just simply about China trying to create indigenous supply chains, but actually to control global supply chains.

Senator KING. That seems to be a deliberate policy, does it not?

Director HAINES. Exactly.

Senator KING. And that goes also about their actions in Africa and South America, where they're trying to corner the market, if you will, on various commodities.

Director HAINES. And you can see it also, as you indicate, not only in their decisions about what they're purchasing and how they're managing it, but also the laws that they pass that give them the capability, for example, in rare earth elements, to actually turn the dial on their export and import policies so that they can actually create that pressure.

Senator KING. You'd think that we'd learn from Europe's dependency on Russian gas that this is a similar thing that we really need to address as a matter of policy.

Let's move to another specific intelligence question. What's the current analysis on the relationship between China and Russia? Is it a temporary marriage of convenience, or is it a long-term love affair?

Director HAINES. It is continuing to deepen, so I think maybe the latter, although I hesitate to characterize it as a love affair. There are some limitations that we would see on where they would go in that partnership. We don't see them becoming allies the way we are with allies in NATO. But nevertheless, we do see it increasing across every sector.

Senator KING. Well, the sector that we're most concerned about right now is aid to Russia in the Ukraine conflict. What do we see there? Is China about to act? Are they issuing any supplies now? That's the highest risk, it seems to me, in terms of the development of this relationship. The immediate risk.

Director HAINES. Yeah, we do see them providing assistance to Russia in the context of the conflict. And we see them in a situation in which they become increasingly uncomfortable about the level of assistance and not looking to do it as publicly as might otherwise occur, and given the reputational costs associated with it. But I think that is a very real concern. And the degree of how close they get and how much assistance they're providing is something we watch very carefully. And we'd be happy to talk to you about that in closed session.

Senator KING. One point I thought could have used more emphasis—there's a whole section on climate change, which is interestingly—it's China, Russia, Iran, North Korea—climate change in terms of risks. And you identify the risk of famine and food insecurity across the developing world. You mentioned migration two or three times, but that, it seems to me, is one of the most serious destabilization risks. Syrian refugees upset European politics—6 million. We're talking 100-plus million. I hope that the Intelligence Community can provide some more-detailed analysis of the migration risk, which I see as one of the real challenges of the next 10 or 15 years as it becomes uninhabitable in areas of North Africa and the Middle East. Could you comment on that?

Director HAINES. Could not agree with you more, Sir. And we will look to try to produce something, and perhaps we can do something publicly along those lines.

Senator KING. And General Nakasone, in a few seconds that I have left, China's cyber posture. My sense is that they're getting more aggressive. Is that true? And is Russia adapting and getting better?

General NAKASONE. Senator, I would say that both for China and Russia, they are very capable cyber adversaries. With regards to China, we see an increasing degree of risk-taking that they've undergone with regards to stealing our intellectual property, even increasing their influence operations. These are concerning efforts for us.

With regards to Russia, we still see them, and we see them very accurately and being able to warn and being able to counteract some of the things that they're doing around the world. And so, we know them very, very well.

Senator KING. But they're getting cleverer, aren't they? About using our infrastructure, for example?

General NAKASONE. Well, certainly they're getting clever. But we still, I would say, Senator, are able to stay ahead of them. And that's the big piece that I want to emphasize.

Senator KING. Maybe the answer would be, so are we getting more clever? Thank you.

General NAKASONE. Well said, Senator.

Senator KING. Thank you.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. On September 11th, 2001, we lost 3,000 Americans. About a week later, Congress authorized the use of military force to go after the terrorists that committed those attacks. Last year alone, we lost 108,000 Americans to drugs that are coming across the southwestern border. I think the figure is roughly 71,000 of those deaths were caused by synthetic opioids, fentanyl.

And we know where the precursors come from. They're coming largely from China. This is like losing a large passenger jet every day for more than a year. Just like 9/11. Just like we would react if, in fact, passenger jets were falling out of the sky each day for a year, we would react in an overwhelming fashion. Yet the Attorney General of the United States has said, we're doing everything, he's doing everything he can.

And so, my question for each of you is what additional authorities, what additional resources do we need to defeat this threat to American lives? Some have suggested that they should be designated a foreign terrorist organization. Others, other Members of Congress have said, well, we need to use an authorization for the use of military force like we did after 9/11.

But I'd like to hear, maybe starting with you, Director Haines, and then I'd like to have Director Burns address the question. What additional authorities, what additional resources do we need in order to save American lives from this threat?

Director HAINES. Thank you, Senator.

I know you've done a lot of work on these issues, and I could not agree more with your characterization of it and the importance that it holds. And you'll hear from my colleagues some of the increasing resources and efforts that all of them have engaged in in this area. I will speak for myself in terms of the ODNI, our Office of the Director of National Intelligence. We have a national intelligence manager that covers this issue and a national intelligence officer.

And one of the things that I've learned in the two years that I've been there is that we do not have as deep a bench of analysts on these issues, and we are therefore not as resourced as we need to be in order to really address this question. That's something that we've been building, and that's something that we need to continue to build.

Senator CORNYN. I agree with you that we are losing. And what I want to know is: what do we need to win?

Director Burns, would you address that?

Director BURNS. Yes, Sir.

From the point of view of CIA, as we've discussed before, we've tried to transform our strategy through our counternarcotic center,

working with partners across the Intelligence Community, and domestic and foreign partners as well, focusing on the entire network that you described. In other words, precursor chemicals, financial flows, the production of fentanyl pills and the equipment that goes into that, as well as disrupting that trafficking as well.

And here I would emphasize that I think we talked earlier about Section 702, I think that has helped us to illuminate that network and has helped us in some successful actions recently with which foreign intelligence collected by CIA has contributed to both recent successes that our Mexican partners have had against the Sinaloa Cartel and also recent successes against fentanyl production and processing equipment in Mexico and in the United States.

So, I couldn't agree with you more about the severity of this problem. For all of us, protecting American lives is our highest priority.

Senator CORNYN. I'd like to follow up with the panel in closed session.

Let me turn to the issue that Senator King raised. COVID exposed our vulnerability to long supply chains, everything from advanced semiconductors to rare earth elements to active ingredients in pharmaceuticals that are manufactured in China. And, in the event that supply was disrupted, it would be not only a tremendous threat to our economy, but to our national security as well. For many years, American businesses have been investing in China. We had a witness that testified last May, I think it was, that the current market value of U.S. investments in China were worth $2.3 trillion. In other words, American investment in China has been financing the rise of China's economy and the rise of their military might, just like CFIUS allows us to review foreign investment in the United States.

Do you support an outbound investment transparency regime that would give us greater insight, give you greater insight into what we are financing? We, in effect, are financing our number one adversary. And we have—it's relatively opaque, I think, to the Intelligence Community, and certainly to the policymakers.

Director Haines.

Director HAINES. Sure, I'll start. Obviously without prejudice to the policy question of what is the right answer for how to deal with this, I think you're absolutely right that there's no question that something that would create greater transparency would give us more information about this. And that would be valuable from our perspective.

Chairman WARNER. And I think Senator Cornyn raised a good point, and something we've discussed at some length: how we have to make sure we're also following what particularly China is doing in other nation-states.

Senator Bennet.

Senator BENNET. Thanks. Thanks, Mr. Chairman.

And I just would make a comment on Senator Cornyn's question to you and your response to Senator Cornyn. Colorado is being overrun by fentanyl. And we're at a point now where, when a kid dies who's the age of my children, I no longer ask, what was the accident? Did they have a car accident? Or was it leukemia? The question is, was it suicide? Was it fentanyl? Or was it guns?

And, I guess from my perspective, I don't see any evidence that we're getting the cooperation that we need from Mexico to deal with this crisis at our border. And I don't know if you want to amend your answer to Senator Cornyn. Maybe if you could? And this is not the only thing I want to ask about, but what would it look like to have a neighbor to the south who is actually taking seriously the fact that we're losing more than 100,000 Americans a year, many of them children, who are taking drugs for the first time in their lives and then drop dead? What would it look like to have a partner in our neighbor country?

Mr. Director or Director Haines?

Director HAINES. I'm happy to start.

Senator BENNET. I mean, this is not about the number of analysts.

Director HAINES. Exactly. That was just the beginning of my answer. But I think it was fair to let others talk. I think we should talk about this in closed session further.

Senator BENNET. Okay, let's do that. I have other things I'd like to talk about, too, but let's do that because we haven't made any progress. Things have gotten a lot worse, and I'm sorry to say they've gotten a lot worse during the course of this Administration.

Second. Director Wray, you mentioned in your answers to Senator Rubio's questions about TikTok how concerned you are and the degree to which they're subject to the CCP in terms of their disgorgement of data and the potential use of that data to run operations against the American people.

I wonder if you could use this open, public opportunity to describe to the American people what the danger to them is of this platform that is run out of Beijing. What is the danger to them?

Director WRAY. Well, let me start by saying the point that I tried to get to towards the end of my exchange with Senator Rubio, which is: understand that the difference between an ostensibly private company and the CCP is essentially a distinction without a difference. So, if you were to ask Americans, would you like to turn over your data, all your data, control of your devices, control of your information to the CCP, most Americans would say, I'm not down with that, as my kids would say.

That's the question we're asking. So, it's really a question of data collection. And we know that they can use it to conduct all sorts of big data operations.

Senator BENNET. And what would a big data operation mean to your average citizen?

Director WRAY. There have been a lot of questions from the Chairman and others about AI and things like that. If you look at the Chinese government's gobbling up of information and data, and then the use of AI and other tools, ultimately supercomputing things like that, to marshal all that data to conduct targeting for espionage, targeting for IP theft, targeting for all the things that I and others on this panel have been calling out about the Chinese government, data is the coin of the realm.

Those who have the best information have the power, and that's what that enables them to do. You just have to look at the Equifax hack, where they essentially stole the PII of half the population of the United States. That's one Chinese government operation. So,

it's the control of the data to conduct all sorts of big data operations. It's the control of the recommendation algorithm, which allows them to conduct influence operations. It's the control of the software, which allows them to then have access to millions of devices.

So, you put all those three things together and again come back to the starting point, which is, this is a tool that is ultimately within the control of the Chinese government. And to me, it screams out with national security concerns.

Senator BENNET. My kids are about the same age as your kids. And what I would say is people ought to find a different platform. The American people don't need to spend three weeks out of the year on a platform that's run out of Beijing for Beijing's purposes. And we can do a better job than that.

I also just, while I have one second left, would say that I don't think the American people have had the kind of negotiation you were just talking about. Even with our own big data platforms in the United States, our big social media platforms, we have not had a negotiation about our privacy rights. We've not had a negotiation about whether your kids or my kids should have the benefit of the economics, the benefit of the economics of their identities, or whether Mark Zuckerberg should have the benefit of the economics of their identities.

And I think, Mr. Chairman, that's something that this Committee, I mean, it's not exactly what we're working on, but I think it's a related topic that is important for us to think about.

Chairman WARNER. I agree with you. I agree with you. Senator Moran.

Senator MORAN. Chairman, thank you.

Maybe to follow along with what the conversation was between the Director, between Director Wray and Senator from Colorado. For most of my time in the Senate, I've been working to try to get data privacy legislation through the Congress. We have failed. We get this close. We get very close. And then issues of private right of action become a barrier between Republicans and Democrats.

I just would make the public offer to any Democrat and any Republican that wants to work to get us to the point that we've been unable to be at. I am still ready, able, and willing to try to accomplish that.

I was going to ask Director—maybe the FBI Director has answered this question, but I was going to ask the CIA Director. What does all this failure to have data privacy mean in the intelligence world? So, when they collect, I think Director Wray was talking about this, but what does it mean to American citizens and to our national security?

Director BURNS. Well, Senator, in terms of our national security, it obviously enables our adversaries' efforts at espionage, as well. It enables them to steal intellectual property. It enables them to get access to sensitive technologies. It enables them to spy on our citizens, as well. So, it offers enormous opportunities, I think, for our adversaries.

Senator MORAN. General Berrier, anything to add to that from a——

General BERRIER. No, I concur with the Director of CIA.

Senator MORAN. Thank you. And General Berrier, what level of urgency would you attach to the issues of shrinking U.S. leadership in key technology areas? It's one of the reasons I voted for the CHIPS Act. What would you identify as the challenges we face, and what can we accomplish in protecting our country if we will invest in greater levels of technical abilities?

General BERRIER. The ability to secure this technology keeps our adversaries from actually obtaining the kinds of kit that they need to develop their most advanced weapon system. So, our ability to protect those chip sets, the ability to produce them in the United States of America is very, very important to keep those out of the hands of our adversaries.

Senator MORAN. I have additional questions on this line, but I think in the public setting this is something I want Americans to know. I think it's our natural instinct to believe we are the best at everything, and we can be. And in many instances, we are. But it's a different world than the one I grew up in, in which we absolutely were.

Tell me again—maybe anyone can answer this question—but the differences in advancements that China is making in advance manufacturing and automation. And maybe to you, General, the military consequences if we fail to advance our emerging technology capabilities?

General BERRIER. Senator, I would say that the Chinese are advancing very, very rapidly in every warfighting domain that exists, whether that's space, cyber, air and air defense, ground combat, command and control, cyber. They are making very, very rapid advances, and the Defense Intelligence Agency is taking note of that and watching it very carefully.

Senator MORAN. We talked a bit about our neighbor to the south, a little bit further south in Latin America. Many countries in Latin America have elected leftist governments. What are the extents of the inroads that our adversaries have made in those countries which have been traditionally friendly to the United States? What's the difference in today's world in Latin America?

Director BURNS. I think there's a broad trend that some of our adversaries take advantage of. We see this when we were talking about technology, whether it's completing deals involving Huawei or ZTE or 5G, which, as we've all been discussing, enable access to data. This is something we remind countries with whom we deal in Latin America all the time of the risk of doing that, especially with regard to the People's Republic of China.

There are economic relationships that can add to corruption in those countries that can make them kind of one-dimensional economies more and more dependent on the export of commodities to China, incur debts which will complicate their own economic growth, sustainably over time as well. And certainly, adversarial intelligence services try to erode our influence in a lot of those countries as well.

So, it's a real challenge as well in some places like Colombia, where we've had long standing relationships in fighting narcotics and in supporting the progress of those countries economically and politically. I think we're still able to sustain a lot of the cooperation

we've built up over the last 20 years or so. So, we just have to work hard at it, relationship by relationship.

Senator MORAN. Director Burns, I was hoping you would answer that in 19 seconds shorter so I could ask Director Haines a question. But you failed. And so, I failed. Thank you.

Chairman WARNER. Well, I would say, Senator Moran, new Member of the Committee, I think you focusing on this technology competition is spot on, and I appreciate it.

Senator Gillibrand.

Senator GILLIBRAND. Thank you, Mr. Chairman.

Director Haines, in last year's Intelligence Authorization Act, Senators Rubio, Warner, Heinrich, Burr, Blunt, and I created the AARO, the All-Domain Anomaly Resolution Office, to break down the stovepipes between the Intelligence Community and the military regarding unidentified aerial, marine, and other phenomenon which could pose a risk to the safety of our service members, as well as collection risks against sensitive facilities and overseas military bases. As recent events have shown, we need more and better sharing between the Intelligence Community and our military. And the stigmatization of the servicemembers and personnel who come forward with this data is unacceptable.

Do I have a commitment from you and each of our witnesses that you will work to reduce stigma, share intelligence between agencies, and as you're able with the public, to ensure that we understand what's happening in our skies and seas?

Director HAINES. Yes, Senator. Absolutely.

And I agree with you that this is an issue, and it's something that we've been trying to work through, both by sending the message from leadership that this is important, but also creating mechanisms that allow for people to do this more easily and with less stigma associated with it.

Senator GILLIBRAND. And is the AARO Office fully funded in your budget?

Director HAINES. Yes, I believe it is.

Senator GILLIBRAND. Can you make sure? Because it was left off last year from both the DoD and Intel's budgets.

Director HAINES. Right. So, it's in DoD, but I think our support is funded in the National Intelligence Program, and I will check to make sure on the details.

Senator GILLIBRAND. Everybody else can answer the question.

General BERRIER. I believe it is funded.

Senator GILLIBRAND. Thank you.

Director BURNS. Yes. I support, Senator.

Senator GILLIBRAND. Thank you.

Director WRAY. Yes.

Senator GILLIBRAND. A somewhat related question is the issue of IC's Agency's assessment with varying levels of confidence that most reported incidents can be explained by medical conditions, environmental, or technical factors. And that it's unlikely that a foreign actor, including Russia, is conducting a sustained worldwide campaign involving hundreds of incidents without detection with regard to the anomalous health incidents.

And that report was received in a very negative way by personnel who have been affected, by their families, because it essen-

tially says there's no external cause, which I think is really problematic. I'm very grateful that the Intelligence Community has been determined to make sure that health care is being met in the healthcare needs, and that each of these service members and personnel are treated appropriately and humanely from that perspective. But I find it unacceptable that we are not continuing diligent analysis of possible causes. I do appreciate that the Department of Defense continues to do research in that regard, and I'd like General Berrier to give us an update on how you're looking at this issue and how you are continuing to assess possible causes, as well as possible delivery mechanisms?

And I'd like to include delivery mechanisms from above, so whether it can be delivered by a drone or a spy balloon, through a collection device or collection technology, I'd like an update, please. Thank you.

General BERRIER. Senator Gillibrand, DIA participated in the Intelligence Community assessment. We had a multidiscipline team of very senior analysts, counterintelligence professionals, and technical people look at the issue. I do concur with the assessment, but I also think our work is not done there. DIA continues to focus on, number one, the care of our officers who have been affected. We are doing some work on the analytical side, and we're doing work on the S&T side to determine causation, and we'll continue that work. And I've made that commitment to my workforce.

Senator GILLIBRAND. And then I'd like a supplemental answer in closed session as well.

General BERRIER. Yes, Ma'am.

Senator GILLIBRAND. Thank you.

Director Haines, I've been working on legislation which would create a One Health Security Council to create a whole-of-government approach to address a broad range of biological threats to human, animal, and agricultural health as part of the Intelligence Community study of the impacts of climate change on food security and social instability. How well positioned are you to support the U.S. in strategic competition for the kind of biotechnology innovations which will ensure our resiliency in the face of a rapid-changing climate?

Director HAINES. This has been an incredibly intense area of focus for us, and you've seen us put forward in budgets, essentially for bio-convergence. We've proposed quite a bit of money on this. We now have the National Center for Biosecurity as opposed to what used to be the National Counter Proliferation Center. It is an area where you'll see even our recent head is somebody, of that center, is somebody with a history in this area.

And we are increasingly working on essentially different mechanisms by which we can both promote greater exchange and access to expertise outside of the Intelligence Community, and biotechnology and work, but also to understand better the innovations that are occurring there and try to make sure that we can take advantage of those, so that we understand them for collection purposes.

Senator GILLIBRAND. And just for the record, post-9/11, we had the 9/11 Commission to assess what went wrong with regard to 9/11. What we could have done to prevent it. The fact that the Intel-

ligence Community still disagrees on the origins of COVID is concerning. And I understand there's a massive lack of transparency from the Chinese government.

However, I have legislation that will require a much more fulsome, deep-dive review, sort of like a 9/11 Commission report, to then inform our legislation about having a one health approach, which is very similar as our post-9/11 approach, to have no siloing, to have everyone at the table, to do constant assessment, both agriculture and CIA and DoD and FBI and Homeland Security.

So, I'd like your assessment of both of those pieces of legislation with an eye towards solving the problem long term.

Thank you, Mr. Chairman. Thank you.

Chairman WARNER. Senator Lankford.

Senator LANKFORD. Mr. Chairman, thank you. Thank you, all of you and your service. Please pass on our gratitude to the great folks that work with you as well. They work very hard, and most Americans don't get to see them and thank them personally in a restaurant, in other places. So, please pass on our thanks.

Director Haines, I do want to be able to talk a little bit about Iran. Many of us on this Committee have traveled, some of us very recently, to the Middle East. Our allies in the Middle East and others in the Middle East are not excited about the JCPOA, they're not supportive of it. This report that's come out seems to be somewhat nostalgic of—if only the JCPOA would have been accepted, none of this would have happened. It is a bit of a challenge when we're watching Iran dramatically increase its enrichment. Now, the IAEA is saying they're at almost 84 percent. And a public statement there, how close is Iran right now? And what are their nuclear ambitions? Are they peaceful, or are they weapon systems, or what are they actually trying to be able to develop towards?

Director HAINES. Thank you, Senator. We should obviously take this up further in closed session. I think we continue to have concerns. You've seen the report and the indication that they are moving closer without a decision at this stage to pursue is our assessment; but nevertheless, getting very concerningly close.

Senator LANKFORD. Is Iran trying to be able to develop surrogate networks, even into the United States, where they're choosing Hezbollah to advance across different regions, but also trying to develop surrogate networks in the United States right now?

Director HAINES. Yes, Senator.

Senator LANKFORD. The Islamic Revolutionary Guard have noted that they are trying to assassinate, for lack of a better term, some American former officials, and have put out a list on that. My question for you and for Director Wray is how are we handling that? And are we providing the adequate level of both information and security to those former American officials that have been specifically named by the RGC as on their target list for assassination?

Director WRAY. Well, I'll start. There's obviously more we could talk about in closed session, but this is a threat stream that I talk about with my folks, my team several times a week, which gives you a measure of what our priority is. And we are certainly engaged in the ways that you would expect with the individuals who are potentially targeted in terms of duties to warn and that sort of thing. Security varies for different individuals depending on the

situation. And we're not the ones that provide the security, but we give them information that helps shape their approach to security.

Senator LANKFORD. Great, thank you.

Let me follow up on this, Director Wray. There's a piece that came out recently out of the Richmond Office that you have then come back and said, oops, that should have never gone out. But it was a piece that's in an unclassified document that came out of the memo. And the memo specifically states in the opening paragraph, violent extremists and radical traditionalist Catholic ideology almost certainly presents opportunities for threat mitigation through the exploration of new avenues for tripwire and source development.

Wow. This goes specifically into these radical traditional Catholics and explains what a traditional Catholic looks like on it. Help me understand what's happened since then, when this came out.

Director WRAY. Well, first let me say that when I first learned of the piece, I was aghast.

Senator LANKFORD. As you should be.

Director WRAY. And we took steps immediately to withdraw it and remove it from FBI systems. It does not reflect FBI standards. We do not conduct investigations based on religious affiliation or practices. Full stop.

We have also now ordered our Inspection Division to take a look at how this happened and try to figure out how we can make sure something like this doesn't happen again. I will note it was a product by one field office, which is—of course, we have scores and scores of these products. And when we found out about it, we took action. We are also taking steps to reinforce with our workforce all of the long-standing policies we have that speak to this kind of thing. We've got refresher training for the relevant employees, et cetera. And we do not and will not target people for religious beliefs. And we do not and will not monitor people's religious practices. That's not acceptable.

Senator LANKFORD. That is completely not acceptable. For the first time a couple of years ago, I had parents that came up to me in-state and said, I went to a parent meeting at my school. Am I going to be monitored now? And after this came out, I have people that catch me and say, okay, I'm Catholic. Am I about to be monitored now? This sends all the wrong messages on it.

I do have to tell you, we've talked about this before. When I saw the memo and looked through it, I was not surprised to be able to see the source document that they came back through was the Southern Poverty Law Center, which we've talked about before, is not the FBI. But for whatever reason, the FBI continues to be able to be able to count on them for who's on a listing of a hate group. They have a long history of having anti-Christian bias, and there's multiple different entities that they actually tried to go after on that as a hate group. But for whatever reason, the FBI continues to be able to count them as a source to be able to identify this. This is a very real problem. And the FBI needs to identify on its own—we have great resources—what are the threats? And not outsource that to a group that is known to be not center-left, but far-left group, and has its own set of biases as well.

Chairman WARNER. Senator Casey.

Senator CASEY. Mr. Chairman, thanks very much. I want to thank the panel for your testimony today, your appearance, and also, of course, your public service.

I'll direct my question or two to Director Haines, but I know this is an issue that has already been spoken to in the hearing. The Chairman, the Vice Chairman, and Director Haines have alluded to the important role that private industry has to play as we consider both economic security and national security, and the inextricable link between the two.

I'm talking, in particular, not only exclusively, but in particular about the People's Republic of China—maybe more specifically the Chinese Communist Party—and investment in China that could undermine our security. I am grateful, as always, that Senator Cornyn and others have worked on this issue with me, and I appreciate his question about the need for an outbound investment review that we're trying to get passed into law. But Director Haines, I wanted to ask you about, in particular, venture capital and private equity firms, as they continue to seek out business opportunities in China with often very little regard for national security risk or other risk.

Can you explain both the national security risks, as well as the economic security risks that are relevant when it comes to the business deals between those kinds of firms and the People's Republic of China?

Director HAINES. Absolutely, Senator. I'll do my best. And others may have something to add on this, too.

China, obviously, is focused, as we've been talking about, on critical foundational technologies that it believes will create a sort of disproportionate impact on their capacity for technological advantage. Right? And we've talked about a number of these technologies—artificial intelligence, quantum computing, high performance computing, all of these different areas, semiconductors, et cetera. That is something that we're in competition with China on. If a company in the United States or in an allied country has an office in Beijing or opens a plant or does other things, China has laws that allow them to get access to information and other things that they have there. And that provides them with an opportunity to basically force those companies to provide information that can be helpful to their intellectual property extension, and to ultimately advance their own competitiveness in this area. And they, through espionage and other means, have also gotten information from our companies, even outside of China and from Western companies. And that in and of itself is an issue.

In addition, we see that they are trying to create control over global supply chains. And what we've been discussing in this hearing, in the context of a variety of technology areas such as rare earth elements or other places where we know that or semiconductors and the CHIPS Act is a kind of a response to this, right? Where if they are capable of controlling certain parts of the supply chain, they can basically have leverage over that in a way that gives them unacceptable advantage in making it harder for us to get those supplies that we need at the moment that we need it for national security purposes or other purposes.

And I think that an example of this is if you just look at Russia and what's happening right now and the export controls that we've been able to use with respect to Russia and semiconductors, you can see how important it is to their capacity to prosecute their conflict. Right? And we don't want in the United States to be subject to that kind of a concern where in effect China would be able to prevent us from getting material that's necessary to our national defense or to our capacity.

So, these are among the challenges that we see for essentially supporting business in China on these sorts of key foundational areas where they can get information that's of need. So, it's not in everything, and it's not suggesting that there can't be any economic relationship, obviously. But I think we just have to be especially conscious of this, and we're trying to educate both our policymakers and the public on these issues.

Senator CASEY. I know I'm almost out of time. Just want to follow up on that for you or anyone else that wants to make a quick comment.

Are there sectors about which you're most concerned, purely from—setting aside economic security—purely from a national security point of view? Are there sectors about which you're most concerned?

Director HAINES. Yes, absolutely. Semiconductors, artificial intelligence, advanced computing, quantum computing, biotechnology, bio-manufacturing. These are some of the most important areas that we have concerns about.

Chairman WARNER. Thank you, Senator Casey, for, again, raising those issues. And we've seen this play out with venture firms and others, sometimes even using false fronts, which is gravely concerning.

Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman.

Once again, let me offer my thanks and appreciation to you and to all the members of your different services for how they contribute to our security.

In Director Haines's original comments, her early comments, she clearly discussed, or at least suggested strongly, the need for the reauthorization of the FISA Section 702. And I think sometimes we talk in terms of codes and so forth. We don't provide the opportunity for the American public to actually understand what this is. And I'm going to ask General Nakasone, because I've heard him in the past very eloquently share what Section 702 does. And in this open setting, I'd really like Director Nakasone to be able to share a little bit about what 702 really is, and the reason why it is so important that we reauthorize 702.

General NAKASONE. Senator, 702 allows the U.S. Intelligence Community to collect communications of foreigners operating outside of the United States that utilize U.S. infrastructure and services. Now why is that important? It's important because if you think about what we've been able to do as authorities since 2008—first of all, provide and shine a light on what our adversaries are doing. What's Iran doing? What's China doing? What's Russia doing? What's North Korea doing? In all parts of the world.

Secondly, disrupting——

Senator ROUNDS. But if I could, that's because they're using platforms that have a nexus to our communications systems within the United States?

General NAKASONE. That's correct.

Senator ROUNDS. But they're doing it from outside of the United States, and it is not necessarily connected with someone from within the United States. They're simply using the platform because it's easy.

General NAKASONE. Right, and again, I think those are the two really important points: non-U.S. person, that's foreigner, and it's outside the United States.

The second piece is, is that we have built up and I think have done a very effective job of ensuring not only national security, but the security and rights and civil liberties of our citizens. Those things are not an either/or, it's an and-statement. And we've been able to do that with internal compliance and external compliance.

Senator ROUNDS. And I want to go into that a little bit. Could you explain the reverse targeting prohibition, and specifically what it prevents the government from doing?

General NAKASONE. So, if one of our analysts in the U.S. Intelligence Community says, hey, I want to be able to get to someone in the United States? Well, I'll go ahead and just target this person outside the United States as a way around it. We do not allow that. In fact, we check that very, very carefully. It's audited. It's a double checked and triple checked. That's interesting. When we make a mistake, we investigate, we mitigate, and then we report on it. That's the type of attention we pay to this authority.

Senator ROUNDS. Okay. And then there's also concern about what is known as incidental collection. Could you explain what is meant by incidental collection and why it's important to our national security?

General NAKASONE. Senator, a lot of times when foreigners are operating outside the United States, and they are conducting their communications, they may reference someone in the United States. If they do in their communications, we have very, very specific ways that we minimize and be able to hide that type of data. So that is, again, the importance of us being able to, again, the national security piece and the protection of civil liberties and privacy.

Senator ROUNDS. Thank you.

Director Wray, would you have anything to comment with regard to the need for 702?

Director WRAY. So, it is absolutely essential to our ability to protect Americans, to protect victims here from foreign threats, and that's the FBI's lens into it. And I would say to pick up on a point that General Nakasone made, that we take very seriously our role as stewards of these important authorities. I know concerns have been raised about compliance. Understandably so. And we have made extensive changes over the past few years to address the root causes and to fix compliance issues.

We've set up a whole new office of internal audit that's focused specifically on FISA compliance. We've made massive changes to our database systems to prevent inadvertent 702 queries. We've enhanced training. We've implemented new oversight and

preapprovals and all of the reports that this Committee and the public have seen about some of those issues all predate those important reforms.

And I look forward to being able to share the impact of those reforms, as well as our focus on trying to make sure people are using the authority in a surgical and judicious way, which is why I'm very pleased to be able to share with the Committee today publicly for the first time that we saw in 2022 a 93 percent year-over-year drop in U.S.-person queries. Ninety three percent drop, and that's not an aberration. That's about an 85 percent drop if you compare it to 2020.

So, this is major impact. This is something we're going to treat as an ongoing effort. But it is part of our focus as stewards of these important authorities to make sure that we are protecting American civil liberties, but also using the tool in a way that is so valuable to protect Americans, in particular, increasingly these days to protect American victims from malicious cyber actors. I've talked before about how the Chinese have the largest hacking program in the world, by far bigger than every major nation combined, and they've stolen more of our personal and corporate data than every nation, big or small, combined. You look at the Russians. We've talked before about their treating of cyber as an asymmetric weapon. And they've invested significant resources in that. You look at the Iranians and their efforts to conduct destructive attacks even in the United States. And all of these powers are trying to build, preposition capabilities in the event of a much more serious conflict.

702 is what enables the FBI to get to victims, to warn them, to take steps to mitigate those cyber threats. And there's a lot more that we could talk about in closed session. But it's an incredibly, incredibly valuable tool to protect Americans, especially as you look out over the next five years in terms of the threats we're going to face with great powers, with cyber, and unfortunately—picking up on some of the questions that were asked earlier—from foreign terrorist organizations again.

Senator ROUNDS. Thank you. My time has expired.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Rounds. Thank you for raising the issue. And I do think for a lot of our colleagues, we're going to need to have this kind of explanation. We're going to need the community to lean in on declassifying specific examples, particularly vis-&-vis China and Russia. And also, a lot has changed since the Congress debated this issue back in, I believe, 2017–2018 in terms of reforms.

Senator Ossoff, you've been very patient. Senator Ossoff.

Senator OSSOFF. Thank you, Mr. Chairman. I want to thank you for your focus on technology, as well. And in that vein, General Nakasone——

Chairman WARNER. Can we check whether we are being listened into at this point or maybe you want to switch microphones.

Senator OSSOFF. Mr. Chairman, we should probably get that looked at. Maybe General Nakasone can.

But speaking of technology and General Nakasone. General, I have an offer I think you can't refuse. You have, of course, tremen-

dous assets and personnel in Georgia. NSA Georgia. The Cyber Center for Excellence at Fort Gordon, just around the corner from Augusta University's Cyber Center as well, an academic resource there. And I would like to invite you to join me, and perhaps we can get some barbecue and pecan pie as well, to visit with your personnel at NSA Georgia and/or at the Georgia Tech Research Institute—which is based in Atlanta with facilities across the country—is conducting much of the advanced research consistent with the Chairman's commitment to technology as a key frontier in our national security. So, will you join me in Georgia, General?

General NAKASONE. I will, Senator.

Senator OSSOFF. Looking forward to that and appreciate the commitment.

Speaking of Georgia, Director Haines, the assessment warns, quote, Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables, and that, quote, the PLA Navy and Air Force already are the largest in the region, meaning the Indo-Pacific region, and continue to field advanced platforms that improve China's ability to try to establish air superiority and project power beyond the first island chain. The assessment doesn't make explicit mention of the submarine domain. But during the Navy's posture hearing last year before the SACS, the CNO testified that submarines are the highest demand capability in both INDOPACOM and EUCOM. We have the Kings Bay, submarine base in Georgia.

I want to ask you first do you share our military's assessment that the undersea domain is critical and one in which we presently enjoy unique advantages?

Director HAINES. Yes, absolutely.

Senator OSSOFF. And so, what I want to ask you to work with my office on is, if and as the Navy considers activities at Kings Bay, and some of the emerging capabilities and technologies in the undersea domain and their potential presence or augmentation at Kings Bay, that you'll work with me to determine how the Intelligence Community can provide intelligence support to those efforts. Will you work with my office on that Director?

Director HAINES. Yes, absolutely, Senator.

Senator OSSOFF. Thank you.

Remaining focused on Georgia, we have the third busiest deepwater port in the country, and Director Wray as a Georgian, you know this. Ports are critical infrastructure. Yes?

Director WRAY. Absolutely.

Senator OSSOFF. And there are threats to our ports and threats that move through our ports. We've seen foreign intelligence services try to infiltrate, according to public reporting in the Wall Street Journal, for example: intelligence-gathering equipment through U.S. ports. There's a risk of drug trafficking through U.S. ports, human trafficking through U.S. ports.

Director Wray, I'd like to ask you to redouble the commitment you've made to me in the past to ensure that the FBI is fully focused on protecting the Port of Savannah and other seaports across the country.

Director WRAY. We're very focused on port security. I haven't forgotten our previous conversations on the subject, both in Savannah

but also in places like Norfolk and other significant ports around the United States. And certainly, a lot of the comments that occurred earlier about other technologies, and the Chinese government's ability to advance their agenda at our expense, apply in spades to ports and port technology and port services.

Senator OSSOFF. So, speaking of ports and critical infrastructure, I'd like to hear from you on this Director Wray and then also from Director Haines.

Director Wray, what are the capabilities that you lack that require the DHS Office of Intelligence and Analysis to undertake its own, with respect to the protection of for example, ports or other critical infrastructure?

And Director Haines so you can contemplate it for a moment before I come to you, the question I'm going to ask you is why we require an independent intelligence office at the Department of Homeland Security and why the FBI can't do that work.

Go ahead, Director.

Director WRAY. Well, I think we work well and closely with that office at DHS. I don't know that I could point to a specific thing that we lack, but certainly more players on the field is a useful exercise.

Senator OSSOFF. Well sometimes, unless there's duplication or overlap or inefficiency, right?

Director WRAY. There is, there is that. I will say that what we focus on the most, and it relates to the overall theme of technology here from a different way, is that we in the FBI, and to some extent throughout the Intelligence Community, have a Big Data problem, to use the cliché, of our own, right? Which is that in every investigation, every intelligence analysis, the amount of data that is available or that is being reviewed has exploded over the last few years.

If you just look at a typical FBI case. In one active shooter situation, for example, to pick something simple, we've had ones where we've had more data, pour in than the entire library of Congress in just one investigation.

So, the ability to have tools and people who can get through that data as quickly as possible, to figure out the important leads, to marshal that data—whether that's AI, whether that's data analysts—all those sorts of things become incredibly important to this community's ability to marshal the data and to inform the people that need to be informed.

Senator OSSOFF. And with the Chairman's permission, could Director Haines answer my questions as well, Mr. Chairman?

Thank you.

Director HAINES. Thank you, Senator.

There are a number of missions that DHS and FBI have in relation to domestic intelligence work that's being done across the Nation, where they're really taking the lead. And, when you look at, for example, cybersecurity issues related to critical infrastructure in the United States, CISA within DHS obviously, has an incredibly important role to play, as does the FBI, in working with the private sector and with others on these contacts. And the advantage, I think, of having intel elements, for example in both the FBI and the DHS, is that they're able to work most closely with their

agency and under those authorities to help to support effectively the mission that those agencies are taking. Does that make sense?

Senator OSSOFF. Well, thank you, Director. We'll follow up. Thank you.

Director HAINES. Thank you.

Chairman WARNER. We're through the first round. I've checked with Senator Collins, Senator King. They're prepared to move to the classified section. Senator Rubio and I are. I think Senator Cotton's in a corner and have one question each, and there's about 80 votes in on the second vote. I've not voted yet. So, we'll try to get through these next questions. We will then ask our witnesses to be able to exit the room first before the audience exits, and we will we reconvene in our SCIF.

Senator Cotton.

Senator COTTON. Thank you. I want to return to the issue I addressed at first, which is politicization of analysis and resources. And that can happen by altering conclusions to fit a party line, but it can also happen, as I stressed, in priorities and focus and resources.

So, Director Haines, I want to return again to page 33 of the threat assessment, where you write, transnational racially- and ethnically-motivated violent extremists continue to pose the most lethal threat to U.S. persons and interests. I just found that astonishing. I compared it to fentanyl. And you said your talk you mean that in the context of terrorism, correct? Do you agree with me that fentanyl is a more lethal threat to Americans than racially- and ethnically-motivated violent extremists?

Director HAINES. Yes, absolutely.

Senator COTTON. But in the context of terrorism, your conclusion is that racially- and ethnically-motivated violent extremists are a more lethal threat to Americans than ISIS or Al-Qaeda or Hezbollah?

Director HAINES. Thank you. Yes, what we say in the piece, and it's under the category, essentially, of global terrorism, right. So, it goes through the different areas of global terrorism, including transnationally-, racially-, and ethnically-motivated violent extremism. The fact that it is the most lethal threat with respect to U.S. persons is something that we actually stated, I think, over two years ago in another report as well that similarly laid out these different issues. And it simply is a question of how many people, how many U.S. persons are killed or wounded as a consequence of attacks.

Senator COTTON. Director Burns, do you agree that racially- and ethnically-motivated violent extremists are a more lethal threat to Americans than ISIS or Al-Qaeda?

Director BURNS. Well, I agree, Senator, with what Director Haines just said, that if you measure this in terms of American lives lost or people who were wounded, I think those statistics bear that out. I mean, we obviously take extremely seriously the threat posed by groups like Al-Qaeda, ISIS, and Hezbollah as well. That's our job as a foreign intelligence service as well.

Senator COTTON. I find this astonishing.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. Just as COVID exposed the vulnerability of our supply chains, I think the war in Ukraine has demonstrated the weakness of our industrial base when it comes to replenishing the weapons that we are supplying to the Ukrainians, which I'm all in favor of. And they're using them to good effect.

But General Berrier, in World War II, we became the arsenal of democracy and saved Britain and Europe. But if we got involved in a shooting war in Asia, we would not be ready. And I just want to ask you in terms of an intelligence assessment, how much should we be concerned about our inability to replenish the weapons that we're supplying to Ukraine and the degradation of our defense industrial base?

General BERRIER. Senator, I do appreciate that question. But that's really a question, I think, for our policymakers and decision-makers inside the Pentagon and Department of Defense. Certainly, our readiness is crucial if we're tested by the People's Republic of China, and I'll leave it there.

Chairman WARNER. Well, we're coming to the close of this open hearing. I want to make two final comments.

One, I know Senator Cotton raised this on his first round of questions, and I raised it in my opening comment. Part of our job is the intelligence oversight of all of your agencies and the other roughly 13 additional agencies. We want, following on Senator Rounds's questions, to help make the case—many of us at least do—about 702. And we're going to push you to declassify more information so that we can, again, convince the American public and for that matter, convince the 85 or 86 or 84, colleagues, 83 colleagues, because we're up to 17 now, who are not on this committee. It's one of the reasons why it just does not pass the smell test. The Administration and the Director's current view about giving this Committee access to the classified documents that we have every right to see—in terms of our oversight role involved in terms of the documents that were found at former President Trump, President Biden, and Vice President Pence's. This trust relationship has to go two ways. And the absurdity of the position that somehow a special prosecutor prosecution, about mishandling of documents is more important than making sure that critical top-secret documents that if we have chance to review those and mitigation efforts have been taken. That is not the kind of collaboration cooperation that we expect. And it will tie and restrain our ability to kind of make the kind of trusting relationship with the non-Members of this Committee on issues like 702.

So, I want to be loud and clear on that. And I can assure you, there's not a Member on this Committee—doesn't matter which side of the dais they sit on, that doesn't believe that.

Last point I want to make then turn it over Senator Rubio is that we get to see you guys. And we get to see many of you who are sitting behind you at these sessions and these hearings. We all want to make sure, though, that the literally thousands of men and women, the vast majority of which who have to work in secret, in many cases can't even tell their loved ones what they're doing, that we have your back, we appreciate what you do. We are a safer Nation and a stronger Nation because of the work of the men and

women of the IC. And we look forward to continuing to support you in any way we can.

But we really do want to make sure that message is relayed to those not only back in headquarters, but in many cases, the men and women who are deployed all around the world.

Senator Rubio.

Vice Chairman RUBIO. So just to echo the point the Chairman just made, okay, on this issue of the documents. Let me just take a hypothetical. Well, let me let me start with this. Every agency of our government, right they come here before Congress have oversight committees, they have public hearings, questions are asked, they have to answer them in public, people have to testify. The unique aspect of what your agencies do is, by necessity, it has to be in secret. Most of what you do has to be kept secret, that's the work of intelligence. So how do you conduct oversight over something like that? For a long time, there really wasn't any congressional oversight until the mid-1970s, when committees uncovered all kinds of situations involving the intelligence community. Actually, it almost destroyed the CIA. And the result is the creation of this committee and our counterpart in the House.

And so basically, it comes down to a handful of Members in the House and Senate who are entrusted with conducting oversight to ensure that not only are the intelligence agencies focused on the right things, but are doing it in a way that protects both civil liberties and our national security. Difficult balance.

So that's our role. And it's one we have to play very carefully and one that that's really important for the country, because we need what you do. But we also understand that, left unsupervised, any agency at any time, especially one with these extraordinary powers, can do things that are really troubling and end up actually threatening these agencies' ability to continue to work.

Now, getting to these classified documents. Just as a hypothetical, if tomorrow I take a folder full of classified information, or anybody does, outside the building inappropriately, Okay? For whatever reason, there's going to be an investigation, and there are going to be two things that are going to happen. And there are two individual tracks. Track number one is, I violated the law. I potentially committed—a crime has been committed—because information that's classified was removed from its proper setting. And the result is that there's going to be an investigation. And it could involve the criminal justice system. In most cases, obviously, when it comes to former Presidents, may require special counsel. But generally, it's the U.S. Attorney that's going to look at that and figure that part of it out. Okay. That's not our oversight. And that's not our job to interfere in that.

Separate from that is the job the intelligence agencies have of assessing, okay, this is the information that was stored and inappropriately. Here's the risks to the country, if that information was seen by someone who shouldn't have seen it. And here's what we are doing to mitigate against that risk. How can we possibly conduct oversight over (a), whether you've assigned the proper risk assessment, and (b), over whether the mitigation is appropriate? How can we possibly do that if we don't know what we're talking about? And that's really the situation that we're at right now. And that

is that, even though undoubtedly, the information that was found in all three sites and so forth, are things that we would have had access to. Unless we can identify them, we can't begin to (A) opine over whether or not the risk assessment is accurate, and (B), whether the mitigation that's been assigned is appropriate. We can't do our job. And a special counsel cannot have veto authority over Congress's ability to do its job. It just can't happen. It won't happen.

And so, it will change the nature of the relationship between this Committee, which I think has been very cooperative, and I know we don't have a lot of competition in terms of cooperation, but we're very cooperative. And I'm very proud of the work this Committee has done. And I don't want it to get to that, and it shouldn't get to that, but this is going to be addressed one way or the other.

Chairman WARNER. Amen. And with the recognition that I run a risk that other Members will come back with one last question, James, you're going to get the last bite. And then once you're done with that question, and I think I can speak for all the Members, we would all echo what all the Members on both sides of the dais would agree with what Senator Rubio and I've just said.

Senator Lankford.

Senator LANKFORD. Chairman, I appreciate that. I know we're headed to closed session. Just a couple of statements I wanted to make in open session format.

One is I wanted to reiterate the whole issue of TikTok that's come up several times and just be able to make the comment I think we'll all agree with. This is not about TikTok. This is about any app, any electronics that are coming from China. That information goes back through China. And so, I don't want us to just zero in and just say this is just a TikTok thing. And if we can deal with TikTok, then it's solved. That's not true. There are other apps, there are other things that are coming out of China that are electronic that are doing the exact same thing, just in different areas. It's just that TikTok is kind of the big dog in this.

It reminds me somewhat of our conversation several years ago on Kaspersky, when Kaspersky used to be the free virus software that you could get at Best Buy. What a great deal that you can get this free virus software that runs through Russia to be able to check your computer for viruses. We've all learned the lesson of that. I don't think we've learned the lesson on China. So, I want to be able to reinforce that this is much bigger than just a TikTok issue, though they are the big dog.

The second one is just the issue about what's happening on our southern border. There are some comments that are made in the public statement about this being a Western Hemisphere. Senator Cornyn and I were just at the border not long ago. When we were in Yuma, Arizona, we looked through the listing there at that that particular week, as we're dealing with, there were more people from Uzbekistan that were coming across the border there than there were actually from El Salvador. When we were there, we actually walked up as the Border Patrol was arresting two Chinese nationals coming across. And we're fully aware we're dealing with more than 100 Russian nationals that are crossing our border every single month illegally.

So, my question/issue is here, this is a national security issue, as we've identified. Individuals crossing our southern border that the FBI has interdicted that were coming to assassinate former President Bush not long ago. That came back out. So, this is a bigger national security issue. And what I want to reiterate is, this is not just an issue of push/pull factors in the Western Hemisphere. The openness of our borders also facilitating individuals that I would assume the FBI is not able to be able to keep tabs on the Chinese nationals and Russian nationals and others that are coming into our country that are quote/unquote, seeking asylum, but we don't know where they are in the country.

Is that true or false on that?

Director HAINES. Yes, I certainly did not mean to suggest that the border is solely, related to the comment made about the Western Hemisphere in my opening remarks. I absolutely agree that there's national security issues with vetting folks who go across the border. We obviously participate in vetting in the Intelligence Community and NCTC takes that role from my office and participates in trying to ensure that we can manage that.

Senator LANKFORD. Director Wray, are you able to keep tabs on these individuals that are coming in, has that been assigned to you?

Director WRAY. We're not able to keep tabs on every single person who comes in, certainly. We have all sorts of investigations into certain people who get in. And we try to work very hard on both sides of the border to support DHS's efforts and to some extent, our neighbors south of the border, from preventing them from coming in.

Senator LANKFORD. Thank you. Mr. Chairman, thank you.

Chairman WARNER. Thank you all again, please take back our thanks to all the members and I would again ask our audience, please to allow our witnesses to leave first. And we will reconvene immediately after those of us who have not voted on the last vote. Thank you.

(Whereupon the hearing was adjourned at 12:34 p.m.)

○