AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 116–75

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

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

TUESDAY, JANUARY 29, 2019

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
34–697 PDF WASHINGTON : 2019

SELECT COMMITTEE ON INTELLIGENCE

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

RICHARD BURR, North Carolina, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
TOM COTTON, Arkansas
JOHN CORNYN, Texas
BEN SASSE, Nebraska

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
KAMALA HARRIS, California
MICHAEL L. BENNET, Colorado

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JAMES INHOFE, Oklahoma, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

JANUARY 29, 2019

OPENING STATEMENTS

Burr, Hon. Richard, Chairman, a U.S. Senator from North Carolina 1
Warner, Mark R., Vice Chairman, a U.S. Senator from Virginia 3

WITNESSES

Coats, Daniel R., Director of National Intelligence; Accompanied by: Haspel, Gina, Director of the Central Intelligence Agency; Nakasone, Gen. Paul, Director of the National Security Agency; Askley, Lt. Gen. Robert, Director of the Defense Intelligence Agency; Wray, Christopher, Director of the Federal Bureau of Investigation; and Cardillo, Robert, Director of the National Geospatial-Intelligence Agency 5
Prepared statement 11

SUPPLEMENTAL MATERIAL

Responses to Questions for the Record 86

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

TUESDAY, JANURY 29, 2019

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

The Committee met, pursuant to notice, at 9:34 a.m., in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

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

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to call this hearing to order. I'd like to welcome our witnesses today, Director of National Intelligence, Dan Coats; Director of the Central Intelligence Agency, Gina Haspel; Director of the Defense Intelligence Agency, General Robert Ashley; Director of the Federal Bureau of Investigation, Chris Wray; Director of the National Security Agency, General Paul Nakasone; and Director of the National Geospatial-Intelligence Agency, Robert Cardillo. I thank all of you for being here this morning.

I'd also like to welcome the Committee's new—two newest members, who in typical Senate fashion, are not here yet, Senator Ben Sasse of Nebraska and Senator Michael Bennet of Colorado. They're both great additions, and I look forward to working with them and with you to fulfill the Committee's critical oversight mandates.

Before I go to my formal remarks, I want to extend my condolences of this Committee to General Ashley and his workforce at the Defense Intelligence Agency, as well as General Nakasone and his workforce at NSA. On January 16th, a DIA employee and a naval chief cryptology technician were killed in northern Syria alongside two other Americans. This is a stark and sobering reminder of the dangerous work that the men and women of the Intelligence Community do around the world on the behalf of the country every single day, often with no public acknowledgment. We thank you for your leadership of this community, and more importantly, for what your officers do and the sacrifices they make on behalf of our Nation.

This Committee has met in open forum to discuss the security threats facing the United States since 1995. The nature, scale, and scope of those threats have evolved greatly over the last 25 years. Hostile nation states, terrorist organizations, malign cyber actors, and even infectious disease and natural disasters at different times have been the focus of the Intelligence Community's efforts. Our intelligence officers have repeatedly proven themselves equal to the task of refocusing, reconfiguring, and relearning the business of intelligence to keep pace with a threat landscape that's never static. When this Nation was attacked on September the 11th, counterterrorism rightly became our Nation's security focus, and the Intelligence Community responded by shifting resources and attention. We learned the ways of our new enemy, and we learned how to defeat it.

We're now living in yet another new age, a time characterized by hybrid warfare, weaponized disinformation—all occurring within the context of a world producing more data than mankind has ever seen. Tomorrow it's going to be deepfakes, artificial intelligence, a 5G-enabled Internet of Things with billions of internet connections on consumer devices. What I hope to get out of this morning is a sense of how well prepared the Intelligence Community is to take on this new generation of technologically advanced security threats. Countering these threats requires making information available to those who can act, and doing so with speed and agility. Sometimes the key actors will be the Federal Government. Other times it will be a city. Many times, it will be a social media company, or a start-up, or a biotech firm.

I see a world where greater collaboration between Government and the private sector is necessary, while still protecting sensitive sources and methods. We have to share what we can, trust who we can, and collaborate because we must. The objective of our enemies has not changed. They want to see the United States weakened, if not destroyed. They want to see us abandon our friends and our allies. They want to see us lessen our global presence. They want to see us squabble and divide. But their tools are different.

I don't need to remind anyone in the room when this country's democracy was attacked in 2016, it wasn't with a bomb, or a missile or a plane. It was with social media accounts that any 13-year-old can establish for free. The enemies of this country aren't going to take us on a straight up fight, because they know they'd lose. They're going to keep finding new ways of attacking us, ways that exploit the openness of our society, and slip through the seams of a national security architecture designed for the Cold War.

What this means is that we can't afford to get complacent. We can't find comfort in being good at doing the same things that we've been doing for 50 years. Those who would seek to harm this Nation are creative, adaptive, and resolute. They're creating a new battlefield, and we have been playing catch-up. Defeating them demands that we, as members of your oversight committee, make sure you have the resources and the authorities you need to win.

Director Coats, I'd appreciate your perspective on how to best strike the balance between satisfying existing intelligence requirements and preparing the IC to take on the technological challenge of the future.

I'd like to recognize that this will be Director Cardillo's last appearance before the Committee. Robert, since 2014 you've served as the consummate ambassador for NGA, and this Committee thanks you for your more than 35 years of honorable service to NGA, the Intelligence Community, and more importantly, to the country.

I'll close here because we have a lot of ground to cover today, but I want to thank you again, and more importantly your officers, for the selfless sacrifices that help keep this Nation safe. Yours is an exceptional mission in that so few will ever truly know how much you do in the service of so many.

Before turning to the distinguished Vice Chairman, I'd like to highlight for my colleagues on the Committee, we'll be convening again at 1:00 p.m. this afternoon, promptly, for the afternoon for a classified continuation of this hearing. Please reserve any questions that delve into classified matters until then, and don't take offense if our witnesses find the need to delay their answers to questions that might be on the fringe for the closed session.

With that, I turn to the Vice Chairman.

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

Vice Chairman WARNER. Well, thank you, Mr. Chairman. And let me also welcome our witnesses. Let me extend my condolences, as well, for their loss. Let me also echo what the Chairman has said, Robert, about your service. Your leadership at NGA, your willingness to always push, push, push, and your recognition that in many ways we need to change our models and how we make sure we make better use of our commercial and other partners.

Today's open hearing comes at an important time for our Nation and the world. As I look over the witnesses' statements for the record, I'm struck by the multiplicity of threats our Nation continues to face, from new threats like cyber and online influence, to those that we're more familiar with, like terrorism, extremism, proliferation of WMDs, rogue actors like Iran and North Korea, and regional instability.

We've also seen, and see on a regular basis, daily basis with some of the news yesterday, an increasingly adversarial stance of major powers like Russia and China. At the forefront of our Nation's defenses against these threats stand the professional men and women of the Intelligence Community who you represent. It is, I believe, unconscionable that some of these men and women, and in particular the FBI, Department of Homeland Security, State Department, and others were forced to work without pay for five weeks because of the Government shutdown. This is no way to run a country. We count on the intelligence and law enforcement professionals to protect us. We cannot ask them to do so with no pay and facing threats of eviction or losing their health insurance. The method of running government via shutdown brinkmanship must come to an end.

The myriad threats we face must also be faced in tandem with our allies and partners around the world. As former Secretary of Defense Mattis wrote in his resignation letter, quote, while the U.S. remains the indispensable Nation in the free world, we cannot protect our interests or serve the role effectively without maintain-

ing strong alliances and showing respect to those allies, end quote. I think that is a lesson we all need to take to heart.

Of the multiple threats we face, I would highlight two that I hope we can especially dive into. First, Russia's use of social media to amplify divisions in our society and to influence our democratic process. This is an area that I know was highlighted in our worldwide threat hearing last year, and the concern that we and the IC have that Russia would continue its malign activities to try to influence the 2018 elections. While we did see Russia continue to try to divide Americans on social media, and we saw cyber activities by unknown actors targeting our election infrastructure in 2018, the good news—in particular General Nakasone, I commend you—is, I think, we did a much better job.

The question, though, is how do we prepare ourselves for 2020? How do we make sure that we're fully organized? What is the IC's role in fighting this disinformation threat? And how can we build upon public-private partnerships with online social media companies in a way that works for both sides? This is a problem, as the Chairman has mentioned, with the question around deepfakes and other areas that technology is only going to make more difficult.

The second issue I'd hope that you would all address today is the threat from China, particularly in the field of technology. I think we all saw the Justice Department announcement yesterday about Huawei. I have to say as a former entrepreneur and venture capitalist, I long held the view that an economically advanced China would eventually become a responsible global citizen that would join the World Trade Organization, and whose system would ultimately be liberalized by market-based economies.

Unfortunately, what we've seen, particularly in the last two or three years, is the opposite. With the consolidation of power by the Communist Chinese party and with President Xi emphasizing nationalistic tendencies, an aggressive posture towards those nations on China's periphery, and an economic policy that seeks by hook or by crook to catch up to and surpass the United States economically—especially in the areas of technology like AI, machine learning, biotech, 5G, and other related areas. Especially concerning have been the efforts of big Chinese tech companies which are beholden to the Communist Chinese party to acquire sensitive technology, replicate it, and undermine the market share of U.S. firms with the help of the Chinese state.

I want to thank DNI Director Coats and FBI Director Wray as well as DHS for working with the Committee to take seriously the threat from China's whole-of-society approach to technology acquisition and to jointly reach out to our business community with whom we must work in partnership to begin to address these issues. Unfortunately, we've still got a long way to go and while Director Coats particularly you—we've gone on some of these roadshows together with the Chairman—I think we need much more of those going forward.

I want to ensure that the IC is tracking the direction of China's tech giants and to make sure that we counter those efforts, particularly as so many of them are beholden to the Chinese government. The truth is this is a challenge that will only continue to grow.

I also in closing want to thank not only you but all of the men and women who stand behind your organizations, who work day in and day out to keep our Nation safe. I look forward to this public hearing.

Thank you, Mr. Chairman. I yield.

Chairman BURR. I thank the Vice Chairman. Before I recognize Director Coats for his testimony let me say to our witnesses: a number of the members of this Committee have competing committee meetings right now on very important things so members are going to be in and out. Please don't take that as a sign of any disinterest in your testimony or your answers but there are a lot of things going on on the Hill today that are priorities from a standpoint of legislative activity.

Director Coats, it is my understanding you are going to give one opening statement for the entire group and then we'll move to questions?

Director COATS. Yes, sir.

Chairman BURR. The floor is yours.

STATEMENT OF DANIEL R. COATS, DIRECTOR OF NATIONAL INTELLIGENCE; ACCOMPANIED BY: GINA HASPEL, DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY; GEN. PAUL NAKASONE, DIRECTOR OF THE NATIONAL SECURITY AGENCY; LT. GEN. ROBERT ASKLEY, DIRECTOR OF THE DEFENSE INTELLIGENCE AGENCY; CHRISTOPHER WRAY, DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION; AND ROBERT CARDILLO, DIRECTOR OF THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Director COATS. Mr. Chairman and Mr. Vice Chairman, members of the Committee, we are here today and I'm here today with these exceptional people who I have the privilege to work with. We are a team that works together in making sure that we can do everything we possibly can to bring the intelligence necessary to our policymakers, to this Committee, and others relative to what decisions they might have to make given this ever-changing world that we are facing right now.

During my tenure as DNI, now two years in, I have told our workforce over and over that our mission was to seek the truth and speak the truth and we work to enhance, to agree with, and enforce that mission on a daily basis. I want our people to get up in the morning to work to think that this is what our job is. Despite the swirl of politics that swirls around on not only the Capitol but the world, our mission is to keep our heads down, our focus on the mission that we have to achieve in order to keep American people safe, and our policy makers aware of what's happening.

So truly the efforts of people sitting here at this table and all of their employees and all of our components is not really released for the public to know well about, but we continue to value our relationship with this Committee in terms of how we share information, how we respond to your legitimate questions that you bring to us and tasks for us, and we value very much the relationship that we have with this Committee.

My goal today is to responsibly convey to you and the American people in this unclassified hearing the true nature of the current

environment and in the interest of time I'd also like to refer you to my statement for the record for a more complete threat picture. As I stated in my recent remarks during the release of the National Intelligence Strategy, we face significant changes in the domestic and global environment that have resulted in an increasingly complex and uncertain world and we must be ready. We must be ready to meet 21st-century challenges and recognize the emerging threats.

The composition of the current threats we face is a toxic mix of strategic competitors, regional powers, weak or failed states, and non-state actors using a variety of tools in overt and subtle ways to achieve their goals. The scale and scope of the various threats facing the United States and our immediate interest worldwide is likely to further intensify this year. It is increasingly a challenge to prioritize which threats are of greatest importance.

I first would like to mention election security. This has been and will continue to be a top priority for the Intelligence Community. We assess that foreign actors will view the 2020 U.S. elections as an opportunity to advance their interests. We expect them to refine their capabilities and add new tactics as they learn from each other's experiences and efforts in previous elections. On the heels of our successful efforts to protect the integrity of the 2018 midterm elections, we are now focused on incorporating lessons learned in preparation for the 2020 elections.

I would now like to turn to the variety of threats that currently exist and may materialize in the coming year. I would like to begin with remarks on what I would describe as the big four: China, Russia, North Korea, and Iran—all of which pose unique threats to the United States and our partners. China's actions reflect a long-term strategy to achieve global superiority. Beijing's global ambition continues to restrict the personal freedoms of its citizens while strictly enforcing obedience to Chinese leadership with very few remaining checks on President Xi's power.

In its efforts to diminish U.S. influence and extend its own economic, political, and military reach, Beijing will seek to tout a distinctly Chinese fusion of strongman autocracy and a form of Western-style capitalism as a development model and implicit alternative to democratic values and institutions. These efforts will include the use of its intelligence and influence apparatus to shape international views and gain advantages over its competitors including especially the United States.

China's pursuit of intellectual property, sensitive research and development plans, and the U.S. person data remains a significant threat to the United States Government and the private sector. China's military capabilities and reach will continue to grow as it invests heavily in developing and fielding advanced weapons, and Beijing will use its military clout to expand its footprint and complement its broadening political and economic influence as we have seen with its One Belt One Road Initiative. As part of this trend we anticipate China will attempt to further solidify and increase its control within its immediate sphere of influence in the South China Sea and its global presence further abroad.

Whereas with China we must be concerned about the methodological and long-term efforts to capitalize on its past decade of a

growing economy and to match or overtake our superior global capabilities, Russia's approach relies on misdirection and obscuration as it seeks to destabilize and diminish our standing in the world.

Even as Russia faces a weakening economy, the Kremlin is stepping up its campaign to divide Western political and security institutions and undermine the post-World War II international order. We expect Russia will continue to wage its information war against democracies and to use social media to attempt to divide our societies. Russia's attack against Ukrainian naval vessels in November is just the latest example of the Kremlin's willingness to violate international norms, to coerce its neighbors and accomplish its goals. We also expect Russia will use cyber techniques to influence Ukraine's upcoming presidential election. The Kremlin has aligned Russia with repressive regimes in Cuba, Iran, North Korea, Syria, and Venezuela. And Moscow's relationship with Beijing is closer than it has been in many decades.

The Kremlin is also stepping up its engagement in the Middle East, Africa, and Southeast Asia, using weapons sales, private security firms, and energy deals to advance its global influence. Regarding North Korea, the regime has halted its provocative behavior related to its WMD program. North Korea has not conducted any nuclear-capable missile or nuclear tests in more than a year and it has dismantled some of its nuclear infrastructure. As well, Kim Jong-Un continues to demonstrate openness to the denuclearization of the Korean Peninsula.

Having said that, we currently assess that North Korea will seek to retain its WMD capabilities and is unlikely to completely give up its nuclear weapons and production capabilities because its leaders ultimately view nuclear weapons as critical to regime survival. Our assessment is bolstered by our observations of some activity that is inconsistent with full denuclearization. While we assess that sanctions on exports have been effective and largely maintained, North Korea seeks to mitigate the effects of the U.S.-led pressure campaign through diplomatic engagement, counter-pressure against the sanction's regime, and direct sanctions evasion.

Now let me discuss Iran. The Iranian regime will continue pursuing regional ambitions and improved military capabilities, even while its own economy is weakening by the day. Domestically, regime hardliners will be more emboldened to challenge rivals' interests and we expect more unrest in Iran in recent months. Tehran continues to sponsor terrorism as the recent European arrests of Iranian operatives plotting attacks in Europe demonstrate. We expect Iran will continue supporting the Houthis in Yemen and Shia militants in Iraq while developing indigenous military capabilities that threaten U.S. forces and allies in the region.

Iran maintains the largest inventory of ballistic missiles in the Middle East. And while we do not believe Iran is currently undertaking activities we judge necessary to produce a nuclear device, Iranian officials have publicly threatened to push the boundaries of the JCPOA restrictions if Iran does not gain the tangible financial benefits it expected from the deal. Iran's efforts to consolidate its influence in Syria and arm Hezbollah have prompted Israeli airstrikes. These actions underscore our concerns for a long-term tra-

jectory of Iranian influence in the region and the risk of conflict escalation.

All four of these states that I have just mentioned—China, Russia, North Korea, and Iran—are advancing their cyber capabilities, which are relatively low-cost and growing in potency and severity. This includes threatening both minds and machines in an expanding number of ways, such as stealing information, attending to influence populations, or developing ways to disrupt critical infrastructures. As the world becomes increasingly interconnected, we expect these actors and others to rely more and more on cyber capabilities when seeking to gain political, economic, and military advantages over the United States and its allies and partners.

Now that I've covered the big four, I'll quickly hit on some regional and transnational threats. In the Middle East, President Bashar al-Assad has largely defeated the opposition and is now seeking to regain control over all of Syrian territory. Remaining pockets of ISIS and opposition fighters will continue, we assess, to stoke violence as we have seen in incidents happening in the Idlib Province of Syria. The regime will focus on retaking territory while seeking to avoid conflict with Israel and Turkey.

And with respect to Turkey, we assess it is in the midst of a transformation of its political and national identity that will make Washington's relations with Ankara increasingly difficult to manage during the next five years. Turkey will continue to see the PKK and related Kurdish groups as the main threat to their sovereignty. Under President Erdogan, U.S./Turkey relations will be important but not necessarily decisive for Ankara.

In Iraq, the underlying political and economic factors that facilitated the rise of ISIS persist, and Iraqi Shia militants' attempts to further entrench their role in the state with the assistance of Iran will increase the threat to U.S. personnel. In Yemen, where 75 percent of the population is reliant on foreign assistance, neither side of the conflict seems committed to end the fighting, and the humanitarian impact of the conflict in 2019 will further compound already acute problems.

In Saudi Arabia, public support for the royal family appears to remain high, even in the wake of the murder of journalist Jamal Khashoggi and the Kingdom's continued involvement in the Yemen conflict that has generated global pushback. In South Asia, the focus of the region will be centered on the potential turmoil surrounding Afghanistan's upcoming presidential election, ongoing negotiations with the Taliban, and the Taliban's large-scale recent attacks.

We assess neither the Afghan government nor the Taliban will be able to gain a strategic advantage in the Afghan war in the coming war year, even if Coalition support remains at current levels. However, current efforts to achieve an agreement with the Taliban and decisions on a possible withdrawal of U.S. troops could play a key role in shaping the direction of the country in the coming years. Militant groups supported by Pakistan will continue to take advantage of their safe haven in Pakistan to plan and conduct attacks in neighboring countries and possibly beyond, and we remain concerned about Pakistan's continued development and control of nuclear weapons.

In Africa, several countries are facing significant challenges that threaten their stability, which could reverberate throughout the region. Libya remains unstable in various groups—and various groups continue to be supported by a variety of foreign actors and competing goals. In the Democratic Republic of Congo, a new government will be challenged to deal with ongoing violence by multiple armed groups and the outbreak of your Ebola in the east of the country. And instability is growing in Sudan, where the population is angry at the country's direction and President Bashir's leadership.

In Europe, political, economic, and social trends will increase political uncertainty and complicate efforts to push back against some autocratic tendencies. Meanwhile, the possibility of a no deal Brexit, in which the UK exits the EU without an agreement, remains. This would cause economic disruptions that could substantially weaken the UK and Europe. We anticipate that the evolving landscape in Europe will lead to additional challenges to U.S. interests as Russia and China intensify their efforts to build influence there at the expense of the United States.

In the Western Hemisphere, flagging economies, migration flows, corruption, narcotics, trafficking, and anti-U.S. autocrats will challenge U.S. interests.

Venezuela is at a crossroads as its economy faces further cratering and political leaders vie for control, all of which are likely to contribute to the unprecedented migration of Venezuelans. We expect the attempts by Cuba, Russia, and to some extent China to prop up the Maduro regime's security or financing will lead to additional efforts to exploit the situation in exchange for access, mostly to Venezuelan oil.

We assessed that Mexico, under new leadership, will pursue cooperation with the United States as it tries to reduce violence and address socioeconomic issues, but authorities still do not have the capability to fully address the production, the flow, and trafficking of the drug cartels. High crime rates and weak job markets will continue to spur U.S.-bound migrants from El Salvador, Guatemala, and Honduras.

To close my remarks, I would like to address several challenges that span the globe. I already mentioned the increased use of cyber capabilities by nefarious actors, but we must be mindful of the proliferation of other threats beginning with weapons of mass destruction. In addition to nuclear weapons, we have heightened concerns about chemical and biological weapons. We assess that North Korea, Russia, Syria, and ISIS have all used chemical weapons over the past two years, which threatens international norms and may portend future use.

The threat from biological weapons has become more diverse as they can be employed in a variety of ways and their development is made easier by dual use technologies. We expect foreign governments to expand their use of space-based reconnaissance, communications, and navigation systems, and China and Russia will continue training and equipping their military space forces and fielding new anti-satellite weapons to hold U.S. and allied space services at risk. Space has become the new global frontier, with competition from numerous nations.

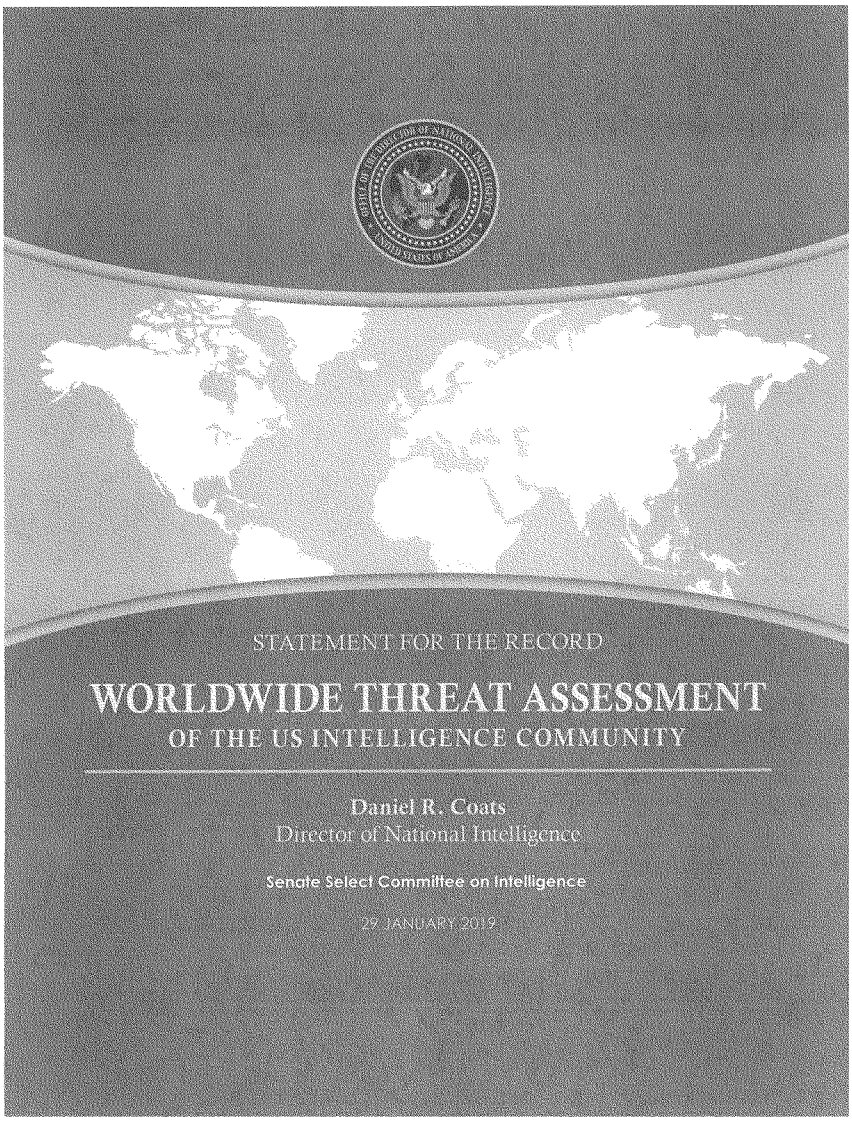
Terrorism remains a persistent threat and, in some ways, is positioned to increase in 2019. The conflicts in Iraq and Syria have generated a large pool of skilled and battle-hardened fighters who remained dispersed throughout the region.

While ISIS is nearing territorial defeat in Iraq and Syria, the group has returned to its guerrilla warfare roots while continuing to plot attacks and direct its supporters worldwide. ISIS is intent on resurging and still commands thousands of fighters in Iraq and Syria. Meanwhile, al-Qaeda is showing signs of confidence as its leaders work to strengthen their networks and encourage attacks against Western interests. We saw this most recently in Kenya as Al-Shabaab attacked a hotel frequented by tourists and Westerners.

Lastly—and this is important because both the Chairman and Vice Chairman have stated this, and it's something that I think is a challenge to the IC and to the American people—the speed and adaptation of new technology will continue to drive the world in which we live in ways we have yet to fully understand. Advances in areas such as artificial intelligence, communication technologies, biotechnology, and materials sciences are changing our way of life, but our adversaries are also investing heavily into these technologies, and they are likely to create new and unforeseen challenges to our health, economy, and security.

Mr. Chairman and Mr. Vice Chairman and members of the Committee, this becomes a major challenge to the IC community to stay ahead of the game and to have the resources directed toward how we need to address these threats to the United States. We look forward to spending more time discussing this issue as both of you have raised. With that, I'll leave it there. We look forward to answering your questions about these and other unmentioned threats.

[The prepared joint statement of the witnesses follows:]


STATEMENT FOR THE RECORD
WORLDWIDE THREAT ASSESSMENT
OF THE US INTELLIGENCE COMMUNITY
Daniel R. Coats
Director of National Intelligence
Senate Select Committee on Intelligence
29 JANUARY 2019

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY

January 29, 2019

INTRODUCTION

Chairman Burr, Vice Chairman Warner, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2019 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary women and men, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of 17 January 2019 was used in the preparation of this assessment.

ATTENTION: This product contains US persons information, which has been included consistent with applicable laws, directives, and policies. Handle in accordance with recipient's intelligence oversight and/or information handling procedures.

CONTENTS

INTRODUCTION 2
CONTENTS 3
FOREWORD 4
GLOBAL THREATS 5
- CYBER 5
- ONLINE INFLUENCE OPERATIONS AND ELECTION INTERFERENCE 7
- WEAPONS OF MASS DESTRUCTION AND PROLIFERATION 8
- TERRORISM 10
- COUNTERINTELLIGENCE 13
- EMERGING AND DISRUPTIVE TECHNOLOGIES AND THREATS TO ECONOMICCOMPETITIVENESS 15
- SPACE AND COUNTERSPACE 16
- TRANSNATIONAL ORGANIZED CRIME 18
- ECONOMICS AND ENERGY 19
- HUMAN SECURITY 21

REGIONAL THREATS 24
- CHINA AND RUSSIA 24
- EAST ASIA 24
- MIDDLE EAST AND NORTH AFRICA 29
- SOUTH ASIA 35
- RUSSIA AND EURASIA 36
- EUROPE 38
- AFRICA 39
- THE WESTERN HEMISPHERE 40

FOREWORD

Threats to US national security will expand and diversify in the coming year, driven in part by China and Russia as they respectively compete more intensely with the United States and its traditional allies and partners. This competition cuts across all domains, involves a race for technological and military superiority, and is increasingly about values. Russia and China seek to shape the international system and regional security dynamics and exert influence over the politics and economies of states in all regions of the world and especially in their respective backyards.

- China and Russia are more aligned than at any point since the mid-1950s, and the relationship is likely to strengthen in the coming year as some of their interests and threat perceptions converge, particularly regarding perceived US unilateralism and interventionism and Western promotion of democratic values and human rights.

- As China and Russia seek to expand their global influence, they are eroding once well-established security norms and increasing the risk of regional conflicts, particularly in the Middle East and East Asia.

- At the same time, some US allies and partners are seeking greater independence from Washington in response to their perceptions of changing US policies on security and trade and are becoming more open to new bilateral and multilateral partnerships.

The post-World War II international system is coming under increasing strain amid continuing cyber and WMD proliferation threats, competition in space, and regional conflicts. Among the disturbing trends are hostile states and actors' intensifying online efforts to influence and interfere with elections here and abroad and their use of chemical weapons. Terrorism too will continue to be a top threat to US and partner interests worldwide, particularly in Sub-Saharan Africa, the Middle East, South Asia, and Southeast Asia. The development and application of new technologies will introduce both risks and opportunities, and the US economy will be challenged by slower global economic growth and growing threats to US economic competitiveness.

- Migration is likely to continue to fuel social and interstate tensions globally, while drugs and transnational organized crime take a toll on US public health and safety. Political turbulence is rising in many regions as governance erodes and states confront growing public health and environmental threats.

- Issues as diverse as Iran's adversarial behavior, deepening turbulence in Afghanistan, and the rise of nationalism in Europe all will stoke tensions.

15

GLOBAL THREATS

CYBER

Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.

At present, China and Russia pose the greatest espionage and cyber attack threats, but we anticipate that all our adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities into their efforts to influence US policies and advance their own national security interests. In the last decade, our adversaries and strategic competitors have developed and experimented with a growing capability to shape and alter the information and systems on which we rely. For years, they have conducted cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk. They are now becoming more adept at using social media to alter how we think, behave, and decide. As we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic competitors almost certainly will gain greater insight into and access to our protected information.

China

China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies. It is improving its cyber attack capabilities and altering information online, shaping Chinese views and potentially the views of US citizens—an issue we discuss in greater detail in the Online Influence Operations and Election Interference section of this report.

- Beijing will authorize cyber espionage against key US technology sectors when doing so addresses a significant national security or economic goal not achievable through other means. We are also concerned about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies.

- China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.

Russia

We assess that Russia poses a cyber espionage, influence, and attack threat to the United States and our allies. Moscow continues to be a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve its political and military objectives. Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat—an issue discussed in the Online Influence Operations and Election Interference section of this report.

- Russian intelligence and security services will continue targeting US information systems, as well as the networks of our NATO and Five Eyes partners, for technical information, military plans, and insight into our governments' policies.

- Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.

Iran

Iran continues to present a cyber espionage and attack threat. Iran uses increasingly sophisticated cyber techniques to conduct espionage; it is also attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries. Tehran also uses social media platforms to target US and allied audiences, an issue discussed in the Online Influence Operations and Election Interference section of this report.

- Iranian cyber actors are targeting US Government officials, government organizations, and companies to gain intelligence and position themselves for future cyber operations.

- Iran has been preparing for cyber attacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017.

North Korea

North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks. North Korea continues to use cyber capabilities to steal from financial institutions to generate revenue. Pyongyang's cybercrime operations include attempts to steal more than $1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated $81 million from the New York Federal Reserve account of Bangladesh's central bank.

Nonstate and Unattributed Actors

Foreign cyber criminals will continue to conduct for-profit, cyber-enabled theft and extortion against US networks. We anticipate that financially motivated cyber criminals very likely will expand their targets in the United States in the next few years. Their actions could increasingly disrupt US critical infrastructure in the health care, financial, government, and emergency service sectors, based on the patterns of activities against these sectors in the last few years.

Terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims. Terrorist groups could cause some disruptive effects—defacing websites or executing denial-of-service attacks against poorly protected networks—with little to no warning.

The growing availability and use of publicly and commercially available cyber tools is increasing the overall volume of unattributed cyber activity around the world. The use of these tools increases the risk of misattributions and misdirected responses by both governments and the private sector.

ONLINE INFLUENCE OPERATIONS AND ELECTION INTERFERENCE

Our adversaries and strategic competitors probably already are looking to the 2020 US elections as an opportunity to advance their interests. More broadly, US adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States and elsewhere. We expect our adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences, suggesting the threat landscape could look very different in 2020 and future elections.

- Russia's social media efforts will continue to focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians. Moscow may employ additional influence toolkits—such as spreading disinformation, conducting hack-and-leak operations, or manipulating data—in a more targeted fashion to influence US policy, actions, and elections.

- Beijing already controls the information environment inside China, and it is expanding its ability to shape information and discourse relating to China abroad, especially on issues that Beijing views as core to party legitimacy, such as Taiwan, Tibet, and human rights. China will continue to use legal, political, and economic levers—such as the lure of Chinese markets —to shape the information environment. It is also capable of using cyber attacks against systems in the United States to censor or suppress viewpoints it deems politically sensitive.

- Iran, which has used social media campaigns to target audiences in both the United States and allied nations with messages aligned with Iranian interests, will continue to use online influence operations to try to advance its interests.

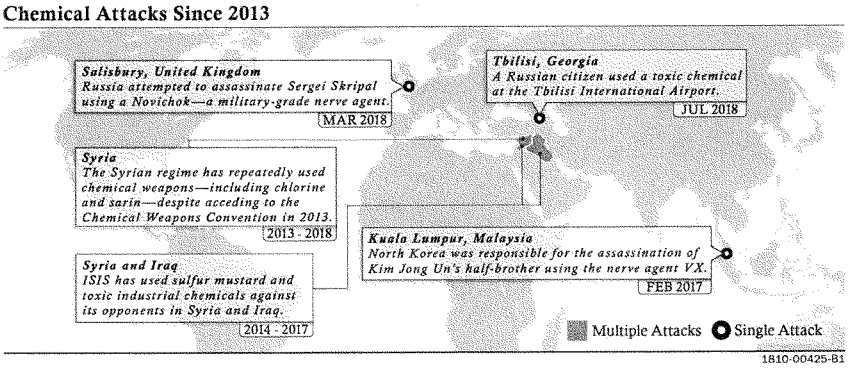
- Adversaries and strategic competitors probably will attempt to use deep fakes or similar machine-learning technologies to create convincing—but false—image, audio, and video files to augment influence campaigns directed against the United States and our allies and partners.

Adversaries and strategic competitors also may seek to use cyber means to directly manipulate or disrupt election systems—such as by tampering with voter registration or disrupting the vote tallying process—either to alter data or to call into question our voting process. Russia in 2016 and unidentified actors as recently as 2018 have already conducted cyber activity that has targeted US election infrastructure, but we do not have any intelligence reporting to indicate any compromise of our nation's election infrastructure that would have prevented voting, changed vote counts, or disrupted the ability to tally votes.

WEAPONS OF MASS DESTRUCTION AND PROLIFERATION

We expect the overall threat from weapons of mass destruction (WMD) to continue to grow during 2019, and we note in particular the threat posed by chemical warfare (CW) following the most significant and sustained use of chemical weapons in decades. This trend erodes international norms against CW programs and shifts the cost-benefit analysis such that more actors might consider developing or using chemical weapons.

Chemical Attacks Since 2013



We assess that North Korea, Russia, Syria, and ISIS have used chemical weapons on the battlefield or in assassination operations during the past two years. These attacks have included traditional CW agents, toxic industrial chemicals, and the first known use of a Novichok nerve agent.

The threat from biological weapons has also become more diverse as BW agents can be employed in a variety of ways and their development is made easier by dual-use technologies.

North Korea

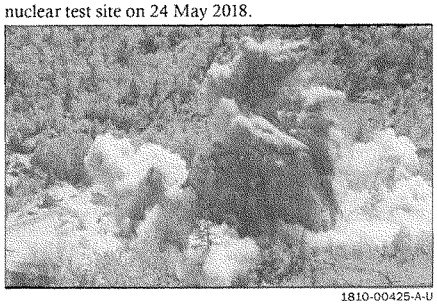
Pyongyang has not conducted any nuclear-capable missile or nuclear tests in more than a year, has declared its support for the denuclearization of the Korean Peninsula, and has reversibly dismantled portions of its WMD infrastructure. However, North Korea retains its WMD capabilities, and the IC continues to assess that it is unlikely to give up all of its WMD stockpiles, delivery systems, and production capabilities. North Korean leaders view nuclear arms as critical to regime survival. For more explanation of the North Korea-WMD issue, see the Regional Threats section of this report.

- In his 2019 New Year's address, Kim Jong Un pledged North Korea would "go toward" complete denuclearization and promised not to make, test, use, or proliferate nuclear weapons. However, he conditioned progress on US "practical actions." The regime tied the idea of denuclearization in the past to changes in diplomatic ties, economic sanctions, and military activities.

- We continue to observe activity inconsistent with full denuclearization. In addition, North Korea has for years underscored its commitment to nuclear arms, including through an order in 2018 to mass-produce weapons and an earlier law—and constitutional change—affirming the country's nuclear status.

North Korea Dismantles Portions of Its Nuclear Test Site

North Korea invited foreign press representatives to witness its explosive destruction of portions of its nuclear test site on 24 May 2018.



1810-00425-A-U

Russia

We assess that Russia will remain the most capable WMD adversary through 2019 and beyond, developing new strategic and nonstrategic weapons systems.

- Russian President Vladimir Putin used his annual address in March 2018 to publicly acknowledge several of these weapons programs, including a new ICBM designed to penetrate US missile defense systems; an intercontinental-range, hypersonic glide vehicle; a maneuverable, air-launched missile to strike regional targets; a long-range, nuclear-powered cruise missile; and a nuclear-powered, transoceanic underwater vehicle.

- Russia has also developed and fielded a ground-launched cruise missile (GLCM) that the United States has determined violates the Intermediate-Range Nuclear Forces (INF) Treaty.

- Moscow probably believes that the new GLCM provides sufficient military advantages to make it worth the risk of political repercussions from a violation.

China

We assess that China will continue to expand and diversify its WMD capabilities.

- China continues its multiyear effort to modernize its nuclear missile forces, including deploying sea-based weapons, improving its road-mobile and silo-based weapons, and testing hypersonic glide vehicles. These new capabilities are intended to ensure the viability of China's strategic deterrent by providing a second-strike capability and a way to overcome missile defenses. The Chinese have also publicized their intent to form a nuclear triad by developing a nuclear-capable, next-generation bomber.

Iran

We continue to assess that Iran is not currently undertaking the key nuclear weapons-development activities we judge necessary to produce a nuclear device. However, Iranian officials have publicly threatened to reverse some of Iran's Joint Comprehensive Plan of Action (JCPOA) commitments—and resume nuclear activities that the JCPOA limits—if Iran does not gain the tangible trade and investment benefits it expected from the deal.

- In June 2018, Iranian officials started preparations, allowable under the JCPOA, to expand their capability to manufacture advanced centrifuges.
- Also in June 2018, the Atomic Energy Organization of Iran (AEOI) announced its intent to resume producing natural uranium hexafluoride (UF_6) and prepare the necessary infrastructure to expand its enrichment capacity within the limits of the JCPOA.
- Iran continues to work with other JCPOA participants—China, the European Union, France, Germany, Russia, and the United Kingdom—to find ways to salvage economic benefits from it. Iran's continued implementation of the JCPOA has extended the amount of time Iran would need to produce enough fissile material for a nuclear weapon from a few months to about one year.

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

The United States determined in 2018 that Iran is in noncompliance with its obligations under the Chemical Weapons Convention (CWC), and we remain concerned that Iran is developing agents intended to incapacitate for offensive purposes and did not declare all of its traditional CW agent capabilities when it ratified the CWC.

South Asia

The continued growth and development of Pakistan and India's nuclear weapons programs increase the risk of a nuclear security incident in South Asia, and the new types of nuclear weapons will introduce new risks for escalation dynamics and security in the region. Pakistan continues to develop new types of nuclear weapons, including short-range tactical weapons, sea-based cruise missiles, air-launched cruise missiles, and longer range ballistic missiles. India this year conducted its first deployment of a nuclear-powered submarine armed with nuclear missiles.

TERRORISM

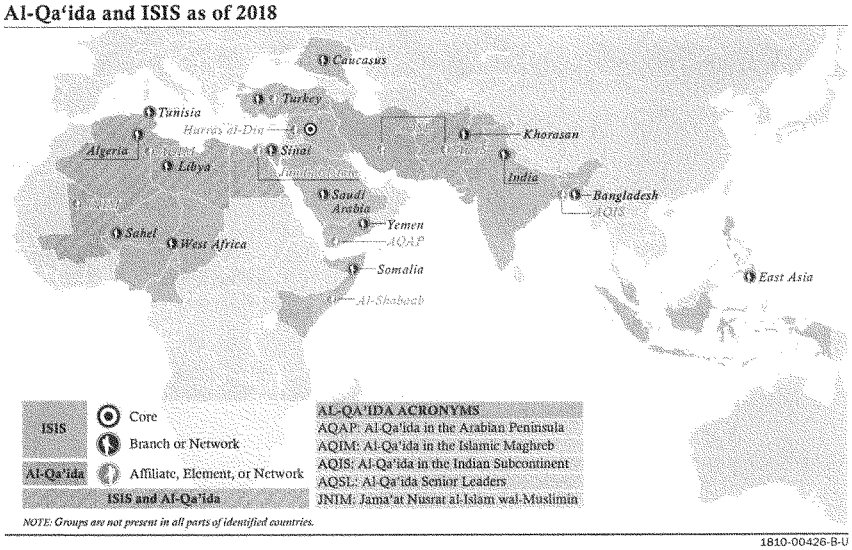
Sunni Violent Extremists

Global jihadists in dozens of groups and countries threaten local and regional US interests, despite having experienced some significant setbacks in recent years, and some of these groups will remain intent on striking the US homeland. Prominent jihadist ideologues and media platforms continue to call for and justify efforts to attack the US homeland.

- Global jihadist groups in parts of Africa and Asia in the last year have expanded their abilities to strike local US interests, stoke insurgencies, and foster like-minded networks in neighboring countries.

- The conflicts in Iraq and Syria have generated a large pool of battle-hardened fighters with the skills to conduct attacks and bolster terrorist groups' capabilities.

Al-Qa'ida and ISIS as of 2018



1810-00426-B-U

ISIS

ISIS still commands thousands of fighters in Iraq and Syria, and it maintains eight branches, more than a dozen networks, and thousands of dispersed supporters around the world, despite significant leadership and territorial losses. The group will exploit any reduction in CT pressure to strengthen its clandestine presence and accelerate rebuilding key capabilities, such as media production and external operations. ISIS very likely will continue to pursue external attacks from Iraq and Syria against regional and Western adversaries, including the United States.

- ISIS is perpetrating attacks in Iraq and Syria to undermine stabilization efforts and retaliate against its enemies, exploiting sectarian tensions in both countries. ISIS probably realizes that controlling new territory is not sustainable in the near term. We assess that ISIS will seek to exploit Sunni grievances, societal instability, and stretched security forces to regain territory in Iraq and Syria in the long term.

Al-Qa'ida

Al-Qa'ida senior leaders are strengthening the network's global command structure and continuing to encourage attacks against the West, including the United States, although most al-Qa'ida affiliates' attacks to date have been small scale and limited to their regional areas. We expect that al-Qa'ida's global network will remain a CT challenge for the United States and its allies during the next year.

- Al-Qa'ida media continues to call for attacks against the United States, including in statements from regional al-Qa'ida leaders, reflecting the network's enduring efforts to pursue or inspire attacks in the West.

- All al-Qa'ida affiliates are involved in insurgencies and maintain safe havens, resources, and the intent to strike local and regional US interests in Africa, the Middle East, and South Asia.

- Al-Qa'ida affiliates in East and North Africa, the Sahel, and Yemen remain the largest and most capable terrorist groups in their regions. All have maintained a high pace of operations during the past year, despite setbacks in Yemen, and some have expanded their areas of influence. Al-Qa'ida elements in Syria, meanwhile, continue to undermine efforts to resolve that conflict, while the network's affiliate in South Asia provides support to the Taliban.

Homegrown Violent Extremists

Homegrown violent extremists (HVEs) are likely to present the most acute Sunni terrorist threat to the United States, and HVE activity almost certainly will have societal effects disproportionate to the casualties and damage it causes.

- The United States' well-integrated Muslim population, fragmented HVE population, and high level of vigilance will ensure the United States remains a generally inhospitable operating environment for HVEs compared to many other Western countries. The isolated nature of self-radicalizing individuals, however, poses a continual challenge to law enforcement to identify them before they engage in violence. The frequency of attacks most likely will be very low compared to most other forms of criminal violence in the US, as long as US CT and law enforcement efforts remain constant.

- Despite territorial losses in Iraq and Syria, ISIS's past actions and propaganda probably will inspire future HVE attacks, similar to the enduring influence of deceased al-Qa'ida ideologues, especially if ISIS can retain its prominence among global jihadist movements and continue to promote its violent message via social and mainstream media.

Shia Actors

Iran

Iran almost certainly will continue to develop and maintain terrorist capabilities as an option to deter or retaliate against its perceived adversaries.

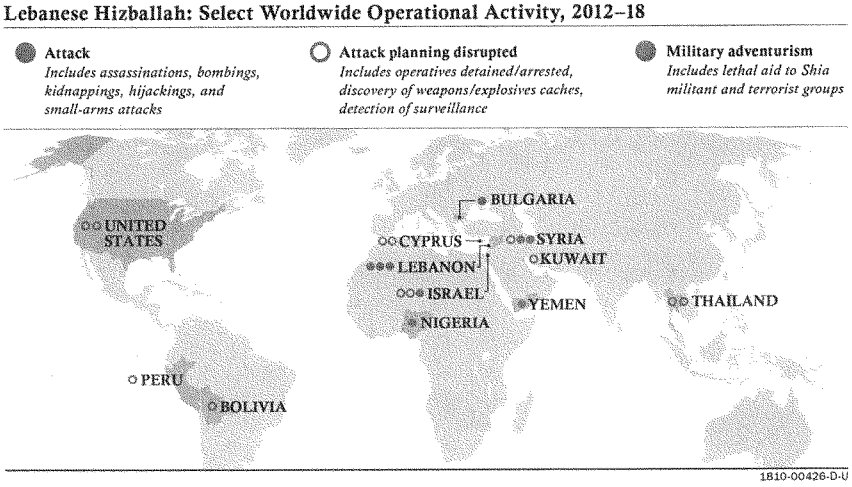
- In mid-2018, Belgium and Germany foiled a probable Iranian Ministry of Intelligence and Security (MOIS) plot to set off an explosive device at an Iranian opposition group gathering in Paris—an event that included prominent European and US attendees.

Lebanese Hizballah

During the next year, Hizballah most likely will continue to develop its terrorist capabilities, which the group views as a valuable tool and one it can maintain with plausible deniability.

- Hizballah most likely maintains the capability to execute a range of attack options against US interests worldwide.

Lebanese Hizballah: Select Worldwide Operational Activity, 2012–18



Violent Ethno-supremacist and Ultranationalist Groups

Some violent ethno-supremacist and ultranationalist groups in Europe will employ violent tactics as they seek ways to cooperate against immigration and the perceived Islamization of Europe, posing a potential threat to US and allied interests.

- In the past two years, individuals with ties to violent ethno-supremacist groups in France, Sweden, and the United Kingdom have either carried out attacks on minorities and politicians or had their plots disrupted by authorities.

COUNTERINTELLIGENCE

The United States faces a complex global foreign intelligence threat environment in 2019. Russia and China will continue to be the leading state intelligence threats to US interests, based on their services' capabilities, intent, and broad operational scopes. Other states also pose persistent threats, notably Iran and Cuba. Geopolitical, societal, and technological changes will increase opportunities for foreign

intelligence services and other entities—such as terrorists, criminals, and cyber actors—to collect on US activities and information to the detriment of US interests.

- Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain a key objective for numerous foreign intelligence services and other entities. In addition, targeting of national security information and proprietary technology from US companies and research institutions will remain a sophisticated and persistent threat.

Russia

We expect that Russia's intelligence services will target the United States, seeking to collect intelligence, erode US democracy, undermine US national policies and foreign relationships, and increase Moscow's global position and influence.

China

We assess that China's intelligence services will exploit the openness of American society, especially academia and the scientific community, using a variety of means.

Iran and Cuba

We assess that Iran and Cuba's intelligence services will continue to target the United States, which they see as a primary threat. Iran continues to unjustly detain US citizens and has not been forthcoming about the case of former FBI agent Robert Levinson (USPER).

China's Technology Development Strategy

China takes a multifaceted, long-term, whole-of-government approach to foreign technology acquisition and indigenous technology development.



1810-00427-B

Nonstate Actors

We assess that nonstate actors—including hacktivist groups, transnational criminals, and terrorist groups—will attempt to gain access to classified information to support their objectives. They are likely to improve their intelligence capabilities—to include recruiting sources and performing physical and technical surveillance—and they will use human, technical, and cyber means to perform their illicit activities and avoid detection and capture.

EMERGING AND DISRUPTIVE TECHNOLOGIES AND THREATS TO ECONOMIC COMPETITIVENESS

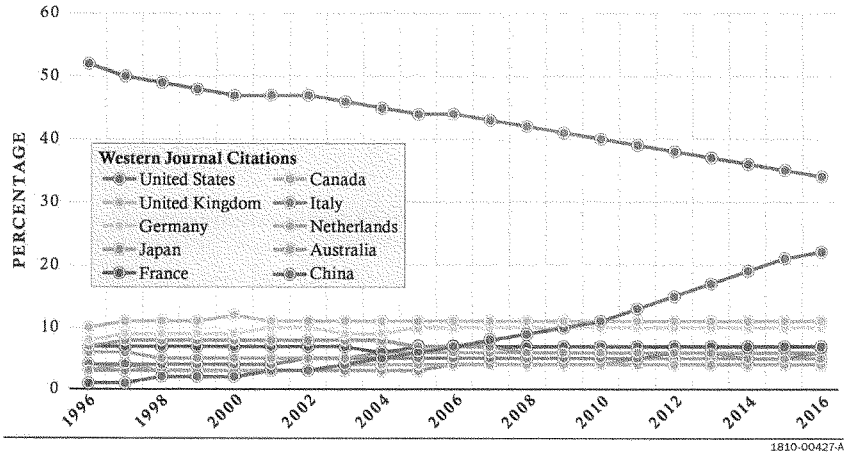
Strategic Outlook

For 2019 and beyond, the innovations that drive military and economic competitiveness will increasingly originate outside the United States, as the overall US lead in science and technology (S&T) shrinks; the capability gap between commercial and military technologies evaporates; and foreign actors increase their efforts to acquire top talent, companies, data, and intellectual property via licit and illicit means. Many foreign leaders, including Chinese President Xi Jinping and Russian President Vladimir Putin, view strong indigenous science and technology capabilities as key to their country's sovereignty, economic outlook, and national power.

Researchers Worldwide Citing More Foreign and Less US Research

During the past two decades, the US lead in S&T fields has been significantly eroded, most predominantly by China, which is well ahead in several areas, according to an analysis of Western journal publications.

However, the United States maintains an overall lead largely because we are at the forefront of the medical sciences, which account for almost a third of S&T publications worldwide.



Artificial Intelligence and Autonomy

The global race to develop artificial intelligence (AI)—systems that imitate aspects of human cognition—is likely to accelerate the development of highly capable, application-specific AI systems with national security implications. As academia, major companies, and large government programs continue to develop and deploy AI capabilities, AI-enhanced systems are likely to be trusted with increasing levels of autonomy and decisionmaking, presenting the world with a host of economic, military, ethical, and

privacy challenges. Furthermore, interactions between multiple advanced AI systems could lead to unexpected outcomes that increase the risk of economic miscalculation or battlefield surprise.

Information and Communications

Foreign production and adoption of advanced communication technologies, such as fifth-generation (5G) wireless networks, most likely will challenge US competitiveness and data security, while advances in quantum computing foreshadow challenges to current methods of protecting data and transactions. US data will increasingly flow across foreign-produced equipment and foreign-controlled networks, raising the risk of foreign access and denial of service. Foreign deployment of a large-scale quantum computer, even 10 or more years in the future, would put sensitive information encrypted with today's most widely used algorithms at greatly increased risk of decryption.

Biotechnology

Rapid advances in biotechnology, including gene editing, synthetic biology, and neuroscience, are likely to present new economic, military, ethical, and regulatory challenges worldwide as governments struggle to keep pace. These technologies hold great promise for advances in precision medicine, agriculture, and manufacturing, but they also introduce risks, such as the potential for adversaries to develop novel biological warfare agents, threaten food security, and enhance or degrade human performance.

Materials and Manufacturing

A global resurgence in materials science and manufacturing technology is likely to enable advanced states to create materials with novel properties and engineer structures not previously possible, while placing high-end manufacturing capabilities within reach of small groups and individuals. These developments are already supplementing or displacing traditional methods in most areas of manufacturing, from complex rocket-engine components to plastic desktop-printed toys, and they are enabling the development of a new generation of engineered materials that combine different materials in complex geometries to alter the overall material properties.

SPACE AND COUNTERSPACE

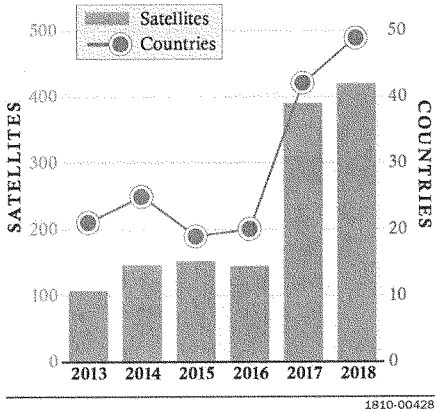
We assess that commercial space services will continue to expand; countries—including US adversaries and strategic competitors—will become more reliant on space services for civil and military needs, and China and Russia will field new counterspace weapons intended to target US and allied space capabilities.

Evolving, Accessible Space Capabilities

We continue to assess that the expansion of the global space industry will further extend space-enabled capabilities and space situational awareness to government, nonstate, and commercial actors in the next several years. All actors will increasingly have access to space-derived information services, such as imagery; weather; communications; and positioning, navigation, and timing (PNT).

- Global access to space services has expanded for civil, commercial, intelligence, and military purposes, in part because of technological innovation, private-sector investment, international partnerships, and demand from emerging markets.

Satellites Launched and Countries Owning the Satellites (2013–18)



Adversary Use of Space

We expect foreign governments will continue efforts to expand their use of space-based reconnaissance, communications, and navigation systems—including by increasing the number of satellites, quality of capabilities, and applications for use. China and Russia are seeking to expand the full spectrum of their space capabilities, as exemplified by China's launch of its highest-resolution imagery satellite, Gaofen-11, in July 2018.

Space Warfare and Counterspace Weapons

We assess that China and Russia are training and equipping their military space forces and fielding new antisatellite (ASAT) weapons to hold US and allied space services at risk, even as they push for international agreements on the nonweaponization of space.

- Both countries recognize the world's growing reliance on space and view the capability to attack space services as a part of their broader efforts to deter an adversary from or defeat one in combat.
- The People's Liberation Army (PLA) has an operational ground-based ASAT missile intended to target low-Earth-orbit satellites, and China probably intends to pursue additional ASAT weapons capable of destroying satellites up to geosynchronous Earth orbit.
- Russia is developing a similar ground-launched ASAT missile system for targeting low-Earth orbit that is likely to be operational within the next several years. It has fielded a ground-based laser weapon, probably intended to blind or damage sensitive space-based optical sensors, such as those used for remote sensing.
- China's and Russia's proposals for international agreements on the nonweaponization of space do not cover multiple issues connected to the ASAT weapons they are developing and deploying, which has allowed them to pursue space warfare capabilities while maintaining the position that space must remain weapons free.

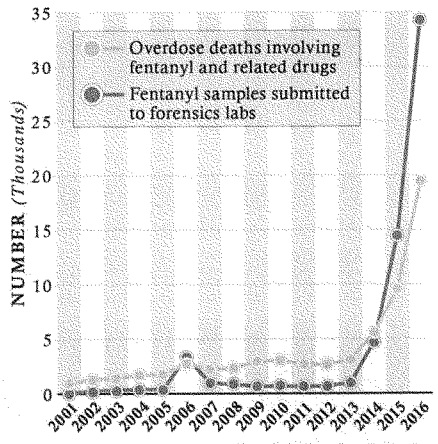
TRANSNATIONAL ORGANIZED CRIME

Global transnational criminal organizations and networks will threaten US interests and allies by trafficking drugs, exerting malign influence in weak states, threatening critical infrastructure, orchestrating human trafficking, and undermining legitimate economic activity.

Drug Trafficking

The foreign drug threat will pose continued risks to US public health and safety and will present a range of threats to US national security interests in the coming year. Violent Mexican traffickers, such as members of the Sinaloa Cartel and New Generation Jalisco Cartel, remain key to the movement of illicit drugs to the United States, including heroin, methamphetamine, fentanyl, and cannabis from Mexico, as well as cocaine from Colombia. Chinese synthetic drug suppliers dominate US-bound movements of so-called designer drugs, including synthetic marijuana, and probably ship the majority of US fentanyl, when adjusted for purity.

US Fentanyl Epidemic, 2001–16



Sources: DEA/NFLIS and CDC/Wonder database

1810-00426-C

- Approximately 70,000 Americans died from drug overdoses in 2017, a record high and a 10-percent increase from 2016, although the rate of growth probably slowed in early 2018, based on Centers for Disease Control (CDC) data.

- Increased drug fatalities are largely a consequence of surging production of the synthetic opioid fentanyl; in 2017, more than 28,000 Americans died from synthetic opioids other than methadone, including illicitly manufactured fentanyl. The CDC reports synthetic opioid-related deaths rose 846 percent between 2010 and 2017, while DHS reports that US seizures of the drug increased 313 percent from 2016 to 2017.

Other Organized Crime Activities

Transnational criminal organizations and their affiliates are likely to expand their influence over some weak states, collaborate with US adversaries, and possibly threaten critical infrastructure.

- Mexican criminals use bribery, intimidation, and violence to protect their drug trafficking, kidnapping-for-ransom, fuel-theft, gunrunning, extortion, and alien-smuggling enterprises.

- Gangs based in Central America, such as MS-13, continue to direct some criminal activities beyond the region, including in the United States.

Transnational organized crime almost certainly will continue to inflict human suffering, deplete natural resources, degrade fragile ecosystems, drive migration, and drain income from the productive—and taxable—economy.

- Human trafficking generates an estimated $150 billion annually for illicit actors and governments that engage in forced labor, according to the UN's International Labor Organization.
- Wildlife poaching and trafficking; illegal, unregulated, unlicensed fishing; illicit mining; timber pilfering; and drug-crop cultivation harm biodiversity, as well as the security of the food supply, water quality and availability, and animal and human health.
- One think tank study estimates that cybercrime, often facilitated by cryptocurrencies, and intellectual property theft resulted in $600 million in losses in 2017; such crimes threaten privacy, harm economic safety, and sap intellectual capital.

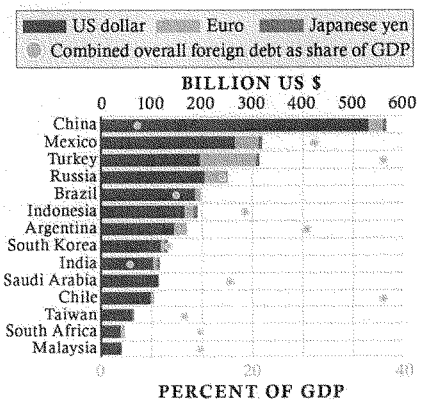
ECONOMICS AND ENERGY

Global growth—projected by the IMF to remain steady in 2019—faces downside risks as global trade tensions persist, many countries contend with high debt levels, and geopolitical tensions continue. Average real growth in advanced economies, operating at close to full capacity, is projected by the IMF to slow in 2019, while emerging markets, key US trading partners, and China's growth face headwinds.

Emerging Markets

Uncertainty about global economic growth will challenge emerging markets—such as Argentina, Brazil, China, Mexico, South Africa, and Turkey—and especially those with weak fundamentals, heavy foreign financing, or close trade linkages with advanced economies. Commodity exporters will remain particularly vulnerable to downward pressure on prices from dampened demand.

Selected Emerging Market Foreign-Denominated Borrowing



Source: Bank for International Settlements

1810-00429

- Since early 2018, investors have pulled capital out of Brazil, India, Indonesia, and Turkey, among others, exacerbating large currency depreciations in those countries and making it more difficult for them to service their US-dollar-denominated debt during the next year.
- Austerity measures imposed by countries to offset budget deficits could prove to be politically difficult to maintain, leading to risks of destabilizing protests, such as occurred in July 2018, when Haiti attempted to comply with an IMF program by reducing fuel subsidies and set off

nationwide protests that forced the Prime Minister and his cabinet to resign. Argentina has agreed to IMF recommendations for austerity, reducing the risk to investors, and Turkey is pursuing its own austerity measures.

Key US Trading Partners

Among major US trading partners the outlook is mixed, with progress being made on US-Canada-Mexico trade discussions but US-China trade frictions and Brexit posing risks to European growth and US-EU trade.

- Mexico and Canada, whose economic prospects are tied closely to the United States-Mexico-Canada Agreement (USMCA), remain concerned about steel and aluminum tariffs and may delay ratifying the USMCA until those concerns are addressed.

- US-EU trade, valued at $1.2 trillion in 2017, would almost certainly suffer disruptions from a no-deal Brexit, which would further dampen UK—and to a lesser extent EU—economic growth. Uncertainty stemming from London's pending exit from the EU is already hurting UK economic growth and the strength of the pound sterling.

- Financial conditions and economic performance generally remain favorable in both Japan and South Korea. However, both countries' economies are dependent on exports, which puts them at continued risk of downward pressure from China's economic slowdown.

China's Economy

China's economic growth is likely to slow in 2019, and a worse-than-expected slowdown could exacerbate trade and budget pressures in emerging-market countries and key commodity exporters, who rely on Chinese demand.

- Since 2017, Beijing has been largely focused on stemming risks in China's financial system, reducing bank credit growth to the lowest rate in a decade, while trying to bolster growth by cutting taxes, calling on banks to lend to private firms, and requiring local governments to plan measures to sustain employment.

- US-China trade tensions had not significantly affected China's total exports as of late 2018, but firms in China have reported a slowdown in new export orders, suggesting China's export sector will suffer in 2019. Some multinational companies are wary of bilateral tensions and have begun to move production to other countries, especially in Southeast Asia, for lower-value-added goods.

Energy and Commodities

Slower economic growth combined with a rising US dollar could lower demand for energy and other commodities, hurting exporters. However, low global spare capacity or a supply disruption might still put upward pressure on oil prices in the coming year, which would further slow overall global economic growth.

- As of December 2018, the US Energy Information Administration forecast that 2019 oil prices would decline 17 percent and 15 percent for West Texas Intermediate and Brent, respectively. Prices for other key commodities declined in 2018. Food prices decreased 6.4 percent in 2018,

and metals prices decreased 11.7 percent, according to the IMF's primary commodities index, reflecting tariffs, sanctions on the Russian company Rusal, and increasing uncertainty about trade policy.

- Production challenges in some oil-exporting countries—notably Libya, Nigeria, and Venezuela—as well as export losses from Iran, would the limit benefits of increased oil prices to those countries. Saudi Arabia, other Persian Gulf oil exporters, and Russia could enjoy increased revenues, but they might also backtrack on the economic reforms they began during periods of lower oil prices.

- In the past year, strong demand for liquefied natural gas (LNG) in China and India, as well as higher oil prices, kept the spot price for LNG close to its highest level in three years, according to the IMF, despite new supplies from the United States and Australia.

HUMAN SECURITY

The United States will probably have to manage the impact of global human security challenges, such as threats to public health, historic levels of human displacement, assaults on religious freedom, and the negative effects of environmental degradation and climate change.

Global Health

We assess that the United States and the world will remain vulnerable to the next flu pandemic or large-scale outbreak of a contagious disease that could lead to massive rates of death and disability, severely affect the world economy, strain international resources, and increase calls on the United States for support. Although the international community has made tenuous improvements to global health security, these gains may be inadequate to address the challenge of what we anticipate will be more frequent outbreaks of infectious diseases because of rapid unplanned urbanization, prolonged humanitarian crises, human incursion into previously unsettled land, expansion of international travel and trade, and regional climate change.

- The ongoing crisis in Venezuela has reversed gains in controlling infectious diseases, such as diphtheria, malaria, measles, and tuberculosis, increasing the risk that these diseases could spread to neighboring countries, particularly Brazil, Colombia, and Trinidad and Tobago. Similarly, the ongoing Ebola outbreak in the Democratic Republic of the Congo—the country's largest ever—underscores the risks posed by the nexus of infectious disease outbreaks, violent conflict, and high population density, including large numbers of internally displaced person (IDPs).

- In the past two years, progress against malaria has halted after more than 15 years of steady reductions, in part because mosquitos and the pathogen have developed a resistance to insecticides and to antimalarial drugs, respectively, while global funding to combat the disease has plateaued.

- The growing proximity of humans and animals has increased the risk of disease transmission. The number of outbreaks has increased in part because pathogens originally found in animals have spread to human populations.

Displacement Hotspots Increase Risk of Infectious Disease Outbreaks

Countries with high internal and regional displacement due to conflict or political instability are at an increased risk for the spread of infectious diseases such as measles, cholera, diphtheria, and Ebola. Highlighted below are some key displacement hotspots and regions at risk.



1810-00430-A

Human Displacement

Global displacement almost certainly will remain near record highs, and host countries are unlikely to see many refugees or internally displaced persons return home, increasing humanitarian needs and the risk of political upheaval, health crises, and recruitment and radicalization by militant groups. The number of people becoming displaced within their own national borders continues to increase, according to the United Nations, placing fiscal and political strain on governments' ability to care for their domestic populations and mitigate local discontent.

Religious Freedom

Violations of religious freedom by governments and nonstate actors—particularly in the Middle East, China, and North Korea—will fuel the growth of violent extremist groups and lead to societal tensions, protests, or political turmoil.

- According to the Pew Research Center's global indexes, the average score for government restrictions on religion rose 39 percent from 2007 to 2016, and the number of states with high or very high government restrictions grew from 40 to 55.

- Since 2017, Chinese authorities have detained hundreds of thousands and possibly millions of Turkic Muslim Uighurs in extrajudicial detainment centers. Beijing has also reached beyond its borders to pursue this campaign, including by pressuring ethnic Uighurs overseas, some of whom are American citizens, to return to China so it can more easily control them. Chinese security services have contacted Uighurs abroad and coerced them to act as informants by threatening to keep Xinjiang-based family members in detention.

Environment and Climate Change

Global environmental and ecological degradation, as well as climate change, are likely to fuel competition for resources, economic distress, and social discontent through 2019 and beyond. Climate hazards such as extreme weather, higher temperatures, droughts, floods, wildfires, storms, sea level rise, soil degradation, and acidifying oceans are intensifying, threatening infrastructure, health, and water and food security. Irreversible damage to ecosystems and habitats will undermine the economic benefits they provide, worsened by air, soil, water, and marine pollution.

- Extreme weather events, many worsened by accelerating sea level rise, will particularly affect urban coastal areas in South Asia, Southeast Asia, and the Western Hemisphere. Damage to communication, energy, and transportation infrastructure could affect low-lying military bases, inflict economic costs, and cause human displacement and loss of life.

- Changes in the frequency and variability of heat waves, droughts, and floods—combined with poor governance practices—are increasing water and food insecurity around the world, increasing the risk of social unrest, migration, and interstate tension in countries such as Egypt, Ethiopia, Iraq, and Jordan.

- Diminishing Arctic sea ice may increase competition—particularly with Russia and China—over access to sea routes and natural resources. Nonetheless, Arctic states have maintained mostly positive cooperation in the region through the Arctic Council and other multilateral mechanisms, a trend we do not expect to change in the near term. Warmer temperatures and diminishing sea ice are reducing the high cost and risks of some commercial activities and are attracting new players to the resource-rich region. In 2018, the minimum sea ice extent in the Arctic was 25 percent below the 30-year average from 1980 to 2010.

34

REGIONAL THREATS

CHINA AND RUSSIA

China and Russia will present a wide variety of economic, political, counterintelligence, military, and diplomatic challenges to the United States and its allies. We anticipate that they will collaborate to counter US objectives, taking advantage of rising doubts in some places about the liberal democratic model.

Chinese-Russian Relations

China and Russia are expanding cooperation with each other and through international bodies to shape global rules and standards to their benefit and present a counterweight to the United States and other Western countries.

- The two countries have significantly expanded their cooperation, especially in the energy, military, and technology spheres, since 2014.
- China has become the second-largest contributor to the UN peacekeeping budget and the third-largest contributor to the UN regular budget. It is successfully lobbying for its nationals to obtain senior posts in the UN Secretariat and associated organizations, and it is using its influence to press the UN and member states to acquiesce in China's preferences on issues such as human rights and Taiwan.
- Russia is working to consolidate the UN's counterterrorism structures under the UN Under Secretary General for Counterterrorism, who is Russian.
- Both countries probably will use the UN as a platform to emphasize sovereignty narratives that reflect their interests and redirect discussions away from human rights, democracy, and good governance.
- China and Russia also have increased their sway in the International Telecommunication Union through key leadership appointments and financial and technical assistance. They seek to use the organization to gain advantage for their national industries and move toward more state-controlled Internet governance.

EAST ASIA

The United States will see mounting threats in Asia, including a variety of challenges from China and North Korea, and rising authoritarianism in the region.

China

The Chinese Communist Party's Concentration of Power

China is deepening its authoritarian turn under President Xi Jinping, and the resulting hardening of Chinese politics and governance probably will make it more difficult for the leadership to recognize and correct policy errors, including in relations with the United States and our allies and partners.

- President Xi removed one of the few remaining checks on his authority when he eliminated presidential term limits in March 2018, and the Chinese Communist Party has reasserted control over the economy and society, tightened legal and media controls, marginalized independent voices, and intensified repression of Chinese Muslims, Christians, and other religious minorities.

- The Chinese Government also is harnessing technology, including facial recognition, biometrics, and vehicle GPS tracking, to bolster its apparatus of domestic monitoring and control.

- Beijing's increasing restrictions on scholars' and researchers' freedom of movement and communication with US counterparts may increase the prospects for misunderstanding and misinterpretation of US policies.

Expanding Global Reach

We assess that China's leaders will try to extend the country's global economic, political, and military reach while using China's military capabilities and overseas infrastructure and energy investments under the Belt and Road Initiative to diminish US influence. However, Beijing is likely to face political pushback from host governments in many locations, and the overall threat to US and partner interests will depend on the size, locations, and offensive military capabilities of the eventual Chinese presence.

- China has built its first overseas military facility in Djibouti and probably is exploring bases, support facilities, or access agreements in Africa, Europe, Oceania, Southeast Asia, and South Asia.

- In most instances, China has not secured explicit permanent basing rights but is using commercial development and military ties to lay the groundwork for gaining future military access.

- Successful implementation of the Belt and Road Initiative could facilitate PLA access to dozens of additional ports and airports and significantly expand China's penetration of the economies and political systems of participating countries.

The Coming Ideological Battle

Chinese leaders will increasingly seek to assert China's model of authoritarian capitalism as an alternative—and implicitly superior—development path abroad, exacerbating great-power competition that could threaten international support for democracy, human rights, and the rule of law.

- The actions of Xi and his advisers—doubling down on authoritarianism at home and showing they are comfortable with authoritarian regimes abroad—along with China's opaque commercial and development practices, reward compliant foreign leaders and can be corrosive to civil society and the rule of law.

- At the 2018 Central Foreign Affairs Work Conference, Xi stated his desire to lead the reform of the global governance system, driving a period of increased Chinese foreign policy activism and a Chinese worldview that links China's domestic vision to its international vision.

- Beijing has stepped up efforts to reshape the international discourse around human rights, especially within the UN system. Beijing has sought not only to block criticism of its own system but also to erode norms, such as the notion that the international community has a legitimate role in scrutinizing other countries' behavior on human rights (e.g., initiatives to proscribe country-specific resolutions), and to advance narrow definitions of human rights based on economic standards.

South China Sea and Taiwan

We assess that China will continue increasing its maritime presence in the South China Sea and building military and dual-use infrastructure in the Spratly Islands to improve its ability to control access, project power, and undermine US influence in the area. A body of open-source reporting shows that China seeks to achieve effective control over its claimed waters with a whole-of-government strategy, compel Southeast Asian claimants to acquiesce in China's claims—at least tacitly—and bolster Beijing's narrative in the region that the United States is in decline and China's preeminence is inevitable.

- Meanwhile, Beijing almost certainly will continue using pressure and incentives to try to force Taipei to accept the One China framework and ultimately Chinese control, and it will monitor the US reaction as an indicator of US resolve in the region.

- Since 2016, Beijing has persuaded six of Taiwan's 23 diplomatic partners, most recently Burkina Faso and El Salvador, to recognize China instead of Taiwan.

Military Capabilities

The People's Liberation Army (PLA) continues to develop and field advanced weapons and hardware while honing its ability to fight in all military domains. The force is undergoing its most comprehensive restructuring ever to realize China's long-held goal of being able to conduct modern, rapid military operations based on high technology to assert and defend China's regional and growing global interests.

- PLA reforms seek to reinforce the Chinese Communist Party's control of the military, improve the PLA's ability to perform joint operations, increase combat effectiveness, and curb corruption.

- As China's global footprint and international interests have grown, its military modernization program has become more focused on investments and infrastructure to support a range of missions beyond China's periphery, including a growing emphasis on the maritime domains, offensive air operations, and long-distance mobility operations.

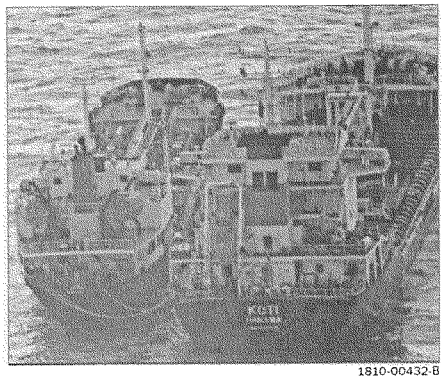
North Korea

Nuclear Ambitions

Pyongyang has not conducted any nuclear-capable missile or nuclear tests in more than a year, has declared its support for the denuclearization of the Korean Peninsula, and has reversibly dismantled portions of its WMD infrastructure. However, ***we continue to assess that North Korea is unlikely to give up all of its nuclear weapons and production capabilities, even as it seeks to negotiate partial denuclearization steps to obtain key US and international concessions.*** North Korean leaders view nuclear arms as critical to regime survival, according to official statements and regime-controlled media.

North Korea Conducting Ship-to-Ship Transfers

This image is of the Koti, a Panamanian-flagged vessel seized by South Korea in December 2017 for illicitly transferring refined petroleum to North Korean vessels. North Korea is using ship-to-ship transfers to circumvent UN sanctions that were designed to bring pressure on Pyongyang to give up its nuclear and WMD programs.



1810-00432-B

- In his 2019 New Year's address, North Korean President Kim Jong Un pledged that North Korea would "go toward" complete denuclearization and promised not to make, test, use, or proliferate nuclear weapons. However, he conditioned progress on US "practical actions." The regime tied the idea of denuclearization in the past to changes in diplomatic ties, economic sanctions, and military activities.
- In Singapore in June 2018, Kim said he sought the "complete denuclearization of the Korean Peninsula"—a formulation linked to past demands that include an end to US military deployments and exercises involving advanced US capabilities.
- We continue to observe activity inconsistent with full denuclearization. North Korea has underscored its commitment to nuclear arms for years, including through an order to mass-produce weapons in 2018 and an earlier law—and constitutional change—that affirmed the country's nuclear status.

Foreign Engagement

North Korea will continue its efforts to mitigate the effects of the US-led pressure campaign, most notably through diplomatic engagement, counterpressure against the sanctions regime, and direct sanctions evasion.

- Kim Jong Un has sought sanctions relief through a campaign of diplomatic engagement that included his first summits with foreign leaders since taking power in 2011. He met with South Korean President Moon Jae-in three times in 2018, leading to agreements to reconnect roads

and rail lines, establish new military parameters, promote reforestation, and facilitate cultural exchanges.

- Kim has also sought to align the region against the US-led pressure campaign in order to gain incremental sanctions relief, and North Korean statements have repeatedly indicated that some sanctions relief is necessary for additional diplomacy to occur. In his annual New Year's address, Kim linked US sanctions to diplomatic progress and threatened to resume nuclear and missile testing.

Sanctions Evasion

We assess that sanctions continue to pressure the North Korean regime, despite North Korean sanctions evasion efforts. By late 2018, the enforcement of new UN sanctions had led to a precipitous decline in North Korea's monthly export revenue compared with 2017, a change that also reduced imports.

- North Korea generates revenue through overseas labor, cyber-theft operations, and illicit commercial exports of UN Security Council-prohibited goods.

- Throughout 2018, the United States and its allies observed North Korean maritime vessels using at-sea, ship-to-ship transfers of petroleum from third-country tankers to acquire additional refined petroleum as a way to mitigate the effects of UNSC sanctions.

Conventional Military Capabilities

North Korea's conventional capabilities continue to pose a threat to South Korea, Japan, and US forces in the region. As a way to offset adversary military advantages, Kim Jong Un continues to pursue advanced conventional weapon programs and capabilities, including more accurate artillery and ballistic missile strike capabilities and UAVs.

Southeast Asia and the Pacific

We expect democracy and civil liberties in many Southeast Asian countries to remain fragile and China to increase its engagement in the region to build its influence while diminishing the influence of the United States and US allies. Russia may also continue its diplomatic and military cultivation of Southeast Asian partners, and some countries will be receptive to Moscow as a balance against China's push for hegemony.

- In the wake of Washington's withdrawal from the Trans-Pacific Partnership, China is promoting a unified stance with the Association of Southeast Asian Nations (ASEAN) in defense of multilateralism and the WTO reform process, while also fostering a shared perception of US freedom of navigation operations through Chinese-claimed waters in the South China Sea as threats to regional stability.

- China is currying favor with numerous Pacific Island nations through bribery, infrastructure investments, and diplomatic engagement with local leaders while intervening in Burma—including by shielding Burma from UNSC sanctions in response to the humanitarian crisis and alleged ethnic cleansing in Rakhine State.

- Russia, too, has been increasing its diplomatic and military cultivation of Southeast Asian partners, some of which have been receptive to Moscow as a power capable of diluting China's nascent hegemony and helping them diversify their hedging options.

- Cambodia's slide toward autocracy, which culminated in the Cambodian People's Party's retention of power and complete dominance of the national legislature, opens the way for a constitutional amendment that could lead to a Chinese military presence in the country. Thailand's coup-installed regime has promised elections in 2019 but appears set to help ensure that its proxy party retains power by tightly controlling the political space ahead of the vote. Burma's civilian authorities continue to make scant progress toward resolving the crisis in Rakhine State, advancing economic reforms, or ending longstanding insurgencies by ethnic minority groups.

MIDDLE EAST AND NORTH AFRICA

Political turmoil, economic fragility, and civil and proxy wars are likely to characterize the Middle East and North Africa in the coming year, as the region undergoes a realignment of the balance of regional power, wealth and resource management, and the relationships among governments, nonstate political groups, and wider populations.

Iran

Iran's regional ambitions and improved military capabilities almost certainly will threaten US interests in the coming year, driven by Tehran's perception of increasing US, Saudi, and Israeli hostility, as well as continuing border insecurity, and the influence of hardliners.

Iran's Objectives in Iraq, Syria, and Yemen

We assess that Iran will attempt to translate battlefield gains in Iraq and Syria into long-term political, security, social, and economic influence while continuing to press Saudi Arabia and the UAE by supporting the Huthis in Yemen.

In Iraq, Iran-supported Popular Mobilization Committee-affiliated Shia militias remain the primary threat to US personnel, and we expect that threat to increase as the threat ISIS poses to the militias recedes, Iraqi Government formation concludes, some Iran-backed groups call for the United States to withdraw, and tension between Iran and the United States grows. We continue to watch for signs that the regime might direct its proxies and partners in Iraq to attack US interests.

Iran's efforts to consolidate its influence in Syria and arm Hizballah have prompted Israeli airstrikes as recently as January 2019 against Iranian positions within Syria and underscore our growing concern about the long-term trajectory of Iranian influence in the region and the risk that conflict will escalate.

- Iran's retaliatory missile and UAV strikes on ISIS targets in Syria following the attack on an Iranian military parade in Ahvaz in September were most likely intended to send a message to potential adversaries, showing Tehran's resolve to retaliate when attacked and demonstrating Iran's improving military capabilities and ability to project force.

- Iran continues to pursue permanent military bases and economic deals in Syria and probably wants to maintain a network of Shia foreign fighters there despite Israeli attacks on Iranian

positions in Syria. We assess that Iran seeks to avoid a major armed conflict with Israel. However, Israeli strikes that result in Iranian casualties increase the likelihood of Iranian conventional retaliation against Israel, judging from Syrian-based Iranian forces' firing of rockets into the Golan Heights in May 2018 following an Israeli attack the previous month on Iranians at Tiyas Airbase in Syria.

In Yemen, Iran's support to the Huthis, including supplying ballistic missiles, risks escalating the conflict and poses a serious threat to US partners and interests in the region. Iran continues to provide support that enables Huthi attacks against shipping near the Bab el Mandeb Strait and land-based targets deep inside Saudi Arabia and the UAE, using ballistic missiles and UAVs.

Domestic Politics

Regime hardliners will be more emboldened to challenge rival centrists by undermining their domestic reform efforts and pushing a more confrontational posture toward the United States and its allies. Centrist President Hasan Ruhani has garnered praise from hardliners with his more hostile posture toward Washington but will still struggle to address ongoing popular discontent.

Nationwide protests, mostly focused on economic grievances, have continued to draw attention to the need for major economic reforms and unmet expectations for most Iranians. We expect more unrest in the months ahead, although the protests are likely to remain uncoordinated and lacking central leadership or broad support from major ethnic and political groups. We assess that Tehran is prepared to take more aggressive security measures in response to renewed unrest while preferring to use nonlethal force.

- Ruhani's ability to reform the economy remains limited, given pervasive corruption, a weak banking sector, and a business climate that discourages foreign investment and trade.

Military Modernization and Behavior

Iran will continue to develop military capabilities that threaten US forces and US allies in the region. It also may increase harassment of US and allied warships and merchant vessels in the Persian Gulf, Strait of Hormuz, and Gulf of Oman.

- Iran continues to develop, improve, and field a range of military capabilities that enable it to target US and allied military assets in the region and disrupt traffic through the Strait of Hormuz. These systems include ballistic missiles, unmanned explosive boats, naval mines, submarines and advanced torpedoes, armed and attack UAVs, antiship and land-attack cruise missiles, antiship ballistic missiles, and air defenses. Iran has the largest ballistic missile force in the Middle East and can strike targets as far as 2,000 kilometers from Iran's borders. Russia's delivery of the SA-20c SAM system in 2016 provided Iran with its most advanced long-range air defense system. Iran is also domestically producing medium-range SAM systems and developing a long-range SAM.

- In September 2018, Iran struck Kurdish groups in Iraq and ISIS in Syria with ballistic missiles in response to attacks inside Iran, demonstrating the increasing precision of Iran's missiles, as well as Iran's ability to use UAVs in conjunction with ballistic missiles.

- We assess that unprofessional interactions conducted by the Iranian Islamic Revolutionary Guards Corps (IRGC) Navy against US ships in the Persian Gulf, which have been less frequent during the past year, could resume should Iran seek to project an image of strength in response to US pressure. Most IRGC interactions with US ships are professional, but in recent years the IRGC Navy has challenged US ships in the Persian Gulf and flown UAVs close to US aircraft carriers during flight operations. Moreover, Iranian leaders since July have threatened to close the Strait of Hormuz in response to US sanctions targeting Iranian oil exports.

Saudi Arabia

Saudi Crown Prince Muhammad bin Salman continues to control the key levers of power in Saudi Arabia, but his simultaneous push for economic and social reform creates potential flashpoints for internal opposition. Saudi public support for the royal family appears to remain high, even in the wake of the murder of journalist Jamal Khashoggi. Moreover, we assess that the Saudi Government remains well positioned to stifle small-scale protests and discontent; it has preemptively arrested or forcibly detained clerics, business leaders, and civil society activists who could be nodes for discontent.

The Kingdom will seek to make progress on its Vision 2030 plan of structural reforms, spearheaded by Crown Prince Muhammad bin Salman and aimed at reducing dependence on oil revenues. The plan's initiatives include reducing subsidies, building a robust private sector, and instituting taxes, all of which upend the longstanding social contract. Some of these reforms have aggravated segments of the Saudi public, including government workers religious conservatives.

Iraq

Iraq is facing an increasingly disenchanted public. The underlying political and economic factors that facilitated the rise of ISIS persist, and Iraqi Shia militias' attempts to further entrench their role in the state increase the threat to US personnel.

- The Iraqi Government will confront a high level of societal discontent, institutional weakness, and deep-seated divisions, as well as protests over a lack of services, high unemployment, and political corruption. Baghdad lacks the resources or institutional capacity to address longstanding economic development and basic services challenges, and it faces reconstruction costs in the aftermath of the counter-ISIS campaign, estimated by the World Bank at $88 billion. Iraq's Kurdistan region is still dealing with political discontent over economic and territorial losses to Baghdad last year.

- ISIS remains a terrorist and insurgent threat and will seek to exploit Sunni grievances with Baghdad and societal instability to eventually regain Iraqi territory against Iraqi security forces that are stretched thin.

Iraqi Shia militants conducted several attacks against US diplomatic facilities in Iraq in September and December 2018. Militias—some of which are also part of the Iraqi Government Popular Mobilization Committee—plan to use newfound political power gained through positions in the new government to reduce or remove the US military presence while competing with the Iraqi security forces for state resources.

Syria

As the Syrian regime consolidates control, the country is likely to experience continued violence. We expect the regime to focus on taking control of the remaining rebel-held territory and reestablishing control of eastern Syria, consolidating gains, rebuilding regime-loyal areas, and increasing its diplomatic ties through 2019 while seeking to avoid conflicts with Israel and Turkey. Russia and Iran probably will attempt to further entrench themselves in Syria.

- The regime's momentum, combined with continued support from Russia and Iran, almost certainly has given Syrian President Bashar al-Asad little incentive to make anything more than token concessions to the opposition or to adhere to UN resolutions on constitutional changes that Asad perceives would hurt his regime.

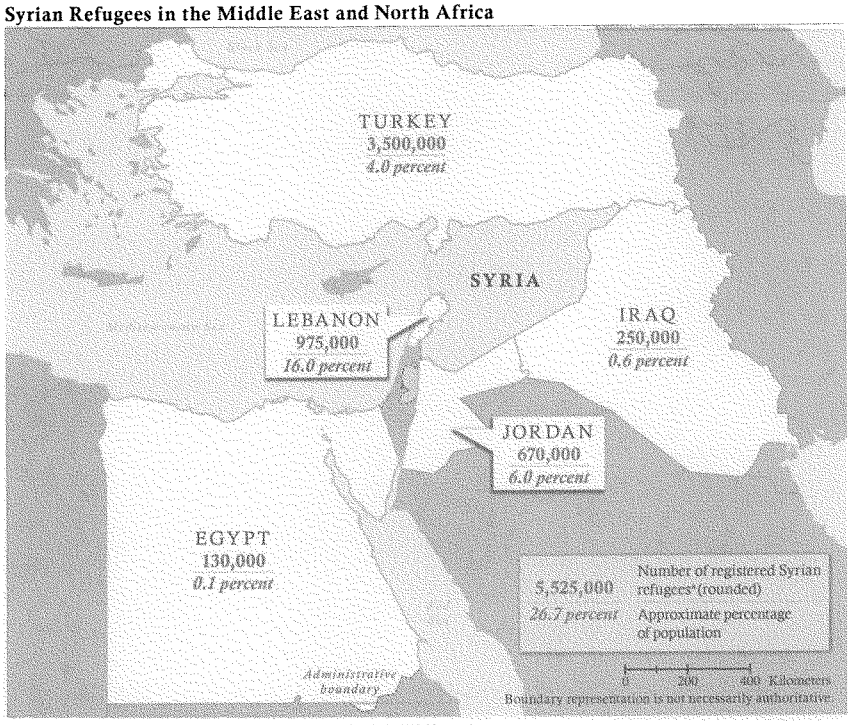
- Opposition groups, which rely on Turkey for continued support, probably are not capable of repelling a regime military operation to retake Idlib Province but may retain enough resources to foment a low-level insurgency in areas the regime recaptures in the coming year.

- The regime probably will focus increasingly on reasserting control over Kurdish-held areas. Damascus probably will seek to exploit any security vacuum and Turkish pressure on the Kurds in order to strike a favorable deal with the Kurds while also seeking to limit Turkey's presence and influence in Syria and reclaim territory in northwestern Syria held by Turkey.

- The regime is unlikely to immediately focus on clearing ISIS from remote areas that do not threaten key military, economic, and transportation infrastructure, judging from previous regime counter-ISIS efforts.

- Damage to the Syrian economy and its infrastructure has reached almost $400 billion, according to UN estimates, and reconstruction could take at least a decade to complete. The effects of the Syrian civil war will continue to be felt by its neighbors, with approximately 5.6 million Syrian refugees registered in neighboring countries as of October 2018. Russia and Iran will try to secure rights to postwar contracts to rebuild Syria's battered infrastructure and industry in exchange for sustained military and economic support.

Syrian Refugees in the Middle East and North Africa



a. The number of refugees for each country is the number registered with the U.N. National governments often report higher estimates for the number of Syrian refugees they host.

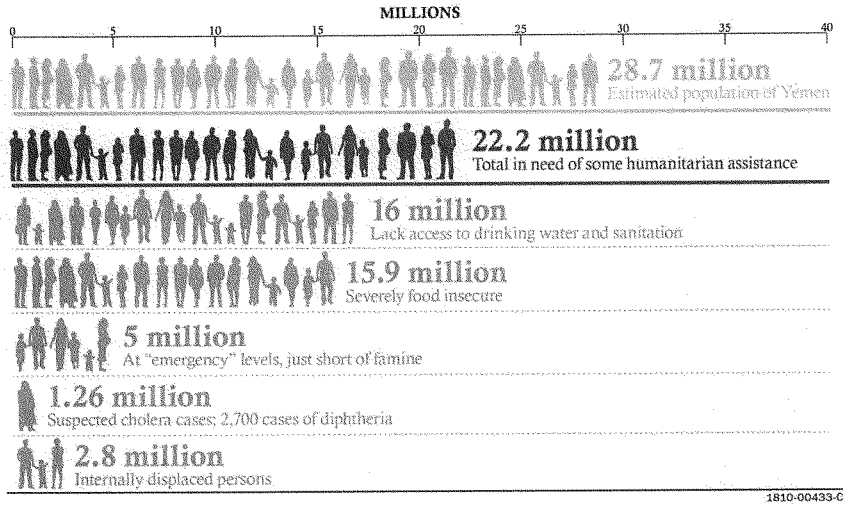
1810-00433-B-U

Yemen

The Huthi movement in Yemen and the Saudi-led coalition, which supports the Yemeni Government, remain far apart in negotiating an end to the conflict, and neither side seems prepared for the kind of compromise needed to end the fighting, suggesting the humanitarian crisis will continue. The coalition, buoyed by military gains in the past year, seems fixed on a Huthi withdrawal from Sanaa and significant Huthi disarmament. These terms remain unacceptable to the Huthis, who believe they can use external attacks to threaten Saudi Arabia and the UAE, undercut Saudi and UAE public support for the conflict, and draw international condemnation of the coalition's intervention in Yemen.

- The humanitarian impacts of the conflict in Yemen—including, famine, disease, and internal displacement—will be acute in 2019 and could easily worsen if the coalition cuts key supply lines to Sanaa. The fighting has left more than 22 million people, or approximately 75 percent of the population, in need of assistance, with millions of people at severe risk of famine by the UN definition—numbers that are likely to rise quickly if disruptions to aid access continue.

Yemen Humanitarian Figures as of 3 December 2018



Libya

Libya is poised to remain unstable into 2019, with poor prospects for reconciliation between competing factions and ongoing threats from ISIS-Libya. Militias aligned with Libya's key political factions fight intermittently for influence and control of resources, resulting in a high-risk security environment that threatens both rival governments and Western interests. The UN-backed, Tripoli-based Government of National Accord (GNA) and eastern-based House of Representatives (House) remain unable to agree on key posts and government structure. ISIS-Libya's capabilities have been degraded, but it is still capable of conducting attacks on local and Western targets in Libya and possibly elsewhere in the region.

SOUTH ASIA

The challenges facing South Asian states will grow in 2019 because of Afghanistan's presidential election in mid-July and the Taliban's large-scale attacks, Pakistan's recalcitrance in dealing with militant groups, and Indian elections that risk communal violence.

Afghanistan Stalemate

We assess that neither the Afghan Government nor the Taliban will be able to gain a strategic military advantage in the Afghan war in the coming year if coalition support remains at current levels. Afghan forces generally have secured cities and other government strongholds, but the Taliban has increased large-scale attacks, and Afghan security suffers from a large number of forces being tied down in defensive missions, mobility shortfalls, and a lack of reliable forces to hold recaptured territory.

Pakistan Recalcitrance

Militant groups supported by Pakistan will continue to take advantage of their safe haven in Pakistan to plan and conduct attacks in India and Afghanistan, including against US interests. Islamabad's narrow approach to counterterrorism cooperation—using some groups as policy tools and confronting only the militant groups that directly threaten Pakistan—almost certainly will frustrate US counterterrorism efforts against the Taliban.

Indian Elections and Ethnic Tensions

Parliamentary elections in India increase the possibility of communal violence if Indian Prime Minister Narendra Modi's Bharatiya Janata Party (BJP) stresses Hindu nationalist themes. BJP policies during Modi's first term have deepened communal tensions in some BJP-governed states, and Hindu nationalist state leaders might view a Hindu-nationalist campaign as a signal to incite low-level violence to animate their supporters. Increasing communal clashes could alienate Indian Muslims and allow Islamist terrorist groups in India to expand their influence.

India-Pakistan Tensions

We judge that cross-border terrorism, firing across the Line of Control (LoC), divisive national elections in India, and Islamabad's perception of its position with the United States relative to India will contribute to strained India-Pakistan relations at least through May 2019, the deadline for the Indian election, and probably beyond. Despite limited confidence-building measures—such as both countries recommitting in May 2018 to the 2003 cease-fire along the disputed Kashmir border—continued terrorist attacks and cross-border firing in Kashmir have hardened each country's position and reduced their political will to seek rapprochement. Political maneuvering resulting from the Indian national elections probably will further constrain near-term opportunities for improving ties.

India-China Tensions

We expect relations between India and China to remain tense, despite efforts on both sides to manage tensions since the border standoff in 2017, elevating the risk of unintentional escalation. Chinese President Xi Jinping and Indian Prime Minister Narendra Modi held an informal summit in April 2018 to defuse tension and normalize relations, but they did not address border issues. Misperceptions of military movements or construction might result in tensions escalating into armed conflict.

RUSSIA AND EURASIA

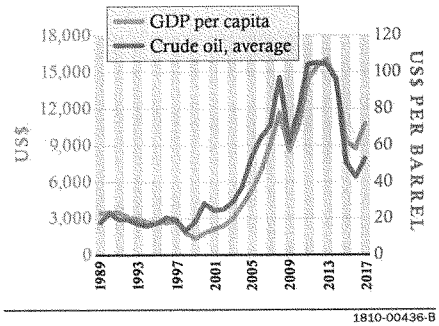
Russian President Vladimir Putin has the tools to navigate challenges to his rule, and he is likely to sustain an assertive, opportunistic foreign policy to advance Russia's interests beyond its borders and contest US influence.

Russia's Domestic Politics

The Russian economy's slow growth and most Russians' disapproval of government officials' performance will foster a more challenging political environment for the Kremlin, although its centralized power structure and the resonance of anti-American themes will buoy Putin, sustaining his push for international stature and challenging US global leadership.

We assess that slow growth and depressed wages are eroding the higher living standards that many Russians once saw as Putin's greatest accomplishment, and corruption is a major issue that Putin cannot attack because his political system rests on it. Following his support for an unpopular pension reform in 2018, Putin's public approval fell to levels not seen since before Russia's illegal annexation of Crimea in 2014. Nevertheless, the Kremlin can rely on its traditional instruments of persuasion to navigate challenges to Putin's control—including the media and the distribution of financial benefits—and it can turn to its security services to impede protests, crack down on the opposition, and intimidate elites.

Russian Economic Performance Highly Dependent on Oil Prices



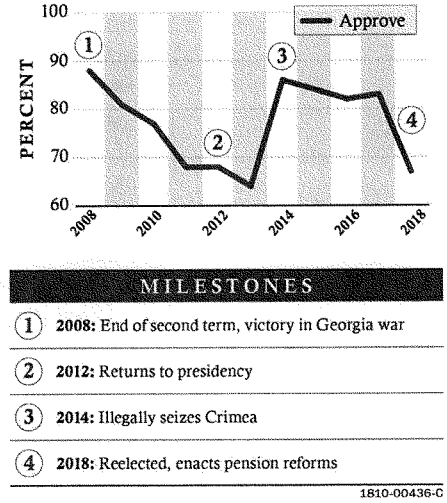
Although we judge that Putin and other elites would like to see cooperation with the United States where US and Russian interests overlap, they view publicly blaming the United States for internal challenges as good politics. Moscow believes it can weather the impact of sanctions, and we expect Putin to remain active on the international stage because the public narrative that he has restored Russia's great-power status remains a pillar of his domestic support.

Global Ambitions

Russia's efforts to expand its global military, commercial, and energy footprint and build partnerships with US allies and adversaries alike are likely to pose increasing challenges. Moscow will continue to emphasize its strategic relationship with Beijing, while also pursuing a higher profile in the Middle East, Southeast Asia, Africa, and Latin America.

We assess that Moscow will continue pursuing a range of objectives to expand its reach, including undermining the US-led liberal international order, dividing Western political and security institutions, demonstrating Russia's ability to shape global issues, and bolstering Putin's domestic legitimacy. Russia seeks to capitalize on perceptions of US retrenchment and power vacuums, which it views the United States is unwilling or unable to fill, by pursuing relatively low-cost options, including influence campaigns, cyber tools, and limited military interventions.

Putin's Popularity Slides Following Short, Victorious Wars and Reelection



- We assess that Moscow has heightened confidence, based on its success in helping restore the Asad regime's territorial control in Syria, but translating what have largely been military wins into a workable settlement in Syria will be one of Moscow's key challenges in the years ahead.

- Russia seeks to boost its military presence and political influence in the Mediterranean and Red Seas, increase its arms sales, expand information operations in Europe, and mediate conflicts, including engaging in the Middle East Peace Process and Afghanistan reconciliation.

Military Capabilities

Moscow views military force as key to safeguarding its vital interests and supporting its foreign policy; it is becoming more modernized and capable across all military domains and maintains the world's largest operational nuclear stockpile.

- After decades of increased spending to support modernization, Russia's defense budget is decreasing to about 3.8 percent of GDP in 2019, from a peak of about 5.4 percent in 2016. Because of momentum in military acquisitions, we judge that the budget is normalizing to pre-peak spending levels.

- In 2019, we assess that Russia will continue to modernize the entire military but particularly will make progress in its air defense, submarine, and electronic warfare capabilities.

Russia and Its Neighbors

The Kremlin will seek to maintain and, where possible, expand its influence throughout the former Soviet Union countries, which it asserts are within its sphere of influence.

We assess that a major offensive by either Ukraine or Russian proxy forces is operationally feasible but unlikely in 2019, unless one side perceives the other is seriously challenging the status quo. Bilateral tensions will continue to rise in the Black and Azov Seas as each side asserts its sovereignty and naval capabilities. Russia will continue its military, political, and economic destabilization campaign against Ukraine to try to stymie Kyiv's efforts to integrate with the EU and strengthen ties to NATO. Russia's interception of Ukrainian ships in the Kerch Strait and detention of the ships' sailors in November 2018 demonstrates Russia's willingness to limit Ukrainian freedom of navigation in the area and exert political pressure on the country's leadership, particularly in advance of Ukraine's elections this year.

- Ukraine will hold a presidential election in March 2019 and legislative elections in the fall. The large field of presidential candidates, high levels of distrust in political elites, and lack of a clear frontrunner may provide Ukrainian President Petro Poroshenko's rivals, as well as lesser known candidates and political newcomers, an opportunity to appeal to the largely undecided Ukrainian electorate.

- Russia is taking steps to influence these elections, applying a range of tools to exert influence and exploit Kyiv's fragile economy, widespread corruption, cyber vulnerabilities, and public discontent in hopes of ousting Poroshenko and bringing to power a less anti-Russia parliament.

The ruling coalition of Moldova, Ukaraine's neighbor, is focused on maintaining power in the legislative election planned for February 2019 and probably will seek to limit Russian influence and preserve a veneer of commitment to EU integration.

Tension between Armenia and Azerbaijan over the Nagorno-Karabakh region remains a potential source for a large-scale military conflict that might draw in Russia.

Russia will continue pressing Central Asia's leaders to support Russian-led economic and security initiatives and reduce engagement with Washington. At the same time, China probably will continue to expand its outreach to Central Asia, largely to promote economic initiatives because of Beijing's concern that regional instability could undermine China's economic interests and create a permissive environment for extremists. Uzbekistan's political opening under President Shavkat Mirziyoyev will improve prospects for intraregional cooperation, but poor governance and vulnerable economics will raise the risk of radicalization.

EUROPE

The United Kingdom's scheduled exit from the EU on 29 March 2019, European Parliament elections in late May, and the subsequent turnover in EU institutional leadership will limit the ability of EU and

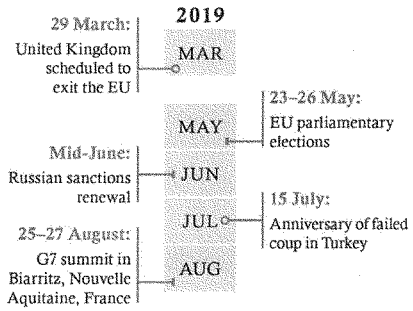
national leaders to contend with increased Russian and Chinese efforts to divide them from one another and from the United States.

- If the United Kingdom's exit from the EU takes place as scheduled, it would remove one of the institution's key voices for strong sanctions policy toward Russia and market liberalism, as well as one of its most capable foreign and security policy actors.
- Russia and China are likely to intensify efforts to build influence in Europe at the expense of US interests, benefiting from the economic fragility of some countries, transatlantic disagreements, and a probable strong showing by anti-establishment parties in the European Parliament elections in late May 2019. Some member states favor a softening of Russian sanctions and probably will resist efforts to tighten investment screening.

Turkey

Turkey's regional ambitions, a distrust of the United States, and the growing authoritarianism of Turkey's leaders are complicating bilateral relations and making Ankara more willing to challenge US regional goals. Turkey will continue to view as existential threats the Kurdistan Workers' Party (PKK), including its People's Protection Units (YPG) militia in Syria, and the movement led by Fethullah Gulen (USPER), a former AKP ally who Turkish leaders claim is responsible for the failed coup of 2016.

Key Events in Europe During 2019



1810-00437

Balkans

The Western Balkans almost certainly will remain at some risk of low-level violence and possibly open military conflict throughout 2019. Russia will seek to exploit ethnic tensions and high levels of corruption to hinder the ability of countries in this region to move toward the EU and NATO.

AFRICA

Several countries and regions in Sub-Saharan Africa are likely to face significant security, counterterrorism, democratization, economic, and humanitarian challenges. Recent political unrest in countries such as Zimbabwe and Sudan highlight the ongoing challenges facing many governments across the continent. African countries' outreach and cooperation with external actors—such as China and Russia—will increase this year.

The Sahel

Countries in the Sahel—particularly Chad, Burkina Faso, Mali, Mauritania, and Niger—almost certainly will be vulnerable to an increase in terrorist attacks in 2019 as they struggle to contain terrorist groups and improve governance and security. Al-Qa'ida-affiliated Jama'at Nusrat al-Islam wal-Muslimin (JNIM)

and its extremist allies present a growing threat, with attacks increasing during the past year. Implementation of Mali's peace accord—an essential step for extending governance into terrorist safe havens in northern and central Mali—probably will be difficult because remaining steps are politically and financially sensitive.

Nigeria

Nigeria, Africa's most populous country and the largest economy, probably will face a contentious presidential election in February 2019 and sustained attacks from Boko Haram and ISIS-West Africa (ISIS-WA). Abuja is also facing continued violence in the politically sensitive Middle Belt region.

Sudan and South Sudan

Violence and the humanitarian crisis in South Sudan are likely to persist this year, while Sudan probably wants to improve relations with the United States but will continue reaching out to other partners to boost its economy. In South Sudan, the peace agreement signed between the government and opposition groups in September 2017 faces delays and implementation difficulties. Acute food insecurity and constraints on aid access—resulting from poor infrastructure, seasonal rains, active hostilities, and government- and opposition-imposed impediments—are likely to contribute to an ongoing humanitarian crisis. Meanwhile, Khartoum, despite facing antigovernment protests over its poor economic situation, is committed to pursuing efforts to improve its relationship with the United States and wants to be removed from the US State Sponsors of Terrorism List. Sudan also will strengthen ties to other partners—including Russia and Turkey—in an effort to diversify its partnerships and improve its economic situation.

Horn of Africa

The states of East Africa will confront internal tension and a continuing threat from al-Shabaab, despite improved intergovernmental relations and Ethiopian-Eritrean rapprochement. Elite competition, corruption, and poor coordination among security services in Somalia will hamper efforts to tamp down violence. The African Union Mission in Somalia (AMISOM) is unlikely to engage in aggressive offensive operations against al-Shabaab in advance of the mission's scheduled withdrawal from Somalia by 2021. Ethiopia and Eritrea will struggle to balance political control with demands for reform from domestic constituencies.

Central Africa

Political unrest across Central Africa is likely to persist through 2019, compounding humanitarian challenges and armed conflict. The Democratic Republic of the Congo (DRC) is recovering from its contentious presidential election in December 2018, as well as dealing with an ongoing Ebola outbreak and internal displacement crisis. Meanwhile, violence among armed groups in several regions of the DRC threatens regional and national stability, and violence in eastern DRC impedes efforts to respond to the Ebola outbreak. The Central African Republic (CAR) is struggling to make progress toward a peace agreement between the government and multiple armed groups.

THE WESTERN HEMISPHERE

Flagging economies, migration flows, corruption, narcotics trafficking, and anti-US autocrats will present continuing challenges to US interests, as US adversaries and strategic competitors seek greater influence in the region. The hemisphere will see several presidential elections this year, including in Argentina,

Bolivia, El Salvador, Guatemala, Panama, and Uruguay, providing opportunities for outside candidates to exploit public frustration with stagnant economic growth, high crime, and corruption. China and Russia will pursue efforts to gain economic and security influence in the region.

Mexico

Newly inaugurated Mexican President Andres Manuel Lopez Obrador almost certainly will focus on meeting steep public expectations for improvements on anticorruption and security following his landslide electoral victory in July. He is likely to pursue mostly practical approaches to US cooperation that complement his ambitious domestic agenda. Lopez Obrador has promised to reduce violence, in part by addressing socioeconomic causes, but he has publicly conceded that Mexico's military must keep up its public security role in the near term, despite his initial preference to end it. Lopez Obrador has supported the US-Mexico-Canada Agreement (USMCA) trade deal, probably hoping to reduce trade-related uncertainty, allowing him to focus on his domestic economic agenda. However, Mexico's $1.15 trillion economy remains vulnerable to investor uncertainty that could weaken the export sector and slow economic growth, which was just 2 percent in 2017. Declining oil revenue will limit the Mexican Government's ability to fund Lopez Obrador's ambitious social programs and infrastructure projects.

Central America

We assess that high crime rates and weak job markets will spur additional US-bound migrants from the Northern Triangle—El Salvador, Guatemala, and Honduras—while a political crackdown in Nicaragua dims that country's already bleak economic outlook. Illicit migration northward from the region shows no signs of abating, despite increased messaging by governments to dissuade potential migrants and stepped-up immigration enforcement by Mexico. Many migrants apparently perceive that traveling in caravans on the journey north affords a certain level of security, and the decision to do so appears to result from a combination of individual motivation, encouragement from social media postings, and politically motivated efforts by some individuals and organizations.

- Nicaraguan President Daniel Ortega's refusal to heed calls for negotiation amid his political crackdown, which has left more than 300 people dead and contributed to allegations of human rights abuses, threatens to deepen a recession in one of the region's weakest economies.

Venezuela

Although the regime of Nicolas Maduro will continue to try to maintain power, he is facing persistent opposition. Falling oil production, economic mismanagement, and legal challenges almost certainly will compound the worsening economic pressure on the country. Living standards have collapsed, and hyperinflation and shortages in basic goods have gripped the country. Since 2014, the UN International Organization for Migration estimates that 2-3 million Venezuelans have left the country. Maduro continues to crack down on the political and military opposition after a failed assassination attempt against him in August 2018 and disrupted coup plots in the past 12 months, but the opposition has shown resilience, as indicated by its challenge to Maduro's rule emerging in late January 2019.

Estimated Venezuelan Migrants and Asylum Seekers by Country (2015–18)

Recipient Nations	Venezuelan Migrants
Colombia	1,000,000
Peru	400,000–580,000
Chile	85,000–300,000
Ecuador	250,000
Panama	21,000–88,000
Brazil	76,000
Argentina	70,000
Dominican Republic	20,000–46,000
Trinidad and Tobago	40,000
Mexico	26,000–33,000
Costa Rica	9,000–23,000
Canada	21,000
Aruba	10,000–20,000
Guyana	12,000
Uruguay	8,500
Bolivia	3,000–7,000
Curacao	5,000

1810-00439-U

Colombia

Colombian President Ivan Duque faces a fraying peace accord with the former Revolutionary Armed Forces of Colombia (FARC) while he is working to stem violence in Colombia's rural departments, carry out his coca eradication ambitions, and manage growing tensions with Caracas. Duque has ordered increased security operations to curb common crime, threats from Colombia's insurgent and criminal groups, and address coca cultivation and trafficking. Coca cultivation in Colombia was at a record 209,000 hectares in 2017, and crop substitution and eradication programs face coordination challenges and local resistance.

Cuba

Cuban President Miguel Diaz-Canel will adhere to former President Raul Castro's blueprint for institutionalizing one-party rule and socialism in Cuba through constitutional reforms. Diaz-Canel has acknowledged that Raul Castro, who still commands the ruling Communist Party, remains the dominant voice on public policy.

Chairman BURR. Director Coats, thank you for that very thorough testimony. Every year this hearing has geographically increased, and I think this year you have left no region of the world untouched with the concern that we might have. And this year especially, the threat landscape continues to increase from a standpoint of the tools used. I'm sure that much of that will be the subject of questions, both this morning and this afternoon.

I want to acknowledge that we have a distinguished group joining us this morning from Austria, who represent their government. I'm not going to ask them to stand or anything, not to distinguish them out of the group, but we're delighted to have them with us—being part of the United States Senate today.

I want to notice members that you will be recognized by seniority for five minutes. We intend to do one round, and I would say sorry to Senator Sasse and Senator Bennet because they will be last, and had they been here on time, they would have heard the great comments that I made about their addition to the Committee.

[Laughter]

Vice Chairman WARNER. Of course, they still would have been last on questioning.

[Laughter]

Chairman BURR. With that the Chair would recognize himself for five minutes.

General Nakasone, this is probably directed at you. This Committee requested independent third-party researchers to produce two reports that comprehensively detail the leveraging of U.S. social media companies by Russia with based actors to conduct a disinformation and influence campaign in the 2016 election. Without speaking to sources and methods under your current authorities, would the IC be able to conduct the same analysis and produce comparable finished intelligence?

General NAKASONE. Mr. Chairman, thank you very much for the question, and thank you for your recognition of Chief Petty Officer Kent.

In terms of the work that was done by the two organizations that the Senate Select Committee on Intelligence had asked, they looked at an internal study with a number of social media groups, which is something, as you know, is outside our authorities, but was very, very effective for us. As we prepared for the 2018 midterm, we took a very, very close look at the information that was provided there. We understood our adversary very well, and we understood where their vulnerabilities also lie.

Chairman BURR. Good. This to Director Wray and to yourself, General Nakasone: is it the IC's assessment that this country's adversaries continue to use U.S. social media platforms as a vehicle for weaponizing disinformation and spreading foreign influence in the United States?

Director Wray.

Director WRAY. Yes, that's certainly the FBI's assessment, not only did the Russians continue to do it in 2018, but we've seen indication that they're continuing to adapt their model and that other countries are taking a very interested eye in that approach.

Chairman BURR. General Nakasone.

General NAKASONE. It is certainly NSA's assessment as well, Mr. Chairman.

Chairman BURR. An area of increasing concern for this Committee is how the production, storage, and usage of data is a national security issue. In 2013, IBM estimated that we were producing 2.5 billion GB of data every day. And that data growth has not been linear. IBM similarly reported that 90 percent of the world's data had been created in the last two years. That data is now being aggregated, curated, and trafficked to enable and enhance data-hungry artificial intelligence algorithms. How much of a concern should we have about protecting data from foreign adversaries? I'll probably turn it to Director Wray and General Nakasone on this again.

Director WRAY. Well, I think it's a great concern. Certainly we see strong interest from a computer intrusion dimension, both from nation states, but also from criminal hackers, and increasingly the two in a blended threat way. So, we see nation states enlisting the help of criminal hackers, which just is a form of outsourcing that makes it even more of a menace. So, it's something that we're extremely focused on and should be a high priority.

Chairman BURR. General.

General NAKASONE. Mr. Chairman, I concur with the importance of data. It's the coin of the realm today. If you think the power of data, not only for information that it can provide us, but also, as you indicated, the weaponization of it. We see our adversaries very interested in being able to procure data. And obviously as Director Wray mentioned, this is something that we're very, very focused on, as well, as the National Security Agency.

Chairman BURR. I'll throw out to whoever would like to answer: what applications of big data by foreign adversaries have you most concerned today?

Director COATS. Well, certainly China has the capacity and the resources to be able to do a lot, but that has not deterred other major nations like Russia and others to be aggressive in doing this. You have identified this as a significant threat. We are awash in data. We have to understand how our adversaries use that data against our interests, and how we can prevent that from happening, as well as use it for our own purposes relative to know what is going on around the world and what influence efforts are being thrown at the United States. So that was why we hold as a very, very high priority, as you mentioned in your opening statement, in terms of how we resource our community, Intelligence Community, with the kind of tools and weapons needed to address this issue.

Chairman BURR. Director

Director WRAY. I was just going to add that as the challenges of encryption become bigger and bigger on the SIGINT side, we're more and more dependent on human sources, and the more big data can be exploited by our adversaries, the harder it is to recruit and retain human sources. And I suspect Director Haspel may have a view on that, as well.

Chairman BURR. Director Haspel.

Director HASPEL. I think Director Wray captured that exactly, and I would just add from the CIA perspective that a big focus for

us is finding out how our adversaries are using big data against us and sharing that with our partners.

Chairman BURR. I'm going to exercise the Chair for just a second for one last question, and this is your opportunity to recruit. Your agencies do cutting-edge research on every technology you could imagine, from classic spycraft like disguising to communications technology that would blow James Bond and Q Branch away. What pitch would you make to those in school now, or perhaps those working in tech and looking to serve a greater purpose, that they should come apply their engineering degrees, coding skills, and creativity and work in the IC?

Director Wray.

Director WRAY. I would say there is nothing more rewarding than protecting the American people. And we've seen with some of our smartest high-tech folks—I can think of one office in particular where two of our brightest stars with great talent briefly left for what they thought would be greener pastures in the private sector, and I was very pleased to see them both independently come back only about eight months later when they realized the grass was browner.

General ASHLEY. If I could Mr. Chairman, I would have probably asked you to release the tape of what you just said, in terms of really how innovative and how creative and the opportunities that the folks in the IC get a chance to engage in, far outstrip anything that you see in a Hollywood movie. And the other thing I would add to that is imagine when you get up every morning that your task, your responsibility is to defend the hopes and dreams of 320 million Americans and that's something that we relish the opportunity to do that every single day and people would want to join that team.

General NAKASONE. Mr. Chairman, our mission sells itself when we talk to our people. I would offer as we talk to young people at the National Security Agency, I saw a big data, artificial intelligence, machine learning, cloud computing in places like Baghdad and Kabul in support of our forces long before we ever called it that. That's the selling point that we emphasize to our people because if it's cutting-edge, we will be doing it at the National Security Agency.

Chairman BURR. Robert.

Director CARDILLO. Mr. Chairman, we are proud of our ability to recruit some of the talent you just described. We don't do it often on fiscal terms, we do it on psychic terms and so serving something greater than oneself for a cause to protect the Nation and our interests is one that both attracts and retains the lifeblood of our agency, which is our people.

Chairman BURR. Director Haspel, do you want to take a shot at selling something that not many people know about?

Director HASPEL. Well, like my colleagues, CIA officers come to Langley for the mission and they stay because of the mission and it's really about being part of something that's bigger than yourself. And in terms of advanced technologies it's a chance to be on the cutting edge and make a difference.

Chairman BURR. Well, let me just conclude by saying the disciplines that come out of higher education and community colleges

today, all of those disciplines are applicable to the agencies that sit before us today. There should be no student that doesn't look at this as a way to apply what they've learned or the degree that they have. That didn't used to be the case. It was all specialized but now it applies to everything.

Director Coats.

Director COATS. Well, Mr. Chairman, as somewhat of an older generation here who has to turn to his grandson to get the TV on the right channel, I'm continually amazed—as I get around the country talking to colleges and graduates and people that are in these STEM positions and studying—of their incredible talent. They bring those kind of talents and skills to our agencies as you have heard. And it is extremely rewarding to see the young people who know they could have a better financial deal, a more settled lifestyle, easier and so forth and so on, they want to serve this country and they see this as meaningful and it exceeds what financial gains they could get on the outside. Plus they are able to do some really cool stuff in all of these agencies, which we can't talk about here, but it is attractive to it. But their commitment to the country and commitment to the mission as has been demonstrated here is awfully rewarding when you go out and see what these young people have and what they are willing to do for their country.

Chairman BURR. I thank all of you.

Vice Chairman.

Vice Chairman WARNER. Well, thank you, Mr. Chairman.

And I agree that the people who work with all of you are extraordinarily special Americans, and the mission is critically important. I would personally add one other item: that if they work for the United States Government they actually ought to be paid on time. And I question—I have seen the number of Federal employees who worked five weeks plus without pay. I'm not sure many folks in the private sector would show up five weeks plus without pay on an ongoing basis. And while I'm appreciative of the fact that particularly the FBI, that your agents will be reimbursed, I do worry; the FBI has a number of contractors. Under our current setting, they will come out of this five week plus, 35-day shutdown with nothing to show.

And if we cannot guarantee that people that work for the United States Government are going to be not used as hostages for either side of the political debate, then I think our ability to recruit and retain will go down dramatically. I don't know if Director Wray, if you want to make any comments on that or maybe just punt. But it is something I saw FBI agents, I saw Homeland Security agents, I saw air traffic controllers working double shifts and then going and driving an Uber. I'm not sure I want somebody showing up maintaining the safety of our airways with four hours of sleep. But I'd be happy to take your comment there.

Director WRAY. Mr. Vice Chairman, needless to say we are still assessing the overall operational impact of the shutdown, but what's quite clear is that it was incredibly negative and painful for the 37,000 men and women of the FBI and their families. But I will also say that I could not be more proud of their professionalism

and their dedication to not let balls drop but to keep charging ahead across all of our various program areas during that time.

Certainly, when you talk about contractors, we are very dependent, just like every government agency, on contractors for a whole range of services and you know we would want to make sure that that aspect of our operations doesn't get disrupted.

Vice Chairman WARNER. And my hope would be that folks from both sides of the aisle will look at how we might make sure—particularly some of those low-priced contractors often times the folks who clean the bathrooms or serve the food—don't have to come out of this 35-day shutdown with absolutely no compensation at all.

Let me start my first question Director Wray and Director Coats. The Chairman has alluded to it, we've all talked about it: this emerging challenge around social media, particularly the fact—whether it's Russians or other foreign entities—that try to masquerade as Americans. They build large followings; they create fake accounts. I think this problem is going to get exponentially harder as we move into deepfake technology. A lot of policy implications.

How do we sort through that? How do we, going forward, work with our social media company partners to put Americans on alert about the volume of foreign-based activity, bots, and others who are masquerading as Americans so they are not able to further manipulate not just our election process but actually to build social divisions?

Director WRAY. Well Mr. Vice Chairman, this is a particularly vexing and challenging problem. I think it's going to require a holistic response, certainly at the FBI through the Foreign Influence Task Force and all of our field offices. We are trying to work much more closely not just with our Intelligence Community partners, especially General Nakasone and the NSA, but also as you say with the private sector.

And I will say that one of the bright spots between 2016 and 2018 is how much more cooperatively we are working with the social media companies, because there's an awful lot that really has to be done by them in this space. And there were a number of success stories only some of which we could really ever share where the social media companies, based on tips that we provided, were able to take action much more effectively, much more quickly to block and prevent some of the information warfare that the Russians were engaged in. And I think we are going to need to see more and more of that. But now that we've got some momentum, we are looking forward to growing that partnership.

Vice Chairman WARNER. And I think you would agree some companies have done well, some have not done as well. I think we are going to need to continue to explore this and just basic notional ideas of—where I think we don't get into First Amendment challenges—where Americans ought to have the right to know whether they are being communicated with by a machine or a bot versus an actual human being. And some of the research done by some of the folks we looked at, in a way, it may be a little more positive, it says that the vast volume of traffic on the far left and the far right in terms of political discourse in social media is actually not Americans but foreign-based bots. There may not be as many

crazies out there as it seems. Editorial comment. But I do think we've still got a long way to go. Thank you, Mr. Chairman.

Director COATS. Mr. Chairman, if I could just add one thing to support Director Wray's remarks. Having served on the Committee and gone through the frustrations of the interaction and information-sharing with private social media companies, we've seen significant progress with that. Many of us have sat down eyeball to eyeball with its leaders. Our tech teams are working with their tech teams. I can't say that's worked with every social media company, but it's significantly better because there is information we can provide them that's in their benefit, and of course we always stress the fact that we need to work together to protect our people from the influence activities from abroad and threats to the American people. So, I'm encouraged having made some trips to several of these companies, encouraged with the openness and willingness to see what we can do while protecting privacy rights, but also ensuring security.

Chairman BURR. Senator Risch.

Senator RISCH. Thank you very much.

First of all, let me say that I'm always astounded in this Committee and in the Foreign Relations Committee with the volume of issues that we have to deal with. I think your opening statement, Director Coats, indicated how difficult this is to process and deal with all of this. In your statement for the record, that all of you joined in, again lays this out for us and tells us the kind of volume that we have to deal with.

And we're certainly only going to scratch the surface here today, but I want to—I want to focus on something that doesn't get as much focus as I think it should. We see these days, every time we pick up media or turn on TV they're talking about Russia and Russia's ham-handed efforts to affect things in the world. And certainly, it's a concern. But in my judgment, and I think for many others, the real concern is China.

We're approaching the end of the first fifth of the 21st century and, if we've learned anything, it's that the last few decades have convinced us that China, in the 21st century, as we proceed through it, is going to be a major competitor of ours in every way that there is. Obviously, economically, militarily, culturally, and in every other way. And look, this is going to happen. We are living in the 21st century. Communications and transportation are so different from what they were, and we, as the United States, are going to wind up having to compete like we never have before with a gorilla that's starting to get to be about the same size we are and, as a result of that, we're going to have to learn to deal with that.

The thing I really want to focus on is how we're going to do with that. We are Americans. We've always competed. We can compete, we innovate, we create, we manufacture, we do the great things that we do that have really led the world. But we can only do it if we are operating under a rule of law and that is something that is greatly missing at the present time as China tries to compete with us.

The poster child for me is a local company we have an Idaho, Micron Technology. Most of you have heard of them. They're the sec-

ond largest manufacturer of memory in the world. And they have had a recent case where Chinese nationals stole intellectual property and then took it back to China and are now suing Micron in China through a state-owned entity and a state-owned court in front of a state-owned judge. And this is the kind of thing that we just can't have.

I had a spirited discussion with the Chinese Ambassador about this as he attempted to defend the undefendable. His suggestion was that things aren't as advanced in China as they are here. Well, I get that. They've come a long, long, long way in a few decades, but if we're going to do this and keep the world order right side up, China is going to have to develop their rule of law and live by it much better than what they have recently. We just saw again, the indictments against the Huawei official. In defense of the Department of Justice, Department of Treasury, and others, they've indicted these Chinese people that have affected Micron.

And the question I have for you is, after listening to the Chinese Ambassador, I'm not wholly convinced that their efforts are going to be as robust as they need to be to get China right-side-up when it comes to the rule of law. And when I'm talking about the rule of law, I don't mean just covert theft, but I mean what I call overt theft. And that is where they require businesses, as we all know, to divulge their information before they can do business in China and then having the kind of restrictions they have on them in China. And all of this causes us real difficulties as we attempt to compete.

Director Coats, I wonder if you could address that, or assign it to somebody there at your panel. I'm looking for what do we see in the future, number one, and number two, how can we try to get our arms around this to do something about it?

Director COATS. Well, I'll start it, but I'd like to turn it to Director Wray, relative to what was just released yesterday, which pointed, I think, in the direction of what you were talking about. But frankly, while we were sleeping in the last decade and a half, China had remarkable rise in capabilities that are stunning. A lot of that was achieved, a significant amount of that was achieved by stealing information from our companies, by inserting Chinese in certain of our labs, or bringing back technological stolen properties, which China engaged. You can talk to any number of everything from automobile manufacturers to sophisticated software as well as R&D for military, and I think General Ashley can speak to that on the military side.

I think we could go down the panel here and discuss for a significant amount of time the kind of actions China has taken to become a competitor, but also to gain superiority and what they're doing and how they're spreading around the world through their Belt and Road Initiative and a number of other initiatives. It is a serious issue that has to be dealt with. You are right on target in terms of saying that rule of law and international norms and fairness in trade and engagements is not the Chinese model.

And to counter it, we have to expose it. It was exposed yesterday and a significant way relative to telecommunications and Director Wray can talk about that. We have alerted our allies. They are now second-guessing and questioning their initial responses to China.

Oh, it's a great market, we need to get over there. Don't worry about anything else except selling a product. They're now finding that their product has been duplicated by the Chinese and sold for half the price because they didn't have to spend as much money on research and development.

So, we are working with the Chairman, Vice Chairman, and with the Committee, actually, to try to be as transparent as possible with our company heads. We have been traveling around the United States meeting with CEOs and others. I think I ought to stop right there and—and the rest of this ought to go into a secure setting in terms of how we are dealing with this. But I'd love to turn to Director Wray relative to what they are doing.

Director WRAY. Senator, I completely share your observations and I would just say that one of the things that the American people I think are now sort of waking up to understand is that the lines between the Chinese government and the Chinese Communist Party are blurred, if not totally erased. The lines between the Chinese government and Chinese state-owned enterprises, the same. The line between the Chinese government and ostensibly private companies, for all the reasons you described, and especially the line between lawful behavior and fair competition and lying and hacking and cheating and stealing.

And one of the things that I've been most encouraged about in an otherwise bleak landscape is the degree to which, as Director Coats was alluding to, American companies are waking up. American universities are waking up. Our foreign partners are waking up. And it's one of the few issues that I find when I engage in the interagency and up on the Hill, covering from one of the spectrum to the other, there seems to be actually more consensus than I've ever seen before in my career. And I think that's a positive and we need to build on that.

Chairman BURR. Do either of the generals have—General Ashley?

General ASHLEY. Yes, sir. Sir, you laid out the problem set very well and what's been highlighted, this isn't just a U.S. issue, this is a global issue. When you think about the Internet of Things, when you think about the nature of global business and how corporations are integrated. And if it touches a company in Australia who may have a relationship with a company in the U.S., then we become connected. From a military standpoint, when you look at major acquisition from a Defense Intelligence Agency, one of the things we put against this is the Supply Chain Risk Management Threat Analysis Center.

So when DoD looks for major acquisition, we do the due diligence and research against those companies, but that challenge is getting more and more complicated, because you think they either buy it, they steal it, or they can build it. But the nature of that business, you have things like white labeling where you don't necessarily have to disclose the relationship, where you could sell a semiconductor, chip, piece of software that ostensibly it is from your company, when in fact it may have been manufactured by a Chinese company. So that's the due diligence that we have to apply to look at the supply chain across all acquisition. And we've got to bring all our partners in and illuminate the challenge and make sure

they're doing the same due diligence, whether it's through CFIUS or other protocols.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

Director Coats, in this hearing last year, you testified that you would recommend minimal access to classified documents to anyone without a permanent security clearance. You made that statement with regard to reports of multiple holders of interim security clearances in the White House. And now we are seeing published reports that dozens of times the White House has overruled the career FBI experts responsible for adjudicating security clearances, granting top-secret clearances to White House officials. Would you still recommend minimal access to classified documents to those White House officials, since FBI experts recommended that they not be given those top-secret clearances?

Director COATS. I do support providing all the information necessary for not only the White House, but for all of our branches relative to providing security clearance. They have the authority to do that. We issue guidelines in terms of what——

Senator HEINRICH. I understand they have the authority.

Director COATS [continuing]. Ought to be adhered to.

Senator HEINRICH. I want to know, do you think that the White House should take seriously the recommendations of those FBI experts?

Director COATS. To my knowledge they do take seriously. It is their decision based on a whole number of factors. We've seen every Administration issue clearances based on how they assess what is provided. Our job is to provide them the best information we have relative to security clearance processes so that they have the full picture in front of them when they make that decision.

Senator HEINRICH. Speaking of the full picture, last year we passed the SECRET Act. As the Director of National Intelligence, do you think it's problematic that the Administration has not complied with the portion of that law requiring the White House to report on its process for conducting security clearance investigations?

Director COATS. I'm not aware that that has happened. I'd be happy to look into that.

Senator HEINRICH. I would appreciate that.

Director Wray, as I mentioned, we're seeing public published reports that numerous times the White House has simply overruled career FBI experts responsible for adjudicating those clearances. In your view, were there valid reasons given for why the FBI's expert advice was overruled so many times?

Director WRAY. Senator, I think there may be some confusion about the way the process actually works. The FBI is, in the context of providing background investigations for people other than its own employees, is what's called an ISP, or the investigative service provider. So, we essentially do it at the request of whoever the requesting entity is. In this instance it would be the White House. And I think where the confusion is, is what we do is we assemble the information, we provide the factual information. We do not actually make recommendations one way or the other about the clearances. The decision about what to do based on those facts is

entrusted by a long-standing process to the requesting entity. So, we provide the information, but then they make the call.

Senator HEINRICH. Thank you, Director.

Director Coats, I want to come back to you for a moment. Your office issued a statement recently announcing that you had submitted the Intelligence Community's report assessing threats to the 2018 midterm elections to the president and to appropriate executive agencies. Our Committee has not seen this report. And despite Committee requests following the election that the ODNI brief the Committee on any identified threats, it took ODNI two months for us to get a simple oral briefing, and no written assessment has yet to be provided.

Can you explain to me why we haven't been kept more fully and currently informed about those Russian activities in the 2018 election?

Chairman BURR. Director Coats, before you respond, let me just acknowledge to the members that the Vice Chairman and I have both been briefed on the report, and it's my understanding that the report at some point will be available.

Director COATS. Yeah, the process that we're going through were two 45-day periods, one for the IC to assess whether there was anything that resulted in a change of the vote or tampering with machines, what the influence efforts were, and so forth. So, we collected all of that, and then the second 45 days, which we then provided to the Chairman and Vice Chairman, and the second 45 days now is with DHS and DOJ—looking at whether there is information enough there to determine what kind of response that they might take. We're waiting for that final information to come in.

Senator HEINRICH. So the rest of us can look forward to——

Director COATS. So that will be coming, coming shortly.

Senator HEINRICH [continuing]. The rest of us can look forward to reading that report?

Director COATS. I think we will be informing the Chairman and the Vice Chairman of that, yes, of their decisions.

Senator HEINRICH. That's not what I asked. Will the rest of the Committee have access to that report, Mr. Chairman? Chairman Burr.

Chairman BURR. Well, let me say to members we're sort of in uncharted ground, but I'd make the same commitment I always do, that anything that the Vice Chairman and I were exposed to, we'll make every request to open the aperture so that all members can see it. I think it's vitally important, especially on this one. We're not to a point where we've been denied, or we're not to a point that negotiations need to start. So, it's my hope that once the final 45-day window is up, that is a report that will be made available probably to members only.

Senator HEINRICH. That would be my hope as well.

Chairman BURR. Senator Rubio.

Senator RUBIO. Thank you.

Director Wray, as we keep talking about China—and this takes off on what Senator Risch has already asked—using the academic community and the universities, commercial espionage, the forced transfer intellectual property, embedding themselves in the potential end of the supply chain, obviously the traditional counterintel-

ligence work that they do and the like, is it not fair to say that China today poses—just looking at the scale and scope of the threat—that China today poses the most significant counterintelligence threat this Nation has faced, perhaps in its history, but certainly in the last quarter century?

Director WRAY. Well, I'd hesitate to speak, you know, categorically about the entire course of history, but I certainly would——

Senator RUBIO. Well, let's limit it to 25 years. How's that?

Director WRAY. But I would certainly agree with you, Senator, that as I look at the landscape today and over the course of my career—I still think of myself as a little bit young—that the Chinese counterintelligence threat is more deep, more diverse, more vexing, more challenging, more comprehensive, and more concerning than any counterintelligence threat I can think of.

Senator RUBIO. And in that realm, would it not make sense—and perhaps this is for you, Director Coats—that we would have a more coordinated approach to educate and prepare all the departments and agencies of government, as well as businesses, universities—I mean just the scale and comprehensive nature of the threat—would it not make sense to have some high-level coordination or coordinated approach to be able to prepare all these different entities in our economy and society to deal with this threat?

Director COATS. We are working carefully with the Committee. Particularly Senator Warner and Senator Burr both have engaged with us in terms of putting a program together to do just that. I'd turn to General Ashley for his comments on it also.

General ASHLEY. So, the fact that we're having this discussion and that you've highlighted that, even last year we talked about the Confucius Institutes. You know, that word gets out. Since 2014, 13 universities have closed down the Confucius Institutes. U.S.-wide, I think the number is about 100. But again, my previous comment in terms of this is a global issue, while we've closed down about 13 in the U.S., there's been about a 23 percent increase globally in Asia, Europe, and other places, and there's probably about 320-plus Institutes that exist globally. So, the education is getting out from a U.S. standpoint, and it's trending the right way slowly. But again, it is a global problem, and we're as weak as the relationships with some of those partners subject to influence.

Senator RUBIO. This is now where I make the obligatory pitch. Senator Warner and I have filed a bill that creates an office of critical technologies to help coordinate the response to this threat across the board, and I know everybody on this Committee is interested in this topic.

I want to switch gears for a moment and maybe ask you this, Director Coats, as well, if we look at the situation in Venezuela, which usually I raise in this Committee, and people know it's important, but now it's really topical. So we've had 3 million migrants flow primarily into Colombia, Peru, and Ecuador. It's projected to be five million, if current trends continue by the end of this year. That would be a rival number to what we've seen in the Syria situation, and it most certainly has had a destabilizing effect on Colombia and other neighboring countries to the point where very few nations could take in one million migrants in one shot, not to mention that quickly. Imagine two million and the impact it's having on

their government budgets, their healthcare systems, and the like. We know from Department of Justice filings and sanctions from Treasury that their government doesn't just tolerate drug trafficking, they give it the protection of government, and many high-level officials are active participants in narco-trafficking. We know that they have a relationship, long-standing relationship, with Iran and with Hezbollah. We know they have openly and repeatedly—at least Maduro has—invited the Russians and Putin to establish either a rotational or permanent presence somewhere in Venezuela, thereby creating a Russian military presence in the Western Hemisphere. In fact, they flew, about three weeks ago or a month ago, two Russian nuclear capable bombers into the Caribbean Sea.

Seeing all these factors, what's happening in Venezuela—we care a lot about democracy, we care a lot about freedom, we care a lot about human rights—but when you add all these things together, the migratory impact on regional partners and how that spills over into the United States, their relationship with Iran and Hezbollah, the drug trafficking—because all that cocaine is destined to come into our streets—the invitation to the Russians to potentially have a military base, whether it's rotational or permanent, in our hemisphere—is it not in the national interest of the United States of America that the Maduro regime fall and be replaced by a democratic and more responsible government?

Director COATS. Well, I think everything you said has been very open to the American public relative to the situation that exists in Venezuela. Our job as an Intelligence Community is to provide all of the relevant information that you just talked about in terms of what the impact of what's happening in Venezuela and then throughout the region, and the threat that evolves from that.

The decision as to how to address that obviously is a decision by the Executive Branch and by the President ultimately with the support of the National Security Council. So, we do obviously face a dire situation that has enormous consequences. I think nobody's more aware of that than you. You've been the person we turn to for—almost ready to invite you into the Intelligence Community given the information that you can provide for us given your interests.

I was remiss in not naming you as someone relative to China who's taken a forward effort on the part of the Committee and joining us in a number of ways to talk to CEOs and others around the country relative to the Chinese threat.

With Venezuela, it's a very tenuous situation right now as you know. We have taken steps in terms of recognition of the opposition as the legitimate president of Venezuela. Yesterday, the Treasury Department announced oil sanctions against a Venezuelan oil company. They are a major company that we do business with here also. So, steps are being taken and we have a lot of support from a lot of our allies. So as I said, it's a very fluid situation that I think hopefully will be successfully resolved with the support of Venezuelan people. But we do assess—and I'll turn to General Ashley here—the influence of the military on that decision, I think—Venezuelan military on that decision probably is key to what direction we might go in.

General ASHLEY. So, I would say that everything you laid out is correct. We expect to see another two million refugees leave, to add to the three million that will go into the region. The relationship that they have with Russia, China, Iran is a long-standing one, pre-existing.

The reference you made to the TU–160 Blackjacks that flew those strategic bombers—third iteration of that—first time was in 2008 and then 2014, and we've seen it again. As far as presence on the ground, we can talk a little bit more detail in a closed session about where we see Russia and China going with that greater instability. But in the open press, what you've seen thus far really is nothing more than just vocal support that's coming out of Moscow and that's coming out of China as well. But there is a relationship there from a military standpoint in the way of training. Lots of Venezuelan officers go to Russia for training and there is a reciprocal relationship for equipping them as well.

Senator BURR. Senator King.

Senator KING. Thank you, Mr. Chair. In light of Senator Rubio's comments, I'd just like a note of caution. He listed refugee flows, human rights abuses, and corruption. There are lots of countries in the world that meet that description and our right or responsibility to generate regime change in a situation like that I think is a slippery slope. I have some real caution about what our vital interests are and whether it's our right or responsibility to take action to try to change the government of another sovereign country. That same description would have led us into a much more active involvement in Syria, for example, five or six years ago, other parts of the country. I just wanted to note that.

Senator Burr, I loved your opening statement. It was very thoughtful and you came up with a wonderful formulation for, I think, a mission of this Committee and also the Intelligence Community of "creative, adaptive, and resolute" and I must say it reminded me immediately of my old high school football coach who put it somewhat less elegantly. He said he wanted us to be agile, mobile, and hostile. I think that may be a less elegant way to put it, but the same principle.

On Huawei, it seems to me they have to decide they are either going to be a worldwide telecommunications company or an agent of the Chinese government. They can't be both, and right now they are trying to be both. And I think the world's customers which the Chinese are certainly sensitive to are the best enforcers of that principle.

Director Haspel, one quick, I think a yes or no question, and I think Sen—I almost said Senator Coats—Director Coats referred to this in his opening testimony. Is Iran currently abiding by the terms of the JCPOA in terms of their nuclear activities?

Director HASPEL. Senator King, I think the most recent information is the Iranians are considering taking steps that would lessen their adherence to JCPOA as they seek to pressure the Europeans to come through with the investment and trade benefits that Iran hoped to gain from the deal.

Senator KING. But since our departure from the deal, they have abided by the terms. You're saying they are considering but at the current moment they're in compliance?

Director HASPEL. Yes, they are making some preparations that would increase their ability to take a step back if they make that decision. So, at the moment, technically they are in compliance, but we do see them debating amongst themselves as they've failed to realize the economic benefits they hoped for from the deal.

Senator KING. Thank you.

Director Haspel and General Ashley, Mr. Khalilzad, our envoy to Afghanistan, has said that part of the basis of the current talks with the Taliban is that they would prevent Afghanistan from ever becoming a platform for international terrorist groups. And of course, that was the basis of our original intervention.

Do we believe them? Are they capable of that? Did they learn something from having given safe haven to Osama bin Laden? Do we believe that there is a mindset change that that could be an enforceable or at least a reasonable expectation?

Director Haspel.

Director HASPEL. Yes, Senator, and you are referring to very recent and fresh news that has come out of Ambassador Khalilzad's very intensive efforts over many months now but particularly over the last eight days in Doha where he has been engaged in talks with the Taliban to seek to achieve a framework under which we can conduct——

Senator KING. Can we believe that the Taliban will do that?

Director HASPEL. Well, because we have inflicted severe damage on al-Qaeda in the AfPak theater, I think that all of us at this table would agree that it's very important that we maintain pressure on the terrorist groups that are there. And so if there were an eventual peace agreement, a very robust monitoring regime would be critical and we would still need to retain the capability to act in our national interests if we needed to.

Senator KING. Thank you.

Another note. Director Coats you mentioned—I wouldn't say almost in passing but it was just a sentence of your introduction which I think is a very important point and maybe the big news of right now what's going on—increased cooperation between Russia and China. For a generation that hasn't been the case. That could turn out to be a very big deal on the horizon in terms of the United States. If those two countries begin to work together systematically, that could be a big problem for us.

One more quick question. Director Wray, you are doing a lot of monitoring and working on the intervention in our election process. One thing we are worried about is deepfake which we've used but not—not defined. That's when they use technology to create essentially a false reality—an apparent speech by a candidate where different words are coming out of their mouth than what they actually said. Here's my question.

If in the next two years and particularly in the year preceding the next election, your agency determines that this is happening and that it's sponsored by a foreign entity, will you inform the candidates that are the victims of this, the committees? My concern is it's one thing for the Intelligence Committee to know that this is happening, but if they don't inform the people who are being victimized, who are being attacked in this way, I think that really blunts the effectiveness of the availability of the intelligence.

Director WRAY. Senator, we have a fairly established protocol that we work through to try to determine whether or not we have information that is reliable enough and immediate enough and actionable enough to be able to notify a victim. The Department of Justice has a set of guidelines that goes through that. They've recently been expanded to provide us more flexibility in the foreign influence or maligned influence arena, which this would be a permutation of and we would expect to follow that process.

Senator KING. I hope you'll review that process, because telling the world of a maligned influence a month after the election doesn't do anybody any good. So, I hope that could be reviewed and thought about in terms of letting people know as soon as possible when there's credible evidence of a foreign deepfake or other kind of cyberattack on a campaign.

Director WRAY. Just to be clear, I wasn't referring to the sort of post-election process.

Senator KING. No, I understand.

Director WRAY. Yeah, the protocol that I'm talking about is that's where the actionable piece of it comes into play, right? Obviously, the ability to be able to contact, just like we do in the cyber arena.

Senator KING. I just want to be sure our policies keep pace with the magnitude and accelerated nature of the threat.

Director WRAY. Well, we clearly need to be, to your point about agility, we clearly need to be able to adapt as the technology adapts and as Director Coats said in his opening, we would expect our foreign adversaries in the maligned influence space to keep adapting as well, which is a source of concern.

Senator KING. We want you to be agile and mobile, maybe not hostile. Thank you.

Director COATS. Mr. Chair, General Ashley has a comment he would like to make.

General ASHLEY. Thank you. If I go back to your comment on Huawei, you know, Huawei needing to make a decision about the direction that they want to take with regards to how do they support the Chinese government, or as an independent business. The challenge in which we've laid out in part of the dialogue is that decision does not lie with Huawei. It lies with the CCP. It lies with Xi Jinping in the way that they are starting to centralize greater the management of those businesses. So therein lies the challenge, where you see a decentralization and execution of capitalism. But really you have this kind of authoritarian capitalism in the way that the government provides oversight and puts very strict rules in place. It makes it very problematic for all of those businessmen to operate without providing that information back to Beijing.

Senator KING. And I think the market has to tell them that's not acceptable. Thank you.

General ASHLEY. Agree.

Chairman BURR. Senator Collins.

Senator COLLINS. Director Haspel, Director Coats described this morning a Russia that is aggressive across all fronts. Did the CIA have any concerns about the Treasury's actions to ease sanctions on companies associated with the close Putin ally, Oleg Deripaska, in terms of his ability to retain some informal control? This isn't a typical American company that we're dealing with.

Director HASPEL. Senator Collins, I don't think I'm expert enough to comment on Treasury's decision, but what I will say is that we work very hard to make sure that every agency, and all of our senior agency leaders, understand Putin's methodologies and what he will do to try and achieve what he perceives as Russia's place in the world and as a great power status. Moscow continues to grapple with the effect of western sanctions. There have been very severe sanctions placed on them. I'm also, I think, as an Intelligence Community, both Director Wray and I were very pleased with the decision to expel 61 Russian intelligence officers. That has a tremendous impact on their ability to hurt us in our own homeland. So, our job is to make sure that everybody understands Putin's efforts to influence globally and to enhance Russia's power status in the world, and we will continue to support Treasury as they look to impose sanctions. I think Treasury has been very, very aggressive on the sanctions.

Senator COLLINS. But did the CIA raise any concerns about the Treasury plan?

Director HASPEL. No, I don't believe we raised any concerns, but we provided all the supporting intelligence about the oligarch in question versus the aluminum company that you're referring to.

Senator COLLINS. Let me switch to a different issue, and that is Syria. Let's assume that after we depart from Syria, the Assad regime takes control of northwest Syria and eastern Syria, which I think is a reasonable scenario. Should this happen, what kind of threat would the United States and its allies expect from the thousands of extremists who are still currently fighting in those areas of Syria, such as ISIS?

Director HASPEL. Senator Collins, to start with the last part of your question, everyone at this table is working very hard to make sure that we can finish the Defeat ISIS Campaign, and also that we understand the foreign fighter picture in eastern Syria and that we don't allow the foreign fighters that have been captured to return to the battlefield. It is, of course, accurate that ISIS has suffered significant leadership losses and near total loss of territorial control. But of course, they're still dangerous, which is your point, and they're the largest Sunni terrorist group, and they still command thousands of fighters in Iraq and Syria. So I think the stance in the Administration and supported by the IC is that we're going to work very hard to finish that mission and that we—that's another example of where we must maintain a very robust monitoring regime and retain the ability to project into Syria should we need to.

Senator COLLINS. Director Coats, you looked like you wanted to add to that.

Director COATS. Well, just to make the point that while we have defeated the Caliphate with a couple of little villages left, we should not underestimate the ability of terrorist groups, particularly ISIS and affiliated groups with al-Qaeda and other terrorist groups, that they are operating not simply on what takes place on the battlefield that gives them strength or weakness, but they are operating on the basis of a theocracy, a theology, an ideology that we will continue to see for perhaps years ahead in various places of the world. So, we see those that were engaged in Syria moving

to other ungoverned spaces. We see the tentacles of ISIS and al-Qaeda tactics in different places in the world, such as North Africa and the Philippines. We've just seen that take place, ISIS claiming credit for that. So, ISIS will continue to be a threat to the United States, and we're going to have to continue, as Director Haspel said, to keep our eyes on that and our interest in the realization that this terrorism threat is going to continue for some time.

Senator COLLINS. Thank you.

Chairman BURR. Senator Bennet.

Senator BENNET. Thank you, Mr. Chairman. Thank you for your welcoming me to the Committee. I apologize for being late, but I also want to say what a privilege it is to hear your testimony this morning and to know that you and agents and officers who work with you are at their posts keeping this democracy safe, and it is a reminder to me what's at stake when our partisan politics can't even keep our Government open. And you guys are still doing your work, and it's an inspiration to me, and I hope to the people that—whoever is watching this at home.

And in that spirit actually, Director Coats, I wanted to start with something that you ended with, which was an observation about concerns that the IC has about political uncertainty in Europe and the ability of European democracies to push back on what you described as autocratic tendencies. Could you say a little bit more about that?

Director COATS. Clearly Europe has seen Russian aggression in hybrid ways. Significant cyber incidents, trying to influence not only their view of our alliance, but their own view of their own alliance within Europe, seeking to sew divisions between countries and between Europe and the United States. It's interesting that some time ago at a meeting with NATO intelligence officials, the question was raised by the Director, did any of the 29 countries of Europe not see Russian influence in their countries and particularly in the political processes of those countries? Not one person raised their hand and said I have not seen that. All 29 have seen some type of influence from the Russians.

So, it's a persistent threat and a pervasive threat that the EU needs to address, and we address with them through our NATO coordination. But I think the warning is there. I think the nations are aware of the threat. We see some issues that threaten some of the alliance coalition. Turkey is a member of NATO, and yet we're having some issues with Turkey. They're at a very geostrategic point in the world, and we've been happy to have them with NATO, so we'd like to keep them there. I don't know if I'm directly answering your question.

Senator BENNET. You are. What about within the domestic politics of those countries? The autocratic impulses, whether aligned with Russia or not aligned with Russia?

Director COATS. Well, I think there's a lot of wariness about aligning with Russia whether you're authoritarian leadership or not. We have seen some countries leaning in that direction, raising issues as to the strength of the alliance. A lot of that is related to the economy, to trade matters, to a number of issues beyond just the military.

Senator BENNET. In the minute I have left, Director, if it's okay I wanted to switch to potential dual-use capabilities that China may attain through its One Belt and One Road Initiative. Recently there were reports that China may press Pakistan for military access.

As Pakistan falls more and more into China's debt, I'm concerned about data access China may control through digital infrastructure projects in countries around the world. What is the IC's assessment of potential dual-use aspects of China's Belt and Road Initiative and what threats do they pose to U.S. interests?

Director COATS. Well, I'd like to also——

Senator BENNET. And where I would say?

Director COATS. Well, you can look at the globe. It's called One Belt/One Road and its global. You can look at the map and see a lot of strategic places where China has real interest in perhaps a dual effort to not only provide infrastructure support, loan support for ports, airports, roads, a lot of infrastructure loans to help with their economy, but also interest in placing strategic military positions.

We've seen that take place off the Horn of Africa. We've seen China looking at different—and if you look at the spots where they're—they are engaging and you see some geopolitical and military aspects. So it is dual and I'd like to turn to General Ashley to give you better detail of what that looks like.

General ASHLEY. So, we can talk in a classified session about the nature of the relationship with Pakistan and I think that we can eliminate what you are seeking there.

In terms of dual-use technologies there is a multitude of things out there and it's not necessarily germane to the Belt and Road Initiative. It's where they are investing and part of that investment is how they are garnering intellectual capital globally, but think about quantum from a communication standpoint, from a computing standpoint, from a sensing standpoint, what those advanced sensors could do, if you look at genetics, bioengineering.

So, there is a multitude of things whether it gets into human engineering, it gets into how do you cure diseases but at the same time there's kind of the flipside nefarious aspect of that and so there is a plus and a negative side to the risk in the middle. There are agricultural aspects of that which are very positive but could have a negative impact as well.

So, there's a number of things—in terms of advanced technologies where they are there investing—that have dual-use capabilities that will really mature over the course of the next decade.

Chairman BURR. Senator Blunt.

Senator BLUNT. Thank you, Chairman.

Thanks to all of you. I want to join everybody in thanking you for what you do and the important service that you provide in securing our freedom and the freedom of lots of other people.

General Ashley, I know we lost a St. Louisan in Syria as part of your defense intelligence operation and certainly reach out to their family and to the families of all who serve who put themselves at that level of risk.

Director Cardillo, I saw "60 Minutes" over the weekend—talked about small satellite data, about all of the commercial imagery

available. If, as you come for what is your last likely appearance in this job before this Committee, there's a legacy that you're leaving it's bringing the commercial data community in, in a way that we are taking advantage of what's out there that we don't have to produce ourselves.

But as we do that, what concerns do you have about cyber activity that might in some way impact that data or the data that we get in other places? How would you describe your concerns about cyber as it relates to commercial data that you've made great steps in using and the other geospatial that we produce ourselves that may be disrupted before it gets analyzed with information that's not really there?

Director CARDILLO. Thanks, Senator, for the question. I don't think there's a more important issue on my desk or I would offer the desk of my colleagues here and that is at the heart of our profession is integrity and credibility, reliability. That's how we get invited to meetings. That's how we get invited back to meetings to provide a sense of confidence to those that we serve to help them make decisions.

What you just described as both an opportunity, that's the connection with new partners, nontraditional sources, small and large companies and universities, etc. Every one of those connections is also a threat or a risk, because if I'm now plugged into this new source, to gain benefit and understanding coherence, I'm also plugging into every aspect of vulnerability that they have. So we work on this very, very hard.

I obviously count on the experts at NSA and FBI on the digital domain and the hygiene that's necessary. I will also say because it was brought up before, this issue of deepfake. As that technology advances, and it will, I do worry about as a community that needs to seek the truth and then speak the truth—in a world in which we can't agree on what's true, our job becomes much more difficult and so go back to your question.

We have to do a better job at protecting what we do so that when we do show up you have the confidence, you know where it came from, you know how we handled it, you know who did or didn't affect or manipulate it. And so again, it's an issue that's in the center of my desk and all of our concerns.

Senator BLUNT. One more question for you, Director. In your plans for geospatial western, the development of that new facility replacing a 75-year-old facility in St. Louis which is fully redundant with what happens in Springfield, Virginia. The difference you're looking at is that 40 percent of the space in that plan is unclassified.

How does IC work in an unclassified environment? How would you calculate success in your future view of how that works and why would it work that way in plowing some new ground in unclassified space in a classified facility?

Director CARDILLO. The short answer is very carefully. I will expand. So, some four years ago when I stepped into this privileged position, I challenged our team to think differently about our value proposition in a world that is much more open now in which there's many more sources of information, some good and some not so good.

And so I coined a phrase that we need to succeed in the open. I modified that a few months later with some help from my teammates. I said what we really need to do is succeed with the open. And to your point about our new campus in St. Louis, which we couldn't be more excited about by the way the infrastructure is closer to 100 years old. But this is much more than an infrastructure project. I think of this as a new canvas. It's almost 100 acres. We can reimagine our profession on that campus, part of that reimagination needs to be engagement with that open community in a way that's protected and that's knowing about who and what we are plugging into.

So, we couldn't be more excited about the ability to take the opportunity that we have in St. Louis now, to redefine that value proposition in a more open world, in a more connected world, in a world in which we are taking on sources that we know and sources that we need to double and triple check. And so, the 40 percent that you referenced is just an estimate that we have now but we just want to build into that infrastructure knowing that we're going to have to work not just in but with the open and so that's why we've laid out that marker at the beginning.

Senator BLUNT. And General Nakasone, how does this fit into what you do, the whole idea of GEOINT, of individual personal geography, all of the things that we didn't used to have access to that we have access to—now not only using it but using it with confidence?

General NAKASONE. Senator, I think your initial question with regards to the data security is a very important one in the terms of how do we ensure the integrity and assurance of the data that Director Cardillo and the men and women of the NGA have to be able to leverage every single day in support of a number of different requirements whether or not it's policy makers, it's forward forces deployed. Our job is to assist in that and to make sure that that data is well-protected and we can rest assured that when we leverage it, it's the right time at the right place and at the right data that we need to be able to utilize it.

Senator BLUNT. Thank you. Thank you, Chairman.

Director COATS. Mr. Chairman, if I could just add something here. Robert Cardillo is finishing up a 30+ year career of working with the Intelligence Community. He's just one of our crown jewels and we hate to see him moving on to maybe greener pastures and easier times. But he's just been a terrific partner with this team and I just wanted to recognize his contributions have just been exceptional. And he won the best dressed of any of us on the panel award this morning.

Chairman BURR. He does that every time. I just want you to know that, Dan.

Senator Harris.

Senator HARRIS. Thank you, Mr. Chairman, and I join with my colleagues in thanking each of you and the men and women of your agencies for honoring the oath that they have taken and often with great sacrifice. So, thank them, please, from all of us.

This question is for Directors Haspel, Coats, and General Ashley, and it's about North Korea. What would you say is the current

state of the threat from North Korea? And perhaps we can start with Director Haspel.

Director HASPEL. Well briefly, of course the regime is committed to developing a long-range nuclear armed missile that would pose a direct threat to the United States. It is positive that we have managed to engage them in a dialogue. They have taken some voluntary measures to close a site, dismantle a site, but ultimately the objective is to lessen that threat by getting them to declare their program and then ultimately dismantle the program. I think others can probably add to that.

Senator HARRIS. Director Coats.

Director COATS. Well, I affirm what Director Haspel has just said. I think we continue to go into this situation eyes wide open. We want to employ the best of assets we can to understand what the Koreans are thinking—North Koreans are thinking—and what they're doing. We have capabilities which we can talk about in a secure session in terms of how we gather that information and how we assess that to give to our policymakers and to give to the negotiating partners relative to where we're going with North Korea.

We hold to the stated premise that denuclearization is the goal which has to be achieved, but I will at that point just say I want to ensure the American people and ensure everybody listening here that we are fully engaged in providing the essential intelligence needed relative to the negotiations that are going on.

Senator HARRIS. And in this setting can you say, at least since you've been in the position you've been in, that their threat, in terms of their ability to strike the United States, is diminished in any way?

Director COATS. I think the assessments we've made up to this particular point hold. Obviously, as I mentioned in my opening statement, that over this past year we have not seen any evidence. They have not done missile—seen a nuclear missile testing or launching. So that's the position we're in right now. But again, we keep open eyes and open ears to exactly what's going on.

Senator HARRIS. General.

General ASHLEY. So, the technologies that they demonstrated—from a technical standpoint, they showed a capability to have an ICBM function still exists. There still is a substantial military capacity that Kim Jong-un wields. Seventy percent of his forces are along the DMZ. So, the capabilities and threat that existed a year ago are still there.

Senator HARRIS. Thank you, General.

Director Haspel, North Korea has obviously a terrible record of human rights, and they're deeply isolated, obviously, from the international community, and this is the result of many policies, intentional probably mostly. Do you believe that North Korea values the legitimacy that comes with direct diplomatic engagement with the United States?

Director HASPEL. Yes, I think our analysts would assess that they value the dialogue with the United States, and we do see indications that Kim Jong-un is trying to navigate a path toward some kind of better future for the North Korean people.

Senator HARRIS. Are you aware of any intelligence suggesting that his behaviors and their human rights record has improved in any substantial way over the last couple of years?

Director HASPEL. It's obviously something we monitor to the degree possible. I do think that a vision for North Korea that further brings them into the community of nations would have a positive effect on our ability to influence them on important things like human rights.

Senator HARRIS. But over the last couple of years have you seen any change in their behaviors?

Director HASPEL. I don't think I can point to any specific changes over the last couple years.

Senator HARRIS. Thank you. And then Director Coats, changing the subject, I'd like to talk with you a bit about social media. And can you tell us, do we have a written strategy for how we're going to counter the influence operations that target social media in the United States?

Director COATS. We are fully engaged in that issue. We have regular communication among the various sectors of the Intelligence Community. Much of that is shared, both verbally and in written form.

Senator HARRIS. So there is a written strategy?

Director COATS. Not a written single strategy, but we're always looking at how we can best address this. It's a fluid situation. We had an earlier discussion relative to our engagement with private-sector social media companies.

Senator HARRIS. Thank you. My time is running out.

Can you tell us, do you have any intention of having a written strategy that will be agreed to and understood by all members of the IC as it relates to the collective responsibility and individual responsibilities for addressing foreign influence on social media in the United States?

Director COATS. As I said, it's a fluid situation. We are making significant progress on that. In terms of one specific written strategy, something that has to—will have to be looked at in a continuum of change. So, I'm not exactly sure why a written strategy would give us anything more—single strategy—that would complete—have to be modified daily, but you can be assured that it is a top priority, as we have talked about before. It is something that we are working on, and we've seen very significant progress.

Senator HARRIS. Mr. Chairman——

Director COATS. And when you go back and read the transcript of what we talked about before, you'll understand that.

Senator HARRIS. I actually have the transcript from February 13 of 2018 when you and I had this discussion at our last worldwide threats hearing, or at least a previous one, when I asked you then, would you provide us and would there be a written strategy for how the IC is dealing with these threats.

So, can you tell us has there been any advancement on that point since February of 2018?

Director COATS. I'll be happy to get back to you with that.

Senator HARRIS. Thank you.

Director COATS. You were referring to 2017? Is that my understanding?

Senator HARRIS. No, 2018. We're in 2019 now.

Director COATS. 2018. Okay, thank you.

Chairman BURR. Senator Cotton.

Senator COTTON. Thank you all very much for your appearance and your continued service to our Nation, and for all the men and women who work in your organizations serving our country. We've talked a lot about Huawei and ZTE today and the potential threats they pose. Let's just make this concrete for Americans watching at home. You can raise your hand if you respond yes to my questions. How many of you would use a telecom product made by Huawei and ZTE?

Director COATS. Senator, I would person—I would think we ought to talk about these kinds of things in a separate, closed session. These are not all yes and no answers, and I think there is information here that could be better described in a closed session than an open session.

Senator COTTON. Like a professional who has once been on the debate stage and not liked raise-your-hand questions, I'll simply say for the written record, though, that I saw no hands go up, and while I'll defer to the closed session, I suspect if I asked a fairer question, which is how many of you would recommend that people who are not heads of intelligence agencies, like your neighbors, or church members, or high school friends use Huawei and ZTE there would also be six no votes of confidence.

Director Coats, in September the House Intelligence Committee voted by voice vote, which I presume means it was bipartisan—not controversial—to send to you several dozen of their transcripts in their investigation into Russia's interference in our 2016 election so they could release those, pending your classification review.

Where does that review stand?

Director COATS. That's another issue which I would like to discuss in a closed session.

Senator COTTON. Thank you.

Director Haspel, we've spoken some about ISIS today and the threat of ISIS if they were to reform. One ongoing threat from ISIS is that the Syrian Democratic Forces have a number of detainees from ISIS. Do you know how many detainees the SDF currently hold?

Director HASPEL. Senator, we do know the number. In this forum I'll say that they have hundreds of foreign fighters. The IC as a whole is working very, very hard to make sure we know who those are, return people to their country of origin, and to make sure that even as ISIS, as we continue to make gains against them on the battlefield, that these foreign fighters do not—are not able to return to the fight.

And I can be more specific this afternoon in terms of the exact numbers.

Senator COTTON. And could you speak broadly about the types of detainees? Are we talking about foot soldiers? Are we talking about major external operations planners, bomb makers, that sort of thing?

Director HASPEL. All of the above, Senator.

Senator COTTON. So, it would be very bad for our Nation if those detainees were released?

Director HASPEL. I think it would be very bad, and the IC has taken great pains to categorize and make sure we know who these individuals are, and we, of course, are working very closely with our foreign allies to do just that.

Senator COTTON. Thank you.

Director Haspel, I'd like to stay with you and turn our attention to Russia since I know you have a lot of experience with that nation.

Senator COTTON. President Putin has publicly stated that they are working on novel nuclear weapon systems like a nuclear-powered cruise missile, hypersonic glide vehicles, and underwater nuclear-powered torpedo. And just last month, he announced Russia's successful test of a hypersonic glide vehicle which he called a new intercontinental strategic system. Is it the case that some of these systems are being designed to explicitly evade the constraints of the New START Treaty?

Director HASPEL. Senator, I believe—and I can go into more detail this afternoon and I'm sure General Ashley would like to add but—I believe some of these systems have in fact been in development long before New START Treaty.

Senator COTTON. General Ashley, do you have anything to add?

General ASHLEY. Actually, if I could go back real quick to your Huawei question and then I'll come back to that one.

When you look at the technology stuff and I think Huawei and ZTE are great examples, but I think the other complexity is the question really is do you know what's in your phone, not just is it a Huawei or a ZTE phone? Do you know who provided the chips, the software and everything that goes into your phone?

We are tracking everything that you just addressed in terms of Putin. I'm not sure if any of that violates the New START Treaty, because right now, I know that the Russians are in compliance and what as you know New START lays out for the systems it can deliver, it's about 700, they can have 1,550 in the number of warheads and they can have 800 in the latter category in terms of other systems. I'm not aware that this violates and I'll take that one for a little bit of research as well, and we may be able to get that to you in the closed session this afternoon.

Senator COTTON. Thank you.

Director Haspel, one final follow-up question. So even if these systems don't violate the New START Treaty, I believe that both this and the past Administration has said that Russia is violating the Intermediate-Range Nuclear Forces Treaty, the Open Skies Treaty, the Chemical Weapons Convention, the Biological Weapon Convention, the Vienna Document, and is no longer adhering to the Presidential Nuclear Initiatives. Is there any treaty that Russia has with the United States to which they are currently adhering?

Director HASPEL. Well, the Russians obviously would have a different interpretation, but I do believe that you are correct in terms of State Department's assessment of Russian compliance with those treaties.

Senator COTTON. Thank you.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you very much and I want to apologize to all our distinguished panel. We had a major hearing in the Finance Committee.

I'm going to start with the matter of Saudi Arabia and the late Mr. Khashoggi. I'm very concerned that the DNI statement for the record barely mentions the threat posed by Saudi Arabia to the rule of law around the world.

Director Haspel, the Senate unanimously passed a resolution stating its belief that the Crown Prince was responsible for the murder of U.S. resident and journalist Jamal Khashoggi. Is that correct?

Director HASPEL. Senator, we can go into a little bit more detail this afternoon, but as you know during the fall months, we spent a significant amount of time briefing and providing written products on our assessment of what happened to Mr. Jamal Khashoggi.

As you know, and as the Saudi regime itself has acknowledged, 15 individuals traveled to Istanbul and he was murdered at their consulate and it was a premeditated murder on 2 October. The trial in Saudi Arabia, I believe, has begun but in terms of further detail on our assessment of involvement, I'll hold it until the afternoon session.

Senator WYDEN. Respectfully, Madam Director, the Senate unanimously passed a resolution that the Crown Prince was responsible. Was the Senate wrong?

Director HASPEL. Senator, it's my job to provide the intelligence to support the Senate's deliberations, and I think we've done that very adequately in this case and we'll continue to do that. And we continue, by the way, to track this issue and to follow it very closely.

Senator WYDEN. A question for you Director Wray and maybe other panel members.

In my home State there are alarming indications that the Saudi government has helped Saudi nationals accused of serious crimes flee the country and this strikes us as an assault on the rule of law right here in the United States.

My question for the Director, Director Wray, will you look at this and come back with any suggestions about what the FBI can do?

And just so you know what has troubled me so much is what looks like evidence that the Saudi government helped these individuals who have been charged with really serious crimes in my home State: rape and manslaughter, helped them with illicit passports, possibly the prospect of private planes to get out of the country.

Will you look at this and come back with any suggestions about what the Bureau can do here?

Director WRAY. Senator, I appreciate the question. I will say I've actually had occasion to visit the Portland field office not only to meet with all of our employees there but all of our State and local partners across your State and I'd be happy to take a close look at anything you want to send our way on this subject.

Senator WYDEN. Could you get back to me within 10 days? You know we are trying to up the ante here to really get these people back. You know, my sense is like a lot of other things people have a full plate. I've requested travel records. We will be in touch with

your office, but I would like a response within 10 days to show that this is the priority that is warranted.

Director WRAY. Senator, of course we have a lot of priorities as I'm acutely aware of, but I'd be happy to take a look at the information that you have and work with your office.

Senator WYDEN. We have a lot of priorities, but the notion that Saudi Arabia can basically say it is above the law, and that's what it looks like to the people of my home State, is just unacceptable. So, I will be back at this and you and I have talked about matters before and both of us have strong views and that will certainly be the case here.

Let me ask one other question for you, Director Haspel and Director Coats, to change the subject to Russia and particularly these Trump-Putin meetings. According to press reports, Donald Trump met privately with Vladimir Putin and no one in the U.S. Government has the full story about what was discussed.

Director Haspel and Director Coats, would this put you in a disadvantaged position in terms of understanding Russia's efforts to advance its agenda against the United States? A question for you two and then I'm out of time. Thank you for letting me have them respond, Mr. Chairman.

Director COATS. Well, Senator, clearly this is a sensitive issue and it's an issue that we ought to talk about this afternoon. I look forward to discussing that in a closed session.

Senator WYDEN. Mr. Chairman, my time is up. To me from an intelligence perspective, it's just Intel 101 that it would help our country to know what Vladimir Putin discussed with Donald Trump and I will respect the rules. Thank you, Mr. Chairman.

Chairman BURR. Senator Cornyn.

Senator CORNYN. When I reflect on the number of people who lost their lives as a result of man-made causes in World War II, by some estimates as many as 39 million people, when we introduced the atomic bomb and Nagasaki and Hiroshima and think about how much more efficient we've gotten when it comes to killing one another potentially, I wanted to ask you about weapons of mass destruction and counterproliferation.

If the theory behind mutually assured destruction and deterrence is that none of the so-called rational actors, let's say Russia, China, for example, would use nuclear weapons because they realize what the consequences of that would be, we know we have less than rational actors that either have acquired nuclear weapons, thinking about North Korea—certainly Pakistan and India are staring at each other, both of whom have nuclear weapons. I worry that we are not spending as much time as we need to be focusing on what is the most lethal threat to our Nation and also to the world.

Let me ask you specifically about Russia. We know Russia continues to be in material breach of the terms of the Intermediate-Range Nuclear Forces Treaty. Most recently our NATO allies have concluded that Russia is in the process of developing a ground-launched cruise missile that's a direct threat to Euro-Atlantic security.

I personally think it's important for us to adequately fund nuclear modernization programs, including the development of a low-yield warhead and enhance the capabilities of critical missile de-

fense systems. I would also point out that China is not bound by the standards imposed by the INF treaty, further putting the U.S. in a compromising position.

Director Coats, does the Intelligence Community assess that a complete withdrawal of the U.S. from the INF Treaty would pose a significant national security risk to the United States?

Director COATS. Well, that risk is there whether we see Russia within the bounds of the restraints on that or whether we don't, because we know Russia has violated the terms of that treaty and has that capability.

Senator CORNYN. And China's not now——

Director COATS. So, whether we withdraw or not——

Senator CORNYN [continuing]. China's not now at all——

Director COATS. You're—they're still going to have that capability. That's correct.

Senator CORNYN. And Director Haspel, perhaps this would be a question for you.

If the U.S. withdraws from the INF Treaty—and I'd welcome anybody's comment on the panel. If the U.S. withdraws from the INF Treaty, does the IC assess that Russia will place INF range missiles in Cuba, or will they attempt to exert pressure in some other way?

Director HASPEL. Senator, what I can say, and perhaps we can go into more detail this afternoon, is we do see that Russia is very concerned about our decision to withdraw. We do see also consideration of ways they can push back due to their own concerns about our forward posture in Eastern Europe.

I think I'll leave it there for now, and we can elaborate this afternoon. I'll ask if General Ashley would like to add something.

Senator CORNYN. Please.

General ASHLEY. Yeah, I would say that—and we can get into some more detail this afternoon—that their actions are not consistent with the ground-launched cruise missile that you already spoke about. It has already been fielded operationally, so it is in utilization and available.

Their actions and what they would do I think would be symmetric to anything we did to move additional capabilities forward. And then those particular symmetric actions we can talk about in a closed session.

Senator CORNYN. Would anybody on the panel care to talk about my statement with regard to production of a low-yield warhead? Maybe General Ashley? I don't know who would be the appropriate person.

General ASHLEY. So, the comment of whether we should be developing——

Senator CORNYN. Correct.

General ASHLEY. Yeah. I'll have to leave that to the policymakers. What you alluded to is our ability to kill and some of the weapons we've developed, and then the utilization and a strategy that we've heard in the past from the Russians of non-strategic nuclear weapons and whether or not a rational actor would use those kinds of weapons in the field.

We know that the Russians have a first-use policy. The threshold where they think that the Kremlin would be at risk is probably

what would drive that first use, whether that—see that as an escalatory control measure that they would put into place. I'll leave it to the policies—policy folks to determine the utilization of one of those weapons.

When we talk about the use of nuclear weapons specifically, one of the things that—you know, the thresholds are pretty high on their use, which is why we see the manifestations of things like hybrid war. And if you look at great power conflict, it kind of flatlined after World War II and things that have taken place in the world order that has been kind of the outgrowth of Bretton Woods. That—the other thing that has come to bear on keeping great power conflict at bay has been the development of nuclear weapons.

Senator CORNYN. Thank you.

Chairman BURR. Last but not least, Senator Sasse.

Senator SASSE. Thank you, Mr. Chairman. Thank you to all six of you for being here. Thanks for your officers and to their families. You lead and represent a community of folks who often have family disruptions, and there aren't folks who know to thank them. So, on behalf of this Committee and the American people, thank you.

General Nakasone, when you were confirmed before the Armed Services Committee, I asked you a question about whether or not Russia or China had ever suffered a sufficient response to their cyber aggressions to warrant behavior change on their behalf, and you said no, they had not. At this point, in a non-classified setting, how would you answer that question today?

General NAKASONE. So, Senator, I think the—the way that I would answer the question is, first of all, what has changed since you and I talked last year is the fact that I think that, from our work collectively across the interagency and the Government, we have been able to show effectiveness against, primarily in this case, the Russians as we take a look at our midterm elections.

Whether or not that spawns long-term behavior change, I think that's still to be determined. But certainly, this afternoon we can talk a little bit more about some of the things we have seen.

Senator SASSE. Thank you for your work on that and your success. And I know, Director Coats, you're going to give us some briefing on that this afternoon as well. I know that a number of people on the Committee have been anxious to get a more fulsome report of some of the successes of the IC from early November. And I would just like to publicly say, whatever portion of that that we can declassify for the American people to know the successes of the U.S. Government and of your community, I would urge that kind of declassification where possible.

Director Wray, you have many priorities at the Bureau, but can you talk about threats we face with the long-term tech war—tech race, maybe—against China? And domestically when you think about Bureau priorities looking at different Chinese actions inside the United States, how do you rank those priorities?

Director WRAY. Well, first, I would say that the—as I said earlier—that I think China writ large is the most significant counterintelligence threat we face. We have economic espionage investigations, for example—that's just one piece of it—in virtually every one of our 56 field offices. And the number of those has probably doubled over the last three or four years. And almost all of them,

not all of them but most of them, lead back to China. In addition to the——

Senator SASSE. Do you have anywhere near sufficient resources for all those investigations? Many of us used to ask Director Comey about Jihadi threats against the United States. We would regularly ask: is the Bureau sufficiently resourced? And we were told that as long as the U.S. was active killing Jihadis or partnering with allies in Syria to kill a lot of Jihadis who were there, he thought there were sufficient domestic resources in the Bureau.

For counterintelligence and for corporate espionage purposes, are you sufficiently resourced?

Director WRAY. Well, I would say this. If the Congress were to entrust us with more resources, I can assure you we would put them to very good use.

Senator SASSE. We've talked about deepfakes a couple of different times today. Our Intelligence Community is a product of history. Seventeen agencies is not the way anybody would design it from scratch, but that doesn't necessarily mean a reorganization is always simplifying. Oftentimes you create more complexity when you're trying to get rid of some of the duplicative functions that we have across different agencies.

But when you think about the catastrophic potential to public trust and to markets that could come from deep fake attacks, are we—Director Coats and Director Haspel in particular, are we organized in a way that we could possibly respond fast enough to a catastrophic deepfakes attack?

Director COATS. We certainly recognize the threat of emerging technologies and the speed at which that threat increases. We clearly need to be more agile. We need to partner with our private sector.

We need to resource our activities relative to dealing with these known technologies and unknown technologies, which we know are going to appear anytime soon because it's just a very quickly evolving flood of technological change that poses a major threat to the United States and something that the Intelligence Community needs to be restructured to address.

We are in a process of transformation right now which incorporates six major pillars that we have to put resources and activity against, and fast. Cyber, trusted agile workforce, artificial intelligence, private sector partnerships, data management, acquisition agility. All six of these are major issues which we have to transform. We cannot rely on status quo, where we are now. We're the best in the world. We have to stay the best in the world. But we've got real competitors, and technology is giving them the opportunity to shorten that gap very, very significantly.

And so, we have a dedicated commitment to this transformation. It's called IC 2025. What do we have to be in 2025, but let alone 2019 and 2020? And we are using that throughout all 17 agencies in terms of how we have to adapt to that. And that's a major change that this IC has to go through. But we're fully intent on making it happen.

Senator SASSE. Thanks, Director. Before the Chairman gavels out a rookie, Director Haspel, are you confident that we could respond fast enough?

Director HASPEL. I think Director Coats captured it very well. I would say that, while the IC is large and unwieldy in some respects, I don't think in my 34-year career I've seen better coordination or synchronization or collaboration among the agencies to try and stay abreast of the technological challenges.

Senator SASSE. I hear that and I've been reading "Intel Daily" now for 18 months. And the pace of upgraded game on the part of the community is a real testament for all of your leadership, but I still think the asymmetric exposure we have or the barrier to entry for deepfake technology is so low now, lots of entities, short of nation state actors, are going to be able to produce this material and again destabilize not just American public trust, but markets very rapidly. And I think we need to be thinking about not just IC 2025 but IC 2021, 2020, 2019.

General ASHLEY. If I could just real quick just go back to our opening question from the Chairman, when he said are you concerned about our protection of data. So how do you get deepfakes that are really, really good, lots of data? That's how you train your algorithms. So, it goes back to kind of where we started and the ability to protect that information, to preclude the training of those algorithms to a degree where you cannot tell the difference. And again, our challenge is how do you build the algorithm to identify the anomaly because every deep fake as a flaw, at least now they do.

Senator SASSE. Thanks, General.

Vice Chairman WARNER. Thank you, Mr. Chairman. I would just want to make one final brief remark and commend Director Coats on the ongoing efforts to make sure that we get through the backlog on the security clearance reform. The Chairman and I have worked on this very hard. We appreciate the progress that has been made. I hope we can. I think we're down to about 500,000. I think we can do much, much better. And my hope would be that particularly any Federal employee that might have had some level of a credit dinging due to the shutdown would not be penalized through that security clearance process for, again, actions, quite frankly, that they had no ability to remediate. It was our responsibility.

Director COATS. We will continue to operate carefully with you, also. You played a major role in all of this. We have made some progress. It's not enough, it's not fast enough. The shutdown deferred some tasks that we could have accomplished if the process was opened and hopefully we won't have to go through that again.

Chairman BURR. I thank the Vice Chairman for his comments. I promised all of you ample time for nutrition in between sessions and I think we have accomplished that.

I want to thank you for your testimony today in open session. The Intelligence Community has always prided itself on making the impossible happen. You go where others cannot. You find what cannot be found. You discover and uncover and create.

This Committee has been privileged to see behind closed doors some of the truly fantastic innovations that are the products of your drive to accomplish impossible missions. Sometimes these come from the minds of in-house geniuses. Sometimes they are the fruits of successful collaboration with contractors. These public-pri-

vate partnerships have always been at the core of American success stories.

However, as with any good competition, our adversaries have watched carefully, and they seem to be catching up. Director Coats, you note in your statement for the record that for 2019 and beyond, the innovations that drive military and economic competitiveness will increasingly originate outside the United States. As the overall U.S. lead in science and technology shrinks, the capability gap between commercial and military technologies evaporates and foreign actors increase their efforts to acquire top talent companies, data, and intellectual property via licit or illicit means.

Innovation is a global race and we must think about how to foster greater innovation at home, mitigate potential risks, and maintain our competitive edge. There is no easy path, but if we concede the innovation race, not only our global competitiveness, but our national security will in fact be at risk. We need to make sure we are monitoring and acting on threat information as quickly as possible and getting the information to the people who need it the most.

The Federal Government should educate the private sector on threats, which we are, and enable a regulatory and financial environment that enables innovation. In turn the private sector needs to listen better and be constructive and thoughtful partners. The simple truth is that we need each other and only through collaboration can we regain in our lead. The architecture of government must change, and our partnerships must grow.

In closing, please convey this Committee's gratitude to the men and women of the Intelligence Community for the work that they do on a daily basis. The American people should know that their hard work, dedication, and innovation are crucial to protecting this country and the democratic principles on which we stand. Although the threats we now face are dynamic, varied, and numerous, I'm confident the Intelligence Community will continue delivering on their mandate to reduce uncertainty in an increasingly uncertain world. With that, this portion of the hearing is adjourned, and we'll gather again at 1:00 p.m.

[Whereupon the hearing was adjourned at 11:52 a.m.]

Supplemental Material

UNCLASSIFIED RESPONSES TO QUESTIONS FOR THE RECORD
SENATE SELECT COMMITTEE ON INTELLIGENCE
HEARING JANUARY 29, 2019
DIRECTOR OF NATIONAL INTELLIGENCE DANIEL COATS

Hearing Date: **January 29, 2019**
Committee: **SSCI**
Member: **Sen. Wyden**
Witnesses: **DNI Coats**
Info Current as of: **March 21, 2019**

Question: In its decision in *Carpenter v. United States*, the U.S. Supreme Court found that the collection of cell-site location information (CSLI) from wireless providers constituted a search under the Fourth Amendment.

- Have the ODNI or any elements of the Intelligence Community issued any guidance regarding how the *Carpenter* decision should be interpreted and/or applied to intelligence programs and operations?

- If so, please provide any relevant memoranda or guidance.

Answer:

Although the *Carpenter* opinion "does not consider other collection techniques involving foreign affairs or national security"[1] the Intelligence Community, as always, carefully considers all Supreme Court precedent, including *Carpenter*, when evaluating how and whether the Fourth Amendment applies to a proposed intelligence activity. The Intelligence Community will continue to assess the potential implications of the *Carpenter* decision and will, in the event a circumstance arises that might implicate the holding of the decision, provide appropriate guidance to the Intelligence Community agencies at that time. That said, the ODNI has not issued any controlling written Intelligence Community-wide guidance regarding how the Carpenter decision should be interpreted or applied.

[1] *Carpenter v. United States*, 585 U.S., at ___, 134 S. Ct. 2206, at 2220 (June 22, 2018).

Hearing Date: January 29, 2019
Committee: SSCI
Member: Sen. Wyden
Witnesses: DNI Coats
Info Current as of: March 21, 2019

Question: Does the Intelligence Community agree with Mr. Evanina's recommendation that encryption be used to protect U.S. government officials' work and personal unclassified telephone communications?

- **If yes, what steps, if any, has the Intelligence Community taken to communicate this recommendation to agencies and to government officials?**

Answer:

The National Cyber Strategy, signed by the President on September 17, 2018, states that responsibility to secure federal networks, including federal information systems and national security systems, falls squarely on the Federal Government. National Security Directive 42 expands the responsibilities for protecting national security information systems to also include national security telecommunications systems. The Intelligence Community has distributed these documents to all federal agencies and has made continued access available through appropriate websites. Thus, encryption should be used to protect U.S. Government officials' work and associated federal information. Although personal unclassified telephone communications do not fall under the category of official government work and are not required to be afforded such protection, Director Evanina has consistently advocated for strong cyber hygiene practices through the Know the Risk – Raise Your Shield campaign. Through this campaign, Director Evanina has issued tips and guidance to the public on how to protect personal information from being exploited by cyber criminals and foreign intelligence services.

Hearing Date: January 29, 2019
Committee: SSCI
Member: Sen. Heinrich
Witnesses: DNI Coats
Info Current as of: March 21, 2019

Question: **As the government's Security Executive Agent, have you reviewed the Executive Office of the President's process for granting access to classified information for compliance with Executive Order 12968?**

- **If so, is the Executive Office of the President compliant?**

Answer:

Congress has sent several letters seeking information on the security clearance process. To ensure a complete response to all of these questions, responses to this question will be included under separate cover.

Hearing Date: January 29, 2019
Committee: SSCI
Member: Sen. Heinrich
Witnesses: DNI Coats
Info Current as of: March 21, 2019

Question: How often do you conduct such compliance reviews, and when was the last review?

Answer:

Congress has sent several letters seeking information on the security clearance process. To ensure a complete response to all of these questions, responses to this question will be included under separate cover.

○