S. HRG. 115–278

OPEN HEARING ON WORLDWIDE THREATS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

TUESDAY, FEBRUARY 13, 2018

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
28–947 PDF WASHINGTON : 2018

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
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
JOE MANCHIN, West Virginia
KAMALA HARRIS, California

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

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

CONTENTS

FEBRUARY 13, 2018

OPENING STATEMENTS

WITNESS

SUPPLEMENTAL MATERIAL

OPEN HEARING ON WORLDWIDE THREATS

TUESDAY, FEBRUARY 13, 2018

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

The Committee met, pursuant to notice, at 9:35 a.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Burr (presiding), Warner, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Cornyn, Feinstein, Wyden, Heinrich, King, Manchin, Harris, and Reed.

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

Chairman BURR. I'd like to call this hearing on worldwide threats to order, and I'd like to welcome our distinguished witnesses today:

Director of National Intelligence Dan Coats;

Director of the Central Intelligence Agency Mike Pompeo;

Director of the Defense Intelligence Agency General Robert Ashley;

Director of the Federal Bureau of Investment Chris Wray;

Director of the National Security Agency, Admiral Mike Rogers;

And Director of the Geospatial Intelligence Agency Robert Cardillo.

We've got a long day in front of us and I thank all of you for being here. I know how forward you look to this one occasion on an annual basis. Since 1995, this Committee has met in open forum to discuss the security threats facing the United States of America. This has never been, nor will it ever be, a comfortable conversation to have.

The threats this country face are complex, evolving, and without easy answers. They exist in multiple domains. They're asymmetrical and they're conventional. They can be launched from across the ocean or be planned in the heart of our homeland. Nonetheless, this conversation serves a vital purpose and it's essential that it takes place in the public square, with as much detail and candor as is possible.

In my view, that is the true value and public service of this hearing. It provides the American people with insight that they just don't normally get. Those insights are about the spectrum of threats we're up against as a Nation. But, importantly, those insights are also about the work that the intelligence community does to push back on those threats. This is work that is both time-

and labor-intensive. It can be frustrating, heartbreaking, and dangerous. It's often thankless, but because of the tireless dedication and patriotism of men and women who make up our intelligence community, it gets done on behalf of the American people every single day.

To this point, I encourage all the witnesses this morning to not only address the threats to our Nation, but to talk about what their organizations are doing to help secure this country and, to the degree they can in an unclassified setting.

Director Coats, your testimony for the record ties together the expertise, capabilities, and wisdom of the entire intelligence community. I encourage everyone to familiarize themselves with its contents. It's lengthy and it's detailed, and it's a testament to the broad range of talents our IC brings to the table. It's also a compelling reminder of why this country invests so substantially in its intelligence apparatus.

Director Pompeo, when we held this hearing last year I invited you to share your assessments of things on the Korean Peninsula. I'm going to ask you again for your insights on the state of North Korea's nuclear and missile program and, importantly, what's going on politically with North Korea's leadership. Perhaps you can help us differentiate between a genuine effort to reconcile with South Korea and an opportunistic attempt to drive a wedge between Washington and Seoul.

General Ashley, the work just never seems to end for our Defense Department. I would value your latest assessment of the battlefield situations in Syria and Afghanistan. Last week we had U.S. advisors and Kurdish allies come under fire in eastern Syria. This prompted a retaliatory strike that killed dozens of pro-regime forces.

In Afghanistan, a string of terrorist attacks in Kabul left 150 dead last month, suggesting to me that, after 16 years of war, the insurgency is nowhere near folding and the government remains hard-pressed to provide the security needed for its own people. I'd particularly value your unvarnished appraisal of where progress is being made in Afghanistan and where it's not.

Admiral Rogers, cyber is clearly the most challenging threat vector this country faces. It's also one of the most concerning, given how many aspects of our daily lives in the United States can be disrupted by a well-planned, well-executed cyber-attack. I'd appreciate your assessment of how well we're doing when it comes to protecting the Nation's most critical computer networks. From the systems that guide our military to the networks that ensure the Nation's energy supply, they are all essential to the functionality of a modern America, and I fear that they're increasingly vulnerable to state and non-state actors.

Director Wray, I'm keenly interested in hearing your assessment of the threat posed by the spread of foreign technology in the United States. This Committee has worked diligently to sound the alarm bells when it comes to the counterintelligence and information security risks that come prepackaged with the goods and services of certain overseas vendors.

The focus of my concern today is China, and specifically Chinese telecom, like Huawei and ZTE, that are widely understood to have

extraordinary ties to the Chinese government. I hope you'll share your thoughts on this, and I also ask you to provide your insights into how foreign commercial investments and acquisitions are jeopardizing the Nation's most sensitive technologies.

Lastly, I'd like to spend a moment on the counterintelligence threat to our national academic, research, and laboratory construct. What's the scale of the problem and what's the FBI doing to fight it?

Finally, Director Cardillo, we've come to associate NGA with the modernization of the intelligence community. The adversaries of this country are investing in innovating faster and with fewer constraints than we have. The threats we face are multidimensional, decentralized, and global. NGA has played an essential role in pushing the envelope with new ways of tackling problems, like having more data than you can feasibly analyze.

As the IC edges closer to automation, machine learning, and eventually artificial intelligence, the computer learning and computer vision work at NGA will be a bridge to help us get there. I look forward to your thoughts on what's next at NGA and how the intelligence community as a whole can make better use of innovation and technology to advance intelligence disciplines that have not changed much in the past 60 years. Our adversaries aren't going to wait for us to catch up.

I'll close there because we have a lot to get to, but I want to thank you and, more importantly, I want to thank those who are not here with you, those who carry out the lion's share of the work on behalf of the American people, the intelligence community. The folks you represent are important to this Committee. We can't do our oversight without the work they perform.

Before turning to the distinguished Vice Chairman, I'd like to highlight for my colleagues: We will reconvene at 2:30 this afternoon in a closed session to hear from the same witnesses in a classified setting. I would ask Members to please reserve anything that remotely gets into a classified question for the afternoon session.

With that, Vice Chairman.

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

Vice Chairman WARNER. Thank you, Mr. Chairman, and let me also welcome all of you here and echo the Chairman's comments. Thank you all for your service and we hope you will convey back to all the brave men and women who work for you, that this Committee will always have your back.

I think this open hearing comes at an extraordinarily important time. Our Nation's intelligence agencies stand at the forefront of our defense against continuing threats from terrorist groups, extremist ideology, rogue regimes, nuclear proliferation, and regional instability.

We all know—and we discussed this at length—in recent years we've also seen the rise of nations who view themselves at least as competitors, if not as adversaries, of the United States. They've begun to use, utilize, new asymmetric weapons to undercut our democratic institutions, to steal our most sensitive intellectual property.

Let me start with Russia. Obviously, certain questions remain with respect to the true extent of the Russian interference in the 2016 elections, and we'll continue to work through them in a bipartisan way on this Committee. However, I think you'll find a broad bipartisan consensus on this Committee on a number of critical issues:

First, that Russia engaged in a coordinated attack to undermine our democracy;

Second, that effort included targeting of State and local elections, electoral activities, in 21 states;

And third, the Russian effort, in a new area, utilized our social media platforms to push and spread misinformation at an unprecedented scale.

Now, we've had more than a year to get our act together and address the threat posed by Russia and implement a strategy to deter further attacks. But I believe, unfortunately, we still don't have a comprehensive plan.

Two weeks ago, Director Pompeo publicly stated that he had every expectation that Russia will try to influence our upcoming elections. Secretary of State Tillerson just last week said that we're already seeing Russian efforts to meddle in the 2018 elections. But I believe, in many ways, we're no better prepared than we were in 2016. Make no mistake, this threat did not begin in 2016, and it certainly didn't end with the election. What we are seeing is a continuous assault by Russia to target and undermine our democratic institutions, and they're going to keep coming at us.

Despite all this, the President, inconveniently, continues to deny the threat posed by Russia. He didn't increase sanctions on Russia when he had a chance to do so. He hasn't even tweeted a single concern.

This threat I believe demands a whole-of-government response, and that response needs to start with leadership at the top.

At the same time, other threats to our institutions come from right here at home. There have been some, aided and abetted by Russian internet bots and trolls, who've attacked the basic integrity of the FBI and the Justice Department. This is a dangerous trend. This campaign of innuendo and misinformation should alarm all of us, regardless of our partisan affiliation.

In addition to this ongoing threat from Russia, I'm concerned that China has developed an all-of-society, not just all-of-government, but all-of-society, approach to gain access to our sensitive technologies and intellectual property. I'm paying a great deal of attention to the rise of China's tech sector. In particular, I'm worried about the close relationship between the Chinese government and Chinese technology firms, particularly in the area of commercialization of our surveillance technology and efforts to shape telecommunication equipment markets.

I want to ensure that the IC is tracking the direction that China's tech giants are heading, and especially the extent to which they are beholden to the Chinese government. In recent years we've seen major technology firms whose rise is attributed in part to their illicit access to U.S. technology and IP. These companies now represent some of the leading market players globally. Most Americans have not heard of all of these companies, but as they

enter Western economic markets we want to ensure that they play by the rules. We need to make sure that this is not a new way for China to gain access to sensitive technology.

There are a number of other concerns I hope to raise both in the hearing this morning and in the closed hearing this afternoon. Let me just briefly mention two. First, how is the IC poised to track foreign influence that relies on social media and misinformation? Just last week, the Chairman and I had a good management with our UK parliamentary colleagues investigating this issue. Russian trolls and bots continue to push divisive content both in the United States and against all our allies in Europe, not only the UK, but, as we talked before, France, Germany, Netherlands. We also heard recent indications of Russian activities in Mexico. The IC needs to stay on top of this issue and I am worried that we don't have a clear line of assignment.

Let me also raise another issue. I believe we need to do more to reform the broken security clearance system, which GAO recently placed on its list of high-risk government programs in need of reform. We've seen close to 700,000 folks now waiting in line, folks that need to serve our country, whether in government or in the private sector, who have been just waiting way too long to get their security clearances. It's obviously hampering your recruitment and retention, and it's costing us millions of dollars in inefficiency.

Again, thank you to all of you for your service. Please convey our best wishes to the men and women who work with you, and I look forward to our hearing.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Vice Chairman.

I'm going to recognize Director Coats and he is the only one who will give official testimony. All members of the panel are open for questions. I will recognize our Members by order of seniority for up to five minutes.

With that, Director Coats, the floor is yours.

STATEMENT OF DANIEL R. COATS, DIRECTOR OF NATIONAL INTELLIGENCE; ACCOMPANIED BY: MICHAEL POMPEO, DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY; ADMIRAL MICHAEL ROGERS, DIRECTOR OF THE NATIONAL SECURITY AGENCY; LIEUTENANT GENERAL ROBERT ASHLEY, DIRECTOR OF THE DEFENSE INTELLIGENCE AGENCY; CHRIS WRAY, DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION; AND ROBERT CARDILLO, DIRECTOR OF THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Director COATS. Mr. Chairman, thank you. I want to start by apologizing for my raspy voice. I've been fighting through some of the crud that's going around, that several of us have endured. I may have to clear my throat a few times, which I apologize for.

But it strikes me, listening to your opening remarks and the Vice Chairman's opening remarks that we have continued to have a very interactive presence with this Committee. The issues that you and the Vice Chairman have raised and that others will raise are issues that we talk about continuously with you, and we want to continue to work with you carefully by both sides of the aisle here,

as we go forward looking at what the intelligence community can provide for this Committee and the issues that we find in common.

Vice Chairman Warner, Members of the Committee: We thank you for the opportunity to be with you here today. There have been some changes on the panel since we were here last year. This will be Admiral Rogers' last visit before this Committee on the threat assessment issue. He deeply regrets not having to come before you in the future years, as he's enjoyed this process so very much.

Chairman BURR. We're considering an emeritus status so that he can be annually invited back.

[Laughter.]

Director COATS. We have two new members, Director Wray and General Ashley, who have been looking forward to this day, I'm sure, with great anticipation.

I say all that because what you are looking at here is a team, a team that works together in terms of how we provide the American people, Congress, and policymakers with the intelligence that they need. So it's an honor for us to be here, and I think this team reflects the hard work of the intelligence community in their testimonies and their answers to questions today.

Before I begin the sobering portion of my remarks, let me take a moment to acknowledge a positive development for the intelligence community and express our thanks to Members of this Committee for their support in the renewing of the authorities in the recent 702 authorization. This is, as we have told you, our most important legislative issue because it is our most important collection issue against foreign terrorists and threats to America, and we appreciate the work that the Committee has done and others have done, and particularly this team has done, in reaching that goal.

As you will hear during these remarks, we face a complex, volatile, and challenging threat environment. The risk of inter-state conflict is higher than at any time since the end of the Cold War, all the more alarming because of the growing development and use of weapons of mass destruction by state and non-state actors.

Our adversaries as well as other malign actors are using cyber and other instruments of power to shape societies and markets, international rules and institutions, and international hot spots to their advantage. We have entered a period that can best be described as a race for technological superiority against our adversaries, who seek to sow division in the United States and weaken U.S. leadership, and non-state actors, including terrorists and criminal groups, are exploiting weak state capacity in Africa, the Middle East, Asia, and Latin America, causing instability and violence both within states and among states.

In the interest of saving time for your questions, I will not cover every topic in my opening remarks. I think that will be a relief to the Committee. We are submitting a written statement, however, for the record with additional details.

Let me turn to global threats, and I'd like to start with the cyber threat, which is one of my greatest concerns and top priorities. Frankly, the United States is under attack, under attack by entities that are using cyber to penetrate virtually every major action that takes place in the United States. From U.S. businesses to the

Federal Government to State and local governments, the United States is threatened by cyber-attacks every day.

While Russia, China, Iran, and North Korea pose the greatest cyber threats, other nation-states, terrorist organizations, transnational criminal organizations, and ever more technically capable groups and individuals use cyber operations to achieve strategic and malign objectives. Some of these actors, including Russia, are likely to pursue even more aggressive cyber-attacks with the intent of degrading our democratic values and weakening our alliances. Persistent and disruptive cyber operations will continue against the United States and our European allies, using elections as opportunities to undermine democracy, sow discord, and undermine our values.

Chinese cyber espionage and cyber-attack capabilities will continue to support China's national security and economic priorities. Iran will try to penetrate U.S. and allied networks for espionage and lay the groundwork for future cyber-attacks. And North Korea will continue to use cyber operations to raise funds, launch attacks, and gather intelligence against the United States. Terrorists will use the internet to raise funds and promote their malign messages. Criminals will exploit cyber tools to finance their operations.

My next topic for you is weapons of mass destruction, WMD. Overall, state efforts to modernize, develop, or acquire WMD, their delivery systems, or the underlying technologies constitute a major threat to the United States and to our allies. North Korea will be the most volatile and confrontational WMD threat in the coming year. In addition to its ballistic missile tests and growing number of nuclear warheads for these missiles, North Korea will continue its longstanding chemical and biological warfare programs.

Russia will remain the most capable WMD power and is expanding its nuclear weapon capabilities. China will continue to expand its weapons of mass destruction options and diversify its nuclear arsenal. Iran's implementation of the Joint Comprehensive Plan of Action, the JCPoA, has extended the time it would take to develop a nuclear weapon from several months to about a year, provided Iran continues to adhere to the deal's major provisions.

Pakistan is developing new types of nuclear weapons, including short-range tactical weapons. And state and non-state actors, including the Syrian regime and ISIS, the remnants of ISIS in Syria, continue to possess and, in some cases, have used chemical weapons in Syria and Iraq, and we continue to be concerned about some of these actors' pursuit of biological weapons.

Turning now to terrorism, the terrorism threat is pronounced and spans the sectarian spectrum from ISIS and Al-Qaeda to Lebanese Hezbollah and other affiliated terrorist organizations, as well as the state-sponsored activities of Iran. U.S.-based home-grown violent extremists, including inspired and self-radicalized individuals, represent the primary and most different to detect Sunni terrorism threat in the United States.

ISIS' claim to having a functioning caliphate that governs populations is all but thwarted. However, ISIS remains a threat and will likely focus on regrouping in request and Syria, particularly in ungoverned portions of those countries, enhancing its global presence, championing its cause, planning international attacks, and

encouraging members and sympathizers to attack their home countries.

Meanwhile, Al-Qaeda almost certainly will remain a major actor in global terrorism as it continues to prioritize a long-term approach and the organization remains intent on attacking the United States and U.S. interests abroad.

Now, moving on, as if we don't have enough threats here on Earth, we need to look to the heavens: threats in space. The global expansion of the space industry will extend space-enabled capabilities and situational awareness to nation-state and commercial space actors in the coming years. Russia and China will continue to expand to space-based reconnaissance, communications, and navigation systems in terms of numbers of satellites, breadth of capability, and applications for use. Both Russian and Chinese counter-space weapon will mature over the next few years, as each country pursues anti-satellite weapons as a means to reduce U.S. and allied military effectiveness and perceptions of U.S. military advantage in space.

The final functional topic is transnational organized crime, which poses a growing threat to U.S. and allied interests. These criminal groups will supply the dominant share of illicit drugs, fueling record mortality rates among our population. They will continue to traffic in human life. They will deplete national resources and siphon money from governments and the global economy.

I'd like to briefly go around the world on regional topics, starting with East Asia. You know, if you went out and hired a private plane and launched from Los Angeles and went around the world and stopped at every hot spot in this world, you would make multiple dozens of stops. That's the kind of threat that we face.

But let me start with East Asia. North Korea continues to pose an ever more increasing threat to the United States and its interests. Pyongyang has repeatedly stated that it does not intend to negotiate its nuclear weapons and missiles away, because the regime views nuclear weapons as critical to its security. Kim also probably sees nuclear ICBMs as leverage to achieve his long-term strategic ambition to end Seoul's alliance with Washington and to eventually dominate the peninsula.

In the wake of its ICBM tests last year, we expect to see North Korea press ahead with additional missile tests this year, and its foreign minister has threatened an atmospheric nuclear test over the Pacific. Pyongyang is committed to fielding a long-range nuclear-armored missile capable of posing a direct threat to the United States, and modest improvements in North Korea's conventional capabilities will continue to pose an ever greater threat to South Korea, Japan, and U.S. targets in those countries.

China will increasingly seek to expand its regional influence and shape even this and outcomes globally. It will take a firm stance on its claims to the East China Sea and South China Sea, its relations with Taiwan and its regional economic engagement. China also intends to use its "One Belt, One Road" initiative to increase its reach to geostrategic locations across Eurasia, Africa, and the Pacific.

From East Asia we head to South Asia. In Afghanistan, Kabul continues to bear the brunt of the Taliban-led insurgency, as dem-

onstrated by recent attacks in the city. Afghan National Security Forces face unsteady performance, but, with coalition support, probably will maintain control of most major population centers.

Complicating the Afghanistan situation, however, is our assessment that Pakistan-based militant groups continue to take advantage of their safe havens to conduct attacks in India and Afghanistan, including U.S. interests therein.

Pakistani military leaders continue to walk a delicate line. Ongoing Pakistani military operations against the Taliban and associated groups probably reflect the desire to appear more proactive and responsive to our requests for more actions against these groups. However, the actions taken thus far do not reflect a significant escalation of the pressure against these groups and are unlikely to have a lasting effect.

In the last month, the Administration has designed—excuse me—designated eight militants affiliated with the Taliban, Haqqani Network, and other Pakistani militant groups, and we assess that Pakistan will maintain ties to these militants while restricting counter-terrorism cooperation with the United States.

Next is Russia, where President Putin will continue to rely on assertive foreign policies to shape outcomes beyond Russia's borders. Putin will resort to more authoritarian tactics to maintain control amid challenges to his rule.

With respect to Russia influence efforts, let me be clear: The Russians utilize this tool because it's relatively cheap, it's low-risk, it offers what they perceive as plausible deniability, and it's proven to be effective at sowing division. We expect Russia to continue using propaganda, social media, false flag personas, sympathetic spokesmen, and other means to influence, to try to build on its wide range of operations and exacerbate social and political fissures in the United States. There should be no doubt that Russia perceives its past efforts have been successful and views the 2018 U.S. midterm elections as a potential target for Russian influence operations.

From Russia I'll turn to the Middle East and North Africa. This region will be characterized by political turmoil, economic fragility, and civil and proxy wars in the coming year. Iran will remain the most prominent state sponsor of terrorism and adversary in the Middle East, especially in Iraq, Syria, and Yemen. Iran will seek to expand its regional influence and will exploit the fight against ISIS to solidify partnerships and translate battlefield gains into political, security, and economic agreements.

We also assess that Iran will continue to develop military capabilities that threaten U.S. forces and U.S. allies in the region. For example, Iran has the largest ballistic missile force in the Middle East. The Islamic Revolutionary Guard Corps navy and its unsafe and unprofessional interactions pose a risk to U.S. naval and allied naval operations in the Persian Gulf. And Lebanese Hezbollah, with the support of Iran, has deployed thousands of fighters to Syria and provides direction to other militant and terrorist groups, all fomenting regional instability. Iran's provocative and assertive behavior, as we saw most recently this past weekend in northern Israel, increases the potential for escalation.

Turkey will seek to thwart Kurdish ambitions in the Middle East and the ongoing Turkish incursion into northern Syria is complicating ongoing counter-ISIS activities in the region and increases the risk to U.S. forces located in the area.

Syria will face unrest and fighting through 2018, even as Damascus recaptures urban areas and violence decreases in some areas.

Iraq is likely to face a lengthy period of political turmoil and conflict. The social and political challenges that gave rise to ISIS remain and Iran has exploited those challenges to deepen its influence in Iraq's military and security elements, diplomatic and political arms.

The war in Yemen between the Iranian-backed Houthis and the Saudi-led coalition is likely to continue and will worsen the already tragic humanitarian crisis for 70 percent of the population of about 20 million people in need of assistance. The situation in Yemen is emblematic of a far larger problem: The number of people displaced by conflict around the world is the highest that it's been since the end of World War II.

Turning to Europe, where I want to draw your attention to two significant developments that are likely to continue to impact European politics and foreign policy in the coming year, let me state first: The continent's center of gravity appears to be shifting to France, where President Macron has taken a more assertive role in addressing European global challenges. The results of the recent German election I think enforce that assessment.

Second, recent efforts by some governments in Central and Eastern Europe to undermine judicial independence and parliamentary oversight and increase government control over public media are weakening the rule of law. These steps could presage further democratic decline and offer opportunity for Chinese and Russian influence.

There are many more topics I could discuss. I haven't even gotten to the Western Hemisphere or Africa. But I would like to close with a discussion of one additional threat, this one internal and somewhat personal. I am concerned that our increasing fractious political process, particularly with respect to Federal spending, is threatening our ability to properly defend our Nation, both in the short term and especially in the long term. The failure to address our long-term fiscal situation has increased the national debt to over $20 trillion and growing. This situation is unsustainable, as I think we all know, and represents a dire threat to our economic and national security.

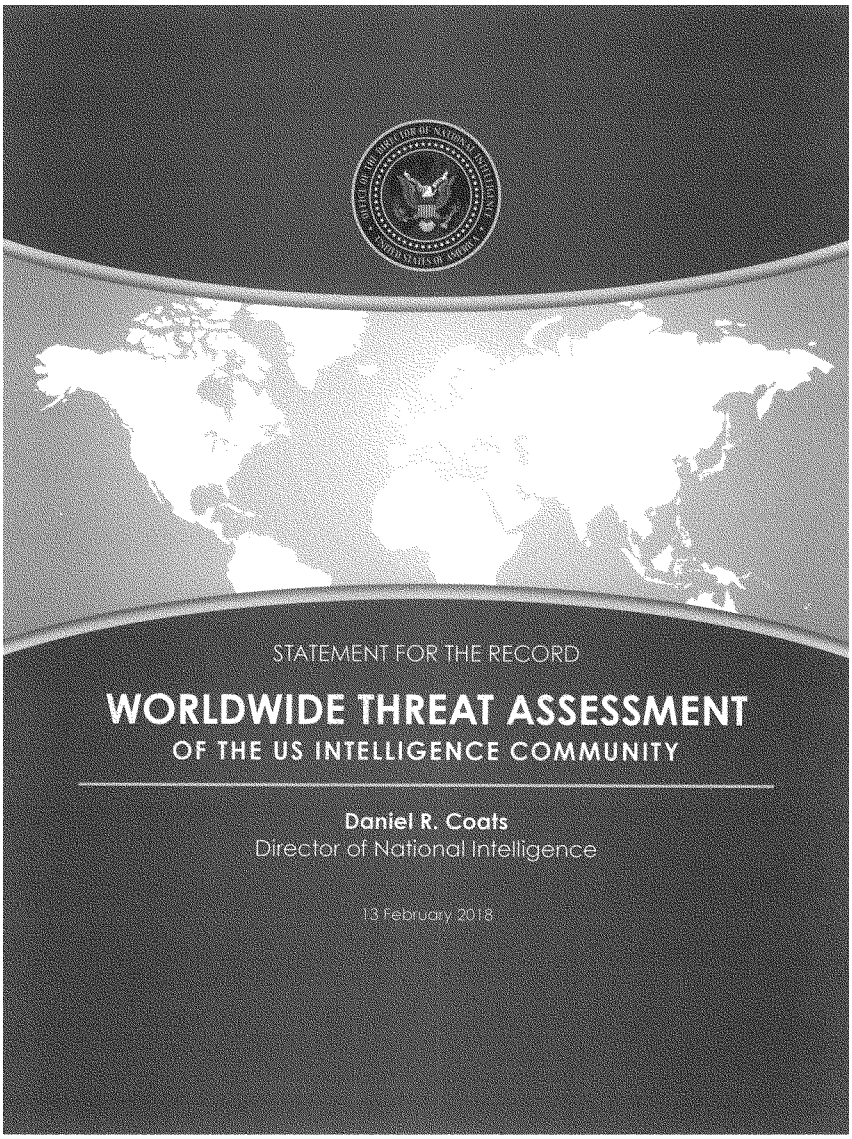
Former Chairman of the Joint Chiefs of Staff Mike Mullen first identified the national debt as the greatest threat to our national security. Since then he has been joined by numerous respected national security leaders of both parties, including former Secretaries of State Madeleine Albright and Henry Kissinger, as well as former Defense Secretaries Bob Gates and Leon Panetta; and our current Defense Secretary Jim Mattis agrees with this assessment.

Many of you know I have spent a lot of time in my last term in the Senate working on this issue and, unfortunately, the problem continues to grow. So I would urge all of us to recognize the need to address this challenge and to take action as soon as possible, be-

fore a fiscal crisis occurs that truly undermines our ability to ensure our national security.

With that, I and the rest of the panel are happy to take your questions. We appreciate the opportunity to be with you today. Thank you, Mr. Chairman.

[The prepared statement of Director Coats follows:]


STATEMENT FOR THE RECORD
WORLDWIDE THREAT ASSESSMENT
OF THE US INTELLIGENCE COMMUNITY
Daniel R. Coats
Director of National Intelligence
13 February 2018

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT
of the
US INTELLIGENCE COMMUNITY

February 13, 2018

INTRODUCTION

Chairman Burr, Vice Chairman Warner, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2018 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 8 February 2018 was used in the preparation of this assessment.

CONTENTS

FOREWORD

Competition among countries will increase in the coming year as major powers and regional aggressors exploit complex global trends while adjusting to new priorities in US foreign policy. The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War. The most immediate threats of regional interstate conflict in the next year come from North Korea and from Saudi-Iranian use of proxies in their rivalry. At the same time, the threat of state and nonstate use of weapons of mass destruction will continue to grow.

- Adversaries and malign actors will use all instruments of national power—including information and cyber means—to shape societies and markets, international rules and institutions, and international hot spots to their advantage.

- China and Russia will seek spheres of influence and to check US appeal and influence in their regions. Meanwhile, US allies' and partners' uncertainty about the willingness and capability of the United States to maintain its international commitments may drive them to consider reorienting their policies, particularly regarding trade, away from Washington.

- Forces for geopolitical order and stability will continue to fray, as will the rules-based international order. New alignments and informal networks—outside traditional power blocs and national governments—will increasingly strain international cooperation.

Tension within many countries will rise, and the threat from Sunni violent extremist groups will evolve as they recoup after battlefield losses in the Middle East.

- Slow economic growth and technology-induced disruptions in job markets are fueling populism within advanced industrial countries and the very nationalism that contributes to tension among countries.

- Developing countries in Latin America and Sub-Saharan Africa face economic challenges, and many states struggle with reforms to tamp down corruption. Terrorists and criminal groups will continue to exploit weak state capacity in Africa, the Middle East, and Asia.

- Challenges from urbanization and migration will persist, while the effects of air pollution, inadequate water, and climate change on human health and livelihood will become more noticeable. Domestic policy responses to such issues will become more difficult—especially for democracies—as publics become less trusting of authoritative information sources.

GLOBAL THREATS

CYBER THREATS

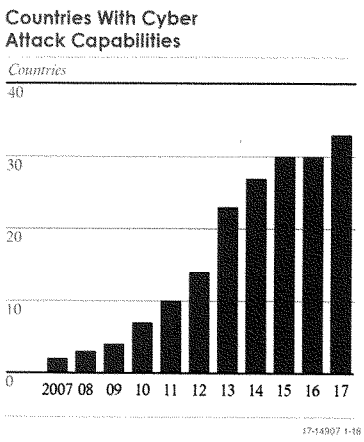
The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits. The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war.

- In 2016 and 2017, state-sponsored cyber attacks against Ukraine and Saudi Arabia targeted multiple sectors across critical infrastructure, government, and commercial networks.
- Ransomware and malware attacks have spread globally, disrupting global shipping and production lines of US companies. The availability of criminal and commercial malware is creating opportunities for new actors to launch cyber operations.
- We assess that concerns about US retaliation and still developing adversary capabilities will mitigate the probability of attacks aimed at causing major disruptions of US critical infrastructure, but we remain concerned by the increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage.

Adversaries and Malign Actors Poised for Aggression

Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations. Nonstate actors will continue to use cyber operations for financial crime and to enable propaganda and messaging.

- The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners.



Russia. We expect that Russia will conduct bolder and more disruptive cyber operations during the next year, most likely using new capabilities against Ukraine. The Russian Government is likely to build on the wide range of operations it is already conducting, including disruption of Ukrainian energy-distribution networks, hack-and-leak influence operations, distributed denial-of-service attacks, and false flag operations. In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy.

China. China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities. The IC and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral US-China cyber commitments of September 2015. Most detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. China since 2015 has been advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015.

Iran. We assess that Iran will continue working to penetrate US and Allied networks for espionage and to position itself for potential future cyber attacks, although its intelligence services primarily focus on Middle Eastern adversaries—especially Saudi Arabia and Israel. Tehran probably views cyberattacks as a versatile tool to respond to perceived provocations, despite Iran's recent restraint from conducting cyber attacks on the United States or Western allies. Iran's cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector.

North Korea. We expect the heavily sanctioned North Korea to use cyber operations to raise funds and to gather intelligence or launch attacks on South Korea and the United States. Pyongyang probably has a number of techniques and tools it can use to achieve a range of offensive effects with little or no warning, including distributed denial of service attacks, data deletion, and deployment of ransomware.

- North Korean actors developed and launched the WannaCry ransomware in May 2017, judging from technical links to previously identified North Korean cyber tools, tradecraft, and operational infrastructure. We also assess that these actors conducted the cyber theft of $81 million from the Bank of Bangladesh in 2016.

Terrorists and Criminals. Terrorist groups will continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations. Given their current capabilities, cyber operations by terrorist groups mostly likely would result in personally identifiable information (PII) disclosures, website defacements, and denial-of-service attacks against poorly protected networks. Transnational criminals will continue to conduct for-profit cyber-enabled crimes, such as theft and extortion against US networks. We expect the line between criminal and nation-state activity to become increasingly blurred as states view cyber criminal tools as a relatively inexpensive and deniable means to enable their operations.

WEAPONS OF MASS DESTRUCTION AND PROLIFERATION

State efforts to modernize, develop, or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and its allies. Both state and nonstate actors have already demonstrated the use of chemical weapons in Iraq and Syria. Biological and chemical materials and technologies—almost always dual-use—move easily in the globalized economy, as do personnel with the scientific expertise to design and use them for legitimate and illegitimate purposes. Information about the latest discoveries in the life sciences also diffuses rapidly around the globe, widening the accessibility of knowledge and tools for beneficial purposes and for potentially nefarious applications.

Russia

Russia has developed a ground-launched cruise missile (GLCM) that the United States has declared is in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. Despite Russia's ongoing development of other Treaty-compliant missiles with intermediate ranges, Moscow probably believes that the new GLCM provides sufficient military advantages to make it worth risking the political repercussions of violating the INF Treaty. In 2013, a senior Russian administration official stated publicly that the world had changed since the INF Treaty was signed in 1987. Other Russian officials have made statements complaining that the Treaty prohibits Russia, but not some of its neighbors, from developing and possessing ground-launched missiles with ranges between 500 and 5,500 kilometers.

China

The Chinese People's Liberation Army (PLA) continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China's strategic deterrent by providing a second-strike capability. China also has tested a hypersonic glide vehicle. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines—armed with JL-2 SLBMs—give the PLA Navy its first long-range, sea-based nuclear capability. The Chinese have also publicized their intent to form a triad by developing a nuclear-capable next-generation bomber.

Iran and the Joint Comprehensive Plan of Action

Tehran's public statements suggest that it wants to preserve the Joint Comprehensive Plan of Action because it views the JCPOA as a means to remove sanctions while preserving some nuclear capabilities. Iran recognizes that the US Administration has concerns about the deal but expects the other participants—China, the EU, France, Germany, Russia, and the United Kingdom—to honor their commitments. Iran's 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, provided Iran continues to adhere to the deal's major provisions. The JCPOA has also enhanced the transparency of Iran's nuclear activities, mainly by fostering improved access to Iranian nuclear facilities for the IAEA and its investigative authorities under the Additional Protocol to its Comprehensive Safeguards Agreement.

Iran's ballistic missile programs give it the potential to hold targets at risk across the region, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Tehran's desire to deter the United States might drive it to field an ICBM. Progress on Iran's space program, such as the launch of the Simorgh SLV in July 2017, could shorten a pathway to an ICBM because space launch vehicles use similar technologies.

North Korea

North Korea will be among the most volatile and confrontational WMD threats to the United States over the next year. North Korea's history of exporting ballistic missile technology to several countries, including Iran and Syria, and its assistance during Syria's construction of a nuclear reactor—destroyed in 2007—illustrate its willingness to proliferate dangerous technologies.

In 2017 North Korea, for the second straight year, conducted a large number of ballistic missile tests, including its first ICBM tests. Pyongyang is committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States. It also conducted its sixth and highest yield nuclear test to date.

We assess that North Korea has a longstanding BW capability and biotechnology infrastructure that could support a BW program. We also assess that North Korea has a CW program and probably could employ these agents by modifying conventional munitions or with unconventional, targeted methods.

Pakistan

Pakistan continues to produce nuclear weapons and develop new types of nuclear weapons, including short-range tactical weapons, sea-based cruise missiles, air-launched cruise missiles, and longer-range ballistic missiles. These new types of nuclear weapons will introduce new risks for escalation dynamics and security in the region.

Syria

We assess that the Syrian regime used the nerve agent sarin in an attack against the opposition in Khan Shaykhun on 4 April 2017, in what is probably the largest chemical weapons attack since August 2013. We continue to assess that Syria has not declared all the elements of its chemical weapons program to the Chemical Weapons Convention (CWC) and that it has the capability to conduct further attacks. Despite the creation of a specialized team and years of work by the Organization for the Prohibition of Chemical Weapons (OPCW) to address gaps and inconsistencies in Syria's declaration, numerous issues remain unresolved. The OPCW-UN Joint Investigative Mechanism (JIM) has attributed the 4 April 2017 sarin attack and three chlorine attacks in 2014 and 2015 to the Syrian regime. Even after the attack on Khan Shaykhun, we have continued to observe allegations that the regime has used chemicals against the opposition.

ISIS

We assess that ISIS is also using chemicals as a means of warfare. The OPCW-UN JIM concluded that ISIS used sulfur mustard in two attacks in 2015 and 2016, and we assess that it has used chemical weapons in numerous other attacks in Iraq and Syria.

TERRORISM

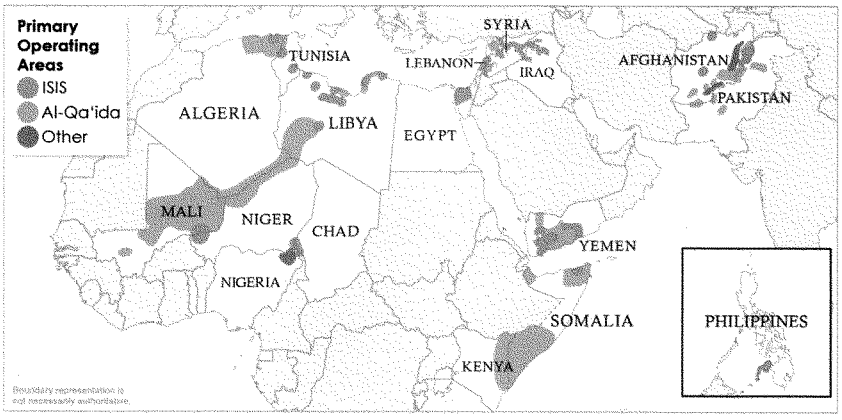
Sunni violent extremists—most notably ISIS and al-Qa'ida—pose continuing terrorist threats to US interests and partners worldwide, while US-based homegrown violent extremists (HVEs) will remain the most prevalent Sunni violent extremist threat in the United States. Iran and its strategic partner Lebanese Hizballah also pose a persistent threat to the United States and its partners worldwide.

Sunni Violent Extremism

Sunni violent extremists are still intent on attacking the US homeland and US interests overseas, but their attacks will be most frequent in or near conflict zones or against enemies that are more easily accessible.

- Sunni violent extremist groups are geographically diverse; they are likely to exploit conflict zones in the Middle East, Africa, and Asia, where they can co-mingle terrorism and insurgency.
- ISIS and al-Qa'ida and their respective networks will be persistent threats, as will groups not subordinate to them, such as the Haqqani Taliban Network.

Sunni Violent Extremists' Primary Operating Areas as of 2017



17-15890 12-17

ISIS

Over the next year, we expect that ISIS is likely to focus on regrouping in Iraq and Syria, enhancing its global presence, championing its cause, planning international attacks, and encouraging its members and sympathizers to attack in their home countries. ISIS's claim of having a functioning caliphate that governs populations is all but thwarted.

- ISIS core has started—and probably will maintain—a robust insurgency in Iraq and Syria as part of a long-term strategy to ultimately enable the reemergence of its so-called caliphate. This activity will challenge local CT efforts against the group and threaten US interests in the region.

- ISIS almost certainly will continue to give priority to transnational terrorist attacks. Its leadership probably assesses that, if ISIS-linked attacks continue to dominate public discourse, the group's narrative will be buoyed, it will be difficult for the counter-ISIS coalition to portray the group as defeated, and the coalition's will to fight will ultimately weaken.

- Outside Iraq and Syria, ISIS's goal of fostering interconnectivity and resiliency among its global branches and networks probably will result in local and, in some cases, regional attack plans.

Al-Qa'ida

Al-Qa'ida almost certainly will remain a major actor in global terrorism because of the combined staying power of its five affiliates. The primary threat to US and Western interests from al-Qa'ida's global network through 2018 will be in or near affiliates' operating areas. Not all affiliates will have the intent and capability to pursue or inspire attacks in the US homeland or elsewhere in the West.

- Al-Qa'ida's affiliates probably will continue to dedicate most of their resources to local activity, including participating in ongoing conflicts in Afghanistan, Somalia, Syria, and Yemen, as well as attacking regional actors and populations in other parts of Africa, Asia, and the Middle East.

- Al-Qa'ida leaders and affiliate media platforms almost certainly will call for followers to carry out attacks in the West, but their appeals probably will not create a spike in inspired attacks. The group's messaging since at least 2010 has produced few such attacks.

Homegrown Violent Extremists

Homegrown violent extremists (HVEs) will remain the most prevalent and difficult-to-detect Sunni terrorist threat at home, despite a drop in the number of attacks in 2017. HVE attacks are likely to continue to occur with little or no warning because the perpetrators often strike soft targets and use simple tactics that do not require advanced skills or outside training.

- HVEs almost certainly will continue to be inspired by a variety of sources, including terrorist propaganda as well as in response to perceived grievances related to US Government actions.

Iran and Lebanese Hizballah

Iran remains the most prominent state sponsor of terrorism, providing financial aid, advanced weapons and tactics, and direction to militant and terrorist groups across the Middle East and cultivating a network of operatives across the globe as a contingency to enable potential terrorist attacks.

Lebanese Hizballah has demonstrated its intent to foment regional instability by deploying thousands of fighters to Syria and by providing weapons, tactics, and direction to militant and terrorist groups. Hizballah probably also emphasizes its capability to attack US, Israeli, and Saudi Arabian interests.

COUNTERINTELLIGENCE AND FOREIGN DENIAL AND DECEPTION

The United States will face a complex global foreign intelligence threat environment in 2018. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their services' capabilities, intent, and broad operational scope. Other states in the Near East, South Asia, East Asia, and Latin America will pose local and regional intelligence threats to US interests. For example, Iranian and Cuban intelligence and security services continue to view the United States as a primary threat.

Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other areas will remain a persistent threat to US interests.

Nonstate entities, including international terrorists and transnational organized crime groups, are likely to continue to employ and improve their intelligence capabilities, including human, technical, and cyber means. As with state intelligence services, these nonstate entities recruit sources and perform physical and technical surveillance to facilitate their illicit activities and to avoid detection and capture.

Trusted insiders who disclose sensitive or classified US Government information without authorization will remain a significant threat in 2018 and beyond. The sophistication and availability of information technology that increases the scope and impact of unauthorized disclosures exacerbate this threat.

Russia and Influence Campaigns

Influence operations, especially through cyber means, will remain a significant threat to US interests as they are low-cost, relatively low-risk, and deniable ways to retaliate against adversaries, to shape foreign perceptions, and to influence populations. Russia probably will be the most capable and aggressive source of this threat in 2018, although many countries and some nonstate actors are exploring ways to use influence operations, both domestically and abroad.

We assess that the Russian intelligence services will continue their efforts to disseminate false information via Russian state-controlled media and covert online personas about US activities to encourage anti-US political views. Moscow seeks to create wedges that reduce trust and confidence in democratic processes, degrade democratization efforts, weaken US partnerships with European allies, undermine Western sanctions, encourage anti-US political views, and counter efforts to bring Ukraine and other former Soviet states into European institutions.

- Foreign elections are critical inflection points that offer opportunities for Russia to advance its interests both overtly and covertly. The 2018 US mid-term elections are a potential target for Russian influence operations.
- At a minimum, we expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople, and other means of influence to try to exacerbate social and political fissures in the United States.

EMERGING AND DISRUPTIVE TECHNOLOGY

New technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems. We assess that technology developments—in the biotechnology and communications sectors, for example—are likely to outpace regulation, which could create international norms that are contrary to US interests and increase the likelihood of technology surprise. Emerging technology and new applications of existing technology will also allow our adversaries to more readily develop weapon systems that can strike farther, faster, and harder and challenge the United States in all warfare domains, including space.

- The widespread proliferation of artificial intelligence (AI)—the field of computer science encompassing systems that seek to imitate aspects of human cognition by learning and making decisions based on accumulated knowledge—is likely to prompt new national security concerns; existing machine learning technology, for example, could enable high degrees of automation in labor-intensive activities such as satellite imagery analysis and cyber defense. Increasingly capable AI tools, which are often enabled by large amounts of data, are also likely to present socioeconomic challenges, including impacts on employment and privacy.

- New biotechnologies are leading to improvements in agriculture, health care, and manufacturing. However, some applications of biotechnologies may lead to unintentional negative health effects, biological accidents, or deliberate misuse.

- The global shift to advanced information and communications technologies (ICT) will increasingly test US competitiveness because aspiring suppliers around the world will play a larger role in developing new technologies and products. These technologies include next-generation, or 5G, wireless technology; the internet of things; new financial technologies; and enabling AI and big data for predictive analysis. Differences in regulatory and policy approaches to ICT-related issues could impede growth and innovation globally and for US companies.

- Advanced materials could disrupt the economies of some commodities-dependent exporting countries while providing a competitive edge to developed and developing countries that create the capacity to produce and use the new materials. New materials, such as nanomaterials, are often developed faster than their health and environmental effects can be assessed. Advances in manufacturing, particularly the development of 3D printing, almost certainly will become even more accessible to a variety of state and nonstate actors and be used in ways contrary to our interests.

TECHNOLOGY ACQUISITIONS AND STRATEGIC ECONOMIC COMPETITION

Persistent trade imbalances, trade barriers, and a lack of market-friendly policies in some countries probably will continue to challenge US economic security. Some countries almost certainly will continue to acquire US intellectual property and propriety information illicitly to advance their own economic and national security objectives.

- China, for example, has acquired proprietary technology and early-stage ideas through cyber-enabled means. At the same time, some actors use largely legitimate, legal transfers and

relationships to gain access to research fields, experts, and key enabling industrial processes that could, over time, erode America's long-term competitive advantages.

SPACE AND COUNTERSPACE

Continued global space industry expansion will further extend space-enabled capabilities and space situational awareness to nation-state, nonstate, and commercial space actors in the coming years, enabled by the increased availability of technology, private-sector investment, and growing international partnerships for shared production and operation. All actors will increasingly have access to space-derived information services, such as imagery, weather, communications, and positioning, navigation, and timing for intelligence, military, scientific, or business purposes. Foreign countries—particularly China and Russia—will continue to expand their space-based reconnaissance, communications, and navigation systems in terms of the numbers of satellites, the breadth of their capability, and the applications for use.

Both Russia and China continue to pursue antisatellite (ASAT) weapons as a means to reduce US and allied military effectiveness. Russia and China aim to have nondestructive and destructive counterspace weapons available for use during a potential future conflict. We assess that, if a future conflict were to occur involving Russia or China, either country would justify attacks against US and allied satellites as necessary to offset any perceived US military advantage derived from military, civil, or commercial space systems. Military reforms in both countries in the past few years indicate an increased focus on establishing operational forces designed to integrate attacks against space systems and services with military operations in other domains.

Russian and Chinese destructive ASAT weapons probably will reach initial operational capability in the next few years. China's PLA has formed military units and begun initial operational training with counterspace capabilities that it has been developing, such as ground-launched ASAT missiles. Russia probably has a similar class of system in development. Both countries are also advancing directed-energy weapons technologies for the purpose of fielding ASAT weapons that could blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense.

Of particular concern, Russia and China continue to launch "experimental" satellites that conduct sophisticated on-orbit activities, at least some of which are intended to advance counterspace capabilities. Some technologies with peaceful applications—such as satellite inspection, refueling, and repair—can also be used against adversary spacecraft.

Russia and China continue to publicly and diplomatically promote international agreements on the nonweaponization of space and "no first placement" of weapons in space. However, many classes of weapons would not be addressed by such proposals, allowing them to continue their pursuit of space warfare capabilities while publicly maintaining that space must be a peaceful domain.

TRANSNATIONAL ORGANIZED CRIME

Transnational organized criminal groups and networks will pose serious and growing threats to the security and health of US citizens, as well as to global human rights, ecological integrity, government revenues, and efforts to deal with adversaries and terrorists. In the most severe cases abroad, criminal enterprises will

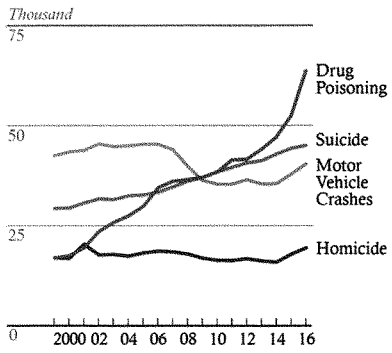
contribute to increased social violence, erode governments' authorities, undermine the integrity of international financial systems, and harm critical infrastructure.

Drug Trafficking

Transnational organized criminal groups supply the dominant share of illicit drugs consumed in the United States, fueling high mortality rates among US citizens.

- Americans in 2016 died in record numbers from drug overdoses, 21 percent more than in 2015.
- Worldwide production of cocaine, heroin, and methamphetamine is at record levels. US mortality from potent synthetic opioids doubled in 2016, and synthetic opioids have become a key cause of US drug deaths.
- Mexican criminal groups will continue to supply much of the heroin, methamphetamine, cocaine, and marijuana that cross the US-Mexico border, while China-based suppliers ship fentanyls and fentanyl precursors to Mexico-, Canada-, and US-based distributors or sell directly to consumers via the Internet.

Causes of US Premature Deaths, 1999-2016



Source: US Centers for Disease Control and Prevention.

17-15892 12-17

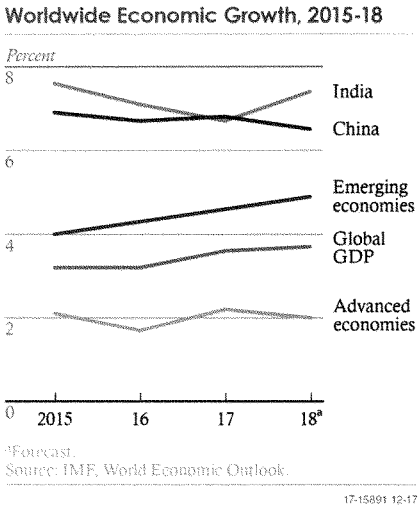
Broader Threats From Transnational Crime

Transnational organized criminal groups, in addition to engaging in violence, will continue to traffic in human beings, deplete natural resources, and siphon money from governments and the global economy.

- Human trafficking will continue in virtually every country. International organizations estimate that about 25 million people are victims.
- The FBI assesses that US losses from cybercrime in 2016 exceeded $1.3 billion, and some industry experts predict such losses could cost the global economy $6 trillion by 2021.
- Criminal wildlife poaching, illegal fishing, illicit mining, and drug-crop production will continue to threaten economies, biodiversity, food supply security, and human health. For example, academic studies show that illicit mining alone adds some 650 to 1,000 tons of toxic mercury to the ecosystem each year.
- Transnational organized criminal groups probably will generate more revenue from illicit activity in the coming year, which the UN last estimated at $1.6-$2.2 trillion for 2014.

ECONOMICS AND ENERGY

Global growth in 2018—projected by the IMF to rise to 3.9 percent—is likely to become more broadly based, but growth remains weak in many countries, and inflation is below target in most advanced economies. The relatively favorable outlook for real economic growth suggests little near-term risk of unfavorable deficit-debt dynamics among the advanced economies. Supportive financial conditions and improving business sentiment will help to drive economic activity in advanced countries. China's growth may decelerate as the property sector cools and if Beijing accelerates economic reforms. India's economy is expected to rebound after headwinds from taxation changes and demonetization, and the continuing upswing in emerging and developing economies could be tempered by capital outflows from a stronger dollar and monetary policy normalization in the United States and Europe.



Oil-exporting countries continue to suffer from the late-2014 oil price drop, and their economic woes are likely to continue, with broader negative implications. Subdued economic growth, combined with sharp increases in North American oil and gas production, probably will continue putting downward pressure on global energy prices, harming oil-exporting economies. The US Energy Information Administration forecasts that 2018 West Texas Intermediate and Brent prices will average $58 and $62 per barrel, respectively, far below the average annual prices of $98 and $109 in 2013.

- Low oil prices and production declines—along with poor economic policies—have pushed Venezuela and the state-owned oil company, Petroleos de Venezuela, to miss debt payments, putting them in selective default.
- Saudi Arabia and other Persian Gulf oil exporters have experienced sharp increases in budget deficits, forcing governments to issue debt and enact politically unpopular fiscal reforms, such as cuts to subsidies, social programs, and government jobs.
- In Africa, declining oil revenue, mismanagement, and inadequate policy responses to oil price shocks have contributed to Angolan and Nigerian fiscal problems, currency strains, and deteriorating foreign exchange reserves.
- OPEC member countries and select non-OPEC producers, including Russia, in early 2017 committed to cut oil production in order to lift prices, with compliance likely to be offset somewhat as Libya or Nigeria—both are exempt from the deal—are able to resume production.

HUMAN SECURITY

Governance shortfalls, violent conflict, environmental stresses, and increased potential for a global health crisis will create significant risks to human security, including high levels of human displacement and migration flows.

Governance and Political Turbulence

Domestic and foreign challenges to democracy and institutional capacity will test governance quality globally in 2018, especially as competitors manipulate social media to shape opinion. Freedom House reported the 11th consecutive year of decline in "global freedom" in 2017, and nearly one-quarter of the countries registering declines were in Europe.

- While the number of democracies has remained steady for the past decade, some scholars suggest the quality of democracy has declined.
- We note that more governments are using propaganda and misinformation in social media to influence foreign and domestic audiences.
- The number and sophistication of government efforts to shape domestic views of politics have increased dramatically in the past 10 years. In 2016, Freedom House identified 30 countries, including the Philippines, Turkey, and Venezuela, whose governments used social media to spread government views, to drive agendas, and to counter criticism of the government online.

Poor governance, weak national political institutions, economic inequality, and the rise of violent nonstate actors all undermine states' abilities to project authority and elevate the risk of violent—even regime-threatening—instability and mass atrocities.

Environment and Climate Change

The impacts of the long-term trends toward a warming climate, more air pollution, biodiversity loss, and water scarcity are likely to fuel economic and social discontent—and possibly upheaval—through 2018.

- The past 115 years have been the warmest period in the history of modern civilization, and the past few years have been the warmest years on record. Extreme weather events in a warmer world have the potential for greater impacts and can compound with other drivers to raise the risk of humanitarian disasters, conflict, water and food shortages, population migration, labor shortfalls, price shocks, and power outages. Research has not identified indicators of tipping points in climate-linked earth systems, suggesting a possibility of abrupt climate change.
- Worsening air pollution from forest burning, agricultural waste incineration, urbanization, and rapid industrialization—with increasing public awareness—might drive protests against authorities, such as those recently in China, India, and Iran.
- Accelerating biodiversity and species loss—driven by pollution, warming, unsustainable fishing, and acidifying oceans—will jeopardize vital ecosystems that support critical human systems. Recent estimates suggest that the current extinction rate is 100 to 1,000 times the natural extinction rate.

- Water scarcity, compounded by gaps in cooperative management agreements for nearly half of the world's international river basins, and new unilateral dam development are likely to heighten tension between countries.

Human Displacement

Global displacement almost certainly will remain near record highs during the next year, raising the risk of disease outbreaks, recruitment by armed groups, political upheaval, and reduced economic productivity. Conflicts will keep many of the world's refugees and internally displaced persons from returning home.

Health

The increase in frequency and diversity of reported disease outbreaks—such as dengue and Zika—probably will continue through 2018, including the potential for a severe global health emergency that could lead to major economic and societal disruptions, strain governmental and international resources, and increase calls on the United States for support. A novel strain of a virulent microbe that is easily transmissible between humans continues to be a major threat, with pathogens such as H5N1 and H7N9 influenza and Middle East Respiratory Syndrome Coronavirus having pandemic potential if they were to acquire efficient human-to-human transmissibility.

- The frequency and diversity of disease outbreaks have increased at a steady rate since 1980, probably fueled by population growth, travel and trade patterns, and rapid urbanization. Ongoing global epidemics of HIV/AIDS, malaria, and tuberculosis continue to kill millions of people annually.

- Increasing antimicrobial resistance, the ability of pathogens—including viruses, fungi, and bacteria—to resist drug treatment, is likely to outpace the development of new antimicrobial drugs, leading to infections that are no longer treatable.

- The areas affected by vector-borne diseases, including dengue, are likely to expand, especially as changes in climatological patterns increase the reach of the mosquito.

- The World Bank has estimated that a severe global influenza pandemic could cost the equivalent of 4.8 percent of global GDP—more than $3 trillion—and cause more than 100 million deaths.

29

REGIONAL THREATS

EAST ASIA

China

China will continue to pursue an active foreign policy—especially in the Asia Pacific region—highlighted by a firm stance on its sovereignty claims in the East China Sea (ECS) and South China Sea (SCS), its relations with Taiwan, and its pursuit of economic engagement across the region. Regional tension will persist due to North Korea's nuclear and missile programs and simmering tension over territorial and maritime disputes in the ECS and SCS. China will also pursue efforts aimed at fulfilling its ambitious Belt and Road Initiative to expand China's economic reach and political influence across Eurasia, Africa, and the Pacific through infrastructure projects.

North Korea

North Korea's weapons of mass destruction program, public threats, defiance of the international community, confrontational military posturing, cyber activities, and potential for internal instability pose a complex and increasing threat to US national security and interests.

In the wake of accelerated missile testing since 2016, North Korea is likely to press ahead with more tests in 2018, and its Foreign Minister said that Kim may be considering conducting an atmospheric nuclear test over the Pacific Ocean. Pyongyang's commitment to possessing nuclear weapons and fielding capable long-range missiles, all while repeatedly stating that nuclear weapons are the basis for its survival, suggests that the regime does not intend to negotiate them away.

Ongoing, modest improvements to North Korea's conventional capabilities continue to pose a serious and growing threat to South Korea and Japan. Despite the North Korean military's many internal challenges and shortcomings, Kim Jong Un continues to expand the regime's conventional strike options with more realistic training, artillery upgrades, and close-range ballistic missiles that improve North Korea's ability to strike regional US and allied targets with little warning.

Southeast Asia

Democracy and human rights in many Southeast Asian countries will remain fragile in 2018 as autocratic tendencies deepen in some regimes and rampant corruption and cronyism undermine democratic values. Countries in the region will struggle to preserve foreign policy autonomy in the face of Chinese economic and diplomatic coercion.

- Cambodian leader Hun Sen will repress democratic institutions and civil society, manipulate government and judicial institutions, and use patronage and political violence to guarantee his rule beyond the 2018 national election. Having alienated Western partners, Hun Sen will rely on Beijing's political and financial support, drawing Cambodia closer to China as a result.

- The crisis resulting from the exodus of more than 600,000 Rohingyas from Burma to Bangladesh will threaten Burma's fledgling democracy, increase the risk of violent extremism, and provide openings for Beijing to expand its influence.

- ***In the Philippines, President Duterte will continue to wage his signature campaign against drugs, corruption, and crime.*** Duterte has suggested he could suspend the Constitution, declare a "revolutionary government," and impose nationwide martial law. His declaration of martial law in Mindanao, responding to the ISIS-inspired siege of Marawi City, has been extended through the end of 2018.

- ***Thailand's leaders have pledged to hold elections in late 2018, but the new Constitution will institutionalize the military's influence.***

MIDDLE EAST AND NORTH AFRICA

Iran

Iran will seek to expand its influence in Iraq, Syria, and Yemen, where it sees conflicts generally trending in Tehran's favor, and it will exploit the fight against ISIS to solidify partnerships and translate its battlefield gains into political, security, and economic agreements.

- Iran's support for the Popular Mobilization Committee (PMC) and Shia militants remains the primary threat to US personnel in Iraq. We assess that this threat will increase as the threat from ISIS recedes, especially given calls from some Iranian-backed groups for the United States to withdraw and growing tension between Iran and the United States.

- In Syria, Iran is working to consolidate its influence while trying to prevent US forces from gaining a foothold. Iranian-backed forces are seizing routes and border crossings to secure the Iraq-Syria border and deploying proregime elements and Iraqi allies to the area. Iran's retaliatory missile strikes on ISIS targets in Syria following ISIS attacks in Tehran in June were probably intended in part to send a message to the United States and its allies about Iran's improving military capabilities. Iran is pursuing permanent military bases in Syria and probably wants to maintain a network of Shia foreign fighters in Syria to counter future threats to Iran. Iran also seeks economic deals with Damascus, including deals on telecommunications, mining, and electric power repairs.

- In Yemen, Iran's support to the Huthis further escalates 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 al Mandeb Strait and land-based targets deep inside Saudi Arabia and the UAE, such as the 4 November and 19 December ballistic missile attacks on Riyadh and an attempted 3 December cruise missile attack on an unfinished nuclear reactor in Abu Dhabi.

Iran will develop military capabilities that threaten US forces and US allies in the region, and its unsafe and unprofessional interactions will pose a risk to US Navy operations in the Persian Gulf.

Iran continues to develop and improve a range of new military capabilities to target US and allied military assets in the region, including armed UAVs, ballistic missiles, advanced naval mines, unmanned explosive boats, submarines and advanced torpedoes, and antishipand land-attack cruise missiles. Iran has the largest ballistic missile force in the Middle East and can strike targets up to 2,000 kilometers from Iran's borders. Russia's delivery of the SA-20c SAM system in 2016 has provided Iran with its most advanced long-range air defense system.

- Islamic Revolutionary Guard Corps (IRGC) Navy forces operating aggressively in the Persian Gulf and Strait of Hormuz pose a risk to the US Navy. Most IRGC interactions with US ships are professional, but as of mid-October, the Navy had recorded 14 instances of what it describes as "unsafe and/or unprofessional" interactions with Iranian forces during 2017, the most recent interaction occurring last August, when an unarmed Iranian drone flew close to the aircraft carrier USS Nimitz as fighter jets landed at night. The Navy recorded 36 such incidents in 2016 and 22 in 2015. Most involved the IRGC Navy. We assess that these interactions, although less frequent, will continue and that they are probably intended to project an image of strength and, possibly, to gauge US responses.

Iranian centrist and hardline politicians increasingly will clash as they attempt to implement competing visions for Iran's future. This contest will be a key driver in determining whether Iran changes its behavior in ways favorable to US interests.

- Centrists led by President Hasan Ruhani will continue to advocate greater social progress, privatization, and more global integration, while hardliners will view this agenda as a threat to their political and economic interests and to Iran's revolutionary and Islamic character.

- Supreme Leader Ali Khamenei's views are closer to those of the hardliners, but he has supported some of Ruhani's efforts to engage Western countries and to promote economic growth. The Iranian economy's prospects—still driven heavily by petroleum revenue—will depend on reforms to attract investment, strengthen privatization, and grow nonoil industries, which Ruhani will continue pursuing, much to the dismay of hardliners. National protests over economic grievances in Iran earlier this year have drawn more attention to the need for major reforms, but Ruhani and his critics are likely to use the protests to advance their political agendas.

- Khamenei has experienced health problems in the past few years, and, in an effort to preserve his legacy, he probably opposes moving Iran toward greater political and economic openness. As their relationship has deteriorated since the presidential election last June, Ruhani has tried to mend relations with Khamenei as well as his allies, but, in doing so, he risks failing to make progress on reforms in the near-term.

Syria

The conflict has decisively shifted in the Syrian regime's favor, enabling Russia and Iran to further entrench themselves inside the country. Syria is likely to experience episodic conflict through 2018, even as Damascus recaptures most of the urban terrain and the overall level of violence decreases.

- ***The Syrian opposition's seven-year insurgency is probably no longer capable of overthrowing President Bashar al-Asad or overcoming a growing military disadvantage.*** Rebels probably retain the resources to sustain the conflict for at least the next year.

- ISIS is likely on a downward trajectory in Syria; yet, despite territorial losses, it probably possesses sufficient resources, and a clandestine network in Syria, to sustain insurgency operations through 2018.

- Moscow probably cannot force President Asad to agree to a political settlement that he believes significantly weakens him, unless Moscow is willing to remove Asad by force. While Asad may engage in peace talks, he is unlikely to negotiate himself from power or offer meaningful concessions to the opposition.

- Russia and Iran are planning for a long-term presence, securing military basing rights and contracts for reconstruction and oil and gas exploitation. Iran is also seeking to establish a land corridor from Iran through Syria to Lebanon. The Kurdish People's Protection Unit—the Syrian militia of the Kurdistan Workers' Party (PKK)—probably will seek some form of autonomy but will face resistance from Russia, Iran, and Turkey.

- As of October 2017, there were more than 5 million Syrian refugees in neighboring countries, and an estimated 6.3 million internally displaced. Reconstruction could cost at least $100 billion and take at least 10 years to complete. Asad's battered economy will likely continue to require significant subsidies from Iran and Russia to meet basic expenses.

Iraq

Iraq is likely to face a lengthy period of political turmoil and conflict as it struggles to rebuild, reconstitute the Iraqi state, maintain pressure on ISIS, and rein in the Iranian-backed Shia militias that pose an enduring threat to US personnel.

- The Iraqi Government, which has accrued $120 billion in debt, requires substantial external assistance to cover hundreds of millions of dollars in humanitarian-aid shortfalls and a World Bank estimated $88.2 billion to restore heavily damaged infrastructure, industry, and service sectors in areas retaken from ISIS.

- Prime Minister Haydar al-Abadi's forceful reassertion of Baghdad's authority after the Kurdistan Regional Government's (KRG) independence referendum in September illustrates the divisions among Iraqi leaders over the future of the state. The move to curb Kurdish autonomy was popular among many Arab Shia and Sunnis and may prompt Iraqi leaders to be uncompromising in political reconciliation discussions in order to consolidate votes in the run-up to elections planned for next spring.

- ISIS will remain a terrorist and insurgent threat, and the group will seek to exploit Sunni discontent to conduct attacks and try to regain Iraqi territory. Baghdad will struggle to reorient the Iraqi Security Forces (ISF) from conventional warfare to counterinsurgency and counterterrorism against ISIS while consolidating state control of territory and integrating the Iranian-backed and Shia-dominated Popular Mobilization Committee (PMC).

- There is an increasing risk that some Shia militants will seek to attack US targets in Iraq because they believe that the US security presence is no longer needed, want to reassert Iraqi sovereignty, and support Iran's goal of reducing US influence in Iraq.

Baghdad will have to contend with longstanding and war-hardened ethnosectarian divisions between Shia, Sunnis, and Kurds that were kept in check by the threat from ISIS. Despite ISIS's loss of territory, the social and political challenges that gave rise to the group remain and threaten the cohesion of the Iraqi state.

Yemen

The war in Yemen is likely to continue for the foreseeable future because the Iranian-backed Huthis and the Saudi-led coalition remain far apart on terms for ending the conflict. The death of former Yemeni President Ali Abdallah Salih is only likely to further complicate the conflict as the Huthis and others scramble to win over those who previously backed Salih. We assess that the Huthis will continue to pursue their goals militarily and that, as a result, US allies and interests on the Arabian Peninsula will remain at risk of Huthi missile attacks until the conflict is resolved.

- Continued fighting almost certainly will worsen the vast humanitarian crisis, which has left more than 70 percent of the population—or about 20 million people—in need of assistance and aggravated a cholera outbreak that has reached nearly 1 million confirmed cases. Relief operations are hindered by security and bureaucratic constraints established by both the Huthi-Salih alliance and the Saudi-led coalition and by international funding shortages.

SOUTH ASIA

Afghanistan

The overall situation in Afghanistan probably will deteriorate modestly this year in the face of persistent political instability, sustained attacks by the Taliban-led insurgency, unsteady Afghan National Security Forces (ANSF) performance, and chronic financial shortfalls. The National Unity Government probably will struggle to hold long-delayed parliamentary elections, currently scheduled for July 2018, and to prepare for a presidential election in 2019. The ANSF probably will maintain control of most major population centers with coalition force support, but the intensity and geographic scope of Taliban activities will put those centers under continued strain. Afghanistan's economic growth will stagnate at around 2.5 percent per year, and Kabul will remain reliant on international donors for the great majority of its funding well beyond 2018.

Pakistan

Pakistan will continue to threaten US interests by deploying new nuclear weapons capabilities, maintaining its ties to militants, restricting counterterrorism cooperation, and drawing closer to China. Militant groups supported by Islamabad will continue to take advantage of their safe haven in Pakistan to plan and conduct attacks in India and Afghanistan, including against US interests. Pakistan's perception of its eroding position relative to India, reinforced by endemic economic weakness and domestic security issues, almost certainly will exacerbate long-held fears of isolation and drive Islamabad's pursuit of actions that run counter to US goals for the region.

India-Pakistan Tension

Relations between India and Pakistan are likely to remain tense, with continued violence on the Line of Control and the risk of escalation if there is another high-profile terrorist attack in India or an uptick in violence on the Line of Control.

India-China Tension

We expect relations between India and China to remain tense and possibly to deteriorate further, despite the negotiated settlement to their three-month border standoff in August, elevating the risk of unintentional escalation.

Bangladesh-Burma Rohingya Crisis

The turmoil resulting from more than 600,000 Rohingyas fleeing from Burma to Bangladesh increases regional tension and may expand opportunities for terrorist recruitment in South and Southeast Asia. Further operations by Burmese security forces against Rohingya insurgents or sustained violence by ethnic Rakhine militias probably would make it difficult to repatriate Burmese from Bangladesh.

RUSSIA AND EURASIA

Russia

In his probable next term in office, President Vladimir Putin will rely on assertive and opportunistic foreign policies to shape outcomes beyond Russia's borders. He will also resort to more authoritarian tactics to maintain control amid challenges to his rule.

Economic and Military Affiliations in Russia's Neighborhood

Moscow will seek cooperation with the United States in areas that advance its interests. Simultaneously, Moscow will employ a variety of aggressive tactics to bolster its standing as a great power, secure a "sphere of influence" in the post-Soviet space, weaken the United States, and undermine Euro-Atlantic unity. The highly personalized nature of the Russian political system will enable Putin to act decisively to defend Russian interests or to pursue opportunities he views as enhancing Russian prestige and power abroad.

Russia will compete with the United States most aggressively in Europe and Eurasia, while applying less intense pressure in "outer areas" and cultivating partnerships with US rivals and adversaries—as well as with traditional US partners—to constrain US power and accelerate a shift toward a "multipolar" world. Moscow will use a range of relatively low-cost tools to advance its foreign policy objectives, including influence campaigns, economic coercion, cyber operations, multilateral forums, and measured military force. Russia's slow

economic growth is unlikely to constrain Russian foreign policy or by itself trigger concessions from Moscow in Ukraine, Syria, or elsewhere in the next year.

President Putin is likely to increase his use of repression and intimidation to contend with domestic discontent over corruption, poor social services, and a sluggish economy with structural deficiencies. He will continue to manipulate the media, distribute perks to maintain elite support, and elevate younger officials to convey an image of renewal. He is also likely to expand the government's legal basis for repression and to enhance his capacity to intimidate and monitor political threats, perhaps using the threat of "extremism" or the 2018 World Cup to justify his actions.

In 2018, Russia will continue to modernize, develop, and field a wide range of advanced nuclear, conventional, and asymmetric capabilities to balance its perception of a strategic military inferiority vis-a-vis the United States.

Ukraine

Ukraine remains at risk of domestic turmoil, which Russia could exploit to undermine Kyiv's pro-West orientation. These factors will threaten Ukraine's nascent economic recovery and potentially lead to changes in its foreign policy that further inflame tension between Russia and the West.

- Popular frustrations with the pace of reforms, depressed standards of living, perceptions of worsening corruption, and political polarization ahead of scheduled presidential and legislative elections in 2019 could prompt early elections.

- Opposition leaders will seek to capitalize on popular discontent to weaken President Petro Poroshenko and the ruling coalition ahead of elections in 2019.

The conflict in eastern Ukraine is likely to remain stalemated and marked by fluctuating levels of violence. A major offensive by either side is unlikely in 2018, although each side's calculus could change if it sees the other as seriously challenging the status quo. Russia will continue its military, political, and economic destabilization campaign against Ukraine to stymie and, where possible, reverse Kyiv's efforts to integrate with the EU and strengthen ties to NATO. Kyiv will strongly resist concessions to Moscow but almost certainly will not regain control of Russian-controlled areas of eastern Ukraine in 2018. Russia will modulate levels of violence to pressure Kyiv and shape negotiations in Moscow's favor.

- Russia will work to erode Western unity on sanctions and support for Kyiv, but the Kremlin is coping with sanctions at existing levels.

Belarus, the Caucasus, Central Asia, Moldova

The Kremlin will seek to maintain and, where possible, expand its influence throughout the former Soviet countries that it asserts are in its self-described sphere of influence.

Russia views Belarus as a critical buffer between itself and NATO and will seek to spoil any potential warming between Minsk and the West. Belarus President Aleksandr Lukashenko will continue close security cooperation with Moscow but will continue to aim for normalized relations with the West as a check on Russia's influence.

Russia's continued occupation of 20 percent of Georgia's territory and efforts to undermine its Western integration will remain the primary sources of Tbilisi's insecurity. The ruling Georgian Dream party is likely to seek to stymie the opposition and reduce institutional constraints on its power.

Tension over the disputed region of Nagorno-Karabakh could devolve into a large-scale military conflict between Armenia and Azerbaijan, which could draw in Russia to support its regional ally. Both sides' reluctance to compromise, mounting domestic pressures, Azerbaijan's steady military modernization, and Armenia's acquisition of new Russian equipment sustain the risk of large-scale hostilities in 2018.

Russia will pressure Central Asia's leaders to reduce engagement with Washington and support Russian-led economic and security initiatives, while concerns about ISIS in Afghanistan will push Moscow to strengthen its security posture in the region. Poor governance and weak economies raise the risk of radicalization—especially among the many Central Asians who travel to Russia or other countries for work—presenting a threat to Central Asia, Russia, and Western societies. China will probably continue to expand outreach to Central Asia—while deferring to Russia on security and political matters—because of concern that regional instability could undermine China's economic interests and create a permissive environment for extremists, which, in Beijing's view, could enable Uighur militant attacks in China.

Moldova's ostensibly pro-European ruling coalition—unless it is defeated in elections planned for November—probably will seek to curb Russian influence and maintain a veneer of European reform while avoiding changes that would damage the coalition's grip on power. The current Moldovan Government probably will move forward on implementing Moldova's EU Association Agreement against the will of openly pro-Russian and Russian-backed President Igor Dodon. Settlement talks over the breakaway region of Transnistria will continue, but progress likely will be limited to small issues.

EUROPE

The European Union and European national governments will struggle to develop common approaches to counter a variety of security challenges, including instability on their periphery, irregular migration to their region, heightened terrorist threats, and Russian influence campaigns, undercutting Western cohesion.

- These concerns are spurring many countries to increase defense spending and enhance capabilities.

- European governments will need to strengthen their counterterrorism regimes to deal with a diverse threat, including ISIS aspirants and returning foreign fighters.

Turkey's counterterrorism cooperation with the United States against ISIS is likely to continue, but thwarting Kurdish regional ambitions will be a foreign policy priority. President Recep Tayyip Erdogan is likely to employ polarizing rhetoric, straining bilateral relations and cooperation on shared regional goals.

AFRICA

Nigeria—the continent's largest economy—will face a security threat from Boko Haram and ISIS West Africa (ISIS-WA) while battling internal challenges from criminal, militant, and secessionist groups. ISIS-WA and Boko Haram are regional menaces, conducting cross-border attacks in Nigeria, Cameroon, Chad, and Niger and posing a threat to Western interests. Meanwhile, militant and secessionist groups in in the southern and central areas of Nigeria are capitalizing on longstanding social and economic grievances as the country nears the 2019 presidential election.

Politically fragile governments in Africa's Sahel region will remain vulnerable to terror attacks in 2018, despite efforts to coordinate their counterterror operations. ISIS and al-Qa'ida–allied groups, along with other violent extremists, will attempt to target Western and local government interests in the region, and a stalled peace process is likely to undercut the presidential election in Mali.

The Ethiopian and Kenyan Governments are likely to face opposition from publics agitating for redress of political grievances. Somalia's recently elected government probably will struggle to project its authority and implement security reforms amid the drawdown of African Union forces in 2018, while al-Shabaab—the most potent terrorist threat to US interests in East Africa—probably will increase attacks.

Clashes between the South Sudanese Government and armed opposition groups will continue, raising the risk of additional mass atrocities as both sides use ethnic militias and hate speech and the government continues its crackdown on ethnic minorities. The South Sudanese are the world's fastest growing refugee population, and the significant humanitarian challenges stemming from the conflict, including severe food insecurity, will strain the resources of neighboring countries hosting refugees.

Sudan is likely to continue some aspects of its constructive engagement with the United States following the suspension of sanctions because it has given priority to shedding its international pariah status and reviving its economy. Khartoum probably will acquiesce to some US requests, such as increasing counterterrorism cooperation and improving humanitarian access, but will be reluctant to take any steps that it perceives jeopardize its national security interests.

Political unrest and security threats across the region are likely to intensify as the Presidents of Burundi and the Democratic Republic of the Congo (DRC) face public and armed opposition to their rule and the Central African Republic (CAR) struggles to cope with a nationwide surge in conflict. Over-stretched UN missions in CAR and DRC are unlikely to stem the rising challenges from their concurrent humanitarian and security crises.

THE WESTERN HEMISPHERE

A key feature of the 2018 political environment in Latin America almost certainly will be popular frustration with low economic growth, corruption scandals, and the specter of endemic criminal activity in some countries. Larger and increasingly sophisticated middle classes—with greater access to social media—are demanding more accountability from their governments. Presidential elections, including those in Mexico and Colombia, will occur at a time when support for political parties and governing institutions is at record lows and could bolster the appeal of outsider candidates.

Mexico

Mexicans are focused on presidential and legislative elections scheduled for July 2018, in which corruption, high violence, and a tepid economy will be key issues. The Mexican Government has made slow progress implementing rule-of-law reforms and will continue to rely on the military to lead counternarcotics efforts. Mexico's $1.1 trillion economy benefits from strong economic fundamentals, but uncertainty over trade relationships and higher-than-expected inflation could further slow economic growth. President Enrique Pena Nieto is focusing on domestic priorities, including recovery from the September 2017 earthquakes and managing impacts from potential US policy shifts ahead of the elections. In recent years, Mexican US-bound migration has been net negative but might increase if economic opportunity at home declined.

Central America

Insecurity and lack of economic opportunities likely will remain the principal drivers of irregular migration from the Northern Triangle countries of El Salvador, Guatemala, and Honduras. Homicide rates in these countries remain high, and gang-related violence is still prompting Central Americans to flee.

Venezuela

Economic woes and international diplomatic pressure probably will put political pressure on the Venezuelan Government in 2018. Living standards have declined and shortages of basic goods are driving the increase in Venezuelans seeking asylum in the United States and the region. Venezuela's negotiations with creditors probably will lead to messy legal battles. Venezuela almost certainly will seek to minimize further disruptions to oil production and exports to maintain its critical oil export earnings. Oil prices have increased slightly this year, but crude oil production continues to decline.

Colombia

President Juan Manuel Santos will seek to cement implementation of the Revolutionary Armed Forces of Colombia (FARC) peace accord, as campaigning intensifies for the May 2018 presidential election. The FARC's new political-party status and the uncertainty around the transitional justice reforms will be a factor in the political environment ahead of elections. Substantial budget constraints will slow major programs or policy changes. The influx of FARC dissidents, drug traffickers, and other illegal actors into remote areas will challenge security forces during the next 12 months. Cocaine production in Colombia is at an all-time high, and crop substitution and eradication programs are facing stiff local resistance.

Cuba

Havana will seek to manage President Raul Castro's planned retirement in April 2018. Castro's successor will inherit a stagnant economy and a stalled economic reform process.

Haiti

As President Jovenel Moise begins his second year in office, he will confront competing interests within his government, a vocal opposition, and a fragile economy. Crime and protest activity will test the Haitian National Police following the departure of the UN Stabilization Mission in October 2017 and the transition to a police-only UN mission.

Chairman BURR. Dan, thank you very much for that very thorough overview of the world and what's at play.

I'll recognize Members based upon seniority for up to five minutes. The Chair recognizes himself.

Admiral Rogers, according to the statement for the record the intelligence community assesses that most detected Chinese cyber operations against the United States' private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks nationwide. Rate the intelligence community's performance when it comes to notifying cleared defense contractors and other sensitive private sector actors about malicious cyber activities on their networks.

Admiral ROGERS. First, in all honesty, you're asking me to rate a function for which I don't have responsibility or day-to-day execution. So I'll give an opinion, but it's not informed by day-to-day experience per se. This is an issue both at NSA and at Cyber Command, although I try to work very aggressively because, as you have outlined, it's a tremendous concern for us in the Department.

Clearly, I think we are not where we need to be. The challenge I think is we've got multiple areas of knowledge and insight across the Federal Government, within the private sector, and how do we bring this together in an integrated team, with some real-time flow back and forth? That is not where we are today, but that's where we've got to get to.

Chairman BURR. In your estimation, are we doing enough to warn the private sector of the threat that's out there?

Admiral ROGERS. I think we are informing them as we become aware of it. But one of my concerns is we're only going to see one slice of this picture. I'm also interested in it from the private sector's perspective. Tell us what you are seeing. If we can bring these two together, we'll have such a broader perspective and much more in-depth knowledge of what's happening. I think that's part of this. It's not just, hey, one side needs to do a better job. I'm not trying to say it's two-sided, but I think it's our ability to bring this together as a team.

Chairman BURR. Given that you've seen the difficulty especially this Committee and the intelligence community has had communicating with the tech companies about a way forward that is in commonality, are you concerned at how this is going to become an increasingly challenging landscape for both Congress and for the intelligence community working as we see new tech firms emerge every day?

Admiral ROGERS. Yes, I am, because, quite frankly, I wonder, how bad does it have to get before we realize we have to do some things fundamentally differently? I would argue if you look at the Internet of Things, you look at the security levels within those components, folks, this is going to orders of magnitude. If we think the problem is a challenge now, if we just wait it's going to get much, much worse, exponentially, from a security perspective.

Chairman BURR. Director Pompeo, the IC assesses that North Korea is likely to press ahead with more tests in 2018, missile tests, noting that North Korea's foreign minister indicated an atmospheric nuclear test over the Pacific may be under consideration

by Pyongyang. What's the IC assess the regional reaction to this kind of test would be?

Director POMPEO. Senator, thanks for the question. If I may just take one minute to say, I've been doing this for a year now and I want to express my appreciation to this Committee for helping the CIA do the things it needs to do, providing us the resources and the authorities we need. We have put a lot of effort against this very problem. You have been incredibly supportive of that. So my team thanks you for that.

We think a test like that would certainly further unite the region. Having said that, our sense is that we have built a global coalition pushing back against Kim Jong Un and his terror regime. With respect to what each particular country might do, I'd prefer to keep that conversation to closed session this afternoon.

Chairman BURR. Great.

What's the IC's assessment of North Korea's willingness to employ its expansive conventional military capabilities?

Director POMPEO. Senator, one of the things that Director Coats referred to in his opening remarks is that Kim Jong Un remains not only intent on staying in power, the thing all dictators prefer to do, die in their sleep fully at the peak of their power; but he has this mission that is a longstanding North Korean idea of reunification. Their capacity to use a nuclear umbrella combined with their conventional forces to exert coercive behavior, certainly inside their country, certainly against South Korea, but more broadly, is something that our analysts are continuing to look at.

We can see as they ratchet up their nuclear capability, making a response more different, their capacity to do harm in the region as a result of their incredible conventional capabilities alone increases.

Chairman BURR. Probably for General Ashley and Admiral Rogers: According to the statement for the record, the widespread proliferation of artificial intelligence is likely to prompt new national security concerns. How is the IC accounting for the possibility of these new national security concerns? Are we seeing indications now that our adversaries are working to harness emerging technologies, like artificial intelligence, and is the IC looking to maximize the potential of emerging technologies in our own processes and analysis of data and intelligence?

General ASHLEY. Sir, if I could take a first shot at that one. You look at DIA—and thanks for all the support the Committee provides to the Defense Intelligence Agency. If you look at our coordination, if you look at foreign militaries and the operational environment, this is central to looking at doctrine and what they're developing. When you think about artificial intelligence, our near-peer competitors are pursuing this. It's a lot of commercial technology that's available. But when you look at the volume, big data and what's available, the ability to digest and pull all that information in, artificial intelligence is going to be integral to that.

An example of one of the projects we're working on—and this is at the open source level—Project Maven. You look at full motion video, for example, or social media. In full motion video, you're never going to be able to have the work force that's going to be able to go through all of the material, whether it's video, whether it's

what Admiral Rogers works in the way of signals intelligence, or what's available in social media. So artificial intelligence, machine learning, which is really kind of where we are right now. It's more machine learning than it is artificial intelligence. We're seeing all of our near-peer competitors invest in these kinds of technologies because it's going to get them to decision cycles faster, allow them to digest information in greater volumes, and have a better situational understanding of what's happening in the battle space, and in some cases just what's happening in the strategic environment.

Admiral ROGERS. Sir, I would agree with General Ashley. I would also highlight, every organization on this table is faced with the challenge of victims of our own success in some ways. The ability to access data at increased levels brings its own set of challenges. So we are collectively all attempting to deal with this.

When I look at potential adversaries, I see them going through the same set of challenges. I would argue when I look at the PRC in particular, there clearly is a national strategy designed to harness the power of artificial intelligence to generate strategic outcomes, along the lines that General Ashley highlighted, to generate positive outcomes.

You look at their research, you look at how it is affecting the amount of data they are going after. I can remember five, ten years ago looking at some data concentrations and thinking to myself: This is so large and has such a disparate amount of information in it, boy, it would be really different for an opponent potentially to generate insight and knowledge from it. I don't have those kinds of conversation any more.

With the power of machine learning, artificial intelligence, and big data analytics, data concentrations now increasingly are targets of attraction to a whole host of actors. We have watched the PRC and others engage in activities designed to access these massive data concentrations.

General ASHLEY. If I could follow up on that also, because this is one of those areas that's debatable in the commercial industry, so you see a lot of investment, academia and others, that are pursuing this. So there's a key piece of this I think is worth addressing as well, which is how do you operationalize it? If I could just use a World War II example, the fact that there were planes, radios, and tanks was not unique to the Germans in World War II. What they did is they came up with an operational concept that allowed them to leverage that.

Peter Singer, if anyone's ever read "Wired for War" or "Ghost Fleet," is a futurist. We sat on a panel with him a couple years ago, and it was interesting when I asked him: As you look at the things that are emerging from the technology and things that are coming out, what do you see in the way of breakthroughs to give somebody a really marked advantage? Peter's comment wasn't that I see something that gives someone such a marked advantage. It's who's able to harness it, who's able to operationalize it and put it to effect. So that's really a key difference, because a lot of that technology is going to be available globally.

Chairman BURR. Thank you.

Director COATS. If I could just ask your permission here, Robert Cardillo's agency NGA has probably taken some very significant

lead on this, given the enormous volume of collection that they take and the inability to process that through the use of humans. I've asked Robert to be prepared to answer that question for you because I think they're taking some leading efforts that might be helpful.

Director CARDILLO. I think it's important to note at the front what hasn't changed. Quite frankly, the mission, the responsibility, this whole table has is to provide you with decision advantage. What's changed is the world around us and now within us. So what we used to hold exclusively because we had capabilities that others didn't, is now more shared. So as Admiral Rogers has said, this is something that we all lock arms on, because it isn't the access that is exclusive anymore; it's the use. It's the concept of operations, as General Ashley said.

I have the same concerns you do about getting the cooperation we need from these companies. I'm rather optimistic about it because I think at the end of the day we can advance the American economy, we can advance American entrepreneurship, and we can advance our understanding of the world in a way that gets back to that first step, which is decision advantage.

Chairman BURR. Rest assured, the processing of data will come up in our closed session with you. I've got you targeted.

Vice Chair.

Vice Chairman WARNER. Thank you, Mr. Chairman.

I think I take with some note the fact that the ODNI Director started his discussion with cyber. I think it's very telling in terms of how we view worldwide threats.

Let me get one question out on the record. We all know it's been over a year since the Russian intervention in our 2016 elections. We've also seen Russia intervene in a number of other Western democracies. I'd like each of you to briefly reconfirm to the American public that our intelligence community understands this threat.

Last year those of you who were on the panel each expressed confidence in the January 2017 IC assessment that Russia interfered in the 2016 elections. I'd like each of you today to, one, reaffirm that; and also, with a simple yes or no, do you agree with Director Pompeo that we haven't seen a significant decrease in the Russian activity and we have every expectation—and, Director Coats, you've already alluded to this—that they'll try to continue to intervene in our elections in 2018 and 2020. We'll start with you, Director Cardillo. A simple yes or no will do.

Director CARDILLO. No change in my view of the 2017 assessment. I support that. And I agree with Director Pompeo's assessment about the likelihood of the 2018 occurrence as well.

Vice Chairman WARNER. Admiral.

Admiral ROGERS. I participated in that 2017 work. I stood by it then and I stand by it now, and I agree with Director Pompeo: This is not going to change or stop.

Vice Chairman WARNER. General Ashley.

General ASHLEY. Yes, it is not going to change, nor is it going to stop.

Director COATS. Throughout the entire community, we have not seen any evidence of any significant change from last year.

Director POMPEO. I agree with Director Pompeo.

[Laughter.]

Vice Chairman WARNER. You've been waiting for that answer.

Director POMPEO. I have. I've had that one in the pocket for a while, yes, sir.

Director WRAY. As do I.

Vice Chairman WARNER. One area that I think we were all a little all caught off guard on, and to a degree understandably, was how the Russians use social media. I realize this is a new area for all of us and there are legitimate issues around American civil rights that have to be balanced. But the fact is I think we have to have an organized plan going forward.

This question will be directed at DNI Coats and Director Wray, but if others want to weigh in. Because of the notion that these companies, while maybe located here, operate in cyber space and when we've got somebody masquerading as Mike Pompeo but is actually Boris Badenov in St. Petersburg, it doesn't fit neatly into a particular flow chart.

Director Coats and Director Wray, who is in charge of addressing the threat posed by foreign nationals or foreign nations in terms of their use and misuse of social media?

Director COATS. There's no single agency, quote, "in charge." There are several agencies throughout the Federal Government that have equities in this, and we are working together to try to integrate that process. It clearly is something that needs to be addressed and addressed as quickly as possible.

You and I have had a number of discussions about that. So we are keen on moving forward in terms of not only identification, but relative response and things that we can do to prevent this from happening. We are gaining more, I think, support from the private sector, who are beginning to recognize ever more the issues that are faced with the material that comes through their processes. We cannot as a government direct them what to do, but we certainly are spending every effort we can to work with them to provide some answers to this question.

Vice Chairman WARNER. Great.

Director WRAY. I would agree with Director Coats. I think it's a team effort, and one of the things that's really jumped out at me since being back in government is how much more of a team the intelligence community is than the last time I was in this space. I have one of Mike's people who sits right in my inner team, and vice versa, and we're dealing with each other every day. So it's teamwork within the intelligence community and then partnership with the private sector, which is I think the other big change I've noticed. There's a lot more forward-leaning engagement with the private sector in terms of trying to share information and raise awareness on their end, because at the end of the day we can't fully police social media, so we have to work with them so that they can police themselves a little bit better as well.

Vice Chairman WARNER. Well, let me say I think the companies themselves are slow to recognize this threat. I think they've still got more work to do. But the fact that we don't have clarity in terms of who's in charge means I believe we don't have a full plan.

Let me just get one last question in quickly on the rise—and the Chairman has alluded to this as well—the rise of Chinese tech

companies. I know Senator Cornyn and Senator Feinstein have got legislation on CFIUS. But my fear is that some of these Chinese tech companies may not even have to acquire an American company before they become pervasive in our market.

Again, I'll start with Director Coats and Director Wray: How do we make sure that we send a signal to the private sector before some of these companies in effect totally invade our market, particularly because so many of them are tied back to the Chinese government?

Director COATS. Well, I think it's not only sending a signal and working together, sharing information with the private sector and the public sector. It also I think involves almost a whole of government issue, in particular legislative, with the legislation that is being looked at in terms of the CFIUS process. I think we need to go beyond what the current process is in terms of evaluating. We as a community will coordinate our intelligence to provide policymakers and those that are making these decisions with the best intelligence we can relative to what the situation is.

So we view this as a top priority, and it's ongoing because, as I mentioned in my earlier remarks here, the Chinese are pervasive on this and we've seen it happen throughout both the public and the private sector.

Director WRAY. We've tried very hard to be more out and about in the private sector in terms of providing what are almost like defensive briefings, so that some of the U.S. telecommunications companies, among other technology industry members, kind of can recognize the threats that are coming their way. I think I've been pretty gratified by the response that we've gotten by most companies once we're able to try to educate them.

I think one of the bigger challenges we face is that, because America is the land of innovation, there's a lot of very exciting stuff that's happening in terms of smaller startup companies. A lot of them are a lot less sophisticated about some of this stuff, and trying to make sure we're touching those and educating them as well is a continuing challenge. The reality is that the Chinese have turned more and more to creative avenues, using nontraditional collectors, which I think we in the intelligence community recognize, but I think the private sector is not used to spotting. So a lot of it is trying to educate them about what to be on the lookout for and to have it be more of a dialogue.

Vice Chairman WARNER. Thank you.

Chairman BURR. Senator Risch.

Senator RISCH. Thank you very much.

First of all, I want to associate myself with the remarks of the Vice Chairman when he said that this Committee will always have your backs. For those of you who've been associated with this Committee—Dan, since you used to sit here; and Director Pompeo, you ran the same operation across the way; Mr. Cardillo, Mr. Rogers—you guys seem like part of the committee, we see you so much up there. You know that's the case, and we sincerely appreciate that.

Every one of us here knows what a tough job each of your agencies has. Speaking for myself and I suspect for most, if not all, of the committee, we have absolute 100 percent confidence in your

ability to, in a very neutral, dispassionate fashion, deliver to us the facts that we need in order to make the policy decisions.

One of the things that does rear its ugly head occasionally and causes issues and that winds up in the media a lot more than it should is when your jobs intersect with domestic political affairs. Mr. Wray, probably you will wind up with this more than anybody else. It gets messy. It gets difficult. I think we've all got to recommit ourselves to what we're actually doing here to reach the right facts.

I would respectfully disagree with my good friend from Virginia that we are no better prepared to handle the Russians' onslaught in 2018 than we were in 2016. When this happened in 2016, those of us on this Committee, those of you at the panel, and most of you, most everyone who works in the IC, were not surprised to find out that the Russians were attempting to meddle in our affairs.

I think probably one of the best hearings we've had this year was the open hearing we had on how they use social media. We saw how disjointed it was, how ineffective it was, how cheap it was for them to do that. But I think after that, with all due respect to my friend from Virginia, I think the American people are ready for this. I think that now they're going to look askance a lot more at the information that is attempted to be passed out through social media.

The American people are smart people. They realize that there's people attempting to manipulate them, both domestic and foreign. I agree with everybody on the panel that this is going to go on. This is the way the Russians have done business. This is no surprise to us. We saw it even more so than we got it in France and Germany in the past year.

So I think the American people are much more prepared than they were before.

Dan, thank you for that analysis of Syria. I doubt it made it any clearer for me or for the American people. It's a Rubik's Cube that is very difficult and, after this weekend, I think it got even more complicated. I think that we're going to have to keep an eye on that.

I agree with you, cyber is certainly something that's right at the top. The financial condition of this country is of critical importance to us.

I want to close and I want to ask a specific question to four of you regarding Korea. I think that's the most existential threat that we face. I think it's something that's at our doorstep. A year ago when we talked about this, it was then. This is now. The movement of North Korea has not slowed down. In fact, if anything I think all of us would agree that it's probably picked up. And it's at our doorstep.

This is going to have to be dealt with in the very, very near future. We've talked about trying to engage in conversations and what conditions would be, etcetera. I think we're still in the process of refining that. But that's moving.

We've all watched over the last week the smile campaign that North Korea has inflicted on the South Korean people. The South Korean people seem to be charmed by it to some degree. Some of them seem to be captivated by it. From my point of view, I think

it's nothing more than a stall by the North Koreans to further develop what they're trying to do; and I suspect in my judgment I think we need to be very, very cautious of this.

Director Coats, Pompeo, Rogers, and Ashley, I'd like to hear your view of this supposed turn in the last couple of weeks by the North Koreans?

Director COATS. Well, this is an existential threat, potentially to the United States, but also to North Korea. Kim Jung Un views any kind of kinetic attack or effort to force him to give up his nuclear weapons as an existential threat to his nation and to his leadership in particular.

As you know, it's a very hard collection nation, given their secrecy and so forth. But we do know that it's a one-man decision. We have processes in place here in the United States to have multiple engagements with various agencies in terms of our policymaking and relative to the decision that ultimately the President makes. That does not appear to be the case in North Korea.

The provocative nature and the instability that Kim has demonstrated potentially is a significant threat to the United States. I agree with you that the decision time is becoming ever closer in terms of how we respond to this. Our goal is a peaceful settlement. We are using maximum pressure on North Korea in various ways, which can be described by my colleagues here, most of that in closed session. But we have to face the fact that this is a potentially existential problem for the United States.

Senator RISCH. Wise words.

Director Pompeo.

Director POMPEO. The last part of your question, about this past now almost week at the Olympics: We should all, the American people should all remember that Kim Jung Un is the head of the propaganda and agitation department. There is no indication there's any strategic change in the outlook for Kim Jung Un and his desire to retain his nuclear capacity to threaten the United States of America. No change there.

Senator RISCH. Admiral Rogers.

Admiral ROGERS. I would just say if KJU thinks he can split the relationship between ourselves and the South Koreans he is sadly mistaken.

Senator RISCH. And finally, Lieutenant General Ashley.

General ASHLEY. No change to his strategic calculus. As a matter of fact, under the KJU regime you've seen a much more deliberate effort in terms of readiness, very different from his father. So you've got a million man army, 70 percent of it is south of Pyongyang, and they train in a very deliberate fashion. The strategic calculus has not changed and we should not be misled by the events that are taking place around the Olympics.

Senator RISCH. Thank you so much.

My time is up, Mr. Chairman. Thank you.

Chairman BURR. Senator Feinstein.

Senator FEINSTEIN. Thanks very much.

I want to associate myself with some of the comments of Senator Risch. We just had a secure briefing last week and I think it was difficult and harsh. I harken back to the words of the Secretary of State on the three nos: one, that we do not seek regime change;

two, we do not—we are not seeking the accelerated reunion of the peninsula; and finally, that we will not bring U.S. forces north of the Demilitarized Zone if the Korean Peninsula is reunified.

Let me ask you, Mr. Pompeo, because you just spoke with some certainty: Does Kim Jung Un really understand and believe that our goals are not regime change or regime collapse?

Director POMPEO. Senator Feinstein, I can't give you any certainty about what Kim Jung Un actually subjectively believes. A very difficult intelligence problem anywhere in the world, most especially difficult there. I have expressed this before: We do remain concerned, our analysts remain concerned, that Kim Jung Un is not hearing the full story. That is, that those around him aren't providing nuance, aren't suggesting to him the tenuous nature of his position both internationally and domestically, the breach with China, and the deep connections between the United States and the Republic of Korea.

We are not at all certain that the leaders around him are sharing that information in a way that is accurate, complete, and full.

Senator FEINSTEIN. In a recent Washington Post op-ed, Victor Cha, who was recently under consideration to be United States Ambassador to South Korea, warned of the dangers of a preventive United States military strike against North Korea. He cautioned that such a strike would not halt North Korea's nuclear weapons program and could spark an uncontrolled conflict in the region that could kill hundreds of thousands of Americans.

He is not the only one. A number of experts on the area have said that. He argued to continue to press for multilateral sanctions at the UN, to provide Japan and South Korea advanced weapons training and intel, and some other things.

Has the intelligence community assessed how the North Korean regime would react to a preventive United States attack?

Director POMPEO. We have. I would prefer to share that with you in closed session this afternoon.

Senator FEINSTEIN. Would you do that this afternoon?

Director POMPEO. Yes, absolutely, Senator, yes. We have written about various forms of actions. We analyze the certainty and uncertainty we have around that analysis, as well as what we think happens in the event that the United States decides not to do that and continues to allow Kim Jung Un to develop his nuclear weapons arsenal.

Senator FEINSTEIN. Have you explored what it would take to bring them to the table?

Director POMPEO. We have. I prefer to share that with you in closed session, yes, ma'am.

Senator FEINSTEIN. Would you bring that to our attention this afternoon as well?

Director POMPEO. Yes, ma'am.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Senator Feinstein.

Senator Rubio.

Senator RUBIO. Thank you.

Thank you all for being here. I also echo the same words everyone else has shared with you about the esteem we have for all of our agencies and the important work they do.

I—and I think this has already been touched upon. I do believe that Russia, Vladimir Putin in particular, efforts around the world are very important. But the biggest issue of our time in my view, and I think in the view of most of the Members of this Committee and I would venture to guess most of the members of this panel, is China and the risks they pose.

I'm not sure, in the 240-some odd year history of this Nation, we have ever faced a competitor and potential adversary of this scale, scope, and capacity. It is my personal view, and it's shared by many people, that they are carrying out a well-orchestrated, well-executed, very patient, long-term strategy to replace the United States as the most powerful and influential nation on Earth.

You see that reflected in this repeated use of this term "community of common destiny," which basically means a retreat from Western values of democracy and freedom and openness towards some other model that benefits them. Their pursuit of this appears to be every element of their national power—military, commercial, trade, economic, information, and media.

The tools they use are everything from hacking into companies and critical infrastructure and defense contractors, everybody you can imagine, to using our immigration system against us, to even our universities.

That's where I wanted to begin. This week I—well, let me just ask this, and I'd start this with Director Coats: Is it your view that the United States today as a government is prepared for the scale, scope, and magnitude of the challenge presented by this plan that China's carrying out?

Director COATS. We have full awareness of what the Chinese are, attempting to have full awareness of what the Chinese are attempting to do on a global basis. There's no question that what you have just articulated is what's happening with China. They're doing it in a very smart way. They're doing it in a very effective way. They are looking beyond their own region. I think they have—it's clear that they have a long-term strategic objective to become a world power and they are executing throughout the whole of government ways in which they can accomplish that.

We have intensive studies going on throughout the intelligence community relative to A to Z on what China is doing. General Mattis has asked us for that. Others have asked us to provide that. Senator Warner called me last week. We had a discussion on that. I assured him that we are pulling all of our elements of intelligence-gathering together to provide a very, very deep dive into what China is doing now and what their plans are for the future and how it would impact on the United States.

Senator RUBIO. Just to highlight the different ways and untraditional ways in which they're pursuing this plan, Director Wray, let me ask you, what in your view could you say in this setting is the counterintelligence risk posed to U.S. national security from Chinese students, particularly those in advanced programs in the sciences and mathematics?

Director WRAY. I think in this setting I would just say that the use of nontraditional collectors, especially in the academic setting, whether it's professors, scientists, students, we see in almost every field office that the FBI has around the country. It's not just in major cities. It's in small ones as well. It's across basically every discipline.

I think the level of naivete on the part of the academic sector about this creates its own issues. They're exploiting the very open research and development environment that we have, which we all revere, but they're taking advantage of it.

So one of the things we're trying to do is view the China threat as not just a whole of government threat, but a whole of society threat on their end. I think it's going to take a whole of society response by us. So it's not just the intelligence community, but it's raising awareness within our academic sector, within our private sector, as part of the defense.

Senator RUBIO. In that vein, last week I wrote a letter to five higher education institutions in Florida about the Confucius Institutes, which are funded by Chinese government dollars, at U.S. schools. It is my view that they're complicit in these efforts to covertly influence public opinion and to teach half-truths designed to present Chinese history, government, or official policy in the most favorable light.

Do you share concerns about Confucius Institutes as a tool of that whole of society effort and as a way to exploit the sort of naive view among some in the academic circles about what the purpose of these institutes could be?

Director WRAY. We do share concerns about the Confucius Institutes. We've been watching that development for a while. It's just one of many tools that they take advantage of. We have seen some decrease recently in their own enthusiasm and commitment to that particular program, but it is something that we are watching warily and in certain instances have developed appropriate investigative steps.

Senator RUBIO. Thank you.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Vice Chairman Warner highlighted in his opening statement the importance of an effective security clearance process. So I've got a question for you, Director Wray. Was the FBI aware of allegations related to Rob Porter and domestic abuse? And if so, was the White House informed this could affect his security clearance? When were they informed? And, who at the White House was informed?

Director WRAY. Well, Senator, there's a limit to what I can say about the content of any particular background investigation, for a variety of reasons that I'm sure you can appreciate. I would say that the background investigation process involves a fairly elaborate set of standards, guidelines, protocols, agreements, etcetera, that have been in place for 20-plus years, and I'm quite confident that in this particular instance the FBI followed the established protocols.

Senator WYDEN. So was the White House informed that this could affect his security clearance? That's a yes or no.

Director WRAY. I can't get into the content of what was briefed to the——

Senator WYDEN. What were they informed?

Director WRAY. What I can tell you is that the FBI submitted a partial report on the investigation in question in March and then a completed background investigation in late July; that soon thereafter we received request for follow-up inquiry; and we did the follow-up and provided that information in November; and that we administratively closed the file in January; and then earlier this month we received some additional information and we passed that on as well.

Senator WYDEN. Okay. Let me turn now to the two recent arbitrary and inconsistent decisions that affect the politicizing of the classification system. The first was the public release of the Nunes memo. The second involved the report that the Congress required on Russian oligarchs, their relationship with President Putin, and indications of corruption. In that case the Secretary of the Treasury released nothing other than a list of rich Russians taken from public sources.

My question—and any of you can respond—Did any of you take a position on either of these two arbitrary classification decisions, and did any of you have any communications with the White House about either of those classification matters?

Director COATS. I'll start, and the answer is no.

General ASHLEY. No.

Admiral ROGERS. I raised concerns on this issue with the DNI.

Director CARDILLO. No.

Director POMPEO. The CIA was not asked to review the classification of the document.

Director WRAY. Not on the second, the oligarch Treasury document. We did have interaction about the memo from Chairman Nunes.

Senator WYDEN. Is there anything you can say that protects sources and methods in an open session with respect to that matter?

Director WRAY. Well, I would just say, as we said publicly, that we had grave concerns about that memo's release.

Senator WYDEN. Okay.

On encryption: Director Wray, as you know—this isn't a surprise because I indicated I would ask you about this—you have essentially indicated that companies should be making their products with back doors in order to allow you to do your job. And we all want you to protect Americans. At the same time, sometimes there's these policies that make us less safe and give up our liberties. That's what I think we get with what you are advocating, which is weak encryption.

Now, this is a pretty technical area, as you and I have talked about, and there's a field known as cryptography. I don't pretend to be an expert on it. But I think there is a clear consensus among experts in the field against your position to weaken strong encryption. So I have asked you for a list of the experts that you have consulted. I haven't been able to get it. Can you give me a date this afternoon when you will give me—this morning—a sense of when we will be told who these people are and who is advising

you to pursue this route? Because I don't know of anybody respected in the field who is advising that it is a good idea to adopt your position to weaken strong encryption. So can I get that list?

Director WRAY. I would be happy to talk more about this topic this afternoon. My position is not that we should weaken encryption. My position is that we should be working together, government and the private sector, to try to find a solution that balances both concerns.

Senator WYDEN. I'm on the program for working together. I just think we need to be driven by objective facts, and the position you all are taking is out of sync with what all the experts in the field are saying. I would just like to know who you are consulting with, and we'll talk some more about it this afternoon.

Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Director Pompeo, last week the New York Times published a report that alleged that U.S. intelligence officials had paid $100,000 to a Russian source for phony secrets, including potentially compromising information about the President and information on certain tools allegedly stolen from the NSA.

First, is it accurate that the CIA has categorically denied the assertions in this story? And second, if so, what would be the motivations of a Russian who peddled this story to the New York Times and other Western media outlets? Is this part of the Russian campaign to undermine faith in Western democracies?

Director POMPEO. Senator Collins, first let me say thanks for the question. Reporting on this matter has been atrocious. It's been ridiculous, totally inaccurate. In our view, the suggestion the CIA was swindled is false. The people who were swindled were James Risen and Matt Rosenberg, the authors of those two pieces. Indeed, it's our view that the same two people who were proffering phony information to the United States Government proffered that same phony information to these two reporters.

The Central Intelligence Agency did not provide any resources, no money, to these two individuals who proffered U.S. Government information directly or indirectly at any time. And the information that we were working to try and retrieve was information that we believed might well have been stolen from the U.S. Government. It was unrelated to this idea of kompromat that appears in each of those two articles.

Senator COLLINS. Thank you.

Director Wray, the President has repeatedly raised concerns about current and former FBI leaders and has alleged corruption and political bias in the performance of the FBI's law enforcement and national security missions. I want to give you the opportunity today to respond to those criticisms. What is your reaction?

Director WRAY. Well, Senator, I would say that my experience, now six months in with the FBI, has validated all my prior experiences with the FBI, which is that it is the finest group of professionals and public servants I could hope to work for. Every day, many, many, many times a day, I'm confronted with unbelievable examples of integrity, professionalism and grit.

There are 37,000 people in the FBI, who do unbelievable things all around the world. Although you would never know it from watching the news, we actually have more than two investigations. And most of them do a lot to keep Americans safe.

Senator COLLINS. Thank you. That's one of the reasons I wanted to give you an opportunity to respond.

Director Coats, we've had a lot of discussion this morning about Russian attempts, which are ongoing, to influence elections in Western democracies, to undermine NATO, and to try to destroy institutions in our country and elsewhere. This is an election year in our country and it's, frankly, frustrating to me that we haven't passed legislation to help states strengthen their security of their voting systems.

Putting that issue aside, there is also going to be an election this year in Latvia, one of our NATO allies. What is your assessment of whether or not the Russians are actively engaged in trying to influence that election, and how concerned is the intelligence community that they might be successful in producing a government that is very sympathetic to Russia's foreign policy objectives?

Director COATS. Not only are we concerned, the 29 nations of NATO are concerned. I returned not that long ago from a meeting in Brussels with the intelligence arm of NATO, all 29 nations. The topic was addressed primarily on Russian meddling in elections and trying to undermine democratic values. At the end of that, the new director of that organization asked for a show of hands or any verbal response from any representatives of the 29 nations if they thought that Russia had not interfered with their processes, and particularly their elections, or had the potential to do so. Not one person raised their hand.

He said: So do I understand that we are unanimous in assessing what the Russians are trying to do to undermine our elections, to undermine our coordination with the United States and relationships with each other, to undermine the very basic principles of sharing with other European countries, everything that is accomplished through NATO? Do I understand that no one has an objection to—you all see this for what it is?

Dead silence. He said: I take silence to be consent. So I think that says that this is pervasive, that the Russians have a strategy that goes well beyond what's happening here in the United States, even though—while they have historically tried to do these kinds of things, clearly in 2016 they upped their game. The took advantage, sophisticated advantage of social media. They're doing that not only in the United States, they're doing that throughout Europe and perhaps elsewhere.

So I think that sends a very strong signal that any elections that are coming up need to be—we need to assume that there might be interference with that, particularly from the Russians and maybe from some other malign actors, and steps need to be taken to work with State and local officials, because many of these elections in the off year will be State and local—governorships, even members of certain houses of representation within the states themselves.

So it clearly is an issue that is whole of government and whole of—I would say this: The more—and we also agreed with this at Brussels and I tried to make that point while I was there. The

more transparency we can provide to the American people, to people of nations that see this threat coming, the better off we will be.

Obviously, we have to take other measures. But we need to inform the American public that this is real, that it's going to be happening, and the resilience needed for us to stand up and say we're not going to allow some Russian to tell us how to vote, how we ought to run our country. I think there needs to be a national cry for that.

Senator COLLINS. Thank you. Very valuable.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

Director Wray, the FBI has been accused of political bias recently against the President, by the President himself. In fact, he said the FBI's reputation is, quote, "in tatters." Do you think the FBI's reputation is in any way in tatters, and are you confident in the independence of your agents?

Director WRAY. Senator, there's no shortage of opinions about our agency, just like every other agency up here and just like the Congress. I can only speak from my experience.

Senator HEINRICH. I think you're doing better than the Congress.

Director WRAY. And my experience has been that every office I go to, every division I go to, has patriots, people who could do anything else with their careers, but have chosen to work for the FBI because they believe in serving others. The feedback I get from our State and local law enforcement partners, from our foreign partners, from the folks we work with in the private sector and the community, office after office after office, has been very, very gratifying and reassuring to me.

I'm a big believer in the idea that the FBI speaks through its work, through its cases, through the victims it protects. I encourage our folks not to get too hung up on what I consider to be the noise on TV and in social media.

Senator HEINRICH. So you haven't seen any evidence of some sort of inherent political bias in the agency?

Director WRAY. No.

Senator HEINRICH. How do statements like that impact the morale of rank and file agents, or are they able to shake that off?

Director WRAY. Well, we have 37,000 people. They're all individuals. They all think in their own way. But I guess I would say that our people are very mission-focused. They're accustomed to the fact that we do some of the hardest things there are to do for a living. And I like to think that our folks are pretty sturdy.

I think of a woman I met just the other day, an agent in the Miami office, who had a bad accident, 12 stitches in her face, and the next day, boom, right back at work. I think about the folks in the San Juan office that I visited recently. You want to talk about people going through a real storm. They do it, and they're out in the community. I can tell you, the community values what they do on the island.

Senator HEINRICH. Thank you.

An op-ed by a number of former intelligence analysts called the Nunes memo and its release, quote, "one of the worst cases of politicization of intelligence in modern American history," end quote. You said you had concerns about that memo. I know you

can't get into the gritty details of that, but can you say in your view whether or not one of those concerns is that it may have selectively cherry-picked information without presenting the entire fact pattern that led up to that FISA warrant application?

Director WRAY. Well, Senator, I would just repeat what we said at the time, which is that we had then and continue to have now grave concerns about the accuracy of the memorandum because of omissions. We provided thousands of documents that were very sensitive and lots and lots of briefings, and it's very hard for anybody to distill all that down to three and a half pages.

Senator HEINRICH. Director Pompeo, have you seen Russian activity in the lead-up to the 2018 election cycle?

[Pause.]

Director POMPEO. Yes. I paused only I'm trying to make sure I stay on the unclassified side. Yes, we have seen Russian activity and intentions to have an impact on the next election cycle here.

Senator HEINRICH. Director Coats.

Director COATS. Yes, we have.

Senator HEINRICH. Anyone else? Admiral Rogers.

Admiral ROGERS. Yes, and I think this would be a good topic to get into greater detail this afternoon.

Senator HEINRICH. This afternoon, right.

According to news reports, there are dozens of White House staff with only interim security clearances still, to include Jared Kushner, until last week to include White House Staff Secretary Rob Porter, what I would assume would have regularly reviewed classified documents as part of his job.

Director Coats, if someone is flagged by the FBI with areas of concern in their background investigations into White House staff with interim clearances, should those staff continue to have access to classified materials?

Director COATS. Let me first just speak in general relative to temporary classifications. Clearly, with a new administration in particular, we're trying to fill a lot of new slots. And the classification process and security clearance process, as has been mentioned——

Senator HEINRICH. I'm only speaking with regard to folks who may have had issues raised, as opposed to just being in the matter of course of going through the long process.

Director COATS. Well, I'm not in a position—and we can talk about this in the classified session. But I'm not in a position to discuss what individual situations are for specified individuals. I might just say that I think sometimes it is necessary to have some type of preliminary clearance in order to fill a slot. But I have publicly stated if that is the case the access has to be limited in terms of the kind of information they can be in a position to receive or not receive.

So I think that's something that we have to do as a part of our security clearance review. The process is broken. It needs to be reformed. As Senator Warner has previously said, it's not evolution; it's revolution. We have 700,000 backups. So we have situations where we need people in places, but they don't yet have that.

Your specific question I think I'd like to take up in the classified session.

Senator HEINRICH. Chairman, I'm over my time.

Thank you, Director Coats.

Chairman BURR. Senator Blunt.

Senator BLUNT. Thank you, Mr. Chairman.

Director Coats, Director Pompeo, Admiral Rogers, I think you all talked about evidence that the Russians would intend to do things to be active in our elections. There really seems to me two divisions of that activity. One is information that's put on the record, misleading, false, trying to develop that level. The other, even more sinister, might be the level of dealing with the election system itself, the voting day system, the registration system. Of those two, clearly the voting day system, the one we need to have the most concerns about that critical infrastructure.

This Committee has been working toward both of those goals, of trying to shore up critical infrastructure on Election Day as well as alert people to and decide what might be done about misinformation on the other side of the ledger.

Voting begins in March. That's next month. If we're going to have any impact on securing that voting system itself, it would seem to me that we need to be acting quickly. I think a great part of the strength of the system is the diversity of the system, different not only from State to State, but from election jurisdictions within those states. That's a strength, not a weakness, in my view.

But what are some of the things we can do to be more helpful to local election officials in encouraging them to share information when they think their systems are being attacked, getting more information to them than we have. There was a lot of criticism in the last cycle that we knew that some election systems were being attacked and didn't tell them they were being attacked.

So the three of you in any order. Let's just do the order that I started with: Director Coats, Director Pompeo, and Admiral Rogers. Any thoughts you have on what we can do to protect the critical infrastructure of the election system and how quickly we need to act if we intend to do that this year?

Director COATS. Well, the intelligence community, all elements of it are aware, and we want to provide, collect and provide, as much information as we can, so that we can give those warnings and alerts, so that we can share information back and forth with local and State on election processes.

With the Federal Government, the Department of Homeland Security, the FBI, obviously are more involved, given these are domestic issues. But we do look to every piece of intelligence we can gather, so that we can provide these warnings. It is an effort that I think the government needs to put together at the State and local level and work with those individuals who are engaged in the election process.

In terms of the security of their machines, cyber plays a major role here. So I think it is clearly an area where the Federal Government, foreign collection on potential threats of interference, warnings, and then processes in terms of how to put in place security and secure that to ensure the American people that their vote is sanctioned and well and not manipulated in any way whatsoever.

Senator BLUNT. Director Pompeo.

Director POMPEO. Senator Blunt, when I answered Senator Heinrich's question earlier I was referring to the former, the first part of your question, not truly to the latter. The things we've seen Russia doing to date are mostly focused on information types of warfare, the things that Senator Warner was speaking on most directly earlier.

With respect to the CIA's role—and I think Admiral Rogers will say his, too—we have two missions. One is to identify, identify the source of this information, make those here domestically aware of it so that they can do the things they need to do, whether that's FBI or DHS, so that they have that information. We are working diligently along many threat vectors to do that.

Then the second thing—and we can talk more about this this afternoon—is we do have some capabilities offensively to raise the cost for those who would dare challenge the United States' elections.

Senator BLUNT. After Admiral Rogers, Director Wray, I may want to come to you and see on that same, sharing information, any impediments to sharing that information with local officials or any reason we wouldn't want to do that.

Admiral Rogers.

Admiral ROGERS. Sir, the only other thing I would add—and this is also shaped by my experience at Cyber Command, where I defend networks—is one of the things that we generally find in that role, many network and system operators do not truly understand their own structures and systems. So one of the things that I think is part of this is how do we help those local, federal, State entities truly understand their network structure and what its potential vulnerabilities, and to harness this information that the intelligence structure and other elements are providing them. It's not necessarily an intel function, but I think it's part of how we work our way through this process.

Senator BLUNT. Director Wray.

Director WRAY. Senator, I think that's just one of the areas that—there's been a lot of discussion about whether we're doing better and this is one of the areas I think we are doing better. We together, at the FBI, together with DHS, recently, for example, scheduled meetings with various election, State election officials. Normally the barrier there would be classification concerns, whether somebody had clearances. We were able to put together briefings, appropriately tailored and with nondisclosure agreements, with those officials. So there are ways, if people are a little bit creative and forward-leaning, to educate the State election officials, which is of course where elections are run in this country.

Senator BLUNT. Well, hopefully we'll be creative and forward-leaning and we'll want to keep track of what we're doing there.

Thank you, Mr. Chairman.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman.

The first statement I want to make is more in sorrow than in anger. I'll get to the anger part in a minute. The sorrow part is that, Director Coats, in response to a question from Senator Collins, you gave an eloquent factual statement of the activities of the Russians and the fact that they're continuing around the world and

that they're a continuing threat to this country. All of you have agreed to that.

If only the President would say that. I understand the President's sensitivity about whether his campaign was in connection with the Russians. That's a separate question. But there is no question—we've got before us the entire intelligence community—that the Russians interfered in the election in 2016, they're continuing to do it, and they're a real imminent threat to our elections in a matter of eight or nine months.

My problem is I talk to people in Maine who say: The whole thing is a witch hunt and it's a hoax because the President told me. I just wish you all could persuade the President as a matter of national security to separate these two issues. The collusion issue is over here, unresolved; we'll get to the bottom of that. But there's no doubt, as you all have testified today. We cannot confront this threat, which is a serious one, with a whole of government response when the leader of the government continues to deny that it exists.

Now let me get to the anger part. The anger part involves cyber-attacks. You have all testified that we're subject to repeated cyber-attacks. Cyber-attacks are occurring right now in our infrastructure all over this country. I am sick and tired of going to these hearings, which I've been going to for five years, where everybody talks about cyber-attacks, and our country still does not have a policy or a doctrine or a strategy for dealing with them.

This is not a criticism of the current Administration. I'm an equal opportunity critic here. The prior Administration didn't do it either.

Admiral Rogers, until we have some deterrent capacity we are going to continue to be attacked. Isn't that true?

Admiral ROGERS. Yes, sir. We have to change this current dynamic, because we're on the wrong end of the cost equation.

Senator KING. And we are trying to fight a global battle with our hands tied behind our back.

Director Coats, you have a stunning statement in your report: "They will work to use cyber operations to achieve strategic objectives, unless they face clear repercussions for their cyber operations." Right now there are none. Is that not the case? There are no repercussions. We have no—we have no doctrine of deterrence. How are we ever going to get them to stop doing this if all we do is patch our software and try to defend ourselves?

Director COATS. Those are very relevant questions and I think everyone, not only at this table but in every agency of government, understands the threat that we have here and the impact already being made through these cyber threats. Our role as the intelligence community is to provide all the information we possibly can as to what is happening, so our policymakers can take that, including the Congress, and shape policy as to how we are going to respond to this and deal with this in a whole of government way.

Senator KING. It just never seems to happen. Director Pompeo, you understand this issue, do you not? We are not going to be able to defend ourselves from cyber-attacks by simply being defensive. We have to have a doctrine of deterrence. If they strike us in cyber, they are going to be struck back in some way. It may not be cyber.

Director POMPEO. I would agree with you. I would also argue that—and while I can't say much in this setting, I would argue that your statement that we have done nothing does not reflect the responses that, frankly, some of us at this table have engaged in and the United States Government has engaged in, both before and after this—excuse me—both during and before this Administration.

Senator KING. But deterrence doesn't work unless the other side knows it. The doomsday machine in Dr. Strangelove didn't work because the Russians hadn't told us about it.

Director POMPEO. It's true that it's important that the adversary know it. It is not a requirement that the whole world know it.

Senator KING. And the adversary does know it in your view?

Director POMPEO. I'd prefer to save that for another forum.

Senator KING. Well, I believe that this country needs a clear doctrine: What is a cyber-attack, what is an act of war, what will be the response, what will be the consequences? Right now I haven't seen it.

Director POMPEO. Senator, I agree with you, we collectively. It is a complicated problem, given the nature of——

Senator KING. I include us, by the way.

Director POMPEO. Yes, I would too. I sat as a member of the House of Representatives for six years. I take responsibility for not having been part of solving that, too.

There is a lot of work here to do. We do need a U.S. Government strategy and clear authorities to go achieve that strategy.

Senator KING. I appreciate it. I just don't want to go home to Maine when there's a serious cyber-attack and say: Well, we never really got to it; we knew it was a problem, but we had four different committees of jurisdiction and we just couldn't work it out.

Director POMPEO. Yes, sir.

Senator KING. That's not going to fly.

Director POMPEO. Yes, sir.

Senator KING. Thank you, gentlemen, for your service.

Director COATS. Senator, I might just add that we don't want to learn this lesson the hard way. 9/11 took place because we were not coordinating our efforts. We are now coordinating our efforts, but we didn't have the right defenses in place because the right information was not there. Our job is to get that right information to the policymakers and get on with it, because it's just common sense. If someone is attacking you and there's no retribution or response, it's just going to incentivize more contacts. Right now there are a lot of blank checks. There's a lot of things that we need to do.

Senator KING. Director Coats, thank you. I appreciate that.

Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Thank you.

Director Coats, you and I talked last year about this same issue that Senator King was just bringing up as well about cyber doctrine and a point person, on who that would be, and a defined person that would give options to the President and the Congress to say, if a response is needed and is warranted, this is the person, this is the entity, that would make those recommendations and

allow the President to be able to make the decisions on what the proper response is.

Has that been completed? Is there a point person to be able to give recommendations on an appropriate response to a cyber-attack to the President?

Director COATS. That has not yet been completed. Of course, your understanding of the standup of Cyber Command and the new director that will be replacing Admiral Rogers—the decision relative to whether there would be a separation between the functions that are currently now NSA and Cyber has yet to be made. General Mattis is contemplating what the next best step is. They've involved the intelligence community in terms of making decisions on that role. But we at this particular point cannot point to one sort of cyber czar, but various agencies throughout the Federal Government are taking this very, very seriously and there are individuals that continue to meet on a regular basis.

The ODNI has something called CTIIC and that is a coordination effort for all the cyber that comes in, so that we don't stovepipe like what we did before 9/11. So things are under way. But in terms of putting a finalized, this is how we're going to do it, together, it's still in process.

Director POMPEO. Senator Lankford, with respect to responses to that, these are Title 10 DOD activities unless they are granted to some other authority, a Title 50 authority. So there is a person responsible. Secretary Mattis has that responsibility to advise the President on the appropriateness of responses in all theaters of conflict with our adversaries.

Senator LANKFORD. Thank you.

I want to bring up the issue of the rising threat of what's happening just south of our border in Mexico. In Mexico the homicide rate went up 27 percent last year. We had 64,000 Americans that died from overdose of drugs. The preponderance of those came through or from Mexico. We have a very rapidly rising threat, it appears to me.

What I'd be interested in from you all is, on a national security level and what you're seeing, what are we facing? What's changing right now in Mexico versus ten years ago in Mexico in our relationship and the threats that are coming from there?

Director COATS. I would defer to Director Wray relative to what his agency is doing. Clearly, we have a continuing problem and the Mexican government has a continuing problem relative to the gangs and the organizations. There have been some high-profile arrests lately. We've taken down some labs. Mexico is cooperating, but they themselves will admit that it's almost overwhelming—their army's been participating—it's almost overwhelming for them to control the situation south of the border. We have our own issues then on border protection and as well as consumption here in the United States.

Senator LANKFORD. Director Wray.

Director WRAY. In many ways what we're seeing is just more of the same. But one of the things that's changed, because I think that was at the heart of your question, I think we're seeing—one of the things we're watching in particular is more black market fentanyl being shipped to transnational criminal organizations in

Mexico, and then their taking advantage of the pricing advantages, and that's being then delivered in large quantities to our streets.

Certainly the Mexico relationship is from a law enforcement perspective and from a domestic security perspective one of our most important. I think the FBI LEGAT office in Mexico is our largest in the world. I'm pretty sure about that, or pretty close to it if not. That's a reflection of how much activity there is.

Senator LANKFORD. Let me ask you a specific Oklahoma question. It's also a national question. There was an individual named Alfallaj that was picked up in Weatherford, Oklahoma, just a couple of weeks ago by the FBI. His fingerprints were identified from a terror training camp in Afghanistan. He'd been in the country for multiple years.

What I'm trying to be able to determine is the coordination of information, the local law enforcement and from data that's gathered from some of the work that's happening overseas in Afghanistan and such. How are those two being married together that we can identify individuals that are a threat to our Nation based on their participation in a terror training camp overseas, now coming to the American shores?

Director WRAY. Well, certainly we've become better at looking at biometric information from overseas and marrying it up with potential threat subjects here in the U.S. as well as in some of our allies. The individual in question, of course, turned out to have his fingerprints on information from the Al-Farooq Camp. It's just a reminder to us that an awful lot of people went through those camps. And while the civilized world, the intelligence community, law enforcement, military, our allies around the world, made a major dent on those people, we're kidding ourselves if we think that an awful lot of them aren't still out there, and it's just a reminder that we need to stay on the balls of our feet.

Senator LANKFORD. Thank you.

General ASHLEY. Senator Lankford, if I could. One additional point. You asked what has changed in Mexico. What has also transpired over the last couple years is you had five principal cartels. We alluded to a number of captures that have taken place, over 100. Those five cartels have kind of devolved into 20, and part of that outgrowth, you see an increase in the level of violence.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

Thank all of you. First let me just tell you, on behalf of the people of West Virginia, I want to thank you for the job you do in keeping us safe, the professionalism. And we have all the utmost confidence in what you're doing and hope to be able to support even further. But thank you. The people really do appreciate it and we appreciate the service you're giving.

Director Coats, I think you and I both were in the Senate at the same time when Mike Mullen, then-Admiral Mullen, said that the greatest threat we face—I was on Armed Services; you were on Intelligence at that time. We were trying to find out what the greatest threat the United States faces. I was thinking of another country, whether it be Russia, China, or whatever. He didn't hesitate when he said that the threat of our Nation, the greatest threat is

the debt of our Nation. I think you just reiterated that in your opening remarks.

Director, I was a little bit mystified by the report, the worldwide threat assessment. You didn't mention the debt in here. It wasn't in the report as a threat to the Nation, and I didn't know if there was a thought process behind that, because you made a tremendous effort to put that in your opening statement. I appreciate that. But tell me what your thought process here was?

Director COATS. Well, my thought process was that I'm getting a little bit out of my lane in terms of what I'm supposed to do, but I felt that——

Senator MANCHIN. I mean, you do think it's a threat? It's not in this assessment.

Director COATS. It's just something that Congress needs to deal with, and I didn't want to come back and preach at you.

Senator MANCHIN. I got you.

Director COATS. But I thought at the very end—in fact, just yesterday—look, I think I have a responsibility to raise this issue because it does affect the military significantly, it affects the intelligence community, which is tied to the military in terms of intelligence. It's going to have a serious effect on us if we can't control it.

Senator MANCHIN. Well, you've sat on both sides of the aisle. The only thing that seems to be bipartisan here today is spending money. Both sides seem to agree on spending more money, without any accountability. So I'm glad to hear your remarks on that.

If I could, to all the witnesses: I share what Senator Lankford has said about concerns about what's killing more Americans than any of the threats discussed that we have today. It's with drugs. My State of West Virginia's been hit harder than any State. I've got more deaths per capita than any State. It's been ravaging as far as my communities, my homes, my schools, the families. It's just unbelievable what we're going through.

I think in a nutshell what I would be asking—all of you are responsible to do everything you can to keep us safe and you've done a tremendous job as far as from the foreign attack and things of that sort. Director Wray, I appreciate what the FBI does and they have a strong presence in West Virginia and we're very, very appreciative of that. What type of efforts from each one of your agencies have you spent as far as—Is drugs and fighting the drug infestation highest on your priority list, one of your greatest dangers, or is it just part of the overall scheme of things?

Director COATS. Just speaking for the intelligence community, it is a high priority for us. We mentioned it in our threat assessment here. So we are the collectors of foreign sources, transnational organizations, etcetera, whether it's coming from overseas, whether it's coming from Afghanistan, whether it's coming from Colombia, what it is, how it's going.

Then of course it is a whole of government, because once it penetrates the United States we then use our domestic agencies to address that.

Senator MANCHIN. Director Wray, as far as the FBI, because you're on the front line—you're here on the homeland—what do you think? What can we do to help?

Director WRAY. Well, I think on the good news side, in a country that's often very divided this is one issue as far as I can tell where everybody agrees about what a major, major threat it is. It covers communities from North to South, from red to blue, from rich to poor, from urban to rural. I think that's the good news.

The bad news is that it's grown to a point where there's no one agency or one approach that's going to solve the problem. So we're doing our part. Some of the things that we're able to do, we're focusing particularly on gatekeepers, because a lot of this is coming through medical professionals and pharmacies. So we're using intelligence-driven operations there, various initiatives. We have a prescription drug initiative that's focused on that part of it.

We're partnering with our foreign counterparts. We're working with DEA, State and local law enforcement, etcetera. We're also trying to do things to raise awareness. We did a video with DEA called "Chasing the Dragon," which has been shown in schools around the country.

But this is a multi-disciplinary problem.

Senator MANCHIN. My time is short. If I can just ask this question, maybe. Whoever wants to answer this one. Based on what we know and the way we distribute money for foreign aid to different countries, knowing that a lot of the countries we distribute to is basically allowing, permitting, this type of scourge coming to our country as far as in the form of drugs, have you all thought and considered and make recommendations that we hold them hostage, if you will, or liable, basically, to the money they're receiving from the United States with the best of intentions? But that best of intentions is their fight against drugs coming to our country, when we know it's coming, from whether it be a China, Afghanistan, or Iraq, wherever it may be coming from, Mexico and all the South American countries?

We should hold that. I've never seen—we're going to lose a whole generation in West Virginia. I have 10,000 jobs they can't fill. The United States has 3 million jobs we can't fill. And most of it is around drugs.

So this is what we're asking for. This has got to be all hands on deck. I don't know if anybody wants to—do you have that as a high priority? Does anyone believe we should withhold foreign aid to countries that basically we know have illicit drugs coming to our country?

Director POMPEO. Senator, I'll answer this. I think the United States should use every tool, whether that's foreign aid or other tools——

Senator MANCHIN. Money talks.

Director POMPEO [continuing]. To get these—that's exactly right—to get these nations that this is coming from to put it as a priority for their country. Some don't have the capacity to fix it. That is, it's a problem that's bigger than their nation. But we ought to—we should be unafraid to use the leverage that comes with our generosity from the American taxpayer to ensure that these countries are doing everything they can to prevent drugs from coming from their country to ours.

Senator MANCHIN. Thank you. I appreciate that.

Director COATS. As you do know, we do provide efforts within countries to help them eradicate. It hasn't been totally successful, but that is one way in which we use some of that aid if it's directly contributed to the eradication of drugs.

Senator MANCHIN. Thank you.

Chairman BURR. Senator Cotton.

Senator COTTON. Thank you, gentlemen, for your appearance, and thanks to all the men and women who you represent and for the work they do for our country.

Mr. Wray, are you aware of a gentleman by the name of Oleg Deripaska?

Director WRAY. I've heard the name.

Senator COTTON. Is it fair to call him a Putin-linked Russian oligarch?

Director WRAY. Well, I'll leave that characterization to others, and certainly not in this setting.

Senator COTTON. Chuck Grassley, the Chairman of the Judiciary Committee, last week sent a letter to a London-based lawyer who represents Mr. Deripaska and asked if Christopher Steele was employed, either directly or indirectly, by Oleg Deripaska at the time he was writing the so-called "Steele dossier." Do you know if Christopher Steele worked for Oleg Deripaska?

Director WRAY. That's not something I can answer.

Senator COTTON. Could we discuss it in the classified setting?

Director WRAY. There might be more we could say there.

Senator COTTON. Thank you. And maybe we'll hear back from the lawyer in London as well to give us a straight answer.

Jim Comey testified before this Committee in an open setting last summer and he referred to the Steele dossier as "salacious and unverified." Does that remain the FBI's position?

Director WRAY. I think maybe there's more we can talk about this afternoon on that.

Senator COTTON. Okay, thank you.

I'd like to turn my attention to the threat posed by China and specifically Chinese telecom companies. Senator Rubio spoke earlier, and I agree with what he said, about the threat of a rising China, and also the threat of Confucius Centers. There's also the threat the telecom companies, specifically Huawei and ZTE, but also Unicom and Telecom, pose to our country. That's why I've introduced legislation with Senator Cornyn and Senator Rubio to say the U.S. Government can't use Huawei or ZTE and that the U.S. Government can't use companies that use them. I'm glad that some companies, like Verizon and AT&T, among others, have taken this threat seriously.

Could you explain what the risk is that we face from ZTE and Huawei being used in the United States, especially here in this public setting, the risks that companies, State governments, local governments might face if they use Huawei or ZTE products and services?

Director WRAY. I think probably the simplest way to put it in this setting would be that we're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks that provides the capacity to

exert pressure or control over our telecommunications infrastructure. It provides the capacity to maliciously modify or steal information, and it provides the capacity to conduct undetected espionage.

So at a 100,000-foot level, at least in this setting, those are the kinds of things that worry us. I will say, like you, Senator, we've been gratified I think to date by the response of the large U.S. telecommunications providers trying to raise awareness on this issue. But I also recognize that the competitive pressures are building. So it's something that I think we have to be very vigilant about and continue, as you are doing, to raise awareness about.

Senator COTTON. Admiral Rogers, would you care to add anything about the threat posed by Huawei?

Admiral ROGERS. I would agree with Director Wray's characterization here. This is a challenge I think that's only going to increase, not lessen, over time for us.

Senator COTTON. So you would suggest to mayors, county judges, university presidents, and State legislatures, to look warily if Huawei or ZTE comes bearing gifts to them?

Admiral ROGERS. I would say you need to look long and hard at companies like this.

Senator COTTON. All the witnesses, I'd like to address this question to you. Will you please raise your hand if you would use products or services from Huawei or ZTE?

[No response.]

None of you would. You obviously lead intelligence services, so that's something of a biased question.

Raise your hand if you would recommend that private American citizens use Huawei or ZTE products or services?

[No response.]

None of you again are raising your hand. Thank you for that.

Finally, I'd like to turn to a question, Director Pompeo, that's been in the news in the last few hours. There are reports that over 200 Russian mercenaries were killed in eastern Syria. Can you confirm or deny those reports?

Director POMPEO. Senator Cotton, I'll leave to the Department of Defense to talk about what transpired there. I can say this. From an intelligence perspective, we have seen in multiple instances foreign forces using mercenaries in battles that will begin to approach the United States.

Senator COTTON. General Ashley, since you represent the Department of Defense, would you like to confirm or deny?

General ASHLEY. If we could take that to a closed session, Senator, I think we can lay out a rather interesting fabric of what is Syria and what transpired over the last few days.

Senator COTTON. We can address that in the afternoon.

Director Pompeo, to come back, as a general matter can I ask, is massing and maneuvering forces against a location where U.S. personnel are present in Syria a good way to get yourself killed?

Director POMPEO. I think I'll defer that to the Department of Defense as well.

Senator COTTON. General Ashley, would you like to answer that question?

General ASHLEY. Sir, that does make you more susceptible. I would leave that also to the operational commander. But you are at greater risk when you start to mass in that situation.

Senator COTTON. Not a good idea if you want to have a long and fruitful life.

Thank you.

Chairman BURR. Senator Harris.

Senator HARRIS. Thank you.

I want to echo the comments of my colleagues in thanking the men and women who serve in your agencies. I am concerned that the political attacks against the men and women of your agencies may have had an effect on your ability to recruit, retain, and also the morale of your agencies. So I would like to emphasize the point that we all I think share in making, which is we thank the men and women of your agencies for their selfless work. They do it on behalf of the American people, without any expectation of award or reward, and we cannot thank them enough for keeping us safe.

Director Wray, Chairman Nunes's memo included sensitive FISA information regarding a person who worked on the President's campaign. According to the White House statement, the President was the one who authorized the memo's declassification. Do you believe there is an actual or at least the appearance of a conflict of interest when the President is put in charge of declassifying information that could complicate an ongoing investigation into his own campaign?

Director WRAY. Well, Senator, we've been very clear what our view was about the disclosure and accuracy of the memo in question. But I do think it's the President's role as Commander-in-Chief under the rule that was invoked to object or not to the declassification. So I think that is the President's responsibility.

Senator HARRIS. Regardless of whether there is an appearance or actual conflict of interest?

Director WRAY. Well, I leave it to others to characterize whether there's an appearance or actual conflict of interest. But I think the President was fulfilling his responsibility in that situation.

Senator HARRIS. If the President asked you tomorrow to hand over to him additional sensitive FBI information on the investigations into his campaign, would you give it to him?

Director WRAY. I'm not going to discuss the investigation in question with the President, much less provide information from that investigation to him.

Senator HARRIS. And if he wanted—if he received that information and wanted to declassify it, would he have the ability to do that, from your perspective?

Director WRAY. Information from the——

Senator HARRIS. However he received it, perhaps from members of the United States Congress.

Director WRAY. I think legally he would have that ability.

Senator HARRIS. Do you believe the President should recuse himself from reviewing and declassifying sensitive FBI material related to this investigation?

Director WRAY. I think recusal questions are something I would encourage the President to talk to the White House counsel about.

Senator HARRIS. Has the FBI done any kind of legal analysis on these questions?

Director WRAY. Well, happily, I'm no longer in the business of doing legal analysis. I now get to be a client and blame lawyers for things, instead of being the lawyer who gets blamed. So we have not done a legal analysis.

Senator HARRIS. Have you blamed any lawyers for their analysis of this issue?

Director WRAY. What's that?

Senator HARRIS. Have you blamed any lawyers for their analysis of this issue?

Director WRAY. I have not yet, no.

Senator HARRIS. Okay.

Is the FBI getting the cooperation it needs from social media companies to counter foreign adversaries' influence on our elections?

Director WRAY. I think the cooperation has been improving. I think we're continuing to work with the social media companies to try to see how we can raise their awareness, so that they can share information with us and vice versa. So I think things are moving in the right direction, but I think there's a lot of progress to be made.

Senator HARRIS. What more do you need from social media companies to improve the partnership that you'd like to have with them to counter these attacks?

Director WRAY. Well, I think we always like to have more information shared more quickly from their end. But I think from their perspective it's a dialogue. They're looking to get information from us about what it is we see, so that they can give responsive information. So I think we're working through those issues.

Senator HARRIS. Do you believe that the social media companies have enough employees that have the appropriate security clearance to make these partnerships real?

Director WRAY. That's not an issue I've evaluated, but I'm happy to take a look at it.

Senator HARRIS. Please do, and follow up with the Committee.

Director Coats, one of the things that makes guarding against foreign intelligence threats on social media so complex is that the threat originates overseas and so that would be within the jurisdiction of the CIA and the NSA, and then it comes to our shores and then it passes on to the FBI and also the social media companies themselves.

I'm not aware of any written IC strategy on how we would confront the threat to social media. Does such a strategy exist in writing?

Director COATS. I would have to get back with you on that. I'd be happy to look into it. From my perspective right now, a written strategy, specific strategy, is not in place, but I want to check on that.

Senator HARRIS. Please do follow up.

Also, last year Congress passed a bipartisan Russia sanctions bill. However, the Administration has not imposed those sanctions. From an intelligence perspective, what is your assessment of how Russia interprets the Administration's inaction?

Director COATS. I don't have information relative to what the Russian thinking is in terms of that particular specific reaction. There are other sanctions, as you know, that are being imposed on Russian oligarchs and others through the United Nations and through other things that have been done in reference to the JCPoA. But specifically on your question, I don't have an answer for that.

Director POMPEO. Senator Harris.

Senator HARRIS. Yes?

Director POMPEO. May I comment? I think we ought to look at that in a broader context. That is, how the Russians view all of the actions of this Administration, not just a particular set of sanctions or the absence thereof. So as we've watched the Russians respond to this Administration's decision to provide defensive weapons in Ukraine, to push back against Russian efforts in Syria, sanctions placed on Venezuela were directly in conflict with Russian interests, the list of places that the Russians are feeling the pain from this Administration's actions are long.

Senator HARRIS. But, Director Pompeo, I'm sure you would agree that in order to understand the full scope of effect it is also important that we analyze each discrete component, including what is the interpretation of this Administration's failure to enact the sanctions as has been passed and directed by the United States Congress in a bipartisan manner. Have you done that assessment?

Director POMPEO. Senator, in closed session I'll tell you what we know and don't know about that discrete issue.

Senator HARRIS. Right.

Director POMPEO. Yes, and I agree with you it is important to look at each one in its own place. But I think what we most often see in terms of Russian response, it's to the cumulative activities in response to Russian activities. That is how the United States responds to those, in a cumulative way.

Senator HARRIS. Thank you. I look forward to our conversation. Thank you.

Director POMPEO. Yes, ma'am.

Chairman BURR. Senator Cornyn.

Senator CORNYN. Director Coats, you alluded to the activities of transnational criminal organizations, and I'm thinking particularly as regards our neighbors down south of our border. Recently I heard somebody refer to the cartels, these transnational criminal organizations, as "commodity agnostic." In other words, they'll traffic in people, they'll traffic in drugs and other contraband, all in pursuit of money.

Director COATS. Whatever brings in the most dollars.

Senator CORNYN. Senator Manchin I know and others have alluded to their concern about—and certainly we all share the concern about the deaths and overdoses caused by drugs in America, much of which comes across our southern borders through our ports of entry. This week we're going to be considering border security measures as part of a larger package that the President has proposed while addressing the so-called "DACA recipients."

But, do you believe that modernizing our ports of entry and providing enhanced technology and other means to surveil, follow and

identify illegal drugs coming across our ports of entry would be a good thing for us to do?

Director COATS. I do. I do think that a layered approach is necessary to—it's clear that just one specific defense put in place is not going to solve the problem. It needs to be a layered interest of not only physical facilities, but also Border Patrol, also how those who arrive and perhaps dissipate in waiting for their court appearance, tracking them—a whole range of things that I think are going to be needed to stop that flow from coming in.

Senator CORNYN. I know it's been alluded to, but just to emphasize my concern with the demand side. Maybe we've given up—I hope not—in addressing the demand side, which of course provides the money and the incentive for these cartels to operate, and it's something I think deserves full attention and focus of the United States Government. I've heard General Kelly in his previous job at DHS talk about that, and I hope we will return to that focus as part of this layered approach, the demand side, because it's something I think that is maybe the hardest thing to deal with, but perhaps might have the greatest impact.

Director COATS. The supply depends on the demand and the demand drives the supply and provides the capital, with which to take extraordinary methods that bypass our defenses in order to get those drugs into the United States.

On the demand side, this is a whole of the American people process. It's PTA's. We growing up got these videos of driving in driver's training and the horrendous look at crashes and so forth and so on. We need to let every student know what the consequences of these drugs are to their lives and to their future. We need to get parents involved, parent-teacher associations involved, so whether they pick up their values from church or from the neighborhood or whatever.

This is a national crisis and we all of us here represent or are from states which are staggering through the process here of watching young people and others die from drugs that are more potent than they've ever been.

Senator CORNYN. Let me just lay down a couple of markers here in my comments, but then I want to end on CFIUS, the Committee on Foreign Investment in the United States.

I will join Senator Rubio and Senator King, Senator Lankford, and others concerned about the failure of the U.S. Government again to have an all-of-government strategy to deal with the cyber threat. I have no doubt in my mind that we have superior capabilities, but they're stovepiped. I don't think we, the policymakers, are doing a good enough job, and I think it's incumbent upon us to try to provide some policy guidance so that you and others in the intelligence community and the national security apparatus can address this threat in the way that it needs to be addressed.

Our adversaries don't suffer from a lack of an all-of-government policy. They are all over that. China, I agree with Senator Rubio about their strategy, and some of you have responded to that.

But one of the strategies that China and other countries have adopted is to avoid some of the review measures in the Committee on Foreign Investment in the United States when it comes to direct investment, buying those dual-use technologies, startup companies

and the like, and then using that to gain strategic advantage against the United States.

I wonder if maybe, Director Wray, could you address that; and then anybody else in the time permitted, I'd be glad to hear what you have to say about that.

Director WRAY. Senator, I think you're exactly right that CFIUS reform is particularly relevant to the China threat, although not exclusively China threat. And there is a degree to which CFIUS as it currently stands is susceptible too much to the kind of "round pegs only go in round holes" kind of thing. It's not hard to come up with other-shaped pegs to get around that process, the obvious example being joint ventures, but there are other ways as well. So that's one of the significant problems.

Another problem is the amount of time that's built into the process to do a thorough review, which is too short. Another problem is the inability to share information, since other countries, our allies, are going through the same thing, to be able to share information, so when they go through their own versions of the CFIUS process they have the benefit of what was attempted in our country, and vice versa.

I think in general we need to take a more strategic perspective on China's efforts to use acquisitions and other types of business ventures, as opposed to just a tactical, looking only within the four corners of one particular transaction.

General ASHLEY. If I could, the Director laid out really kind of the bigger issue at the strategic level and for us at DIA, we're kind of taking on the tactical. So we're the ones that are right about ready to penetrate the line. So if you look at supply chain risk management, we actually run the Threat Analysis Center that is hooked into CFIUS. So we bring the services together and look at supply chain risk management for CI issues associated with whomever may get a contract and ties back to China and other nations.

But you allude to the fact that every case for CFIUS comes back and we take a look at it. We get about three days with it. We could use more time to make a more thorough scrub.

Senator CORNYN. Thank you.

Chairman BURR. Thank you.

Senator Reed.

Senator REED. Thank you, Mr. Chairman. I apologize for being late. We had a simultaneous hearing in the Armed Services Committee on SOCOM.

All morning, gentlemen, we've heard the story of Russia influencing our campaigns and indeed in the current campaign for the midterms. So let me begin with Mr. Wray and say: Has the President directed you and your agency to take specific actions to confront and blunt Russian influence activities that are ongoing?

Director WRAY. We're taking a lot of specific efforts to blunt——

Senator REED. Directed by the President?

Director WRAY. Not specifically directed by the President.

Senator REED. Director Pompeo, have you received a specific presidential direction to take steps to disrupt these activities?

Director POMPEO. I'm not sure how specific. The President's made very clear we have an obligation from our perspective, from a foreign intelligence perspective, to do everything we can to make

sure that there's a deep and thorough understanding of every threat, including threats from Russia.

Senator REED. But has he singled out the Russian threat, which appears to be critical to this election coming up? I know there are threats from many different vectors, but have you received a specific threat, i.e., it's very important to him to get this done correctly?

Director WRAY. Yes, I think the President's been very clear that he has asked our agency to cooperate with each of the investigations that's ongoing and do everything we can to ensure that we thoroughly understand this potential threat.

Senator REED. Director Coats, have you received a specific directive to take specific steps to disrupt, understand first and then disrupt, Russian activities directed at our elections on 2018?

Director COATS. I would echo what Director Pompeo just said. We work together on this throughout. The agency has full understanding that we are to provide whatever intelligence is relevant and make sure that that is passed on to our policymakers, including the President.

Senator REED. Passing on relevant intelligence is not actively disrupting the operations of an opponent. Do you agree?

Director COATS. No. We pass it on and they make the decision as to how to implement it.

Senator REED. As the Director of Intelligence, are you aware of or leading an inter-agency, an inter-governmental working group that is tasked with countering Russian activities? Not merely reporting on it, but tasked with countering those activities? Are you aware of any type of inter-agency group, any inter-governmental groups since State elections are critical or State elected officials are critical?

Director COATS. Well, we essentially are relying on the investigations that are under way, both with this Committee and the HPSCI Committee, as well as the Special Counsel.

Senator REED. So you're not taking any specific steps, based on the intelligence, to disrupt Russian activities that are occurring at this moment?

Director COATS. We take all kinds of steps to disrupt Russian activities in terms of what they're trying to do. I think I'll turn it over to Director Pompeo to——

Senator REED. Let me finish with the rest of the gentlemen. Are you finished, Mr. Coats, Director Coats?

Director COATS. Yes.

Senator REED. Thank you. Thank you.

Director POMPEO. Senator Reed, we have a significant effort. I'm happy to talk to you about it in closed session. The CIA—and it is not just our effort. It is a certainly all-of-IC effort—there may be others participating as well—to do our best to push back against this threat. It's not just the Russian threat. It's the Iranians and Chinese. It's a big, broad effort.

Senator REED. I understand, Mr. Director, we have mutual threats, but one threat that has been central. And you've testified to this publicly. The last election there was Russian influence. This election, they seem to be more prepared. They've learned their lessons. The simple question I pose is: Has the President directed the

intelligence community in a coordinated effort, not merely to report, but to actively stop this activity? The answer seems to be that I'm hearing is the reporting's going on, as we're reporting about every threat coming in to the United States.

Let me get back quickly. Do any of the other panelists have anything to add on this point?

Admiral ROGERS. For us, I can't say that I've been explicitly directed to, quote, "blunt" or actively stop. On the other hand, it's very clear, generate knowledge and insight, help us understand this so we can generate better policy. That clearly—that direction has been very explicit, in fairness.

Senator REED. But I think again—you may agree or disagree—collecting intelligence, then acting on it in a coordinated fashion, are two different things.

Admiral ROGERS. Yes, sir. I'd also argue, what's our role as intelligence professionals in all of this?

Senator REED. Let me just end. I've got very few moments remaining. We've talked a lot about China, CFIUS, and their involvement in trying to buy companies in the United States. What I think has to be pointed out, too, is they are undertaking significant national investment in artificial intelligence and quantum computing that is dwarfing anything that the Administration is proposing or suggesting.

If artificial intelligence has even half of the benefits that its promoters claim, it is going to be extraordinarily disruptive. Quantum computing has the capacity to undercut cryptology as we know it, and the experts can correct me if I'm wrong. Some of the mechanisms that quantum computing can generate could, based on infinite measurements of gravity, detect devices underground and under the water, which for anybody who's a submariner, you've got to be wondering.

So where is our national Manhattan program for AI and quantum computing that will match the Chinese? Director Coats, you seem to be anxious to answer that. I'll let you do that.

Director COATS. I think there are some things that we'll talk about in a classified setting here. We're treading a very narrow line here relative to discussing this in an open meeting.

Senator REED. I don't want to tread that line, but we do have to recognize that, again, the Chinese activity to appropriate our intellectual property is obvious. They are generating their own intellectual property at a rate that could be disruptive and we are not matching them. Again, this Manhattan analogy might be a little bit out of date, but when we saw the potential effects of a scientific development back in the forties, we spared no expense so that we would get it first before our opponents.

The Chinese seem to be making that type of commitment very publicly: hundreds of millions, billions of dollars. They've said publicly; they have a plan and they're working the plan.

Director COATS. And we provide that information to the extent that we can collect that information. But just like the Manhattan Project, we don't openly share what steps that we're taking to address it.

Senator REED. I respect that.

Thank you, Mr. Chairman.

Thank you, sir.

Chairman BURR. Thank you, Senator Reed, and I do hope you'll come back to the closed session if you can this afternoon. I think that you'll get some fidelity in that closed session.

I want to turn to—we're about to wrap up. Everybody can look up. There are no more questions, so you don't have to lose eye contact with us hoping you're not the guy that they're going to ask to answer.

[Laughter.]

You can tell who the newbies are. They've stayed focused on the Members the entire time; and the ones that have been here before have been like this (indicating.).

I want to turn to the Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

We look forward to seeing you all this afternoon. Robert, we hope to get some overhead questions to you this afternoon.

Echoing what we've all said, appreciate your service. But I think we're hearing again a lot of commonality as we think about cyber, misinformation, and disinformation. It really is asymmetrical.

One of the things that has struck me is that if you do a rough calculation and add up the costs to Russia in terms of their intervention in America, elections, the Dutch elections where they hand-counted all the ballots, the French elections where Facebook acknowledged taking down 30,00 sites. You add that all together, it's less than the cost of one new F–35 airplane. Pretty good bang for the buck.

I remember a year or so ago at Langley looking at some of our fighter technology, stealth technology, and the colonel showing me around bemoaning the fact that the Chinese had gotten this again on the cheap by stealing a lot of the intellectual property that underlies that technology.

Echoing what Senator Reed said—and again, I think this is where we all need to put our heads together—we just made a massive additional investment in DOD. We're at roughly ten times the size on our spend versus our near-peer adversaries like China and Russia. I do feel, not from a criticism standpoint, but more from just where we ought to be thinking about going forward, that we may be buying the best twentieth century military that money can buy, when we see our near-peer adversaries making these massive investments in areas like AI, machine learning, quantum computing. I think we all need to think through this from a general strategic standpoint.

I worry that we've got certain low-hanging fruit as we think about Chinese tech companies and how to get CFIUS right. One of the things some of us discussed with you in the past is, if you look simply at IoT-connected devices, we're going to double the number from about 10 billion to 20 billion in the next three to five years. Yet we have no even de minimis security requirements for the Federal Government purchasing of IoT devices.

I would—I know I've talked with General Ashley on this. I don't believe there is, even across the IC and DOD, prerequisite that before we buy some of these connected refrigerators or sensors or common consumer goods, that there be that patchability or no embedded passcodes.

So I think again there's a lot of work we can do, but we don't have the luxury of short time.

Senator Blunt raised some of the questions around election security. I know the Chairman's going to make this comment in his closing remarks. I think this Committee has done some very good bipartisan work in a series of areas that arose out of the Russia investigation. It's our hope that on election security we can come forward with a set of recommendations very quickly, because we have primaries coming up as early as March. My hope is that there will be able to be bipartisan legislation to try to start addressing this issue.

So thank you, gentlemen. I look forward to our session this afternoon. With that, I'll turn it over to the Chairman.

Chairman BURR. Thank you, Vice Chairman.

Admiral Rogers, I can't remember whether it was you or somebody else at the table said when we had a closed session about investment: It's not how much we spend; it's how we deploy the capital that we've devoted to a particular thing. I think as a general statement we get much better at the way we deploy capital, and I think we deploy it with a measurement tool today on return that's totally different than it was 10 and 20 and 30 years ago. I think that's important.

This Committee has a global mandate, a mandate that I think has been reflected, I think, in the statements and the questions of the Members of this Committee today. It's my hope that the American people got a sense of the breadth of topics this Committee deals with on a daily basis, and so do you.

What was unsaid today? What was unsaid is that the Special Counsel is not the only investigation that's going on in Washington. The scope of the Special Counsel's investigation was clearly stated by the DAG when he hired Bob Mueller. I think the media has spent some portion of every day trying to portray that the scope of that investigation has changed.

The truth is I don't know. I'm not sure that anybody in this room knows. But here's what I do know: I know the Senate Intel investigation continues. We're hopefully wrapping up some important areas that we have focused on. The Vice Chairman just alluded to the fact that it is our hope and our belief that before the primaries begin we intend to have an overview of our findings that will be public. We intend to have an open hearing on election security. And it's the Committee's intent to make recommendations that will enhance the likelihood that the security of our election process is in place.

In addition to that, our review of the ICA, the Intel Community Assessment which was done in December of 2016, we have reviewed in great detail, and we hope to report on what we found, to support the findings where it's appropriate, and to be critical if in fact we saw areas that we found came up short. We intend to make that public. To begin with, none of these would be without a declassification process, but we will have a public version that we air as quickly as we can.

The third piece is the review of when we learned of Russia's intrusions into our system, what we did or what we didn't do, and again with the intent of sharing as much of that with the American

public as we can find through open hearings and through an overview.

Lastly, we will continue to work towards conclusions related to any cooperation or collusion by any individual, campaign, or company with efforts to influence the outcome of elections or to create societal chaos in the United States.

I want to thank each of you at the table for an unprecedented access to intelligence products, legal documents, and other materials that were needed for us to do our job.

We have a very talented group of individuals who have conducted this investigation. The remarks of every individual who has come in before us has commented on their professionalism and the fact that at the end of eight hours they couldn't tell who was a Democrat and who was a Republican. So the effort to be bipartisan has not just been public; it is private as well, and permeates all the way down through our staff.

They couldn't do this in a timely fashion without the access that each of you have provided us and your agencies. Let me just reiterate again: We understand that this is an unprecedented access to this information.

I promised you when we started a year ago that the sensitive nature of that material would in fact be protected. The Vice Chairman and I have done everything in our power to do that. We think we have maintained that promise. There have been times where information has found its way out, some of recent, where it didn't come from us, but certainly have portrayed it did. And that's okay, because you know and we know the security measures we've got in place to protect the sensitivity of that material.

We have also protected the sensitivity of the individuals that have been interviewed, voluntarily. The individuals who have come in, what they've shared with us; to date we have not released any interview notes, because that's not for public consumption. We ask people to come in and share with us things that help us understand what happened. It's our responsibility to take that information and to put it into some form that furthers the American people's understanding and assurance that we have thoroughly reviewed this.

We will continue the promise that we made to each of you until the conclusion of this investigation and on. There are no expectations that everything you have shared with us is now a precedent that you have to continue. I hope it's not. I have said publicly, and criticized for it, that our Committee was created to operate in secrecy, I believe that's where we perform our best work, and we're given the opportunity and the need for the American people to have a better understanding, that we should provide that for them in as controlled an atmosphere as we do.

Today is an example of that, and we can now move from a public setting to a more private and closed setting to continue to get some clarity on some of the issues that our Members need.

I want you to understand the take-away here. The take-away is this Committee has and will continue to focus on answering the question that was given to this Committee from an investigation standpoint: What Russia did to influence the 2016 elections? There are efforts to expand our efforts. They are not internal. We realize

we have to answer for the American people: What did Russia do to mess with the 2016 elections?

Like many of you, on some of the questions when we've asked that were specific about it in public and in private, we find it's multi-jurisdictional. We've got to begin to sort that out for us, us the American people.

So I thank you for your willingness to be here today. I thank you for the performance of your employees, who have worked tirelessly with very little thanks, and of late with a lot of criticism, to keep this country safe, and I might say to keep other countries safe, because we are very generous when we know that bad things are going to happen.

The Committee is appreciative of the relationship that we have. We will continue to work to earn your trust, because that's the only way we can perform the type of oversight that we believe the Committee is mandated to do. And for the cooperation that each one of you provides us, we're grateful for that.

With this, this hearing's adjourned until a closed session at 2:30.

[Whereupon, at 12:10 p.m., the hearing was adjourned.]

Supplemental Material

UNCLASSIFIED RESPONSES TO QUESTIONS FOR THE RECORD
SENATE SELECT COMMITTEE ON INTELLIGENCE
HEARING FEBRUARY 13, 2018

Hearing Date: February 13, 2018
Committee: SSCI
Member: Sen. Rubio
Witnesses: Director Coats
Info Current as of: April 2, 2018

Question: The National Security Strategy of the United States emphasizes, "The United States also remains committed to supporting and advancing religious freedom."

What kind of violations and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?

Answer:

Most foreign government violations of religious freedom—from the persecution of small communities of Baha'is and Jehovah's Witnesses in many countries to North Korean prohibitions against all faiths—can be categorized as human rights concerns that might create conditions for future harm to U.S. national security interests. More direct threats to U.S. interests primarily arise when religious repression fuels either the growth of anti-Western violent extremism or instability in a country, such as majority-Buddhist Burma's crackdown on its population of 2 million Muslim Rohingyas, which the United Nations and others have described as ethnic cleansing. Violations by governments against Muslims, for example, can bolster Islam-under-attack narratives that jihadist groups use to attract recruits and advance their agendas against the West and its partners. Government violations of religious freedom also can fuel societal intolerance against the targeted faiths, which in turn can lead to societal tensions, protests, political turmoil, or other forms of instability in a wide variety of places around the globe, including China and Western Europe.

- Among the governments that violate religious freedoms—Burma, China, Eritrea, Iran, North Korea, Saudi Arabia, Sudan, Tajikistan, Turkmenistan, and Uzbekistan—are designated by the Department of State as Countries of Particular Concern (CPC) for engaging in or tolerating "systematic, ongoing, and egregious" violations. In 2017, the U.S. Commission on International Religious Freedom (USCIRF) recommended designating Russia and Syria as CPCs and placed Egypt, Indonesia, and Malaysia on the second-highest tier of concern.

- Of the non-CPC countries, Egypt, Indonesia, Malaysia, Russia, and Syria ranked highest on the Pew Research Center's most recent index of government violators compiled in December 2015. Sunni terrorist groups are internationally notorious for being among the more egregious violators of religious freedom globally.

Hearing Date:	**February 13, 2018**
Committee:	**SSCI**
Member:	**Sen. Rubio**
Witnesses:	**Director Coats**
Info Current as of:	**April 2, 2018**

Question: The National Security Strategy of the United States emphasizes, "The United States also remains committed to supporting and advancing religious freedom."

What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security or countering extremism?

Answer:

The depth and breadth of religious freedom violations around the world varies from country to country but is historically elevated, according to diplomatic, UN, and other open-source reporting. The level of violations in the early and mid-1990s that spurred passage of the 1998 International Religious Freedom Act has since worsened, according to the USCIRF and other open-source reporting. Government restrictions on religious practice increased in all major regions of the world between 2007 and 2015, according to the Pew Research Center, while social hostilities and violations by nonstate actors also steadily increased in most regions. Department of State and USCIRF reporting highlights the growth in recent years of government violations of religious freedom tied to laws intended to counter terrorism or extremism.

Hearing Date:	**February 13, 2018**
Committee:	**SSCI**
Member:	**Sen. Wyden**
Witnesses:	**Director Coats**
Info Current as of:	**April 23, 2018**

Question: Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior US government officials, defense contractors, and scientists through their personal email accounts. (AP, "'Fancy Bear' hackers took aim at US defense contractors," February 7, 2018.)

Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?

Answer:

The personal accounts and devices of government officials can contain information that is useful for our adversaries to target, either directly or indirectly, these officials and the organizations with which they are affiliated.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Wyden**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

Question: Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior U.S. government officials, defense contractors, and scientists through their personal email accounts. (AP, "'Fancy Bear' hackers took aim at U.S. defense contractors," February 7, 2018.)

What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?

Answer:

We have the resources we need to continue our respective education and awareness programs, which are the most important weapons in the cyber-battlefield when it comes to personal devices and accounts. We also need to continue to harden our government systems, both classified and unclassified, to prevent the potential compromise of a Government-issued personal device or account from becoming a major cyber-intrusion or cyber-success against our government networks or programs; I have made this a priority for the IC. If these programs require additional resources, I will inform this committee.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Cotton**
Witnesses: **Director Coats**
Info Current as of: **March 29, 2018**

Question: In 2017, the Director of the Central Intelligence Agency referred to WikiLeaks as a "non-state hostile intelligence service" that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

Do you agree with Director Pompeo and this Committee that WikiLeaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?

Answer:

Yes, WikiLeaks should be viewed as a non-state hostile foreign intelligence entity whose actions, both individually and in collaboration with others, have caused harm to U.S. national security and interests.

Hearing Date:	**February 13, 2018**
Committee:	**SSCI**
Member:	**Sen. Heinrich**
Witnesses:	**Director Coats**
Info Current as of:	**April 23, 2018**

Question: How long can personnel from the Executive Office of the President (EOP) hold an interim clearance before the clearance process is terminated and access suspended?

Answer:

Under Executive Order 12968 (EO 12968), where official functions must be performed prior to the completion of the investigation and adjudication process, temporary eligibility for access to classified information may be granted. EO 12968 imposes no time limit on temporary access.

Hearing Date:	**February 13, 2018**
Committee:	**SSCI**
Member:	**Sen. Heinrich**
Witnesses:	**Director Coats**
Info Current as of:	**April 23, 2018**

Question: What accountability is there to the DNI, as the government's security executive agent, for the granting of interim security clearances generally, and the interim SCI clearances, specifically?

Answer:

While the DNI has policy and oversight responsibilities for Government personnel security programs and access to SCI, under authorities set forth in statute and Executive Order, Agency Heads are responsible for establishing and maintaining an effective program to ensure that temporary access to classified information by personnel is clearly consistent with the interest of national security. Agency Heads are responsible for following the DNI's policy guidance when granting such clearances.

Hearing Date:	**February 13, 2018**
Committee:	**SSCI**
Member:	**Sen. Heinrich**
Witnesses:	**Director Coats**
Info Current as of:	**April 23, 2018**

Question: Has the DNI reviewed all the cases of interim access to SCI, both in the EOP and across the government?

Answer:

The DNI does not routinely review cases of interim access to SCI in the government. The DNI does not recommend temporary accesses be granted or denied in specific cases unless an Agency Head specifically requests guidance.

Hearing Date: February 13, 2018
Committee: SSCI
Member: Sen. Heinrich
Witnesses: Director Coats
Info Current as of: April 23, 2018

Question: Are personnel with interim access to SCI under a Continuous Evaluation protocol, and if so, who manages that?

Answer:

Personnel with interim access may be under Continuous Evaluation. Identification of the population covered by Continuous Evaluation is the responsibility of the Agency Head.

Hearing Date:	**February 13, 2018**
Committee:	**SSCI**
Member:	**Sen. Heinrich**
Witnesses:	**Director Coats**
Info Current as of:	**April 23, 2018**

Question: Are there executive branch and EOP personnel who have held interim access to SCI for longer than one year, and if so, how many such personnel and in what agencies do they work?

Answer:

In terms of EOP interim SCI access, the best source of information would be EOP, and I would defer to them to address questions regarding EOP personnel with interim access to SCI.

Hearing Date: February 13, 2018
Committee: SSCI
Member: Sen. Harris
Witnesses: Director Coats
Info Current as of: April 16, 2018

Question: You have the authority to issue Intelligence Community Directives that establish policy across the IC. Your predecessor used that authority to establish specific duties to warn victims?

Will you commit to using that same authority to establish a specific duty to warn states about election related cybersecurity threats? If not, why not?

Answer:

We appreciate the importance of this issue, and the IC remains committed to warning our intelligence consumers about the wide range of serious threats facing the United States that are prioritized and disseminated commensurate with oversight by select committees for intelligence. We do not intend to issue a policy specifically establishing a duty to warn states about election-related cybersecurity threats. The referenced policy, ICD 191, *Duty to Warn*, was issued in 2015 directing IC elements to warn U.S. and non-U.S. persons of impending threats of intentional killing, serious bodily injury, or kidnapping. The Duty to Warn Directive was established to account for intelligence that, when encountered, would be acted upon in a time-sensitive manner directly by IC elements. We do have policies in place that were established to ensure the IC is providing intelligence information, at an appropriate clearance level, to support the Department of Homeland Security (DHS) and other Executive Branch agencies, as appropriate, in their ability to provide useful information to state, local, and tribal governments in a timely manner. The first of these policies, ICD 209, *Tearline Production and Dissemination*, was issued at the request of DHS to expand the utility of intelligence to a broad range of customers. The second Directive, ICD 208, *Write for Maximum Utility*, was issued to ensure intelligence products were written and disseminated in a manner that provides the greatest use for our customers. The IC will continue to support our customers by providing useful and timely intelligence information as appropriate.

○