S. HRG. 115–205

OPEN HEARING ON WORLDWIDE THREATS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

THURSDAY, MAY 11, 2017

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

25–888 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

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 III, 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

MAY 11, 2017

OPENING STATEMENTS

WITNESS

SUPPLEMENTAL MATERIAL

OPEN HEARING ON WORLDWIDE THREATS

THURSDAY, MAY 11, 2017

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

The Committee met, pursuant to notice, at 10:08 a.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Committee Members Present: Senators Burr, Warner, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Cornyn, Feinstein, Wyden, Heinrich, King, Manchin, and Harris.

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

Chairman BURR. I'd like to call the hearing to order. I'd like to welcome our witnesses today: Director of National Intelligence Dan Coats—Dan, it's good to see our former colleague here—Director of the Central Intelligence Agency Mike Pompeo—good to see you, Mike—Director of Defense Intelligence General Vince Stewart; Director of National Security Agency, Admiral Mike Rogers; Director of Geospatial-Intelligence Agency, Robert Cardillo; and Acting Director of the Federal Bureau of Investigation, Andrew McCabe. I thank all of you for being here this morning, especially to you, Director McCabe, for filling in on such short notice.

Since 1995, this committee has met in an open forum to hear about and discuss the security threats facing the United States of America. I understand that many people tuned in today are hopeful we'll focus solely on the Russian investigation of their involvement in our elections. Let me disappoint everybody up front: While the committee certainly views Russian intervention in our elections as a significant threat, the purpose of today's hearing is to review and highlight to the extent possible the range of threats that we face as a Nation.

The national security threat picture has evolved significantly since 1995. What used to be a collection of mostly physical and state-based national security concerns has been replaced by something altogether different. Today our traditional focus on countries like North Korea, Russia, and Iran is complicated by new challenges like strategic threats posed by non-state actors in the cyber arena and the danger of transnational terrorists who can use the internet to inspire violence and fear in the homeland, all without leaving their safe havens in the Middle East.

What has not changed, however, is the tireless dedication and patriotism of the women and men who make up the United States

intelligence community, the very people represented by our witnesses this morning.

One of the many reasons I find so much value in this hearing is that it provides the American public with some insight into the threats facing our country. But it also lets people know what's being done in their behalf to reduce those threats. I encourage all the witnesses today to not only address the threats to our Nation, but to talk about what their organizations are doing to help secure this country, to the degree they can in an unclassified setting.

Director Coats, your written statement for the record represents the collective insight of the entire intelligence community. It is a lengthy and detailed account of what this country is facing. It is also evidence of why the substantial resources and investments this committee authorizes are in fact necessary.

From the human tragedy of the refugee crisis in the Middle East to the risk that territorial ambitions will set off a regional conflict in the South China Sea, it's a complicated and challenging world. Director Pompeo, the Korean Peninsula is a point of particular concern to me and to many on this committee. I'd like your insights into what is behind North Korea's unprecedented level of nuclear and missile testing and how close they are to holding the U.S. mainland at risk of a nuclear attack. I'd also value your sense of how Tuesday's election of a new President in South Korea is going to impact things for us on that peninsula.

General Stewart, I'm sure you're aware of the reinvigorated policy discussions on Afghanistan. While we all respect that you can't offer your own recommendations on what that policy should be, I would very much value your assessments of the situation in Afghanistan today, including the state of governance in Kabul, the sustainability and proficiency of the Afghan National Security Forces, and whether Taliban reconciliation is a realistic objective. If the U.S. is ramping up in Afghanistan, we need to know the IC's views on what we're getting into.

I also hope you'll share your assessments of the battlefield in Iraq and in Syria with us this morning. Your insights into conditions on the ground, including ongoing operations to dislodge ISIS from Mosul, and sustainability of the Mosul Dam would be of great value to the members of this committee and to the public.

Admiral Rogers, I've made a couple references to cyber already and that's for good reason. Of the many difficult challenges we're going to discuss this morning, nothing worries me more than the threat of a well-planned, well-executed widescale attack on the computer networks and systems that make America work. From banking and health care to military and critical infrastructure, the functionality of our modern society is dependent on computers. When the first line of the DNI's statement reads, and I quote, "Nearly all information, communications networks, and systems will be at risk for years," unquote, that alarms me. Admiral Rogers, I look forward to hearing from you on this line of assessments.

Director Cardillo, as head of the NGA you sit at the nexus of innovation and data collection and analysis. Given the complexity of the intelligence questions the IC is being confronted with and the global nature of our national security threats that this country faces, expectations of the NGA are high. We know the IC can't be

everywhere at once, but that's still kind of what we look to the NGA to do. I'd appreciate your sense of what NGA analytic strengths are today and what the role of commercial imagery is in NGA's future.

Director McCabe, welcome to the table and into the fray. To the extent possible, I hope you'll discuss the Bureau's assessments of the terrorist threat within our borders. Your agents are often our last line of defense here at home and I will say continue to do outstanding work.

We're fortunate to have six people with the experience and the dedication that we have today. I'll close there, but I'd like to highlight for my colleagues: the committee will be holding a classified hearing on worldwide threats this afternoon at 1:30. I will do everything I can to make sure that the questions that you ask in this open session are appropriate to the venue that we're in. I would ask you to think about that long and hard, and if there's a question to move to a staffer to ask them whether this is the appropriate area; and if you as our witnesses feel that there's something that you can't sufficiently answer in an open setting, that you will pause long enough to get my attention and I will try to make sure that we move to the appropriate setting.

With that, I turn to the Vice Chairman for any comments he might make.

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

Vice Chairman WARNER. Thank you, Mr. Chairman, and thank you for your leadership on this Committee. I also want to join in welcome the witnesses. It's good to see you all.

But it is impossible to ignore that one of the leaders of the intelligence community is not here with us today. The President's firing of FBI Director Comey Tuesday night was a shocking development. The timing of Director Comey's dismissal to me and to many members on this committee on both sides of the aisle is especially troubling. He was leading an active counterintelligence investigation into any links between the Trump campaign and the Russian government or its representatives and whether there was any coordination between the campaign and Russia's efforts to interfere in our election.

For many people, including myself, it's hard to avoid the conclusion that the President's decision to remove Director Comey was related to this investigation. And that is truly unacceptable.

We were scheduled to hear directly from Director Comey today in open session. We and the American people were supposed to hear straight from the individual responsible for the FBI investigation. We anticipated asking Director Comey a series of questions about his actions and the actions of the FBI in terms of looking into which Trump associates, if any, and some of their actions during the campaign as it relates to the Russians. However, President's Trump's actions this week cost us an opportunity to get at the truth, at least for today.

You may wonder a little bit how seriously I know the White House continues to dismiss this investigation. I point out simply for the record the front page of the "New York Times," which shows

a picture of clearly an Administration that doesn't take this investigation too seriously.

It is important to restate the critical importance of protecting the independence and integrity of Federal law enforcement. This is central to maintaining the confidence of the American people in the principle that all Americans, no matter how powerful, are accountable before the law. The President's actions have the potential to undermine that confidence, and that should be deeply concerning no matter which political party you belong to.

This week's remarkable developments make our Committee's investigation into Russia's influence on the 2016 U.S. presidential election even more important. And while it is clear to me now more than ever that an independent special counsel must be appointed, make no mistake, our Committee will get to the bottom of what happened during the 2016 presidential election. Again, I want to compliment the Chairman on his work in this effort.

We will not be deterred from getting to the truth. These actions will do nothing to undermine our resolve to follow the evidence wherever it leads. We hope to speak to Mr. Comey. We will speak to anyone and everyone who has something to offer in this investigation.

Mr. McCabe, while I didn't necessarily expect to see you here today, we don't know how long you'll be Acting FBI Director. But while I will adhere to what the Chairman has indicated in terms of the line of questioning, I will want to make sure my first question for you, even in this public setting, will be for you to assure the Committee that if you come under any political influence from the White House or others to squash this investigation or impede it in any way, that you'll let the Committee know.

This investigation has had its ups and downs and again some, including myself, sometimes have been frustrated with the pace. We will no doubt face other challenges in the future. But ups and downs and bumps sometimes is how bipartisanship works. It's a constant struggle, but one worth making, and I'm proud of the way Members of this Committee from both sides of the aisle have conducted themselves in one of the most challenging political environments we've ever seen.

At the same time, Chairman Burr and I have put this investigation on what we believe to be a solid bipartisan footing, with the shared goal of getting the truth. In spite of the events of the last 24 hours, I intend to maintain our Committee's focus on the investigation. Indeed, the recent actions only increase the burden of responsibility on all of us to ensure that we live up to this challenge and to uncover the truth, wherever that leads.

There is, obviously, consensus agreement among the U.S. intelligence community that Russia massively intervened with active measures in the 2016 presidential elections. Nor do I imagine that any member of this Committee was surprised to see the exact same Russian playbook just being run during the French elections that just took place last weekend. And no one should forget back in mid-2015—Director Coats, we had some of the folks in from the German services recently—that there was a hacking into the German Bundestag. It's fair to say the Germans should anticipate seeing

more cyber attacks directed against their elected officials with their upcoming national elections in September.

In short, Russia's direct interference in democratic processes around the globe is a direct assault that we must work on together and it's clearly one of the top worldwide threats.

That being said, gentlemen, I want to start again by thanking you for your service to the Nation. I want to particularly note that Director Coats is testifying before this Committee in the first time since his confirmation. Dan, I know that you and Marsha were ready for retirement and I thank you both for being willing to serve your country one more time.

I also want to recognize the men and women who you represent here today. These thousands of dedicated intelligence professionals toil in the shadows, put their lives on the line, and make sacrifices most of us will never know in order to keep our country safe. I also want to make sure they know that I appreciate their efforts and am proud to represent them, not only as the Vice Chair of the Intelligence Committee, but as a Senator from Virginia, where so many of those intelligence professionals live.

This Committee's annual Worldwide Threat hearing is an important opportunity to review the threats and challenges we face as a Nation. Obviously, these threats continue to multiply. As the world becomes more complex and challenging, good intelligence gives our policymakers and national leaders a heads-up on the challenges they need to address.

The intelligence community in many ways is our Nation's early warning system. However, a fire alarm only works if you pay attention to it. You cannot ignore it simply because you do not like what it's telling you. Similarly, we need to make sure that all our policymakers pay attention to the warnings provided by you, the independent, nonpartisan intelligence professionals.

Since the Second World War, America has relied, as we all know, on a global system of alliances, institutions, and norms to ensure our stability and prosperity. Today many challenges threaten that system, that system that has been built up over the last 70 years. As the Chairman mentioned, countries like China and Russia are challenging many of the global institutions. They are in many cases seeking to undercut and delegitimize them. We must work together to stand vigilant against that threat.

Similarly, rogue states such as North Korea have sought to undercut the global nonproliferation regime. Obviously, North Korea is one of the most pressing issues our country faces. And, Admiral Rogers, as the Chairman mentioned, we all share enormous concern about both the up side and down side of new technologies and the asymmetrical threats that are posed by cyber and other technology actors. I would add as well—Director Cardillo, I think we've discussed this as well—our dominance in terms of overhead in many ways is at threat as well from emerging nations.

Terrorist groups and extremists are also able to access a lot of these new technologies. And while ISIS in particular continues to suffer losses in Syria, Iraq, and Libya, unfortunately it continues to spread its hateful ideology through social media and encrypted communications.

Gentlemen, I have only lightly touched on a few of the challenges we face. I look forward to the discussion we're about to have. But again, I thank you for being here and look forward to this hearing.

Thank you, Mr. Chairman.

Chairman BURR. I thank the Vice Chairman.

For members' purposes, we have a vote scheduled on the floor at 11:00 o'clock. It's the intent of the Chair and Vice Chair that we will rotate the gavel so that the hearing continues through. Members will be recognized by seniority for five minutes. When we conclude the open session, hopefully with enough gap for our witnesses to have some lunch, we will reconvene at 1:30. The afternoon vote to my knowledge is not set yet, but we will work around that, so plan to be back at the SCIF by 1:30 for that hearing to start.

With that, Director Coats, the floor is yours.

STATEMENT OF HON. DAN COATS, DIRECTOR OF NATIONAL INTELLIGENCE; ACCOMPANIED BY LT. GEN. VINCENT STEWART, DIRECTOR OF THE DEFENSE INTELLIGENCE AGENCY, MIKE POMPEO, DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY; ANDREW MCCABE, ACTING DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION; ADMIRAL MICHAEL ROGERS, DIRECTOR OF THE NATIONAL SECURITY AGENCY; AND ROBERT CARDILLO, DIRECTOR OF THE NATIONAL GEOSPATIAL–INTELLIGENCE AGENCY

Director COATS. Chairman Burr, Vice Chairman Warner, members of the committee: Thank you for the opportunity to appear before you today. I'm here with my colleagues from across the IC community and I'm sure I speak for my colleague Mike Pompeo, the new Director of the CIA, that the two of us, new to the job, have inherited an intelligence community with leadership and professionals, with expertise, that is exceptional. It is a great privilege to hold these positions and know that we have the support from across 17 agencies relative to gathering intelligence, analyzing and synthesizing that intelligence, and several of those leaders are sitting here today and we're most appreciative of their contributions to their country and to this issue.

The complexity of the threat environment is ever expanding and has challenged the IC to stay ahead of the adversary, and it has not been an easy task. Given the tasks we face around the world, the IC continues its work to collect, to analyze, and integrate these and other issues.

We appreciate very much the support from your committee to address these threats in a way that will give the President, the Congress, and other policymakers the best and most integrated intelligence we can assemble.

In the interest of time and on behalf of my colleagues at the table, I'll discuss just some of the many challenging threats that we currently face. The intelligence community's written statement for the record that was submitted earlier discusses these and many other threats in greater detail.

Let me start with North Korea. North Korea is an increasingly grave national security threat to the United States because of its growing missile and nuclear capabilities combined with the aggressive approach of its leader, Kim Jong Un. Kim is attempting to

prove he has the capability to strike the U.S. mainland with a nuclear weapon. He has taken initial steps toward fielding a mobile intercontinental ballistic missile, but it has not yet been flight tested.

North Korea updated its constitution in 2012 to declare itself a nuclear power and its officials consistently state nuclear weapons are the basis for regime survival, suggesting Kim does not intend—not intend—to negotiate them away.

Although intelligence collection on North Korea poses difficulties given North Korea's Isolation, the IC will continue to dedicate resources to this key challenge. It requires some of our most talented professionals to warn our leaders of the pending North Korean actions and of the long-term implications of their strategic weapons programs.

In Syria, we assess that the regime will maintain its momentum on the battlefield provided, as is likely, that it maintains support from Iran and Russia. The continuation of the Syrian conflict will worsen already disastrous conditions for Syrians in regional states. Furthermore, on April 4th the Syrian regime used the nerve agent sarin against the opposition in Khan Sheikhoun in what is probably the largest chemical attack by the regime since August 2013. The Syrian regime probably used chemical weapons in response to battlefield losses along the Hama battle front in late March that threatened key infrastructure.

We assess that Syria is probably both willing and able to use CW, chemical warfare, in future attacks, but we do not know if they plan to do so. We are still acquiring and continuing to analyze all intelligence related to the question of whether Russian officials had foreknowledge of the Syrian CW attack on 4 April, and as we learn this information we will certainly share it with this committee.

Cyber threats continue to represent a critical national security issue for the United States for two key reasons. First, our adversaries are becoming bolder, more capable, and more adept at using cyber space to threaten our interests and shape real-world outcomes. And the number of adversaries grows as nation-states, terrorist groups, criminal organizations, and others continue to develop cyber capabilities.

Secondly, the potential impact of these cyber threats is amplified by the ongoing integration of technology into our critical infrastructure and into our daily lives.

Our relationships and businesses already rely on social media and communication technologies and on critical infrastructure. It is becoming increasingly reliant on the internet. As such, this raises the potential for physical, economic, and psychological consequences when a cyber attack or exploitation event occurs.

The worldwide threat of terrorism is geographically diverse and multifaceted, and it poses a continuing challenge for the United States, for our allies and partners who seek to counter it. ISIS is experiencing territorial losses in Iraq and Syria, with persistent counterterrorism operations degrading its strength. However, ISIS will continue to be an active terrorist threat to the United States due to its proven ability to direct and inspire attacks against a wide range of targets around the world.

Outside Iraq and Syria, ISIS is seeking to foster interconnectedness among its global branches and networks, align their efforts to its strategy, and withstand counter-ISIS efforts. We assess that ISIS maintains the intent and capability to direct, enable, assist, and inspire transnational attacks.

Al-Qaeda and its affiliates continue to pose a significant terrorist threat overseas as they remain primarily focused on local and regional conflicts. Homegrown violent extremists remain the most frequent and unpredictable terrorist threat to the United States homeland. This threat will persist, with many attacks happening with little or no warning.

In Turkey, tensions in Turkey might escalate rapidly and unpredictably in 2017 as the government's consolidation of power, crackdowns on dissent, and restrictions on free media continue.

Let me now take just a quick run through some key areas of the Middle East. In Iraq, Baghdad's primary focus through 2017 will be recapturing and stabilizing Mosul and other territory controlled by ISIS. ISIS in Iraq is preparing to regroup, however, and continue an insurgency and terrorist campaign even as it loses territory. We assess that Iraq will still face serious challenges to its stability, political viability, and territorial integrity even as the threat from ISIS is reduced. Reconstruction will cost billions of dollars and ethnosectarian and political reconciliation will be an enduring challenge.

In Iran, Teheran's public statements suggest that it wants to preserve the Joint Comprehensive Plan of Action because it views the deal as a means to remove sanctions while preserving some nuclear capabilities. Iran's implementation of the deal has extended the amount of time Iran would need to produce enough fissile material for a nuclear weapon from a few months to about a year.

Teheran's malignant activities, however, continue. For example, Iran provides arms, financing, and training and manages as many as 10,000 Iraqi, Afghan, and Pakistani Shia fighters in Syria to support the Assad regime. Iran has sent hundreds of its own forces, to include members of the Islamic Revolutionary Guard Corps and the IRGC Quds Force, to Syria as advisers.

In Yemen, fighting—we assess fighting will almost certainly persist in 2017 between Houthi-aligned forces trained by Iran and the Yemeni government, backed by a Saudi-led coalition. Neither side has been able to achieve decisive results through military force to this point. Al-Qaeda in the Arabian Peninsula, an ISIS branch in Yemen, have exploited the conflict and the collapse of government authority to gain new recruits and allies and expand their influence.

In South Asia, the intelligence community assesses that the political and security situation in Afghanistan will almost certainly deteriorate through 2018, even with a modest increase in military assistance by the United States and its partners. This deterioration is undermined by its dire economic situation. Afghanistan will struggle to curb its dependence on external support until it contains the insurgency or reaches a peace agreement with the Taliban.

Meanwhile, we assess that the Taliban is likely to continue to make gains, especially in rural areas. Afghan Security Forces' per-

formance will probably worsen due to a combination of Taliban operations, combat casualties, desertions, poor logistics support, and weak leadership.

Pakistan is concerned about international isolation and sees its position through the prism of India's rising international status, including India's expanded foreign outreach and deepening ties to the United States. Pakistan will likely turn to China to offset its isolation, empowering a relationship that will help Beijing to project influence into the Indian Ocean.

In addition, Islamabad has failed to curb militants and terrorists and Pakistan. These groups will present a sustained threat to the United States' interests in the region and continue to plan and conduct attacks in India and Afghanistan. Pakistan is also expanding its nuclear arsenal and pursuing tactical nuclear weapons, potentially lowering the threshold for their use.

Let me now turn to Russia. We assess that Russia is likely to be more aggressive in foreign and global affairs, more unpredictable in its approach to the United States, and more authoritarian in its approach to domestic policies and politics. We assess that Russia will continue to look to leverage its military support to the Assad regime to drive a political settlement process in Syria on their terms. Moscow is also likely to use Russia's military intervention in Syria in conjunction with efforts to capitalize on fears of a growing ISIS and extremist threat to expand its role in the Middle East.

We assess that Moscow's strategic objectives in Ukraine—maintaining long-term influence over Kiev and frustrating Ukraine's attempts to integrate into Western institutions—will remain unchanged in 2017. Russia's military intervention in eastern Ukraine contains more than two years—continues, excuse me—more than two years after the Minsk 2 Agreement. Russia continues to exert military and diplomatic pressure to coerce Ukraine into implementing Moscow's interpretation of the political provisions of the Minsk agreement, among them constitutional amendments that would effectively give Moscow a veto over Kiev's strategic decisions.

In China, China will continue, we assess, to pursue an active foreign policy, especially within the Asia Pacific region, highlighted by a firm stance on competing territorial claims in the East China Sea and South China Sea, relations with Taiwan, and its pursuit of economic engagement across East Asia. China views a strong military as a critical element in advancing its interests. It will also pursue efforts aimed at fulfilling its ambitious "One Belt, One Road" initiative to expand their strategic influence and economic role across Asia through infrastructure projects.

Just a quick look at sub-Saharan Africa, home to more than a billion people and expected to double in size by mid-century. African governments face the threat of coups, popular uprisings, widespread violence, and terrorist attacks, including from Al-Qaeda and its ISIS affiliates.

In the Western Hemisphere, Venezuela's unpopular autocratic government will turn to increasingly repressive means to contain political opponents and street unrest. Oil has long been the regime's cash cow, but mismanagement has led to declining output and revenue. We assess the Venezuelan government will struggle

to contain inflation, make debt payments, and pay for imports of scarce basic goods and medicines.

Mexico's government will focus on domestic priorities to prepare for the 2018 presidential election while seeking to limit fallout from strained relations with the United States. Public demand for government action against crime and corruption will add to political pressure.

As Cuba heads into the final year of preparations for a historic transition to a next generation leader in early 2018, the government's focus will be on preserving control while managing recession. Cuba, which continues to use repressive measures to stifle human rights and constrain democracy activists, blames its slowing economy on lower global commodity prices, the U.S. embargo, and the economic crisis in Venezuela, a key benefactor.

Let me just make a statement on the threat from illegal drugs. The threat to the United States from foreign-produced drugs, especially heroin, synthetic opioids, meth, and cocaine, has grown significantly in the past few years. This is contributing to previously unseen levels of U.S. drug-related mortality, which now exceeds all other U.S. causes of injurious death.

Finally, I'd like to make a few points here that are important to the IC going forward. As you are all very aware, Section 702 of the FISA Amendments Act is due to expire at the end of the year. I cannot stress enough the importance of this authority in how the IC does its work to keep Americans safe, and I know that is shared by everyone at this table.

Section 702 is an extremely effective tool to protect our Nation from terrorists and other threats. As I described in my confirmation hearing, 702 is instrumental to so much of the IC's critical work in protecting the American people from threats from abroad.

The intelligence community is committed to working with all of you, in both classified and unclassified sessions, to ensure that you understand not only how we use our authorities, but also how we protect privacy and civil liberties in the process.

Additionally, many of you have asked me as part of my confirmation process about the status of the IC, its effectiveness and efficiency, and how it can be improved. As part of the Administration's goal of an effective and efficient government, the ODNI has already begun a review of the entire intelligence community, to include the Office of the DNI, and to answer the very questions about how we can make our process even more streamlined, more efficient, and more effective.

My office is proud to lead this review and I look forward to the confirmation of my principal deputy in order to shepherd this process to completion, and I have total confidence in her that she has the capacity and capability to effectively lead this effort.

The recently passed intelligence authorization bill also includes the requirement for a review of the IC focused on structures and authorities ten years beyond the intelligence reforms of the mid-2000s. Between these two reviews, I am confident that I will be able to report back to the committee with constructive recommendations on the best ways forward for the whole of the IC.

In the short time I've been on this job, I have learned that the IC is full of dedicated, talented, creative, and patriotic men and

women who are committed to keeping America safe. We must retain this posture while looking for ways to improve.

In conclusion, the intelligence community will continue its tireless work against these and all threats, but we will never be omniscient. Although we have extensive insight into many threats and places around the world, we have gaps in others. Therefore, we very much appreciate the support provided by this committee and will continue to work with you to ensure that the intelligence community has the capabilities it needs to meet its many mission needs.

With that, we are ready to take your questions.

[The prepared statement of Director Coats follows:]

Statement for the Record

Worldwide Threat Assessment of the US Intelligence Community

Senate Select Committee on Intelligence

Daniel R. Coats

Director of National Intelligence

May 11, 2017

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT
of the
US INTELLIGENCE COMMUNITY

May 11, 2017

INTRODUCTION

Chairman Burr, Vice Chairman Warner, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2017 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary 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 April 24, 2017 was used in the preparation of this assessment.

TABLE OF CONTENTS

GLOBAL THREATS

CYBER THREAT

Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years.

Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the US and global economies. Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors. These threats are amplified by our ongoing delegation of decisionmaking, sensing, and authentication roles to potentially vulnerable automated systems. This delegation increases the likely physical, economic, and psychological consequences of cyber attack and exploitation events when they do occur. Many countries view cyber capabilities as a viable tool for projecting their influence and will continue developing cyber capabilities. Some adversaries also remain undeterred from conducting reconnaissance, espionage, influence, and even attacks in cyberspace.

Cyber Threat Actors

Russia. Russia is a full-scope cyber actor that will remain a major threat to US Government, military, diplomatic, commercial, and critical infrastructure. Moscow has a highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture. This aggressiveness was evident in Russia's efforts to influence the 2016 US election, and we assess that only Russia's senior-most officials could have authorized the 2016 US election-focused data thefts and disclosures, based on the scope and sensitivity of the targets. Outside the United States, Russian actors have conducted damaging and disruptive cyber attacks, including on critical infrastructure networks. In some cases, Russian intelligence actors have masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. Russia has also leveraged cyberspace to seek to influence public opinion across Europe and Eurasia. We assess that Russian cyber operations will continue to target the United States and its allies to gather intelligence, support Russian decisionmaking, conduct influence operations to support Russian military and political objectives, and prepare the cyber environment for future contingencies.

China. We assess that Beijing will continue actively targeting the US Government, its allies, and US companies for cyber espionage. Private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral Chinese-US cyber commitments of September 2015. Beijing has also selectively used offensive cyber operations against foreign targets that it probably believes threaten Chinese domestic stability or regime legitimacy.

Iran. Tehran continues to leverage cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats—including against US allies in the region. Iran has also used its cyber capabilities directly against the United States. For example, in

2013, an Iranian hacker conducted an intrusion into the industrial control system of a US dam, and in 2014, Iranian actors conducted a data deletion attack against the network of a US-based casino.

North Korea. Pyongyang has previously conducted cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014—and remains capable of launching disruptive or destructive cyber attacks to support its political objectives. Pyongyang also poses a cyber threat to US allies. South Korean officials have suggested that North Korea was probably responsible for the compromise and disclosure of data in 2014 from a South Korean nuclear plant.

Terrorists. Terrorists—to include the Islamic State of Iraq and ash-Sham (ISIS)—will also continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations. Hizballah and HAMAS will continue to build on their cyber accomplishments inside and outside the Middle East. ISIS will continue to seek opportunities to target and release sensitive information about US citizens, similar to their operations in 2015 disclosing information about US military personnel, in an effort to inspire attacks.

Criminals. Criminals are also developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities. "Ransomware," malware that employs deception and encryption to block users from accessing their own data, has become a particularly popular tool of extortion. In 2016, criminals employing ransomware turned their focus to the medical sector, disrupting patient care and undermining public confidence in some medical institutions.

Physical Consequences

Our adversaries are likely to seek capabilities to hold at risk US critical infrastructure as well as the broader ecosystem of connected consumer and industrial devices known as the "Internet of Things" (IoT). Security researchers continue to discover vulnerabilities in consumer products including automobiles and medical devices. If adversaries gain the ability to create significant physical effects in the United States via cyber means, they will have gained new avenues for coercion and deterrence. For example, a cyber attack on a Ukrainian power network in 2015 caused power outages for several hours.

Economic and Security Consequences

Adversaries will continue to use cyber operations to undermine US military and commercial advantage by hacking into US defense industry and commercial enterprises in pursuit of scientific, technical, and business information. Examples include theft of data on the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet, and the MV-22 Osprey. In addition, adversaries often target personal accounts of government officials and their private-sector counterparts. This espionage reduces cost and accelerates the development of foreign weapon systems, enables foreign reverse-engineering and countermeasures development, and undermines US military, technological, and commercial advantage.

Psychological Consequences

The impact of cyber threats extends beyond the physical and commercial realms. Online threats—from both states and non-state actors—distort the perceptions and decisionmaking processes of the target, whether they are countries or individuals, in ways that are both obvious and insidious. Information from

cyber espionage can be leaked indiscriminately or selectively to shape perceptions. Furthermore, even a technically secure Internet can serve as a platform for the delivery of manipulative content crafted by foes seeking to gain influence or foment distrust.

Global Security, Diplomacy, and Norms

We assess that as foreign countries seek to balance security, economic growth, and interoperability objectives, many will implement new laws and technical changes to monitor and control access to information within and across their borders. Some states will continue to seek to control user access through means such as restrictions on encryption and steps to reduce anonymity online. However, these states will probably not significantly erode the overall global connectivity of the Internet. Furthermore, some state information control efforts will almost certainly be challenged by a broad coalition of states and non-state cyber stakeholders, including innovative technologists, industry leaders, privacy advocates, "hackers," and others with an interest in opposing censorship or government control of cyberspace.

Although recognition is widespread that existing international law applies to states' conduct in cyberspace, how that law applies to states' use of information and communication technologies (ICT) remains a subject of significant international discussion. In addition, although efforts are ongoing to gain adherence to certain voluntary, non-binding norms of responsible state behavior in cyberspace, they have not gained universal acceptance, and efforts to promote them are increasingly polarized. Despite the existence and widespread ratification of the Budapest Convention—the treaty on cybercrime of the Council of Europe—some states have called for the drafting of new international treaties to regulate cybercrime and other cyber-related issues. Moreover, although some countries might be willing to explore limits on cyber operations against certain targets, few would likely support a ban on offensive capabilities.

EMERGING AND DISRUPTIVE TECHNOLOGIES

Strategic Outlook

Continued rapid technological progress remains central to economic prosperity and social well-being, but it is also introducing potential new threats. Artificial intelligence (AI) is advancing computational capabilities that benefit the economy, yet those advances also enable new military capabilities for our adversaries. Genome editing has the potential to cure diseases and modify human performance, which presents new ethical and security issues. The Internet of Things (IoT) is connecting billions of new devices to the Internet, but it also broadens the attack potential of cyber actors against networks and information. Semiconductors remain core to the economy and the military, yet new national security risks might arise from next-generation chips because of technology plateaus and investments by other states.

Artificial Intelligence

A surge of commercial and government research is improving AI capabilities while raising national security issues. Semi-autonomous cars, the victory of an AI-based system over the world champion in the game Go, and devices with AI-enabled personal assistants have drawn global attention to the field.

Corporations around the globe are investing in a range of AI applications including marketing, crime detection, health, and autonomous vehicles. Although the United States leads AI research globally, foreign state research in AI is growing. Foreign governments cite AI in their science and technology strategies or have planned specific efforts to enhance their AI capabilities. The implications of our adversaries' abilities to use AI are potentially profound and broad. They include an increased vulnerability to cyber attack, difficulty in ascertaining attribution, facilitation of advances in foreign weapon and intelligence systems, the risk of accidents and related liability issues, and unemployment.

Genome Editing

The development of genome-editing technologies is accelerating the rate at which we can develop new approaches to address medical, health, industrial, environmental, and agricultural challenges and revolutionize biological research. However, the fast pace of development and broad range of applications are likely to challenge governments and scientific communities alike to develop regulatory and ethical frameworks or norms to govern the responsible application of the technology.

Internet of Things

The widespread incorporation of "smart" devices into everyday objects is changing how people and machines interact with each other and the world around them, often improving efficiency, convenience, and quality of life. Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks.

Next-Generation Semiconductors

Continual advancement of semiconductor technologies during the past 50 years in accordance with Moore's Law—which posits that the overall processing power of computers will double every two years—has been a key driver of the information technology revolution that underpins many US economic and security advantages. Industry experts, however, are concerned that Moore's Law might no longer apply by the mid-2020s as the fundamental limits of physics to further miniaturize transistors are reached, potentially eroding US national security advantages. Meanwhile, China is increasing its efforts to improve its domestic technological and production capabilities through mergers and acquisitions to reduce its dependence on foreign semiconductor technology, according to Western experts and business analysts.

TERRORISM

The worldwide threat from terrorism will remain geographically diverse and multifaceted—a continuing challenge for the United States, our allies, and partners who seek to counter it. Sunni violent extremists will remain the primary terrorist threat. These extremists will continue to embroil conflict zones in the Middle East, Africa, and South Asia. Some will also seek to attempt attacks outside their operating areas.

- Iran continues to be the foremost state sponsor of terrorism and, with its primary terrorism partner, Lebanese Hizballah, will pose a continuing threat to US interests and partners worldwide. The Syrian, Iraqi, and Yemeni conflicts will continue to aggravate the rising Sunni-Shia sectarian conflict, threatening regional stability.

Terrorist Threat to the United States

US-based homegrown violent extremists (HVEs) will remain the most frequent and unpredictable Sunni violent extremist threat to the US homeland. They will be spurred on by terrorist groups' public calls to carry out attacks in the West. The threat of HVE attacks will persist, and some attacks will probably occur with little or no warning. In 2016, 16 HVEs were arrested, and three died in attacks against civilian soft targets. Those detained were arrested for a variety of reasons, including attempting travel overseas for jihad and plotting attacks in the United States. In addition to the HVE threat, a small number of foreign-based Sunni violent extremist groups will also pose a threat to the US homeland and continue publishing multilingual propaganda that calls for attacks against US and Western interests in the US homeland and abroad.

Dynamic Overseas Threat Environment

The **Islamic State of Iraq and ash-Sham (ISIS)** continues to pose an active terrorist threat to the United States and its allies because of its ideological appeal, media presence, control of territory in Iraq and Syria, its branches and networks in other countries, and its proven ability to direct and inspire attacks against a wide range of targets around the world. However, territorial losses in Iraq and Syria and persistent counterterrorism operations against parts of its global network are degrading its strength and ability to exploit instability and societal discontent. ISIS is unlikely to announce that it is ending its self-declared caliphate even if it loses overt control of its de facto capitals in Mosul, Iraq and Ar Raqqah, Syria and the majority of the populated areas it once controlled in Iraq and Syria.

Outside Iraq and Syria, ISIS is seeking to foster interconnectedness among its global branches and networks, align their efforts to ISIS's strategy, and withstand counter-ISIS efforts. We assess that ISIS maintains the intent and capability to direct, enable, assist, and inspire transnational attacks. The number of foreign fighters traveling to join ISIS in Iraq and Syria will probably continue to decline as potential recruits face increasing difficulties attempting to travel there. The number of ISIS foreign fighters leaving Iraq and Syria might increase. Increasing departures would very likely prompt additional would-be fighters to look for new battlefields or return to their home countries to conduct or support external operations.

During the past 16 years, US and global counterterrorism (CT) partners have significantly reduced **al-Qa'ida's** ability to carry out large-scale, mass casualty attacks, particularly against the US homeland. However, al-Qa'ida and its affiliates remain a significant CT threat overseas as they remain focused on exploiting local and regional conflicts. In 2016, **al-Nusrah Front and al-Qa'ida in the Arabian Peninsula (AQAP)** faced CT pressure in Syria and Yemen, respectively, but have preserved the resources, manpower, safe haven, local influence, and operational capabilities to continue to pose a threat. In Somalia, **al-Shabaab** sustained a high pace of attacks in Somalia and continued to threaten the northeast and coastal areas of Kenya. Its operations elsewhere in East Africa have diminished after the deaths of many external plotters since 2015, but al-Shabaab retains the resources, manpower,

influence, and operational capabilities to pose a real threat to the region, especially Kenya. In North and West Africa, **al-Qa'ida in the Lands of the Islamic Maghreb (AQIM)** escalated its attacks on Westerners in 2016 with two high-profile attacks in Burkina Faso and Cote d'Ivoire. It merged with allies in 2017 to form a new group intended to promote unity among Mali-based jihadists, extend the jihad beyond the Sahara and Sahel region, increase military action, and speed up recruitment of fighters. In Afghanistan and Pakistan, remaining members of al-Qa'ida and its regional affiliate, **al-Qa'ida in the Indian Subcontinent (AQIS)**, continued to suffer personnel losses and disruptions to safe havens in 2016 due to CT operations. However, both groups maintain the intent to conduct attacks against the United States and the West.

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 allies. Both state and non-state actors have already demonstrated the use of chemical weapons in the Levant. 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 Pressing Forward With Cruise Missile That Violates the INF Treaty

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 that 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 in the past complaining that the Treaty prohibits Russia, but not some of its neighbors, from developing and possessing ground-launched missiles with ranges between 500 to 5,500 kilometers.

China Modernizing Its Nuclear Forces

The Chinese People's Liberation Army (PLA) has established a Rocket Force—replacing the longstanding Second Artillery Corps—and 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. 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—will give the PLA Navy its first long-range, sea-based nuclear capability.

Iran and JCPOA

Tehran's public statements suggest that it wants to preserve the Joint Comprehensive Plan of Action (JCPOA)—because it views the JCPOA as a means to remove sanctions while preserving some nuclear capabilities. It expects the P5+1 members to adhere to their obligations, although Iran clearly recognizes the new US Administration is concerned with the deal. 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 a year. The JCPOA has also enhanced the transparency of Iran's nuclear activities, mainly through improved access by the International Atomic Energy Agency (IAEA) and its investigative authorities under the Additional Protocol to its Comprehensive Safeguards Agreement.

Iran is pursuing capabilities to meet its nuclear energy and technology goals and to give it the capability to build missile-deliverable nuclear weapons, if it chooses to do so. Its pursuit of these goals will influence its level of adherence to the JCPOA. We do not know whether Iran will eventually decide to build nuclear weapons.

We judge that Tehran would choose ballistic missiles as its preferred method of delivering nuclear weapons, if it builds them. Iran's ballistic missiles are inherently capable of delivering WMD, 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 intercontinental ballistic missile (ICBM). Progress on Iran's space program could shorten a pathway to an ICBM because space launch vehicles use similar technologies.

North Korea Continues To Expand WMD-Applicable Capabilities

North Korea's nuclear weapons and missile programs will continue to pose a serious threat to US interests and to the security environment in East Asia in 2017. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance to Syria's construction of a nuclear reactor, destroyed in 2007, illustrate its willingness to proliferate dangerous technologies.

North Korea has also expanded the size and sophistication of its ballistic missile forces—from close-range ballistic missiles (CRBMs) to ICBMs—and continues to conduct test launches. In 2016, North Korea conducted an unprecedented number of ballistic missile 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 has publicly displayed its road-mobile ICBMs on multiple occasions. We assess that North Korea has taken steps toward fielding an ICBM but has not flight-tested it.

We have long assessed that Pyongyang's nuclear capabilities are intended for deterrence, international prestige, and coercive diplomacy.

Chemical Weapons in Iraq and Syria

We assess 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 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) attributed three chlorine attacks in 2014 and 2015 to the Syrian regime.

We assess that non-state actors in the region are also using chemicals as a means of warfare. The OPCW-UN JIM concluded that ISIS used sulfur mustard in an attack in 2015. ISIS has allegedly used chemicals in attacks in Iraq and Syria, suggesting that attacks might be widespread.

SPACE AND COUNTERSPACE

Space

Global Trends. Continued global space industry expansion will further extend space-enabled capabilities and space situational awareness to nation-state, non-state, and commercial space actors in the coming years, enabled by increased availability of technology, private-sector investment, falling launch service costs, and growing international partnerships for shared production and operation. Government and commercial organizations will increasingly have access to space-derived information services such as imagery, weather, Internet, communications, and positioning, navigation, and timing (PNT) for intelligence, military, scientific, or business purposes. For instance, China aims to become a world leader in PNT as it completes its dual-use global satellite navigation system by 2020.

Military and Intelligence. Russia aims to improve intelligence collection, missile warning, and military communications systems to better support situational awareness and tactical weapons targeting. Russian plans to expand its imagery constellation and double or possibly triple the number of satellites by 2025. China intends to continue increasing its space-based military and intelligence capabilities to improve global situational awareness and support complex military operations. Many countries in the Middle East, Southeast Asia, and South America are purchasing dual-use imaging satellites to support strategic military activities, some as joint development projects.

Counterspace

Space Warfare. We assess that Russia and China perceive a need to offset any US military advantage derived from military, civil, or commercial space systems and are increasingly considering attacks against satellite systems as part of their future warfare doctrine. Both will continue to pursue a full range of anti-satellite (ASAT) weapons as a means to reduce US military effectiveness. In late 2015, China established a new service—the PLA Strategic Support Force—probably to improve oversight and command of Beijing's growing military interests in space and cyberspace. Russia and China remain committed to developing capabilities to challenge perceived adversaries in space, especially the United States, while publicly and diplomatically promoting nonweaponization of space and "no first placement" of weapons in space. Such commitment continues despite ongoing US and allied diplomatic efforts to dissuade expansion of threats to the peaceful use of space, including international engagements through the UN.

Counterspace Weapons. The global threat of electronic warfare (EW) attacks against space systems will expand in the coming years in both number and types of weapons. Development will very likely focus on jamming capabilities against dedicated military satellite communications (SATCOM), Synthetic Aperture Radar (SAR) imaging satellites, and enhanced capabilities against Global Navigation Satellite Systems (GNSS), such as the US Global Positioning System (GPS). Blending of EW and cyber-attack capabilities will likely expand in pursuit of sophisticated means to deny and degrade information networks. Chinese researchers have discussed methods to enhance robust jamming capabilities with new systems to jam commonly used frequencies. Russia intends to modernize its EW forces and field a new generation of EW weapons by 2020. Iran and North Korea are also enhancing their abilities to disrupt military communications and navigation.

Some new Russian and Chinese ASAT weapons, including destructive systems, will probably complete development in the next several years. Russian military strategists likely view counterspace weapons as an integral part of broader aerospace defense rearmament and are very likely pursuing a diverse suite of capabilities to affect satellites in all orbital regimes. Russian lawmakers have promoted military pursuit of ASAT missiles to strike low-Earth orbiting satellites, and Russia is testing such a weapon for eventual deployment. A Russian official also acknowledged development of an aircraft-launched missile capable of destroying satellites in low-Earth orbit. Ten years after China intercepted one of its own satellites in low-Earth orbit, its ground-launched ASAT missiles might be nearing operational service within the PLA. Both countries are advancing directed energy weapons technologies for the purpose of fielding ASAT systems that could blind or damage sensitive space-based optical sensors. Russia is developing an airborne laser weapon for use against US satellites. Russia and China continue to conduct sophisticated on-orbit satellite activities, such as rendezvous and proximity operations, at least some of which are likely intended to test dual-use technologies with inherent counterspace functionality. For instance, space robotic technology research for satellite servicing and debris-removal might be used to damage satellites. Such missions will pose a particular challenge in the future, complicating the US ability to characterize the space environment, decipher intent of space activity, and provide advance threat warning.

COUNTERINTELLIGENCE

The United States will face a complex global foreign intelligence threat environment in 2017. 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 South Asia, the Near East, 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.

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

Trusted insiders who disclose sensitive or classified US Government information without authorization will remain a significant threat in 2017 and beyond. The sophistication and availability of information technology that increases the scope and impact of unauthorized disclosures exacerbate this threat.

TRANSNATIONAL ORGANIZED CRIME

Rising US Drug Threat

The illicit drug threat the United States is intensifying, as indicated by soaring US drug deaths, foreign drug production, and drug seizures.

- Deaths from synthetic opioids—including fentanyl and its analogues—increased 73 percent in 2015 compared to 2014, and mortality from all other illicit drugs increased 36 percent for the same period, according to the US Centers for Disease Control and Prevention (CDC). Preliminary data for 2016 from some states suggest that deaths have continued to increase.

- Seizures of cocaine and methamphetamine increased along the US southwest border in 2016 over 2015.

Rising foreign drug production, the staying power of Mexican trafficking networks, and strong demand are driving the US drug threat.

- In Mexico, the dominant source of US heroin, potential heroin production doubled from 2014 to 2016, according to the US Government estimates.

- Production of cocaine reached the highest levels on record for Colombia in 2016 and for Peru and Bolivia in 2015—the last years for which estimates are available—driven in part by a decline in coca eradication efforts.

Synthetic drugs from Asia—including synthetic opioids, cannabinoids, and cathinones—pose a strong and probably growing threat and have the potential to displace some traditional drugs produced from plants. Such drugs are often traded via the Internet or—in the case of cannabinoids and cathinones—sold over the counter in products marked "not intended for human consumption." Counterfeit and substandard pharmaceutical trafficking is also on the rise, with the Internet being the primary means by which transnational criminal organizations target US citizens.

- Approximately 18-20 new illegal online pharmacy domain names are registered every day, according to estimates of the Food and Drug Administration, adding to the tens of thousands of existing illegal online pharmacies in operation.

Crime Enables Other Nefarious Actors

Transnational Organized Crime (TOC) will pose a continuing threat to the United States and its allies through close relationships with foreign states and non-state actors. Some states use TOC networks as proxies to engage in activities from which the states wish to distance themselves. TOC networks also have the ability to capture territory in states or portions of states and control it with violence and corruption of public officials. They often receive sanctuary as a result of providing social services, incorporating corruptive methods, and creating dependencies. TOC networks facilitate terrorism by providing money and services, such as selling weapons. They also engage in cyber-based theft and extortion and offer their capabilities to other cyber actors.

- Hong Kong police arrested six individuals with suspected Chinese organized crime links in connection with death threats to a lawmaker elected in September 2016 who advocated for greater autonomy from China.

- In 2015, MS-13 gang members in San Pedro Sula, Honduras provided meals to children and the elderly, shielded residents from rival criminals, meted out justice for unauthorized crimes, and halted criminals from unofficially taxing residents and small businesses. Such support to local communities undermines government legitimacy and engenders public support for the criminal groups.

Global Human Trafficking Risks Rising

The number of individuals at risk of human trafficking will almost certainly rise in 2017 because internal conflict, societal violence, and environmental crises are increasing the populations of refugees and Internally Displaced Persons (IDP). Risks of human trafficking vulnerability intensify during crisis situations when individuals often lose their support networks and sources of livelihood. In addition to crisis-induced displacement, entrenched structural factors—including political instability, government corruption, weak rule of law, soft economies, low levels of democracy, and discrimination toward women, children, and minorities—will very likely continue to increase potential victims' vulnerability to human trafficking worldwide.

Wildlife Trafficking and Illegal Fishing

Wildlife trafficking and poaching are widespread in many countries, especially those grappling with corruption, weak judiciaries, and scarce state resources. Some wildlife traffickers also move other contraband, such as drugs and weapons, at times relying on the same corrupt protectors. Awareness of wildlife crime and its impact is growing among source and demand countries, and regional leaders in Africa increasingly acknowledge the links among poaching, wildlife trafficking, instability, corruption, crime, and challenges to the rule of law.

Global fisheries face an existential threat in the decades ahead from surging worldwide demand, declining ocean health, and continued illegal, unreported, and unregulated (IUU) fishing. IUU fishing also harms legitimate fishing activities and livelihoods, jeopardizes food and economic security, benefits transnational crime, distorts markets, contributes to human trafficking, and undermines ongoing efforts to implement sustainable fisheries policies. It can also heighten tensions within and between countries and encourage piracy and frequently involves forced labor, a form of human trafficking.

ECONOMICS AND NATURAL RESOURCES

Global growth is likely to remain subdued in 2017 amid growing headwinds in China's economy and tepid growth in advanced economies. Worldwide gross domestic product (GDP) growth was virtually unchanged in 2016 from the previous year at 3.1 percent and is forecast to grow 3.5 percent in 2017, according the International Monetary Fund (IMF). Improving growth in commodity-dependent economies is likely to boost global economic activity beyond 2017. Adverse shocks, however, such as a greater slowdown in China than the IMF projects or capital outflows from emerging markets stemming from rising US interest rates, would put the modest global economic recovery at risk.

Macroeconomic Stability

The outlook for emerging markets and developing countries is improving, primarily because of stabilizing commodity prices and increased capital inflows. The IMF forecasts that growth in emerging economies will accelerate to 4.5 percent in 2017 as recoveries start to take hold in several countries. However, rising non-performing loans in China could reinforce the deceleration in Chinese economic growth, weighing on global economic and financial conditions and dampening global demand, particularly for commodities. Moreover, the prospect of higher interest rates in the United States and a strengthening dollar might lead to sustained capital outflows again from emerging markets.

Continued solid performance by the United States and increasingly stable conditions in many European states will probably help to support growth in developed economies. Many European countries and Japan, however, continue to rely on low interest rates and accommodative monetary policies to counter weak demand. Policy uncertainty also poses risks to the global economy.

Energy and Commodities

Subdued growth, particularly in the industrialized economies, had a negative impact on commodity prices in recent years, which have been particularly harmful for emerging market economies, with the exception of net commodity importers, such as China and India. A collapsing economy in Venezuela—the result of the oil-price decline and years of flawed economic policy and profligate government spending—will leave Caracas struggling to avoid default in 2017. Saudi Arabia and other Persian Gulf oil exporters, who generally have more substantial financial reserves, have nonetheless seen a sharp increase in budget deficits that have forced politically unpopular fiscal reforms such as cuts to subsidies, government spending, and government jobs. In Africa, declining oil revenues, past mismanagement, and inadequate policy responses to oil price shock have contributed to Angolan and Nigerian fiscal problems, currency strains, and deteriorating foreign exchange reserves. The World Bank forecasts that prices for most commodities, however, will increase slightly in 2017 as markets continue to rebalance, albeit at lower levels than earlier in the decade.

Sluggish growth of global demand for oil and low prices continue to discourage plans to develop new resources and expand existing projects—particularly in high-cost areas such as the Arctic, Brazilian pre-salt region, or West Africa's deepwater. Projects already under development will probably be completed during the next five years, but longer-term prospects have been slashed, potentially setting the stage for shortfalls and higher prices when demand recovers.

The Arctic

Arctic countries face an array of challenges and opportunities as diminishing sea ice increases commercial shipping prospects and possible competition over undersea resources in coming decades. In August 2016, the first large-capacity cruise ship traversed the Northwest Passage, and more such trips are planned. In September 2016, NASA measured the Arctic sea ice minimum extent at roughly 900,000 square miles less than the 1981-2010 average. Relatively low economic stakes in the past and fairly well established exclusive economic zones (EEZs) among the Arctic states have facilitated cooperation in pursuit of shared interests in the region, even as polar ice has receded and Arctic-capable technology has improved. However, as the Arctic becomes more open to shipping and commercial exploitation, we assess that risk of competition over access to sea routes and resources, including fish, will include countries traditionally active in the Arctic as well as other countries that do not border on the region but increasingly look to advance their economic interests there.

HUMAN SECURITY

Environmental Risks and Climate Change

The trend toward a warming climate is forecast to continue in 2017. The UN World Meteorological Organization (WMO) is warning that 2017 is likely to be among the hottest years on record—although slightly less warm than 2016 as the strong El Nino conditions that influenced that year have abated. The US National Oceanic and Atmospheric Administration (NOAA) and the National Aeronautics and Space Administration (NASA) reported that 2016 was the hottest year since modern measurements began in 1880. This warming is projected to fuel more intense and frequent extreme weather events that will be distributed unequally in time and geography. Countries with large populations in coastal areas are particularly vulnerable to tropical weather events and storm surges, especially in Asia and Africa.

Global air pollution is worsening as more countries experience rapid industrialization, urbanization, forest burning, and agricultural waste incineration, according to the World Health Organization (WHO). An estimated 92 percent of the world's population live in areas where WHO air quality standards are not met, according to 2014 information compiled by the WHO. People in low-income cities are most affected, with the most polluted cities located in the Middle East, Asia, and Africa. Public dissatisfaction with air quality might drive protests against authorities, such as those seen in recent years in China, India, and Iran.

Heightened tensions over shared water resources are likely in some regions. The dispute between Egypt and Ethiopia over the construction of the massive Grand Ethiopian Renaissance Dam (GERD) on the Nile is likely to intensify because Ethiopia plans to begin filling the reservoir in 2017.

Global biodiversity will likely continue to decline due to habitat loss, overexploitation, pollution, and invasive species, according to a study by a nongovernmental conservation organization, disrupting ecosystems that support life, including humans. Since 1970, vertebrate populations have declined an estimated 60 percent, according to the same study, whereas populations in freshwater systems declined

more than 80 percent. The rate of species loss worldwide is estimated at 100 to 1,000 times higher than the natural background extinction rate, according to peer-reviewed scientific literature.

We assess national security implications of climate change but do not adjudicate the science of climate change. In assessing these implications, we rely on US government-coordinated scientific reports, peer-reviewed literature, and reports produced by the Intergovernmental Panel on Climate Change (IPCC), which is the leading international body responsible for assessing the science related to climate change.

Health

The Zika virus is likely to continue to affect the Western Hemisphere through 2017. Although it is causing minor or no illness for most infected people, it is producing severe birth defects in about 10 percent of babies born to mothers who were infected while pregnant and is likely causing neurological symptoms for a small number of infected adults. A separate strain of the virus will likely continue to affect Southeast Asia, where scientists believe it has circulated since the 1960s. However, scientists do not know whether the virus will cause a spike in birth defects there. Previous outbreaks in Asia and Africa might provide at least partial immunity and hinder the virus's spread in those regions.

The continued rise of antimicrobial resistance—the ability of pathogens, including viruses, fungi, and bacteria, to resist drug treatment—is likely to outpace development of new antimicrobial drugs. This resistance will result in increasingly difficult or impossible-to-cure infections of previously curable diseases. Drug-resistant forms of malaria and tuberculosis are on the rise, threatening progress in controlling these diseases. Meanwhile, some strains of gonorrhea are showing resistance to nearly all classes of antibiotics, leaving only treatments of last resort, greatly increasing the risk of incurable strains.

HIV/AIDS, malaria, and tuberculosis continue to kill millions of people annually and hinder development in many resource-constrained countries despite significant progress to alleviate the global burden of infectious diseases. Stagnating or declining funding for global health initiatives and lack of domestic resources threaten the continued progress against health threats despite the availability of more cost-effective treatments. Rapidly expanding populations, particularly in Sub-Saharan Africa, put additional stress on scarce resources. Malnutrition; weak healthcare systems, conflict, migration, poor governance, and urbanization will worsen the emergence, spread, and severity of disease outbreaks.

The emergence of a severe global public health emergency is possible in any given year and can have negative impacts on the security and stability of a nation or region. A novel or reemerging microbe that is easily transmissible between humans and is highly pathogenic remains a major threat because such an organism has the potential to spread rapidly and kill millions. Threats such as avian influenza and Middle East Respiratory Syndrome Coronavirus (MERS-CoV) have pandemic potential. The World Bank has estimated that a severe global influenza pandemic could cost the equivalent of 4.8 percent of global GDP, or more than $3 trillion, during the course of an outbreak.

Atrocities and Instability

Risk of large-scale, violent or regime-threatening instability and atrocities will remain elevated in 2017. Poor governance, weak national political institutions, economic inequality, and the rise of violent non-state actors all undermine states' abilities to project authority.

- Weak state capacity can heighten the risk for atrocities, including arbitrary arrests, extrajudicial killings, rape, and torture.

Groups that promote civil society and democratization are likely to continue to face restrictions in 2017. Freedom House reported the eleventh consecutive year of decline in "global freedom" in 2017. Middle East and North Africa had ratings as one of the worst regions in the world in 2015.

Global Displacement

In 2015, the number of people forcibly displaced reached the highest levels ever recorded by the UN. In many cases, US partners and allies were either the source of refugees and other migrants—such as Afghanistan and South Sudan—or hosted them—such as Ethiopia, Europe, Jordan, Kenya, Lebanon, Turkey, and Uganda. These countries and others will look to the United States, the UN, and other international donors to help meet unprecedented assistance demands in 2017. Ongoing conflicts will continue to displace people, keeping displacement at record highs because few people can safely return home and family members seek to join those who left. Europe and other host countries will face accommodation and integration challenges in 2017, and refugees and economic migrants will probably continue to seek to transit to Europe.

- Primary drivers of global displacement include: conflicts, such as those in Afghanistan, Somalia, South Sudan, and Syria; weak border controls, such as in Libya, which broadened a route from Africa to Europe; relatively easy and affordable access to routes and information; endemic violence, such as in parts of Burundi, Central America, Nigeria, and Pakistan; and persecution, such as in Burma and Eritrea.

- The UN estimated that 65.3 million persons had been forcibly displaced worldwide at the end of 2015, including approximately 21.3 million refugees, 40.8 million IDPs, and 3.2 million asylum seekers. Refugees displaced for five or more years are more likely to remain in their host communities than to return home, according to academic research.

- In 2016, thousands of Syrian, Somali, Sudanese, and Afghan refugees who had fled their countries in preceding years were returned to their countries of origin, which are still undergoing intense conflict. These returnees are now internally displaced in areas still in conflict.

The scale of human displacement in 2017 will continue to strain the response capacity of the international community and drive record requests for humanitarian funding. Host and transit countries will struggle to develop effective policies and manage domestic concerns of terrorists exploiting migrant flows, particularly after attacks in 2016 by foreigners in Belgium, France, Germany, and Turkey.

REGIONAL THREATS

EAST ASIA

China

China will continue to pursue an active foreign policy—especially within the Asia Pacific region—highlighted by a firm stance on competing territorial claims in the East China Sea (ECS) and South China Sea (SCS), relations with Taiwan, and its pursuit of economic engagement across East Asia. Regional tension will persist as China completes construction at its expanded outposts in the SCS despite an overwhelmingly strong ruling against it by a UN Convention on the Law of the Sea (UNCLOS) arbitral tribunal in July 2016. China will also pursue efforts aimed at fulfilling its ambitious "One Belt, One Road" initiative to expand China's economic role and outreach across Asia through infrastructure projects.

China will seek to build on its hosting of the G20 Summit in Hangzhou in September 2016, its "One-Belt, One-Road" initiative, and progress on launching the Asia Infrastructure Investment Bank to increase its global presence on international economic issues. China will increasingly be a factor in global responses to emerging problems, as illustrated by China's participation in UN peacekeeping operations, its expanding counterterrorism cooperation, and infrastructure construction in Africa and Pakistan as part of the China-Pakistan Economic Corridor.

Domestically, Chinese leaders will move cautiously on their ambitious reform agenda, maintain their anti-corruption campaign, and try to manage China's slowing economy. China's economic growth continues to be driven by unsustainable debt accumulation, but Beijing has made limited progress on reforms needed to boost economic efficiencies. Debates among Chinese leaders over policy and personnel choices will intensify before the leadership transition at the 19th Party Congress in fall 2017 when Chinese President Xi Jinping will begin his second term as the head of the Chinese Communist Party.

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 increasingly grave national security threat to the United States and its interests.

North Korea's unprecedented level of testing and displays of strategic weapons in 2016 indicate that Kim is intent on proving he has the capability to strike the US mainland with nuclear weapons. In 2016, the regime conducted two nuclear tests—including one that was claimed to be of a standardized warhead design—and an unprecedented number of missile launches, including a space launch that put a satellite into orbit. These ballistic missile tests probably shortened North Korea's pathway toward a reliable ICBM, which largely uses the same technology. Kim was also photographed beside a nuclear warhead design and missile airframes to show that North Korea has warheads small enough to fit on a missile, examining a reentry-vehicle nosecone after a simulated reentry, and overseeing launches from a submarine and from mobile launchers in the field, purportedly simulating nuclear use in warfighting scenarios. North

Korea is poised to conduct its first ICBM flight test in 2017 based on public comments that preparations to do so are almost complete and would serve as a milestone toward a more reliable threat to the US mainland. Pyongyang's enshrinement of the possession of nuclear weapons in its constitution, while repeatedly stating that nuclear weapons are the basis for its survival, suggests that Kim does not intend to negotiate them away at any price.

North Korea has long posed a credible and evolving military threat to South Korea and, to a lesser extent, Japan. North Korea possesses a substantial number of proven mobile ballistic missiles, capable of striking a variety of targets in both countries, as demonstrated in successful launches in 2016. Kim has further expanded the regime's conventional strike options in recent years, with more realistic training, artillery upgrades, and new close-range ballistic missiles that enable precision fire at ranges that can reach more US and allied targets in South Korea.

After five years in power, North Korean leader Kim Jong Un continues to defy international sanctions for his country's behavior and reinforce his authority through purges, executions, and leadership shuffles, restricting fundamental freedoms, and enforcing controls on information. He notably unveiled new ruling structures in conjunction with the first Korean Workers Party Congress in a generation, held in May 2016.

Southeast Asia

Democracy in many Southeast Asian countries will remain fragile in 2017. Elites—rather than the populace—retain a significant level of control and often shape governance reforms to benefit their individual interests rather than to promote democratic values. Corruption and cronyism continue to be rampant in the region, and the threat of ISIS and domestic terrorist groups might provide some governments with a new rationale to address not only the terrorist threat but also to curb political opposition movements, as some regional leaders did in the post-9/11 environment.

In the **Philippines**, aggressive campaigns against corruption, crime, and drugs will probably continue despite charges by Filipino critics and international organizations that it is fostering a permissive environment for extrajudicial killings. Philippine efforts to diversify Manila's foreign relations away from the United States have increased uncertainty about the future of Philippine-US security ties. **Thailand** is undergoing its most significant transition in 70 years following the death of the king. In **Burma**, the government led by the National League for Democracy (NLD) seeks to continue the country's democratic transition process, but the military, which has retained significant political and economic power and exclusive control over the security forces, sometimes undermines the civilian government's objectives. In addition, the NLD will be challenged by its lack of governing experience and provisions of the 2008 Constitution that do not align with democratic norms. Burma's Government will continued to be challenged in dealing with the status of the Muslim minority Rohingya in western Burma.

Cohesion of the Association of Southeast Asian Nations (ASEAN) on economic and security issues will continue to be challenged by differing development levels among ASEAN members, their varying economic dependencies on China, and their views of the threat of Beijing's regional ambitions and assertiveness in the SCS. Southeast Asian SCS claimants will continue to seek various ways to strengthen cooperation in the region and, in some cases, with the United States on maritime security issues.

RUSSIA AND EURASIA

Russia

In 2017, Russia is likely to be more assertive in global affairs, more unpredictable in its approach to the United States, and more authoritarian in its approach to domestic politics. Emboldened by Moscow's ability to affect battlefield dynamics in Syria and by the emergence of populist and more pro-Russian governments in Europe, President Vladimir Putin is likely to take proactive actions that advance Russia's great power status.

Putin will seek to prevent any challenges to his rule in the runup to presidential elections scheduled for 2018. Putin remains popular at home, but low turnout in the Duma elections in 2016 and sustained economic hardship will probably enhance Putin's concerns about his ability to maintain control. Putin is likely to continue to rely on repression, state control over media outlets, and harsh tactics to control the political elite and stifle public dissent.

Russia is likely to emerge from its two-year recession in 2017, but the prospects for a strong recovery are slim. Russia is likely to achieve 1.3 percent GDP growth in 2017 and 1.7 percent in 2018, according to commercial forecasts. Putin has long sought to avoid structural reforms that would weaken his control of the country and is unlikely to implement substantial reforms before the presidential elections.

We assess that Russia will continue to look to leverage its military support to the Asad regime to drive a political settlement process in Syria on its terms. Moscow has demonstrated that it can sustain a modest force at a high-operations tempo in a permissive, expeditionary setting while minimizing Russian casualties and economic costs. Moscow is also likely to use Russia's military intervention in Syria, in conjunction with efforts to capitalize on fears of a growing ISIS and extremist threat, to expand its role in the Middle East.

We assess that Moscow's strategic objectives in Ukraine—maintaining long-term influence over Kyiv and frustrating Ukraine's attempts to integrate into Western institutions—will remain unchanged in 2017. Putin is likely to maintain pressure on Kyiv through multiple channels, including through Russia's actions in eastern Ukraine, where Russia arms so-called "separatists. Moscow also seeks to undermine Ukraine's fragile economic system and divided political situation to create opportunities to rebuild and consolidate Russian influence in Ukrainian decisionmaking.

Moscow will also seek to exploit Europe's fissures and growing populist sentiment in an effort to thwart EU sanctions renewal, justify or at least obfuscate Russian actions in Ukraine and Syria, and weaken the attraction of Western integration for countries on Russia's periphery. In particular, Russia is likely to sustain or increase its propaganda campaigns. Russia is likely to continue to financially and politically support populist and extremist parties to sow discord within European states and reduce popular support for the European Union.

The Kremlin is also likely to continue to see defense modernization as a top national priority even as the cumulative effect on the economy of low oil prices, sanctions, and systemic problems serves as a drag on key military goals. Moscow is pursuing a wide range of nuclear, conventional, and asymmetric

capabilities designed to achieve qualitative parity with the United States. These capabilities will give Moscow more options to counter US forces and weapons systems.

Ukraine, Belarus, and Moldova

Russia's military intervention in eastern **Ukraine** continues more than two years after the "Minsk II" agreement concluded in February 2015. Russia continues to exert military and diplomatic pressure to coerce Ukraine into implementing Moscow's interpretation of the political provisions of the agreement—among them, constitutional amendments that would effectively give Moscow a veto over Kyiv's strategic decisions. Domestic Ukrainian opposition to making political concessions to Russia—especially while fighting continues in eastern Ukraine—will limit Kyiv's willingness and ability to compromise, complicating prospects for implementing the Minsk agreement. Russia largely controls the level of violence, which it uses to exert pressure on Kyiv and the negotiating process, and fluctuating levels of violence will probably continue along the front line. The struggle of Ukraine to reform its corrupt institutions will determine whether it can remain on a European path or fall victim again to elite infighting and Russian influence.

Rising popular discontent in **Belarus** will probably complicate the government's efforts to maintain its improved relations with the United States and the EU, which are aimed at bolstering its flagging economy and preserving some diplomatic maneuvering room with Russia. Minsk will continue close security cooperation with Moscow but will probably continue to oppose the establishment of Russian military bases in Belarus.

Moldova will probably also seek to balance its relations with Russia and the West rather than pursue a major shift in either direction. The Moldovan Government will almost certainly seek to move forward on implementing Moldova's EU Association Agreement despite the election of a more pro-Russian president. Settlement talks over the breakaway region of Transnistria will continue, but any progress is likely to be limited to smaller issues.

The Caucasus and Central Asia

In **Georgia,** the ruling Georgian Dream (GD) coalition's decisive electoral victory in 2016 is likely to facilitate GD's efforts to target the former ruling United National Movement and expand political control. GD will continue to pursue greater Euro-Atlantic integration by attempting to cement ties with NATO and the EU.

Tensions between **Armenia** and **Azerbaijan** over the separatist region of Nagorno-Karabakh flared in April 2016, and both sides' unwillingness to compromise and mounting domestic pressures suggest that the potential for large-scale hostilities will remain in 2017. In **Azerbaijan**, ongoing economic difficulties are likely to challenge the regime and increase its tendency to repress dissent to maintain power while it continues to try to balance relations with Russia, Iran, and the West.

Central Asian states will continue to balance their relations among Russia, China, and the West to pursue economic and security assistance and protect their regimes' hold on power. They remain concerned about the threat of extremism to their stability, particularly in light of a reduced Coalition presence in Afghanistan. Russia and China share these concerns and are likely to use the threat of instability in Afghanistan to try to increase their involvement in Central Asian security affairs. Economic

challenges stemming from official mismanagement, low commodity prices, declining trade and remittances associated with weakening economies of Russia and China, ethnic tensions, and political repression are likely to present the most significant threats to stability in these countries.

EUROPE

Key Partners

The severity of multiple crises facing Europe—irregular migration, security threats, slow economic growth, and protracted debt issues—will challenge European policy cohesion and common action. Additionally, the form and substance of the UK's exit (Brexit) from the European Union will distract European policymakers.

Migration

The EU-Turkey Statement addressing migration issues concluded in March 2016 and that tightened border controls in the Balkans will continue to limit migration to Europe. Preserving the EU-Turkey agreement, completing trade deals and making investments offered to five African countries, and ensuring the success of a repatriation deal with Afghanistan will likely remain a focus for Europe.

Security

Terrorists have taken advantage of the influx of migrants and a potential rise in returning foreign fighters from the conflicts in Iraq and Syria might compound the problem. Europe will remain vulnerable to terrorist attacks, and elements of both ISIS and al-Qa'ida are likely to continue to direct and enable plots against targets in Europe

Some European states see Russia as less of a threat to Europe than others do, even as the Baltic states and Poland begin to host multinational battalions as part of NATO's enhanced Forward Presence.

Economic/Financial Issues

The European Commission projects that euro-zone growth will be about 1.6 percent in 2017. Its projections are based on weak investment growth, uncertainty stemming from Brexit, potential disruptions to trade, and political and practical limits to expanding monetary and fiscal efforts to support growth.

Turkey

President Recep Tayyip Erdogan's narrow win in the mid-April popular referendum on expanding his powers and the ruling Justice and Development Party's (AKP's) post-coup crackdowns are increasing societal and political tension in Turkey.

Turkey's relations with the United States are strained because Ankara calculates that the United States has empowered Turkey's primary security threat—the Kurdistan Workers' Party (PKK)—by partnering

with the Syrian Kurdish People's Protection Units (YPG), which Turkey alleges is aligned with the PKK. European admonition of Turkey's conduct during the referendum—including limitations European countries placed on Turkish campaigning on their soil—is further straining Turkish ties to the EU.

- Two major Turkish complaints are Washington's unwillingness to meet Turkish demands to extradite US-person Fethullah Gulen—accused by the Turkish Government of orchestrating the failed coup in July 2016—and US support to the YPG in Syria.

- In November 2016, the Turkish president indicated that he would be willing to consider joining the Russian-led Shanghai Cooperation Organization (SCO) as an alternative to the EU.

MIDDLE EAST AND NORTH AFRICA

Syria

We assess that the Syrian regime, backed by Russia and Iran, will maintain its momentum on the battlefield but that the regime and the opposition are not likely to agree on a political settlement in 2017. Damascus has committed to participate in peace talks but is unlikely to offer more than cosmetic concessions to the opposition. The opposition, although on the defensive, is able to counterattack, which will probably prevent the regime from asserting territorial control over western and southern Syria, and remains committed to President Bashar al-Asad's departure.

The Islamic State of Iraq and ash-Sham (ISIS) has lost about 45 percent of the territory it held in Syria in August 2014, but it still controls much of the eastern section of the country, including the city of Ar Raqqah. ISIS will likely have enough resources and fighters to sustain insurgency operations and plan terrorists attacks in the region and internationally.

Asad's foreign supporters—Russia, Iran, and Lebanese Hizballah—want to keep an allied regime in power and maintain their influence in Syria. Moscow's deployment of combat assets to Syria in late 2015 helped change the momentum of the conflict; Russia has provided combat aircraft, warships, artillery, arms, and ammunition. Iran provides military advice, fighters, weaponry, fuel, and Shia militants. Lebanese Hizballah provides fighters and helps control the Lebanon-Syria border.

Most opposition backers maintain their support, in part by linking Asad's regime to Iran's malign influence in the region, but their lack of unity will hamper their effectiveness.

Syrian Kurdish People's Protection Units (YPG) control much of northern Syria and have worked closely with coalition forces to seize terrain from ISIS. The YPG's goal to unite its "cantons" across northern Syria is opposed by most Syrian Arabs and by Turkey, which views these Kurdish aspirations as a threat to its security. To weaken ISIS and check the Kurds, Ankara has used Syrian opposition groups, backed by Turkish artillery, aircraft, and armored vehicles, to establish a border security zone in Syria.

The continuation of the Syrian conflict will worsen already-disastrous conditions for Syrians and regional states and maintain migration pressure on Europe. As of late March 2017, more than 4.9 million Syrians

have left the country from a pre-conflict population of approximately 23 million, and an additional 6.3 million were internally displaced. ISIS's presence in Syria and ability to stage cross-border attacks will continue to jeopardize Iraq's stability.

Iraq

The Iraqi Government's primary focus through 2017 will be recapturing and stabilizing Mosul, the largest urban ISIS stronghold in Iraq, and other ISIS-held territory. The Iraqi Security Forces (ISF) and Kurdish Peshmerga with coalition support and forces of the Shia-dominated Popular Mobilization Committee (PMC) are all involved in the Mosul campaign. Faced with the eventual loss of Mosul, ISIS is preparing to regroup and continue an insurgency and terrorist campaign.

- As the Mosul campaign progresses, Baghdad faces potential tensions between the Kurds and the Iranian-backed PMC members over disputed territory while also managing the Turkish presence in northern Iraq. Baghdad has rebuked Ankara for its presence at Bashiqa and warned of potential conflict if Turkey intervenes any farther in northern Iraq. Tensions might persist well after major counter-ISIS combat operations cease as external actors continue to pursue their political and strategic goals in Iraq.

Meanwhile, the Iraqi prime minister is trying to fend off political challenges and cope with an economy weakened by the fight with ISIS and depressed oil prices. A loose "reform" coalition in the Council of Representatives (COR) exploited political divisions in fall 2016 to remove the defense and finance ministers. Political factionalism has prevented the passage of needed political reform, heightened distrust among sectarian groups, and undermined governance.

- Iraq will probably need international financial support throughout 2017, but Iraq's finances could stabilize if oil prices continue to slowly rise and Baghdad makes progress on its reform program. In 2016, Iraq's revenue from crude oil sales averaged $3.3 billion per month, less than half the monthly revenue in 2014, despite a rise in the number of barrels of oil exported. Oil sales account for about 90 percent of government revenues and make up almost 50 percent of Iraq's GDP. The United States and Iraq concluded a sovereign loan agreement in late January 2017 that could help Baghdad access international funds that it sorely needs to reconstruct areas liberated from ISIS.

Iraq will face serious challenges to its stability, political viability, and territorial integrity after control of Mosul is wrested from ISIS. More than 200,000 individuals have been displaced from Mosul due to the fighting. However, about a third have since returned to their homes, and as many as 1 million civilians might be eventually displaced, adding to the 3 million displaced persons in Iraq as of February 2016.

- Reconstruction of infrastructure and tens of thousands of civilian structures destroyed by fighting in Sunni areas once occupied by ISIS will cost billions of dollars and take years.
- Ethnosectarian reconciliation will also be an enduring challenge. Iraqi Shia, Sunnis, and Kurds increasingly view themselves as having diverging futures. ISIS will seek to exploit any Sunni discontent with Baghdad and try to regain Iraqi territory, whereas the Kurds will probably continue efforts to establish an independent state.

Iran

The Islamic Republic of Iran remains an enduring threat to US national interests because of Iranian support to anti-US terrorist groups and militants, the Asad regime, Huthi rebels in Yemen, and because of Iran's development of advanced military capabilities. Despite Supreme Leader Khamenei's conditional support for the JCPOA nuclear deal implemented in January 2016, he is highly distrustful of US intentions. Iran's leaders remain focused on thwarting US and Israeli influence and countering what they perceive as a Saudi-led effort to fuel Sunni extremism and terrorism against Iran and Shia communities throughout the region.

Iran is immersed in ongoing conflicts in Iraq, Syria, and Yemen. Iranian officials believe that engaging adversaries away from Iran's borders will help prevent instability from spilling into Iran and reduce ISIS's threat to Iran and its regional partners. Iran's involvement in these conflicts, including sending hundreds of its own forces plus arming, financing, and training thousands of Iraqi, Afghan, and Pakistani Shia fighters to support the Asad regime, has aggravated sectarianism and increased tensions with other regional states. Tehran's provision of aid to the Huthis, including unmanned aerial vehicles (UAVs), explosive boat technology, and missile support, risks expanding and intensifying the conflict in Yemen and the broader Iranian-Saudi dispute. We assess that Iran's leaders intend to leverage their ties to local actors in Iraq, Syria, and Yemen to build long-term Iranian influence in the region. Iran will also utilize its relationship with Moscow to try to expand Iranian influence and counter US pressure.

Hardliners, who believe that the West is attempting to infiltrate Iran to undermine the regime, have driven the increase of arrests of citizens since 2014 who are dual nationals. The Islamic Revolutionary Guard Corps (IRGC) will likely continue to scrutinize, arrest, and detain individuals with ties to the West, particularly dual US-Iranian and UK-Iranian citizens. This practice will weaken prospects of attracting foreign investment into Iran's economy.

Iran continues to develop a range of new military capabilities to monitor and 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 anti-ship and 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 surface-to-air missile system in 2016 provides Iran with its most advanced long-range air defense system.

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, although US Navy operators consider approximately 10 percent to be unsafe, abnormal, or unprofessional. We assess that limited aggressive interactions will continue and are probably intended to project an image of strength and possibly to gauge US responses.

Yemen

Fighting in Yemen will almost certainly persist in 2017 despite international attempts to forge cease-fires between Huthi-aligned forces, trained by Iran, and the Yemeni Government, backed by a Saudi-led coalition. Neither the alliance between the Huthis and former Yemeni President Ali Abdallah Salih nor the government of Yemeni President Abd Rabuh Mansur Hadi has been able to achieve decisive results through military force, despite their prominent international backers. Efforts at peace talks are nascent, and both sides remain wary of the other's intentions.

As of late 2016, the fighting had displaced more than 2 million people and left 82 percent of Yemen's population in need of humanitarian aid. Temporary cease-fires have allowed for some increased access for humanitarian organizations, but relief operations are hindered by lack of security, bureaucratic constraints, and funding shortages. More than half the population is experiencing crisis or emergency levels of food insecurity.

AQAP and ISIS's branch in Yemen have exploited the conflict and the collapse of government authority to gain new recruits and allies and expand their influence. Both groups threaten Western interests in Yemen and have conducted attacks on Huthi, Yemeni Government, and Saudi-led coalition targets.

SOUTH ASIA

Afghanistan

The overall situation in Afghanistan will very likely continue to deteriorate, even if international support is sustained. Endemic state weaknesses, the government's political fragility, deficiencies of the Afghan National Security Forces (ANSF), Taliban persistence, and regional interference will remain key impediments to improvement. Kabul's political dysfunction and ineffectiveness will almost certainly be the greatest vulnerability to stability in 2017. ANSF performance will probably worsen due to a combination of Taliban operations, ANSF combat casualties, desertions, poor logistics support, and weak leadership. The ANSF will almost certainly remain heavily dependent on foreign military and financial support to sustain themselves and preclude their collapse. Although the Taliban was unsuccessful in seizing a provincial capital in 2016, it effectively navigated its second leadership transition in two years following the death of its former chief, Mansur, and is likely to make gains in 2017. The fighting will also continue to threaten US personnel, allies, and partners, particularly in Kabul and urban population centers. ISIS's Khorasan branch (ISIS-K)—which constitutes ISIS's most significant presence in South Asia—will probably remain a low-level developing threat to Afghan stability as well as to US and Western interests in the region in 2017.

Pakistan

Pakistani-based terrorist groups will present a sustained threat to US interests in the region and continue to plan and conduct attacks in India and Afghanistan. The threat to the United States and the West from Pakistani-based terrorist groups will be persistent but diffuse. Plotting against the US homeland will be conducted on a more opportunistic basis or driven by individual members within these groups.

Pakistan will probably be able to manage its internal security. Anti-Pakistan groups will probably focus more on soft targets. The groups we judge will pose the greatest threat to Pakistan's internal security include Tehrik-e Taliban Pakistan, Jamaat ul-Ahrar, al-Qa'ida in the Indian Subcontinent, ISIS-K, Laskhar-e Jhangvi, and Lashkar-e Jhangvi al-Alami. The emerging China Pakistan Economic Corridor will probably offer militants and terrorists additional targets.

Pakistan's pursuit of tactical nuclear weapons potentially lowers the threshold for their use. Early deployment during a crisis of smaller, more mobile nuclear weapons would increase the amount of time that systems would be outside the relative security of a storage site, increasing the risk that a coordinated attack by non-state actors might succeed in capturing a complete nuclear weapon.

India-Pakistan

Relations between India and Pakistan remain tense following two major terrorist attacks in 2016 by militants crossing into India from Pakistan. They might deteriorate further in 2017, especially in the event of another high-profile terrorist attack in India that New Delhi attributes to originating in or receiving assistance from Pakistan. Islamabad's failure to curb support to anti-India militants and New Delhi's growing intolerance of this policy, coupled with a perceived lack of progress in Pakistan's investigations into the January 2016 Pathankot cross-border attack, set the stage for a deterioration of bilateral relations in 2016. Increasing numbers of firefights along the Line of Control, including the use of artillery and mortars, might exacerbate the risk of unintended escalation between these nuclear-armed neighbors. Easing of heightened Indo-Pakistani tension, including negotiations to renew official dialogue, will probably hinge in 2017 on a sharp and sustained reduction of cross-border attacks by terrorist groups based in Pakistan and progress in the Pathankot investigation.

SUB-SAHARAN AFRICA

South Sudan

Clashes between Juba and the armed opposition will continue, heightening ethnic tensions and exacerbating the humanitarian crisis and famine amid a declining economy. Both sides' use of ethnic militias, hate speech, and the government's crackdown against ethnic minorities raise the risk of additional mass atrocities. The government will probably continue to restrict political freedoms and civil liberties and obstruct humanitarian assistance.

Sudan

Khartoum probably hopes to continue constructive engagement with the United States following Washington's decision in January 2017 to suspend some sanctions on Sudan. The regime will probably largely adhere to a cessation of hostilities in conflict areas—required to receive sanctions relief—but skirmishing between the Sudanese military and rebel forces is likely to result in low levels of violence and population displacement. The regime's military gains since March 2016 and divisions among armed opponents will almost certainly inhibit the insurgents' ability to make significant political or military gains.

Public dissatisfaction over a weakened economy and austerity measures, however, will test the government's ability to maintain order.

Nigeria

The Nigerian Government will confront a wide range of challenges in 2017, many of which are deeply rooted and have no "quick fix." Despite Nigeria's progress in 2016 reclaiming territory from ISIS in West Africa (ISIS-WA) and Boko Haram, both terrorist groups will remain a threat to military and civilians in northeastern Nigeria, as well as in neighboring Cameroon, Chad, and Niger. Moreover, Nigeria, with Africa's largest economy, is suffering a recession brought on by low oil prices and militant attacks on its oil infrastructure. This recession is handicapping Abuja's efforts to combat the terrorists and respond to a growing humanitarian crisis in the northeast.

Sahel

Governments in Africa's Sahel region—particularly Chad, Mali, Mauritania, and Niger—will remain at risk of internal conflict and terrorist attacks in 2017. The region's shared geography, ethnic and religious connections, and a pervasive lack of border security have facilitated a rise in extremist groups, traffickers, and antigovernment militias since the collapse of Libya in 2011 and the northern Mali uprising in 2012. Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM), al-Murabitun, Ansar al-Din, and other violent extremist groups will continue attacking Western and local interests in the region.

Somalia

The Somali Government will continue to rely on international assistance, including in the areas of civilian protection, service provision, dispute resolution, security, and humanitarian relief. Progress in these areas is critical to maintain support from troop-contributing countries of the African Union Mission in Somalia (AMISOM), which plans to begin withdrawing from Somalia in 2018.

Ethiopia

Ethiopia has faced widespread public protests and ethnic tensions and will struggle to address the underlying grievances while preserving the power of the ruling party. The risk of instability is high. Addis Ababa declared a state of emergency in October 2016 and continues mass arrests, targeting opposition leaders.

Democratic Republic of the Congo

A deal between the government of the Democratic Republic of the Congo (DRC) and Congolese opposition and civil society over President Joseph Kabila's term extension has bought the regime time. Kabila named an opposition member as prime minister in April, but elections are unlikely to be held by the end of 2017 as called for under the agreement. Meanwhile, armed conflict in the east perpetrated by militia groups will exacerbate serious humanitarian challenges.

WESTERN HEMISPHERE

Mexico

The Mexican Government will focus on domestic priorities to help position the country for the presidential election in 2018 while also seeking to limit fallout from potential shifts in the bilateral relationship with the United States. Mexico will be challenged to make gains against corruption and rising crime and will continue to rely on the military to stymie criminal violence. Its $1.1 trillion economy has benefitted from strong economic fundamentals and robust exports, but changes in trade relationships might weaken the export sector and slow economic growth. Mexican migration to the United States, which has decreased in recent years, might increase if economic opportunity at home declines. Apprehensions of undocumented Mexicans fell from about 268,000 in FY 2013 to 193,000 in FY 2016, according to DHS statistics.

Central America

Insecurity, lack of economic opportunities, desire for family reunification, and views of US immigration policy are likely to remain the principal drivers of migration from the Northern Triangle countries of El Salvador, Guatemala, and Honduras to the United States. Human smuggling networks will continue to help migrants navigate travel routes and security at the US and Mexican border. Homicide rates in these countries remain high despite a decline in 2016, and gang-related violence is still prompting Central Americans to flee. DHS apprehensions along the southwest border of migrants from the Northern Triangle reached nearly 200,000 in FY 2016 but have declined sharply since February 2017.

Colombia

The Colombian Government's ability to implement its historic peace deal with the Revolutionary Armed Forces of Colombia (FARC) in 2017 will be key to the country's prospects for fully harnessing economic and investment opportunities. The peace deal ended the country's 52-year civil war with the FARC and demobilized the Western Hemisphere's largest and longest-running insurgency. Colombia was already politically stable and markedly less violent than 20 years ago. Even so, some immediate post-conflict challenges will include stemming rising drug production and addressing social and economic inequality in rural areas.

Cuba

As Cuba heads into the final year of preparations for its planned historic leadership transition in early 2018, the government's focus will be on preserving the regime's hold on power and dealing with the falling economic growth rate. Cuba blames its slowing economy on lower global commodity prices, the US embargo, and the economic crisis in Venezuela, a top trade partner and important source of political support and petroleum at generous financing terms. Havana, however, has stalled implementation of its own reform program, including changes to investment laws needed to address longstanding investor concerns and plans to unify its dual currency and exchange rate system.

Some Cuban migration to the United States via land routes through Central America and Mexico—especially by Cubans already in transit—is likely to continue despite a significant decrease following the end of the US "Wet Foot, Dry Foot" policy in January 2017. That policy allowed most undocumented Cubans who reached US soil—as opposed to being intercepted at sea—to remain in the United States and then apply for lawful permanent residency status after one year under the Cuban Adjustment Act of 1966. In FY 2016, some 42,000 Cuban migrants arrived at the US southwest border and maritime flows exceeded 7,300 migrants because of poor economic prospects in Cuba and apprehension about potential US policy shifts.

Venezuela

Venezuela's regime and the political opposition will remain at odds in 2017 as Venezuela's domestic political and economic tensions intensify. The regime is struggling to contain spiraling inflation and finance imports, creating shortages of foodstuffs and medicines in the oil-rich country. The unpopular government charges that the opposition is waging an economic war and trying to stage a political coup and will probably ratchet up repression to maintain power. Shortages of food, medicine, and basic supplies will probably continue to stoke tensions through 2017.

Chairman BURR. Director Coats, thank you for that very thorough and comprehensive testimony on behalf of the intelligence community. Dan, quite frankly, you make us proud, seeing one of our own now head the entire intelligence community, and I want to thank you and Marsha personally for your willingness to do that.

Director COATS. Thank you.

Chairman BURR. And to also pass to you, we are anxious for your deputy to be considered by the committee. Would you please send us a nomination?

Director COATS. We are doing our very best to do that. Nobody's more anxious than me.

Chairman BURR. I'm sure that's the case.

I'm going to recognize myself for five minutes.

Director McCabe, did you ever hear Director Comey tell the President that he was not the subject of an investigation? Excuse me. Did you ever hear Director Comey tell the President he was not the subject of an investigation?

Director MCCABE. Sir——

Chairman BURR. Could you turn on your microphone, please.

Director MCCABE. Rookie mistake. I'm sorry.

Sir, I can't comment on any conversations the Director may have had with the President.

Chairman BURR. Okay.

General Stewart, you heard Director Coats state on everybody's behalf that there is an expected deterioration of conditions in Afghanistan. Can you give us DIA's assessment of the situation today in Afghanistan and what would change that deterioration?

General STEWART. Thanks, Mr. Chairman. I pay close attention to the operations in Afghanistan. I make two trips there each year, one before the fighting season and one following the fighting season. That way I get on the ground my own personal assessment of how things are going.

I was there about six weeks ago. The ANDSF, two years into taking control of the security environment, has had mixed results in this past year. Those mixed results can characterize the security environment as a stalemate and, left unchecked, that stalemate will deteriorate in favor of the belligerents. So we have to do something very different than what we've been doing in the past.

Let me back out just a little bit and talk about the fact that the Taliban failed to meet any of their strategic objectives that they outlined during the last fighting season. They controlled no district centers. They were able to execute high-visibility attacks, which causes a psychological effect, that has a debilitating effect. They maintained some influence in the rural areas, but they controlled none of the large district centers.

Having said that, the Afghan National Defense Security Forces did not meet their force generation objectives. They had some success in training the force. They were able to manage a crisis better than they have in the past. They were able to deploy forces, but failed in my opinion to employ the ISR and the fire support to make them as effective on the battlefield as possible.

Unless we change something where we introduce either U.S. forces or NATO forces, that changes the balance of forces on the

ground, changes the fighting outputs on the ground, or add additional training and advising capability at lower levels than we do now, the situation will continue to deteriorate and we'll lose all the gains that we've invested in over the last several years.

So they've got to get more trainers below the corps level, I believe—not sure how far down—or they'd have to get more personnel on the ground, generate greater forces, greater fire support, greater use of ISR, or this will in fact deteriorate further.

Chairman BURR. Thank you, General.

Admiral Rogers, every aspect of our daily lives continues to become part of a traceable, trackable, interacting environment now known as the Internet of Things. In addition, artificial intelligence, or AI, has increasingly enabled technology to become autonomous. What is the IC's current assessment of the ever-changing capabilities of the Internet of Things and what it presents?

Admiral ROGERS. It represents both opportunity, but from an information assurance or computer network defense perspective it represents great concern, where the ability to harness literally millions of devices that were built to very simple, day to day activities, suddenly can be tied together and focused and oriented to achieve a specific outcome. We've seen this with denial of service attempts against a couple significant companies on the East Coast of the United States in the course of the last year.

This is going to be a trend in the future. It's part of the discussions we're having. I'm in the midst of having some discussions in the private sector. This is going to be a problem that's common to both of us. How can we work together to try to, number one, understand this technology and, number two, ask ourselves how do we ensure that it's not turned around, if you will, against us.

Chairman BURR. Thank you for that.

Admiral Rogers, I'll probably put this to you as well. Section 702 of the FISA Amendments Act authorizes the government to target only non-U.S. persons reasonably believed to be located outside the United States for the purposes of acquiring foreign intelligence information. Section 702 cannot be used to target any person located inside the United States, and the law prohibits the government from reverse targeting, that is targeting a non-U.S. person outside the United States specifically for the purpose of collecting the communications of a person inside the United States. The IC uses FISA 702 collection authority to detect, identify, and disrupt terrorist and other national security threats.

How would you characterize 702 authority and its importance to the current intelligence collection platform overall?

Admiral ROGERS. If we were to lose 702's authorities, we would be significantly degraded in our ability to provide timely warning and insight as to what terrorist actors, nation-states, and criminal elements are doing that is of concern to our Nation, as well as our friends and allies. This 702 has provided us insight that is focused both on counterterrorism quite as well as counter-proliferation, understanding what nation-states are doing. It's given us tremendous insights in the computer network defense arena. I would highlight much—not all—much of what was in the intelligence community's assessment, for example, on the Russian efforts against the U.S.

election process in 2016 was informed by knowledge we gained through 702 authority.

Chairman BURR. Thank you for that.

Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

I've got a couple questions that hopefully will only require yes or no answers. First, for the whole panel, the assembled leadership of the intelligence community: do you believe that the January 2017 Intelligence Community Assessment accurately characterized the extent of Russian activities in the 2016 election in its conclusion that Russian intelligence agencies were responsible for the hacking and leaking of information and using this information in order to influence our elections? A simple yes or no would suffice.

Director CARDILLO. I do, yes, sir.

General STEWART. Yes, Senator.

Admiral ROGERS. Yes, I do.

Director COATS. Yes, I do.

Director MCCABE. Yes.

Director POMPEO. Yes.

Vice Chairman WARNER. I guess the presumption, the next presumption—I won't even ask this question—is, consequently that community assessment was unanimous and is not a piece of fake news or evidence of some other individual or nation-state other than Russia. So I appreciate that again for the record.

I warned you, Mr. McCabe, I was going to have to get you on the record as well on this. Mr. McCabe, for as long as you are Acting FBI Director do you commit to informing this Committee of any effort to interfere with the FBI's ongoing investigation into links between Russia and the Trump campaign?

Director MCCABE. I absolutely do.

Vice Chairman WARNER. Thank you so much for that. I think, in light of what's happened in the last 48 hours, it's critically important that we have that assurance. And I hope you'll relay, at least for me, to the extraordinary people who work at the FBI that this Committee supports them, supports their efforts, supports the professionalism, and supports their independence.

Director MCCABE. I will, sir. Thank you.

Vice Chairman WARNER. In light of the fact that we just saw French elections where it felt like déjà vu all over again in terms of the release of a series of emails against Mr. Macron days before the election, and the fact that this committee continues to investigate the type of tactics that Russia has used, where do we stand as a country in terms of preparation to make sure this doesn't happen again in 2018 and 2020?

Where have we moved in terms of collaboration with State voter files, in terms of working more with the tech community, particularly the platform entities, in terms of how we can better assure real news versus fake news? And is there some general sense—Director Coats, I know you've only been in the job for a short period of time—of how we're going to have a strategic effort? Because while it was Russia in 2016, other nation-states could launch similar-type assaults.

Director COATS. Well, we will continue to use all the assets that we have in terms of collection and analysis relative to what the in-

fluence has been and potentially could be in future. The Russians have spread this across the globe. Interestingly enough, I met with the Prime Minister of Montenegro, the latest nation to join NATO, the number 29 nation. What was the main topic? Russian interference in their political system.

So it sweeps across Europe and to other places. It's clear, though, the Russians have upped their game using social media and other opportunities in ways we haven't seen before. So it's a great threat to our democratic process, and our job here is to provide the best intelligence we can to the policymakers as they develop a strategy in terms of how to best reflect a response to this.

Vice Chairman WARNER. One of the things I'm concerned about is, we've all expressed this concern, but since this doesn't fall neatly into any particular agency's jurisdiction, who's taking the point on interacting with the platform companies, à la the Google, Facebook, and Twitters? Who's taking the point in terms of interacting with DHS, I imagine, in terms of State boards of election? How are we trying to ensure that our systems are more secure?

If we could get a brief answer on that because I have one last question for Admiral Rogers.

Director COATS. Well, I think obviously our office tasks and takes the point, but there's contribution from agencies across the IC. I might ask Director Pompeo to address that, and others might want to address that also. But each of us, each of the agencies, to the extent that they can and have the capacity, whether it's NSA through SIGINT, whether it's CIA through HUMINT or other sources, will provide information to us that we want to use as a basis to provide to our policymakers.

Relative to a grand strategy, I am not aware right now of any—I think we're still assessing the impact. We have not put a grand strategy together, which would not be our purview. We would provide the basis of intelligence that would then be the foundation for what that strategy would be.

Vice Chairman WARNER. My hope would be that we need to be proactive in this. We don't want to be sitting here kind of looking back at it after a 2018 election cycle.

Last question very briefly. Admiral Rogers, do you have any doubt that the Russians were behind the intervention in the French elections?

Director ROGERS. Let me phrase it this way. We are aware of some Russian activity directed against the Russian—excuse me—directed against the French election process. As I previously said before Congress earlier this week, we in fact reached out to our French counterparts to say: We have become aware of this activity; we want to make you aware; what are you seeing?

I'm not in a position to have looked at the breadth of the French infrastructure, so I'm not really in a position to make a whole simple declaratory statement.

Vice Chairman WARNER. Thank you, Mr. Chairman.

Chairman BURR. Senator Rubio.

Senator RUBIO. Thank you, Mr. Chairman.

Mr. McCabe, can you—without going to the specifics of any individual investigation, I think the American people want to know, has the dismissal of Mr. Comey in any way impeded, interrupted,

stopped, or negatively impacted any of the work, any investigation, or any ongoing projects at the Federal Bureau of Investigation?

Director MCCABE. As you know, Senator, the work of the men and women of the FBI continues despite any changes in circumstance, any decisions. So there has been no effort to impede our investigation to date. Quite simply put, sir, you cannot stop the men and women of the FBI from doing the right thing, protecting the American people and upholding the Constitution.

Senator RUBIO. This is for all the Members of the Committee. As has been widely reported—and people know this—Kaspersky Lab software is used by, not hundreds of thousands, millions of Americans. To each of our witnesses, I would just ask: would any of you be comfortable with Kaspersky Lab's software on your computers?

Director COATS. A resounding no for me.

Director ROGERS. No.

Director POMPEO. No, Senator.

Director MCCABE. No, sir.

Director STEWART. No, Senator.

Director CARDILLO. No, sir.

Senator RUBIO. Director Pompeo, on Venezuela, which was mentioned in Director Coats' statement, as all of you are probably well aware, armed civilian groups or colectivos, these militias in the street, have been armed by the regime for purposes of defending, for lack of a better term, the regime from protesters. We all are aware of the Maduro regime's cozy relationship with Hezbollah, with the FARC, which is a designated terrorist organization, and links to narcotrafficking.

Among the weapons in the stockpile of the military in Venezuela are Igla-S, these basically Russian variants of our Stinger missiles. Director Pompeo, if you could comment on the risk that I believe exists that as these groups become more desperate, potentially even operate at some point outside the control of the Maduro regime, running around in the streets, also in search of money and food and anything else that they want to get their hands on, the threat of any advanced weaponry such as what I just mentioned being sold or transferred to the FARC, a terrorist organization, sold to drug cartels in Mexico potentially, or even sold to terrorist organizations on the black market? Is that a real threat? Is that something we should be cognizant of?

Director POMPEO. Senator, it is a real threat. As we have all seen, the situation in Venezuela continues to deteriorate. Maduro gets more desperate by the hour. The risk of these colectivos acting in a way that is not under his control increases as time goes on as well.

In a classified setting, I'm happy to share with you a little bit more about the details of what we know. We have not seen any of those major arms transfers take place. We don't have any evidence that those have taken place to date. But those stockpiles exist, not only in the Maduro regime, but other places as well. There are plenty of weapons running around in Venezuela and this risk is incredibly real and serious and ultimately a threat to South America and Central America, in addition to just in Venezuela.

Senator RUBIO. Staying in the Western Hemisphere for a moment—and this potentially is also to the Director, Director McCabe,

and to you, Director Pompeo. I continue to be concerned about the potential and I believe is the reality of a concerted effort on the part of the Cuban government to recruit and unwittingly enlist Americans, business executives and others, even local and state political leaders, in an effort to have them influence U.S. policymaking on Cuba, and particularly the lifting of the embargo.

Would this be a tactic consistent with what we have seen in the past from other nation-states, including the regime in Cuba?

Director POMPEO. I'll let Mr. McCabe comment as well, but yes, of course. Frankly, this is consistent with—the attempt to interfere in the United States is not limited to Russia. The Cubans have deep ties. It is in their deepest tradition to take American visitors and do their best to influence them in a way that's adverse to U.S. interests.

Director MCCABE. Yes, sir, fully agree. We share your concerns about that issue.

Senator RUBIO. My final question is, with all this focus on Russia and what's happened in the past, is it the opinion of all of you or those of you—certainly all have insight on this—that even as we focus on 2016 and the efforts leading up to that election, efforts to influence policymaking here in the United States vis-à-vis the Russian interests are ongoing, that the Russians continue to use active measures even at this moment, even on this day, to try, through the use of multiple different ways, to influence the political debate and decisions made in American politics, particularly as they pertain to Russia's interests around the world? In essence, these active measures are an ongoing threat, not simply something that happened in the past.

Director MCCABE. Yes, sir, that's right.

Director POMPEO. Senator, it's right. In some sense, though, we ought to put it in context. This has been going on for a long time. There's nothing new. Only the cost has been lessened, the cost of doing it.

Director COATS. I would just add that the use of cyber and social media significantly increased the impact and the capabilities. Obviously, this has been done for years and years, even decades. But the ability to have—to use the interconnectedness and all that provides, that it didn't provide before—they've literally upped their game to the point where it's having a significant impact.

Director ROGERS. From my perspective, I would just highlight, cyber is enabling them to access information in massive quantities that weren't quite attainable to the same level previously. That's just another tool in their attempt to acquire information, misuse of that information, manipulation, outright lies, inaccuracies at times, but in other times actually dumping raw data, which we also saw during this last presidential election cycle for us.

Chairman BURR. Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

There's obviously more than one threat to our country. I would argue that the greatest danger to the United States is North Korea. I'm one of those who has been very worried and trying to follow this as close as possible.

In the statement for the record, you state, and I quote: "North Korea's nuclear weapons and missile programs will continue to

pose a serious threat to U.S. interests in to the security environment in East Asia in 2017." You go on to state: "Pyongyang is committed to developing a long-range nuclear-armed missile that is capable of posing a direct threat to the United States."

These assessments, combined with North Korea's behavior, recent ballistic missile launches, and proximity to U.S. forces and allies in Asia, are deeply concerning. For the purpose of this open hearing, could each of you express the threat posed by North Korea in this public setting and then address, most importantly, some of the specific actions we're taking as a Nation? Some of it you may want to do in the closed hearing later.

Director COATS. I think we could get into greater detail in the closed hearing. But it's clear that we have assessed this as a very significant, potentially existential, threat to the United States that has to be addressed. You're aware there has been considerable discussion among the policymakers, with our providing intelligence with the Administration, relative to steps moving forward. General Mattis has taken a major role in this, as well as our Secretary of State and others.

The interaction with the Chinese of late we think can play a significant role in terms of how we deal with this. We have dedicated a very significant amount of our intelligence resources to the issue of North Korea. I think we'd look forward to going deeper into all of that in the classified session.

Senator FEINSTEIN. Well, let me ask this. Is it possible in this hearing to estimate when they will have an intercontinental ballistic missile capable of taking a nuclear warhead?

Director COATS. I think it would be best if we save that, those kind of details, for the closed session.

Senator FEINSTEIN. Can you say in this session how effective China has been in stopping some of the testing?

Director POMPEO. Senator Feinstein, let me try and answer that as best I can. I actually just returned from Korea. I was there last week. I had a chance to be with our great soldier, General Brooks, and his team, as well as the great soldiers of the Republic of Korea Army who are on the front lines there. They're doing amazing work in a difficult condition.

With respect to the Chinese, they have made efforts in a way that they have not made before in an effort to close down the trade that they have and putting pressure, diplomatic pressure as well, on the North Koreans. The intelligence would suggest that we're going to need more to shake free this terribly challenging problem, and that they could do more and they have the capacity to do more as well.

Senator FEINSTEIN. Could you be specific? Have they entirely stopped coal? To what degree have they reduced it? How about oil and other commodities?

Director POMPEO. I'd prefer to defer the details of that to the classified setting, but there have been restrictions on coal that have been significant.

Senator FEINSTEIN. Is there any other comment?

Director STEWART. If I could, Senator. North Korea has declared its intent. It said it publicly. It produces propaganda images that show their intent to develop intercontinental missiles, nuclear-

armed. What we have not seen them do is do a complete end to end test of an ICBM with a nuclear device.

In the closed session we can talk about how close they might be to doing that. But they're certainly on parallel paths: a nuclear device, processing enough fissile material for nuclear warheads, and developing a wide range of missile technology—short, intermediate, long-range missile technology. So they're going to put those two together at some point, but we have not seen them do that, test it end to end, missile launch, intercontinental range, miniaturization, and survival of a reentry vehicle. But they're on that path and they're committed to doing that.

Senator FEINSTEIN. Thank you.

Director CARDILLO. I'd just add, Senator, on top of General Stewart's comments that they are in a race. He's pushing very hard on the accelerator here. This whole panel is well aware of that and we are doing everything in our power—and we can give you the details in closed—to make sure that we give you and our customers the advantage to win that race.

Senator FEINSTEIN. If I might just say, Mr. Cardillo, you've given us very good information, very solid information. It is much appreciated. I think it is time for the American people to begin to understand that, as the Director said, we do in fact have an existential threat in the Pacific Ocean and we need to come to grips with it.

Chairman BURR. Senator Blunt.

Senator BLUNT. Thank you, Mr. Chairman.

Director Coats, let me join everybody else in welcoming you back to the Committee, this time on the other side of the hearing table, but pleased along with others as you take this responsibility.

It's my understanding—I want to talk just a little bit about two executive orders on vetting that the President has been challenged on in court. My understanding is you're, as the DNI, involved in that vetting, in that process; is that right? The screening process, is that something that reports up through you?

Director COATS. You're talking about the classification process?

Senator BLUNT. Well, I'm talking about the extreme vetting, where the President's issued—the first executive order was January the 27th, where the President's order said that we'd suspend refugee admissions from certain countries for 90 days pending a review. There's also 120 days mentioned in that order.

Since we're beyond 90 days and approaching 120 days, my real question is, are we, in spite of what's happening outside of the organization, are we continuing to pursue that time line and are we about to get to the 120 days of having that review period behind us?

Director COATS. I would like to take that question and get back to you with the specifics relative to the days away, what has been done to this particular date, and are we on target. Obviously, this is going forward. I don't have the details in front of me right now, but I'd be happy to get that information for you.

Senator BLUNT. Good. I'd be interested in that. And I'd be very concerned, frankly, if we're now over 100, close to 120, days into that time frame, to find out that the 120 days didn't get the job done because we were waiting to figure out how the order could be properly enforced. So I'd be very interested in that.

On the cyber front, Director Cardillo, I know, among other things, your organization has conducted what you've called hackathons, or at least have been called hackathons. What has that done in terms of bringing other people into the discussion of how we protect ourselves better from these cyber attacks?

Director CARDILLO. Thank you, Senator. We're quite proud at NGA of our history of support to the community and to you, but through predominantly historically closed systems, government-owned systems, etcetera. As the committee has already discussed and the panel has responded, clearly the high-tech reality of our world, the interconnectedness of the internet, etcetera. What we're trying to do is take that historic success of our expertise and our experience and then engage with that community in a way that we can better leverage our data in a way to inform and warn you.

I'm trying to tap into the agility and the innovation of that community. We use these hackathons to put out challenge questions in which we can engage with industry and academia in a way that will enable us to do our job better.

Senator BLUNT. Let me ask one more question of you. We had a witness before this committee on March 30th in an open hearing, Clint Watts, who observed that—he said, quote: "The intelligence community is very biased against open source information." That ends his quote.

I may come to you on that, too, Director Pompeo. But in terms of Geospatial, what are you doing there with open source information?

Director CARDILLO. We're engaging. As Admiral Rogers mentioned, though, there's an up side to this connectedness and the fact that the commercial market and the commercial imagery market is getting into a business that was prior a government-only entity has great advantage. We seek to build on that and take advantage of those developments.

We also need to go in eyes wide open and realize that there is a risk. So I don't have a bias. I have an awareness and appreciation for this open development and innovation. My commitment is to smartly engage with it, to make sure that we use the best of it, while we're aware that there is a risk as we do so.

Senator BLUNT. Director Pompeo, do you think that was a fair criticism, that the intelligence community is biased against using open source information?

Director POMPEO. Senator Blunt, I think historically that may well have been true. I don't think that's the case today. We have an enormous open source enterprise that does its best to stay up with and be world class in information management and get information that is not stolen secrets, but open source information, to the right place at the right time to help inform the intelligence that we provide to you and to our other customers.

So today I would say that statement is inaccurate.

Senator BLUNT. Thank you, Director.

Thank you, Chairman.

Chairman BURR. Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman.

Let me ask—let me highlight one issue and ask a question, Director Coats, about another issue. And I'd invite comment from

anyone who has something they want to offer. I've been increasingly concerned about foreign governments hiring lobbyists here in Washington and, unbeknownst to members of Congress, actually lobbying Congress to enact policies which may be contrary to the best interests of the American people.

Of course, the Foreign Agent Registration Act provides some level of transparency for that. But I just highlight that issue and we can come back to it at a later time because I want to ask you about another topic as well.

The Committee on Foreign Investment in the United States, or CFIUS, provides a very important role in determining whether there are technology transfers from the United States to foreign governments. I'm happy to see, Director Coats, your comments on page 4 of your written statement specifically regarding China's increasing effort to use investment as a way to improve its technological capabilities.

China we've seen continues to use an aggressive campaign to vacuum up advanced U.S. technology however and whenever it can, whether stealing it through cyber or buying it on the open market. Do you feel like the current CFIUS process adequately protects against this threat vector, and are all elements of the U.S. Government cognizant of these vulnerabilities?

Director COATS. I can't speak to how many agencies of the U.S. Government are as cognizant as perhaps they should be, but I certainly think that, given China's aggressive approach relative to information-gathering and all the things that you mentioned, it merits a review of CFIUS in terms of whether or not it needs to have some changes or innovations to address the aggressive, aggressive Chinese actions, not just against our companies but across the world.

They clearly have a strategy through their investments. They started a major investment bank. You name a part of the world, the Chinese probably are there, looking to put investments in. We've seen the situation in Djibouti where they're also adding military capability to their investment in a strategic area on the Horn of Africa there, that you wouldn't necessarily expect this. But they're active in Africa, northern Africa. They're active across the world.

Their "One Belt, One Road" process opens their trade and what other interests they have to the Indian Ocean in a different way to address nations that they've had difficulty connecting with.

So it's clearly an issue that we ought to take a look at.

Senator CORNYN. Thank you.

Director POMPEO. Senator Cornyn, if I might just add one comment, two quick comments, one on CFIUS. It mostly deals with change of control transactions, purchases. There are many other ways one could invest in an entity here in the United States and exert significant control over that entity. I think that ought to be looked at.

Then second and apart from CFIUS, there are many vectors. You mentioned several. Other places are educational institutions, where there are many folks coming here, some who are coming here in good faith to learn, but others who are being sent here with less noble undertakings and missions.

Director ROGERS. The only additional comment I was going to make is, it is clear as we watch China and other nations they are gaining greater insights as to our CFIUS processes, the criteria that we use that tend to shape our decision process. So I think that's also an issue of concern that we're aware of here.

Senator CORNYN. Thank you. I look forward to visiting with you in the closed session later on.

Thank you, Mr. Chairman.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman.

Gentlemen, it's fair to say I disagreed with Director Comey as much as anyone in this room. But the timing of this firing is wrong to anyone with a semblance of ethics. Director Comey should be here this morning testifying to the American people about where the investigation he has been running stands.

At our public hearing in January when he refused to discuss his investigation into connections between Russia and Trump associates, I stated my fear that if the information didn't come out before Inauguration Day it might never come out. With all the recent talk in recent weeks about whether there is evidence of collusion, I fear some colleagues have forgotten that Donald Trump urged the Russians to hack his opponents.

He also said repeatedly that he loved WikiLeaks. So the question is not whether Donald Trump actively encouraged the Russians and WikiLeaks to attack our democracy. He did. That is an established fact. The only question is whether he or someone associated with him coordinated with the Russians.

Now, Mr. McCabe, the President's letter to Director Comey asserted that on three separate occasions the Director informed him that he was not under investigation. Would it have been wrong for the Director to inform him he was not under investigation? Yes or no?

Director MCCABE. Sir, I'm not going to comment on any conversations that the Director may have had——

Senator WYDEN. I didn't ask that. Would it have been wrong for the Director to inform him he was not under investigation? That's not about conversations. That's a yes or no answer.

Director MCCABE. As you know, Senator, we typically do not answer that question. I will not comment on whether or not the Director and the President of the United States had that conversation.

Senator WYDEN. Will you refrain from these kinds of alleged updates to the President or anyone else in the White House on the status of the investigation?

Director MCCABE. I will.

Senator WYDEN. Thank you.

Director Pompeo, one of the few key unanswered questions is why the President didn't fire Michael Flynn after Acting Attorney General Yates warned the White House that he could be blackmailed by the Russians. Director Pompeo, did you know about the Acting Attorney General's warnings to the White House or were you aware of the concerns behind the warning?

Director POMPEO. I don't have any comment on that.

Senator WYDEN. Well, were you aware of the concerns behind the warning? I mean, this is a global threat. This is a global threat question. This is a global threat hearing. Were you aware?

Director POMPEO. Senator, tell me what global threat it is you're concerned with, please? I'm not sure I understand the question.

Senator WYDEN. Well, the possibility of blackmail. I mean, blackmail by an influential military official, that has real ramifications for the global threat. So this is not about a policy implication. This is about the National Security Adviser being vulnerable to blackmail by the Russians. The American people deserve to know whether in these extraordinary circumstances the CIA kept them safe.

Director POMPEO. Yes, sir, the CIA has kept America safe, and the people at the Central Intelligence Agency are committed to that and will remain committed to that. And we will do that in the face of——

Senator WYDEN. You won't answer the question.

Director POMPEO. We will do that in the face of political challenges that come from any direction, Senator.

Senator WYDEN. But you will not answer the question of whether or not you were aware of the concerns behind the Yates warning?

Director POMPEO. Sir, I don't know exactly what you're referring to with "the Yates warning." I wasn't part of any of those conversations.

Senator WYDEN. The Yates warning was——

Director POMPEO. Senator, I have no——

Senator WYDEN [continuing]. That the White House could be blackmailed.

Director POMPEO. I have no firsthand information with respect to the warning that was given. She didn't make that warning to me. I can't answer that question, Senator, as much as I would like to.

Senator WYDEN. Okay.

Director Coats, how concerned are you that a Russian government oil company run by a Putin crony could end up owning a significant percentage of U.S. oil refining capacity, and what are you advising the Committee on Foreign Investment in the United States about this?

Director COATS. I don't have specific information relative to that. I think that's something that potentially we could provide intelligence on in terms of what the situation might be.

Senator WYDEN. I'd like you to furnish that in writing.

Let me see if I can get one other question in. There have been mountains of press stories with allegations about financial connections between Russia and Trump and his associates. The matters are directly relevant to the FBI. My question is, when it comes to illicit Russian money and in particular its potential to be laundered on its way to the United States, what should the Committee be most concerned about?

We hear stories about Deutschebank, Bank of Cyprus, shell companies in Moldova, the British Virgin Islands. I'd like to get your sense, because I'm over my time, Director McCabe. What should we be most concerned about with respect to illicit Russian money and its potential to be laundered on its way to the United States?

Director MCCABE. Certainly, sir. As you know, I am not in a position to be able to speak about specific investigations and certainly

not in this setting. However, I will confirm for you that those are issues that concern us greatly. They have traditionally and they do even more so today. As it becomes easier to conceal the origin and the track and the destination and purpose of illicit money flows, as the exchange of information becomes more clouded in encryption and more obtuse, it becomes harder and harder to get to the bottom of those investigations that would shed light on those issues.

Senator WYDEN. Thank you, Mr. Chairman.

Vice Chairman WARNER [presiding]. Senator Risch.

Senator RISCH. Thank you very much.

Gentlemen, the purpose of this hearing, as the Chairman expressed, is to give the American people some insight into what we all do which they don't see pretty much at all. So I think what I want to do is I want to make an observation and then I want to get your take on it, anybody who wants to volunteer, and I'm going to start with you, Director Coats, as a volunteer.

I've been on this Committee all the time I've been here in the Senate and all through the last Administration, and I have been greatly impressed by the current Administration's hitting the ground running during the first 100 days as far as their engagement on intelligence matters and their engagement with foreign countries.

The national media here is focused on domestic issues, which is of great interest to the American people, be it health care, be it personnel issues in the government, and they don't—the media isn't as focused on this Administration's fast, and in my judgment, robust engagement with the intelligence communities around the world and with other governments.

My impression is that it's good and it is aggressive. I'd like your impression of where we're going. Almost all of you had real engagement in the last Administration. All administrations are different. Director Coats, do you want to take that on to start with?

Director COATS. I'd be happy to start with that. I think most Presidents that come into office come with an agenda in mind in terms of what issues they'd like to pursue, many of them issues that affect—domestic issues that affect infrastructure, education, a number of things, only to find that this is a dangerous world, that the United States—the threats that exist out there need to be given attention to.

This President, who I think the perception was not interested in that—I think Director Pompeo and I can certify the fact that we have spent far more hours in the Oval Office than we anticipated. The President is a voracious consumer of information and asking questions and asking us to provide intelligence. We are both part of a process run through the National Security Council, General McMaster, all through the deputies committees and the principals committees, consuming hours and hours and hours of time, looking at the threats, how do we address those threats, what is the intelligence that tells us, that informs the policymakers in terms of how they put a strategy in place.

So what I initially thought would be a one or two time a week, 10 to 15-minute quick brief has turned into an every day, sometimes exceeding 45 minutes to an hour or more just in briefing the President. I have brought along several of our directors to come

and show the President what their agencies do and how important it is, the information they provide, for the basis of making policy decisions.

I'd like to turn to my CIA colleague here to let him give you, and others, to give you their impression.

Senator RISCH. I appreciate that. We're almost out of time. But I did—Director Pompeo, you kind of sat in the same spot we all sit in through the last several years. I'd kind of like your observations along the line of Director Coats.

Director POMPEO. I think Director Coats had it right. He and I spend time with the President every day briefing him on the most urgent intelligence matters that are presented to us in our roles. He asks good hard questions, makes us go make sure we're doing our work in the right way.

Second, you asked about engagement in the world. This Administration has reentered the battle space in places that the previous administration was completely absent. You all travel some, too.

Senator RISCH. Yes.

Director POMPEO. You will hear that when you go travel. I have now taken two trips to places and they welcome American leadership. They're not looking for American soldiers. They're not looking for American boots on the ground. They're looking for American leadership around the globe. And this President has reentered that space in a way that I think will serve America's interests very well.

Senator RISCH. I couldn't agree more. We deal with them not only overseas, but they come here, as you know, regularly.

Director POMPEO. Yes, sir.

Senator RISCH. And the fact that the President has pulled the trigger twice as he has in the first 100 days, and done it in a fashion that didn't start a world war, and was watched by both our friends and our enemies, has made a significant and a huge difference as far as our standing in the world.

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

Vice Chairman WARNER. Thank you, Senator.

Senator Heinrich.

Senator HEINRICH. Director McCabe, you obviously have several decades of law enforcement experience. Is it your experience that people who are innocent of wrongdoing typically need to be reassured that they're not the subject of an investigation?

Director MCCABE. No, sir.

Senator HEINRICH. I ask that because I'm still trying to make heads or tails of the dismissal letter from earlier this week from the President, where he writes: "While I greatly appreciate you informing me on three separate occasions that I am not under investigation." I'm still trying to figure out why that would even make it into a dismissal letter.

But let me go to something a little more direct. Director, has anyone in the White House spoken to you directly about the Russia investigation?

Director MCCABE. No, sir.

Senator HEINRICH. When did you last meet with the President, Director McCabe?

Director MCCABE. I don't think I'm going to comment on that.

Senator HEINRICH. Was it earlier this week?

Director MCCABE. I have met with the President this week, but I don't really want to go into the details of that.

Senator HEINRICH. But Russia did not come up?

Director MCCABE. That's correct, it did not.

Senator HEINRICH. Thank you.

We've heard in the news claims that Director Comey had lost the confidence of rank and file FBI employees. You've been there for 21 years. In your opinion, is it accurate that the rank and file no longer supported Director Comey?

Director MCCABE. No, sir, that is not accurate. I can tell you, sir, that I worked very, very closely with Director Comey from the moment he started at the FBI. I was his Executive Assistant Director of National Security at that time; then worked for him running the Washington Field Office; and of course I've served as Deputy for the last year.

I can tell you that I hold Director Comey in the absolute highest regard. I have the highest respect for his considerable abilities and his integrity, and it has been the greatest privilege and honor of my professional life to work with him.

I can tell you also that Director Comey enjoyed broad support within the FBI and still does to this day. We are a large organization. We are 36,500 people across this country, across this globe. We have a diversity of opinions about many things. But I can confidently tell you that the majority, the vast majority, of FBI employees enjoyed a deep and positive connection to Director Comey.

Senator HEINRICH. Thank you for your candor.

Do you feel like you have the adequate resources for the existing investigations that the Bureau is invested in right now to follow them wherever they may lead?

Director MCCABE. Sir, if you're referring to the Russia investigation, I do. I believe we have the adequate resources to do it and I know that we have resourced that investigation adequately.

If you're referring to the many constantly multiplying counterintelligence threats that we face across the spectrum, they get bigger and more challenging every day and resources become an issue over time. But in terms of that investigation, sir, I can assure you we are covered.

Senator HEINRICH. Thank you.

Director Coats, welcome back. Would you agree that it is a national security risk to provide classified information to an individual who has been compromised by a foreign government, as a broad matter?

Director COATS. As a broad matter, yes.

Senator HEINRICH. If the Attorney General came to you and said one of your employees was compromised, what sort of action would you take?

Director COATS. I would take the action as prescribed in our procedures relative to how we report this and how it is processed. It's a serious issue. I would be consulting with our legal counsel and consulting with our inspector general and others as to how best to proceed with this. But obviously we would take action.

Senator HEINRICH. Would one of the options be dismissal, obviously?

Director COATS. That very potentially could be a dismissal, yes.

Senator HEINRICH. Thank you, Director.

Vice Chairman WARNER. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman or Mr. Vice Chairman.

Mr. McCabe, is the agent who is in charge of this very important investigation into Russian attempts to influence our elections last fall still in charge?

Director MCCABE. We have many agents involved in the investigation at many levels. So I'm not sure who you're referring to here.

Senator COLLINS. The lead agent overseeing the investigation.

Director MCCABE. Certainly almost all of the agents involved in the investigation are still in their positions.

Senator COLLINS. So has there been any curtailment of the FBI's activities in this important investigation since Director Comey was fired?

Director MCCABE. Ma'am, we don't curtail our activities. As you know, are people experiencing questions and are reacting to the developments this week? Absolutely. Does that get in the way of our ability to pursue this or any other investigation? No, ma'am. We continue to focus on our mission and get that job done.

Senator COLLINS. I want to follow up on a question of resources that Senator Heinrich asked your opinion on. Press reports yesterday indicated that Director Comey requested additional resources from the Justice Department for the Bureau's ongoing investigation into Russian active measures. Are you aware of that request? Can you confirm that that request was in fact made?

Director MCCABE. I cannot confirm that request was made. As you know, ma'am, when we need resources we make those requests here. So I'm not aware of that request and it's not consistent with my understanding of how we request additional resources.

That said, we don't typically request resources for an individual case. As I mentioned, I strongly believe that the Russia investigation is adequately resourced.

Senator COLLINS. You've also been asked a question about target letters. Now, it's my understanding that when an individual is the target of an investigation, at some point a letter is sent out notifying the individual that he is a target. Is that correct?

Director MCCABE. No, ma'am, I don't believe that's correct.

Senator COLLINS. So before there is going to be an indictment there is not a target letter sent out by the Justice Department?

Director MCCABE. Not that I'm aware of.

Senator COLLINS. That's contrary to my understanding. But let me ask you the reverse——

Director MCCABE. Again, I'm looking at it from the perspective of the investigators. So that's not part of our normal case investigative practice.

Senator COLLINS. That would be the Justice Department, though, the Justice Department.

Director MCCABE. Yes, ma'am. I see.

Senator COLLINS. I'm asking you, isn't it standard practice when someone is the target of an investigation and is perhaps on the verge of being indicted that the Justice Department sends that individual what is known as a target letter?

Director MCCABE. Ma'am, I'm going to have to defer that question to the Department of Justice.

Senator COLLINS. Well, let me ask you the flip side of that, and perhaps you don't know the answer to this question. But is it standard practice for the FBI to inform someone that they are not a target of an investigation?

Director MCCABE. It is not.

Senator COLLINS. So it would be unusual and not standard practice for there to have been a notification from the FBI Director to President Trump or anyone else involved in this investigation, informing him or her that that individual is not a target, is that correct?

Director MCCABE. Again ma'am, I'm not going to comment on what Director Comey may or may not have done.

Senator COLLINS. I'm not asking you to comment on the facts of the case. I'm just trying to figure out what's standard practice and what's not.

Director MCCABE. Yes ma'am. I'm not aware of that being a standard practice.

Senator COLLINS. Admiral Rogers, I want to follow up on Senator Warner's question to you about the attempted interference in the French election. Some researchers, including the cyber intelligence firm Flashpoint, claim that APT28 is the group that was behind the stealing of and the leaking of the information about the President-elect of France. The FBI and DHS have publicly tied APT28 to Russian intelligence services in the joint analysis report last year after the group's involvement in stealing data that was leaked in the run-up to the U.S. elections in November.

Is the IC in a position to attribute the stealing and the leaking that took place prior to the French election to be the result of activities by this group, which is linked to Russian cyber activity?

Admiral ROGERS. Again, ma'am, right now I don't think I have a complete picture of all the activity associated with France. But as I have said publicly both today and previously, we are aware of specific Russian activity directed against the French election cycle in the course particularly of the last few weeks, to the point where we felt it was important enough we actually reached out to our French counterparts to inform them and make sure they had awareness of what we were aware of and also to ask them, is there something we are missing that you are seeing?

Senator COLLINS. Thank you.

Chairman BURR. Senator King.

Senator KING. Mr. McCabe, thank you for being here today under somewhat difficult circumstances. We appreciate your candor in your testimony.

On March 20th, Director Comey—then-Director Comey testified to the House of Representative: "I have been authorized by the Department of Justice to confirm that the FBI, as part of our counterintelligence mission, is investigating the Russian government's efforts to interfere in the 2016 presidential election and that includes investigating the nature of any links between individuals associated with the Trump campaign and the Russian government and whether there was any coordination between the campaign and Russian efforts. As with any counter intelligence investigation, this

will also include an assessment of whether any crimes were committed." Is that statement still accurate?

Director MCCABE. Yes, sir, it is.

Senator KING. And how many agents are assigned to this project? How many—or personnel generally within the FBI, roughly?

Director MCCABE. Sir, I can't really answer those sorts of questions in this forum.

Senator KING. Well, yesterday a White House press spokesman said that this is one of the smallest things on the plate of the FBI. Is that an accurate statement?

Director MCCABE. It is——

Senator KING. Is this a small investigation in relation to all—to all the other work that you're doing?

Director MCCABE. Sir, we consider it to be a highly significant investigation.

Senator KING. So you would not characterize it as one of the smallest things you're engaged in?

Director MCCABE. I would not.

Senator KING. Thank you.

Let me change the subject briefly. We're—we've been talking about Russia and—and their involvement in this election. One of the issues of concern to me, and perhaps I can direct this to—well, I'll direct it to anybody in the panel. The allegation of Russian involvement in our electoral systems, is that an issue that is of concern and what do we know about that? And is that being followed up on by this investigation?

Mr. McCabe, is that part of your investigation? Now, I'm—I'm not talking about the presidential election. I'm talking about State-level election infrastructure.

Director MCCABE. Yes, sir. So obviously not discussing any specific investigation in detail, the issue of Russian interference in the U.S. democratic process is one that causes us great concern. And quite frankly, it's something that we've spent a lot of time working on over the past several months. And to reflect comments that were made in response to an earlier question that Director Coats handled, I think part of that process is to understand the inclinations of our foreign adversaries to interfere in those areas.

So we've seen this once; we are better positioned to see it the next time. We're able to improve not only our coordination with—primarily through the Department of Homeland—through DHS, their—their expansive network, and to the State and local election infrastructure, but to interact with those folks to put them in a better position to defend against whether it's cyber attacks or any sort of influence-driven interactions.

Senator KING. Thank you. I think that's a very important part of this issue.

Admiral Rogers, yesterday a camera crew from Tass was allowed into the Oval Office. There was no any American press allowed. Was there any consultation with you with regard to that action in terms of the risk of some kind of cyber penetration or communications in that incident?

Admiral ROGERS. No.

Senator KING. Were you—you were—your agency wasn't consulted in any way?

Admiral ROGERS. Not that I'm aware of. I wouldn't expect that to automatically be the case. But no, not that I'm aware of.

Senator KING. Did it raise any concerns when you saw those pictures that those cameramen and crew were in the Oval Office without——

Admiral ROGERS. I'll be honest. I wasn't aware of where the images came from.

Senator KING. All right, thank you.

Mr. Coats, Director Coats, you lead the intelligence community. Were you consulted at all with regard to the firing of Director Comey?

Director COATS. I was not.

Senator KING. So you had no—there were no discussions with you even though the FBI's an important part of the intelligence community?

Director COATS. There were no discussions.

Senator KING. Thank you.

Mr. Chairman, thank you.

Chairman BURR. Thank you, Senator King.

Senator Lankford.

Senator LANKFORD. Thank you.

Let me just run through some quick questions on this. Director McCabe, thanks for being here as well. Let me hit some high points of some of the things that I've heard already, just to be able to confirm. You have the resources you need for the Russia investigation, is that correct?

Director MCCABE. Sir, we believe it's adequately resourced.

Senator LANKFORD. Okay, so there's not limitations on resources? You have what you need? The—the actions about Jim Comey and his release has not curtailed the investigation from the FBI? It's still moving forward?

Director MCCABE. The investigation will move forward, absolutely.

Senator LANKFORD. No agents have been removed that are the ongoing career folks that are doing the investigation?

Director MCCABE. No, sir.

Senator LANKFORD. Is it your impression at this point that the FBI is unable to complete the investigation in a fair and expeditious way because of the removal of Jim Comey?

Director MCCABE. It is my opinion and belief that the FBI will continue to pursue this investigation vigorously and completely.

Senator LANKFORD. Do you need somebody to take this away from you and somebody else to do?

Director MCCABE. No sir.

Senator LANKFORD. Okay. Let me ask you a separate question. As I go through the report tracking through the worldwide threats that were put out, that Director Coats put out, there's a section on it on narcotics and the movement of illegal drugs. And there's a section on it about tens of thousands of illegal pharmacies that are online at this point distributing narcotics. And 18 to 20 of those go online a day still.

Can you help me understand a little more about what the FBI is doing to be able to interdict, to be able to engage? How many of those are American? How many of those are international, and what we can do to be able to stop the movement of narcotics through our mail system?

Director MCCABE. Yes, yes, sir. It's a great question and one that we spend a great deal of time on. As you know, the traffic of illegal narcotics is something that we, along with our partners at the DEA and other law and Federal, State, and local law enforcement partners have focused on for many years. We've had great success.

But the issue, the threat continues to change, continues to develop and confront us in new ways. The profusion of illegal online pharmacies is certainly one of those ways. And quite frankly, it's something that we are learning more about, spending more time on every day.

Senator LANKFORD. Well, I'm glad that it is highlighted in the report. With tens of thousands of these pharmacies that are out there in the distribution systems, it's no longer a drug dealer on the corner anymore. They just deliver it to your house now and there's a whole different set of issues that we aggressively need to address on this.

Director Coats, I have a—I have a question for you. We've talked often about a cyber doctrine and it's one of the issues that keeps being raised that other nations and nation-states and actors need to understand what our boundaries are and how we're going to do this. This seems to be talked to death and everyone that I raise it with says yes, it needs to occur.

What I need to know is, who has the ball on leading out to make sure a year from now we're not talking about we need to get a cyber doctrine? I guess specifically, when we do this hearing next year who should we hold accountable if we don't have a cyber doctrine?

Director COATS. Well, that's a very good question. I think all of us would agree we need a cyber doctrine because clearly it is one of the top, if not the number one threat today, that we're dealing with. As you know, the President tasked an effort under the direction of former Mayor Giuliani with this. That has not led to a conclusion at this particular point in time. I don't have the details on that.

I would agree with you, however, that this is a threat that our policymakers need to—need to address. I'm hoping that when we are here next year, we will have a solid response to your question, but at this particular point in time, frankly, given the proliferation of issues that we're trying to deal with, it's almost overwhelming getting our hands on all of them.

Senator LANKFORD. And it is and that's been there are just so many things that are flying around, this keeps getting left, and it has been for years, been left. And what we need to try to figure out is how do we actually find out who's got the ball and who do we hold to account to be able to help us work through this or is this something that we need to be able to work through?

I noticed as I read through your report, which was excellent by the way, on all the worldwide threats, every single section of your report, every section of it, had a section on Iran, every part of it,

that there was a threat. In fact, in one section of it you wrote "Iran continues to be the foremost state sponsor of terrorism."

Whether it was cyber, whether it is active terrorism, whether it is involvement in every different nefarious action, it seems to always circle back to Iran at some point in some way of facilitating this. So this is one of those areas that we've got to be able to figure out how to be able to deal with.

Just in a broad question on it, and maybe, General Stewart, you'd be the right one to be able to deal with this, but anyone could—could answer this. My concern is that when we're dealing with Syria the focus seems to be on Russia in Syria or ISIS in Syria and we're losing track of the movement of Iran through Iraq into Syria. We're losing track of what's happening in Yemen and other places.

What is your perception of Iran's goal through the Middle East? Is their goal higher for Yemen or is it higher going into Syria and into Iraq and to be able to occupy and stay? And is the perception that the Russians want to remain there or Iran wants to remain in Syria and be the dominant force there?

General STEWART. Clearly, Iran views themselves as the regional—the dominant regional power. They will continue to use militia forces and asymmetric forces to achieve the aims of controlling large parts of the region. And if they can't control them physically, they tend to influence them politically. Syria becomes a very key strategic point for them. It allows them to leverage the Syrian forces, Lebanese, Lebanese Hezbollah, and move capability and forces across the region. They will be in competition, at some point, with Russia.

Russia views themselves as the regional power, at least the dominant regional power today. I'm not sure that Russian and Iran's influence will remain aligned in the long term. In the near term they're very closely aligned as it relates to propping up and securing the Syrian regime.

Senator LANKFORD. Thank you.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

Thank all of you for being here. I really appreciate it. And I know that, Mr. McCabe, you seem to be of great interest of being here. And we're going to look forward to really hearing from all of you all in the closed hearing this afternoon, at which I think that we'll able to get into more detail. So I appreciate that.

I have just one question for Mr. McCabe. It's basically the morale of the agency, the FBI agency and the morale basically starting back from July 5th to July 7th, October 28th, November 6th, and Election Day. Did you all ever think you'd be embroiled in an election such as this and did—what did it do to the morale?

Director MCCABE. Well, I—I don't know that anyone envisioned exactly the way these things would develop. You know, as I said earlier, Senator, we are a large organization. We are—we have a lot of diversity of opinions and—and viewpoints on things. We are also a fiercely independent group.

Senator MANCHIN. I'm just saying that basically before July 5th, before the first testimony that basically Director Comey got in-

volved in, prior to that, did you see a change in the morale? Just a yes or no, yes a change, more anxious, more concern?

Director MCCABE. I think morale has always been good. However, we had—there were folks within our agency who were frustrated with the outcome of the Hillary Clinton case and some of those folks were very vocal about those concerns.

Senator MANCHIN. I'm sure we'll have more questions in the closed hearing, sir. But let me say to the rest of you all, we talked about Kaspersky, the lab, KL Lab. Do you all—has it risen to your level, being the head of all of our intelligence agencies and people that are mostly concerned about the security of our country, of having a Russian connection in a lab as far outreaching as KL Labs?

Has it come with your IT people coming to you or have you gone directly to them making sure that you have no interaction with KL or any of the contractors you do business with? Just down the line there. Mr. Cardillo?

Director CARDILLO. Well, we count on the expertise of Admiral Rogers and the FBI to protect our systems and so I value——

Senator MANCHIN. But you have IT—you have IT people, right?

Director CARDILLO. Absolutely.

Senator MANCHIN. Have you talked to the IT people? Has it come to your concern that there might be a problem?

Director CARDILLO. I'm aware of the Kaspersky Lab challenge and/or threat.

Senator MANCHIN. Let me tell you, it's more of a challenge—more than a challenge, sir. And I would hope that—I'll go down the line, but I hope that all of you—we are very much concerned about this, very much concerned about security of our country and their involvement.

Director CARDILLO. We share that.

Senator MANCHIN. General.

General STEWART. We are tracking Kaspersky and their software. There is, as well as I know, and I've checked this recently, no Kaspersky software on our networks.

Senator MANCHIN. Any contractors?

General STEWART. Now, the contractor piece might be a little bit harder to define, but at this point we see no connection to Kaspersky in contractors supporting our IT——

Senator MANCHIN. Admiral Rogers.

Admiral ROGERS. I'm personally aware and involved as the Director of the National Security Agency of Kaspersky Lab issue, yes, sir.

Director COATS. It wasn't that long ago I was sitting up there talking, raising issues about Kaspersky and its position here. And that continues in this new job.

Director POMPEO. It has risen to the Director of the CIA as well, Senator Manchin.

Senator MANCHIN. Great.

Director MCCABE. We're very concerned about it, sir, and we are focused on it closely.

Senator MANCHIN. The only thing I would ask all of you, if you can give us a report back if you've swept all of your contractors to make sure they understand the certainty you have, concern that you have, about this, and making sure that they can verify to you

all that they're not involved whatsoever with any Kaspersky hardware.

I'm going to switch to a couple different things because of national security. But you know, the violent gangs that we have in the United States, and I know—we don't talk about them much. And when you talk about you have MS–13, the Crips, you've got Hells Angels, Aryan Brotherhood, it goes on and on and on, it's quite a few.

What is are we doing and what is it to your level—has it been brought to your level the concern we have with these gangs within our country, really every part of our country? Anybody on the gangland?

Director MCCABE. Yes sir. We spend a lot of time talking about that at the FBI. It's one of our highest priorities.

Senator MANCHIN. Do you have the resources to go after each one of these? Because they're interspersed all over the country.

Director MCCABE. We do, sir. We have been focused on the gang threat for many years. It, much like the online pharmacy threat, it continues to change and develop. We think it's likely having an impact on some of the elevated violent crime rates we see across the country, so we're spending a lot of time focused on that.

Senator MANCHIN. One last question real quick—my time is running out—is on rare earth elements. I'm understanding ever since the closure of the California, which is the Mountain Pass mine, which was the last mine that we had that was giving us a domestic source of rare earth elements, that's been closed and now we're 100 percent dependent of foreign, on basically foreign purchases of rare earth elements for what we need every day to run this country.

We don't do any of it in this country anymore. And most of it comes from China. Do any of you have a concern about that?

Director POMPEO. Senator Manchin, I'll speak to that. Yes, we're concerned. We are—we do a lot of work to figure out where they are and help the intelligence community—help the policy community shape policy surrounding how we ought to treat this issue. But it's a very—it's a very real concern, and it obviously depends on the element. But we use them for important technologies that keep us all safe, those very rare earth elements.

Senator MANCHIN. Let me just say that I—it's been told to me that the Department of Defense needs about 800 tons of rare earth elements per year, and I want to make sure that you know, West Virginia has the opportunity to provide this country with the rare earth elements it has because of our mining process and all of that that we have extracted through the mining process. We are happy to come to aid, sir.

Director POMPEO. Thank you, Senator.

Chairman BURR. Thank you, Senator Manchin.

Before I turn to Senator Cotton, can I say for members, the Vice Chair and I have to step out for a meeting that we can't push off. I would ask Senator Harris, Senator Cotton, to complete their first round of questions. Any member that seeks additional questions will be recognized by the Chair. I would ask you to limit those questions, if you can, but the Chair will ask—will say we're not going over five minutes for the second round of questions.

It is my hope that we will give sufficient time to these six gentlemen to have some nutrition before we reconvene at 1:30 in 219. It's my understanding that there will be a vote circa 2:00, and we will decide exactly how we handle that. But the closed hearing, we like to make sure that nobody misses anything, so we—we might slightly adjust what we are doing.

Senator WYDEN. Mr. Chairman, just an inquiry, and I appreciate your thoughtfulness. So in your departure, as we work through it, it's still acceptable to begin another five-minute round for those——

Chairman BURR. Up to five minutes.

Senator WYDEN. Thank you.

Chairman BURR. Senator Cotton.

Senator COTTON. Inmates are running the asylum.

[Laughter.]

So, I think everyone here in this room and most Americans have come to appreciate the aggressiveness with which Russia uses active measures or covert influence operations, propaganda, call them whatever you will, as your agencies assess they did in 2016, and hacking into those e-mails and releasing them, as news reports suggest they did, in the French election last week.

That's one reason why I sought to revive the Russian Active Measures Working Group in the FY17 Intelligence Authorization Act.

These activities, though, go far beyond elections, I think, as most of our witnesses know. Former Director of the CIA, Bob Gates in his memoir "From the Shadows," detailed Soviet covert influence campaigns designed to slow or thwart the U.S. development of nuclear delivery systems and warheads, missile defense systems, and deployment of Intermediate-range Nuclear Forces systems to Europe.

Specifically, on page 260 of his memoir, he writes: "During the period the Soviets mounted a massive covert action operation aimed at thwarting INF deployments by NATO. We at CIA devoted tremendous resources to an effort at the time to uncovering this Soviet covert campaign. Director Casey summarized this extraordinary effort in a paper he sent to Bush, Schultz, Weinberger, and Clark on January 18, 1983. We later published it and circulated it widely within the government and to the allies, and finally provided an unclassified version for the public to use." End quote.

I'd like to thank the CIA for digging up this unclassified version of the document and providing it to the Committee, "Soviet Strategy to Derail U.S. INF Deployment," specifically undermining NATO's solidarity in those deployments. I ask unanimous consent that it be included as part of the hearing transcript and, since the inmates are running the asylum, hearing no objection, we'll include it in the transcript.

[Laughter.]

[The material referred to follows:]

22355

Directorate of Intelligence

Soviet Strategy To Derail US INF Deployment

An Intelligence Assessment

This assessment was prepared by
Office of Soviet Analysis,
with contributions from
, SOVA, the Office of European Analysis, the Arms Control Intelligence Staff, and the Directorate of Operations. Comments and queries are welcome and may be addressed to
SOVA

Soviet Strategy To Derail US INF Deployment

Key Judgments

Information available as of 24 February 1983 was used in this report.

In attempting to forestall US deployments of intermediate-range nuclear forces (INF) in Europe, scheduled to begin late this year, the Soviets will continue a complex strategy of inducements and threats designed to influence NATO governments, particularly West Germany before its March elections. With time growing short, their near-term objective evidently is to pressure NATO to delay the deployments and to move from its zero option proposal.

Moscow has begun an intensive effort to brief West European governments on the new Soviet proposal for a subceiling on missile launchers in Europe. The subceiling would result in substantial reductions in the number of Soviet medium-range ballistic missile launchers opposite NATO but would be linked to the number of French and British ballistic missile launchers and would preclude the deployment in Europe of US INF missiles. The Soviets have argued that their new proposal demonstrates "flexibility," in sharp contrast to US "intractability" in adhering to its zero option proposal. They also have hinted in vague terms to West European governments of certain "concessions" they might adopt at the INF negotiations in return for greater US flexibility.

At the same time, Moscow has warned NATO of the serious consequences should the US position remain unchanged in Geneva and the United States proceed with its deployments. Such consequences probably include: the lifting of their unilateral SS-20 moratorium, deployment of additional SS-20s in Europe, and the development of new cruise and ballistic missiles for deployment opposite NATO. Thus Moscow is trying to persuade the Europeans that their security would be better served by its proposal for a missile subceiling than by US INF deployments offset by corresponding Soviet counterdeployments.

Along with these diplomatic moves, the Soviets have actively promoted the European "peace movement" through aggressive propaganda and covert activities. They have focused their efforts primarily on those countries scheduled to base the new NATO missiles, with the chief emphasis on West Germany. Their campaign covers a whole spectrum of activities--from overt efforts to create a fear of nuclear war to covert measures, including forgeries and disinformation, to put NATO governments in the worst possible light.

Should US deployments begin without "acceptable" progress in the talks, the Soviets probably would continue to negotiate, but on a different basis—the Soviet side then would offer to trade off its "new" systems in exchange for US INF systems. Nevertheless the Soviets probably hope that the situation will not deteriorate to the point where they would find it necessary to counter NATO's deployments with hundreds of their own missiles. Having acknowledged in Geneva that they expect NATO to proceed with its plans, they must have seriously contemplated a negotiated outcome in which NATO is allowed some level of deployment. Given their particular concern over the Pershing II, the Soviets might continue to call for a ban on it, while grudgingly accepting some level of GLCM deployment—albeit sharply reduced from the planned 464 launchers. In return, they probably would merely reiterate their missile subceiling proposal. In fact, they could insist that any US GLCM deployment (augmenting the French and British missile launchers) be offset by deployments of additional Soviet missile launchers

By late 1983 Moscow should be able to assess whether an INF agreement is possible. If it sees little prospect for one and is convinced that the NATO deployments will begin as scheduled in December 1983, it probably will begin implementing the military countermeasures foreshadowed last March by Brezhnev and more recently by Andropov. In his 21 December address, the new General Secretary pledged to deploy a new long-range cruise missile if Washington proceeds with cruise missile deployment. This response could be in the form of sea-launched cruise missile deployment off US shores as well as ground-launched cruise missile deployment opposite NATO. The Soviets also could choose to develop a new IRBM more capable than the SS-20 for deployment against Western Europe.

Moscow almost certainly would accompany such military moves with a sharply increased effort in covert activities in the five INF-basing countries. It probably would feel less constrained than before in promoting demonstrations and supporting radical peace groups, including some which might engage in sabotage against NATO facilities. Moscow also will use propaganda, disinformation, and support to Communist party and front groups to increase the political pain of the governments in the INF-basing countries. It will hope that this, in turn, will cause those countries to bring pressure on the United States to accede to an agreement that caps NATO deployment at a low level and minimizes reductions in Soviet forces

Nevertheless, the Soviets realize that their overt "peace" campaign in Western Europe has been their most effective tactic. They also recognize that the peace movement there has indigenous roots and has acquired a momentum of its own. They will do what they can to nurture it without appearing too heavyhanded.

Contents

Soviet Strategy To Derail US INF Deployment

A key goal in Moscow's security policy since 1979 has been to derail NATO's plans to deploy the Pershing II medium-range ballistic missile (MRBM) and the ground-launched cruise missile (GLCM). By blocking these deployments, scheduled to begin in late 1983, the USSR would retain its current predominance in intermediate-range nuclear forces (INF) as well as further its long-term objective of weakening NATO and dividing Western Europe from the United States.

I. Moscow's View of NATO Deployment Plans

The Soviets see US deployment of the Pershing II and GLCM not only as an effort to upset the theater nuclear balance, but as an attempt to skew the global nuclear balance in favor of the United States. In their view, the deployment of these systems—with the range and accuracy to strike hardened targets deep in the USSR—would change the linkage between theater and intercontinental war to the advantage of the United States. Without resorting to use of its central systems, the United States would be able to threaten the Soviet homeland, including a portion of the USSR's strategic forces and its command, control, and communications network (see map).

The Soviets see the new US systems as an effective counter to their SS-20 IRBM force and may believe that the scale of NATO's deployments would nullify the advantage in escalation control that they had planned to secure with that force. For example, Moscow would have to consider that NATO, if confronted with a conventional attack by the Warsaw Pact, would be tempted to use its new INF systems before they were destroyed. If the Soviets believed NATO would use these systems, they might feel even more compelled to launch a theater-wide preemptive strike.

The Soviets probably would expect that Pershing IIs and GLCMs would be used concurrently and in conjunction with air- and sea-launched cruise missiles (ALCMs and SLCMs) and strikes by tactical and strategic aircraft in a full-scale nuclear attack. They see the Pershing II as particularly dangerous because its short flight time and accuracy would make it a threat to major elements of their command structure and some of their strategic forces, which would not have adequate warning time to react. In December [redacted] that Moscow perceives the *Pershing II* as the most serious threat to its security, even more than the Minuteman III ICBM, because of the flight time factor.

The Soviets probably regard the GLCM as an effective complement to the Pershing II in that it could be used against strategic and tactical targets that are not time urgent and, when used with sea-launched and air-launched cruise missiles, would severely complicate Soviet air defense strategy. The deployment of both the Pershing II and the GLCM would seriously strain Soviet capabilities to locate and attack NATO's nuclear means in Europe early in a war. From a Soviet targeting standpoint, the GLCM would pose the greater problem because it would be dispersed among five countries, four of them deep in NATO's rear and behind NATO's air defense belt.

II. Soviet Negotiating and Overt Political Strategy Until Now

The Soviets have employed a multifaceted strategy to achieve their INF arms control objectives. They clearly view the West European governments as the key to blocking US INF deployments. While negotiating with the United States in Geneva, they have carried out a propaganda and covert action offensive—primarily focused on the peace movement in Western Europe—similar to the one they waged in 1977-78 to stop NATO from deploying enhanced radiation weapons. In this campaign they have tried both overt and covert means, inducements as well as threats, to exploit anti-INF sentiment in West European governments. Perhaps the most heavyhanded threat intended

for these governments was contained in an interview Brezhnev had with *Der Spiegel* in November 1981. He said that "in order to neutralize [NATO's] mobile missiles it would be necessary [for Moscow] to deal retaliatory strikes of great yield at the supposed areas of their deployment

Later that same month President Reagan announced his zero option proposal, which to the Soviets' dismay was eagerly embraced by Western Europe. The tenacity with which Washington adhered to this proposal during the last negotiating round probably convinced Moscow that a new Soviet initiative was needed to bring further pressure on the United States and NATO. Previous initiatives—for example, the unilateral moratorium on SS-20 deployment in the western USSR and the threat to put the United States and Western Europe in an "analogous" position if NATO deploys new INF systems—have not yielded measurable results in the negotiations or in West European capitals

One of Moscow's recent threats was a warning that NATO's INF deployment would necessitate the adoption of a Soviet launch-on-warning policy. This was implied in a statement issued by the Novosti press agency on 30 November that apparently was aimed at intimidating the West Europeans. This threat, like the others, probably was counterproductive because many West European governments saw it as a rather crude and clumsy attempt to pressure them to forgo INF deployment.

Negotiating Strategy. Although Brezhnev had hinted in an address last October that the SS-20 deployment moratorium might be lifted soon, Defense Minister Ustinov, in a 6 December interview, implied that it was still in effect. Whatever the fate of the moratorium, Moscow has other diplomatic options to explore, particularly with the West Europeans, in the hope that they will exert pressure on the United States to change its bargaining position

In an address on 21 December, General Secretary Andropov officially announced the missile subceiling proposal and emphasized the reductions that would be made, including "tens of the latest missiles, known in the West as SS-20s." The Soviets could reduce their missile launchers to 162 by retiring 250 SS-4s and SS-5s and 81 SS-20s (see table). This cutback in SS-20s would amount to one-third of the force in the European USSR. Although the Soviets have the option, under their proposal, of either dismantling their excess SS-20 launchers or removing them to the eastern USSR, they have hinted [redacted] willingness to destroy at least some of them

The Missile Balance in Europe

	Present		Andropov's Subceiling Offer		US Zero Option Proposal	
	Missiles	Warheads	Missiles	Warheads	Missiles	Warheads
Soviet	493	979	162	486	0	0
SS-20 IRBM	243	729	162	486	0	0
SS-4 MRBM and SS-5 IRBM	250	250	0	0	0	0
NATO	162	162	162	162	162	162
Pershing II MRBM (US)	0	0	0	0	0	0
GLCM (US)	0	0	0	0	0	0
SS-3 IRBM (France)	18	18	18	18	18	18
M-20 SLBM (France)	80	80	80	80	80	80
A-3 SLBM (UK)	64	64	64	64	64	64

[redacted]

Overt Political Strategy. The Soviets have begun a campaign to highlight their new INF initiative and are intensifying their efforts to undermine the NATO deployment plan as the West German national elections approach in March.

[redacted]

[redacted] the Soviets have sent briefing memoranda on their view of the INF negotiations to most of the major West European capitals. They probably believe they will have their best shot at influencing Allied positions if they appear to be flexible in the negotiations

[redacted] that a postponement of NATO's INF deployment would satisfy Moscow for the present. This goal became more evident in early November, when Brezhnev sent a letter to West German Chancellor Kohl requesting that such deployment not proceed automatically because more time was needed to achieve results at the INF negotiations. After the Brezhnev funeral, Andropov made a similar request in a meeting with West German President Carstens.

The Soviets are directing their efforts primarily toward public diplomacy—to avoid risking the adverse public reaction that would result if covert operations were exposed. They are emphasizing the carrot of Moscow's negotiating flexibility rather than the stick of threatening retaliation to NATO deployments. As Gromyko's recent visit to Bonn demonstrates, Moscow is seeking to present an image of caution and reason, presumably to leave the door open for future cooperation with the Christian Democrats if they win the elections, and to avoid discrediting the Social Democratic Party's attempts to broker an agreement on INF between the United States and the USSR.

III. Soviet "Active Measures" Against INF: The Covert Campaign

In the past three years, in support of its direct diplomatic efforts to block deployment of US INF on West European soil, Moscow has conducted an ambitious campaign to infiltrate, manipulate, and exploit the European peace movement. To conduct such a campaign, the Soviets rely on a full range of so-called "active measures"—a term they use to refer to activities worldwide that are intended to promote Soviet foreign policy goals but which go beyond traditional diplomatic, propaganda, and military means. Many of the active measures currently being employed in the anti-INF campaign are adaptations of those that proved effective in the 1977-78 campaign against the "neutron bomb." The scope and intensity of the USSR's public and covert campaigns can be expected to grow as scheduled deployment dates approach. It has already surpassed the scale of the anti-neutron bomb campaign

Use of Communist Parties and Front Organizations. Moscow has instructed West European Communists and the leaders of pro-Soviet international organizations to make the anti-INF campaign their foremost concern and has provided funding and political guidance for their peace movement activity.

The Soviets have directed West European Communist parties specifically to assume a leading role in organizing antinuclear demonstrations and meetings and to coordinate their efforts with non-Communist peace activities. Moscow has been most active with regard to the INF-basing countries, particularly West Germany, the Netherlands, and Belgium. For example:

[redacted] the West German Communist Party (DKP), which takes direction from Moscow and East Berlin, was instrumental in organizing the blockage of the NATO weapons arsenal in Baden-Wuerttemberg on 1-8 August 1982 and some subsequent demonstrations in West Germany.

[redacted] the West Berlin Communist Party (SEW) functions under the close supervision of the East Germans. The party has long contributed an organizational support network for local peace activity that apparently was accepted even by groups that are opposed to the party ideologically.

The Dutch Communist Party (CPN) maintains frequent contact with Moscow and East Berlin and, [redacted] receives regular and detailed guidance from the Soviets and East Germans regarding anti-INF activity.

[redacted] the head of the Belgian National Action Committee for Peace and Development (CNAPD) and three other peace activists visited East Berlin in late September 1981 at the invitation of the Helsinki-based World Peace

Council (WPC), the major Soviet-controlled international organization. The CNAPD head later discussed plans for the 25 October anti-INF demonstration in Brussels with officials of the East German Embassy.

[redacted] reported that PCI officials visiting Moscow in [redacted] 1981 were subjected to heavy pressure to raise strong opposition to INF and subsequently ordered regional party secretaries to step up anti-INF propaganda and initiate demonstrations and marches.

The Soviets also are using their international front organizations to initiate and direct some of the antinuclear activities in Western Europe and to try to attract non-Communist participants to lend credibility to Soviet objectives:

- The WPC is particularly active in planning and trying to coordinate and control antinuclear activity in the West. The WPC's draft "action program" for 1983 provides for several international conferences—some specifically suggested by the Soviets. The highlight will be the "World Peace Assembly" planned for 15-19 June in Prague; this can be expected to feature the anti-INF theme.

The Soviet-backed International Union of Students (IUS) was working in early October 1981 to attract mass participation in IUS-sponsored peace movement activities

As early as 1978, [redacted] the Soviets were even exploring the possibility of using the United Nations Education, Scientific, and Cultural Organization (UNESCO) as an unwitting front organization to promote peace and disarmament themes [redacted] access to broadcast services, the availability of funding for publications, and the other opportunities available to Soviet personnel who could be placed on the staff of the UNESCO Information Service

Financial Support. The USSR and its East European allies contribute considerable financial and material support covertly to the West European peace movement through Communist parties and front organizations:

- The West German Government publicly charged in December that the East Germans secretly provide more than $2 million a month to the West German Communist Party (DKP). [redacted]

- In October 1981 the Danish Government expelled KGB officer Vladimir Merkulov, a second secretary in the Soviet Embassy in Copenhagen for, among other things, using a Danish journalist agent to manipulate and fund the Danish peace movement.

- The World Peace Council was given an estimated $63 million by Moscow in 1980 and also received contributions from other Communist parties, particularly in Eastern Europe

- Italian Communist Party officials believe that an independent member of Parliament who has organized a "Group for World Peace" and publishes a magazine, *Struggle for Peace*, receives instructions and financial aid from the Soviet

The Soviets also fund the peace movement openly:

- In an interview last May in the Austrian press, Soviet Central Committee official Vadim Zagladin provided details about the "Soviet Peace Fund" and its support to Western peace groups, including the WPC and its affiliates in various West European countries.

- A former Soviet Peace Fund chairman asserted in an article in the English-language *Moscow News* in the spring of 1981 that his clients included "leaders of the international democratic organizations working for peace" and cooperated with another ostensibly "public" Soviet organization, the Committee for the Defense of Peace (SCDP) to "render financial aid to organizations, movements, and personalities."

Propaganda Guidelines. The Soviets have sought to direct the focus of the West European peace movement by providing Communist parties and front organizations with propaganda themes keyed to local concerns and to US and NATO policies. [redacted] the Soviet Peace Committee reportedly tried to aggravate existing concerns that the United States would force Western Europe to accept more Pershing II missiles than originally agreed.

Soviet propaganda guidance also has reflected concern about the growing tendency among West European peace activists to blame the USSR as well as the United States for the arms race:

- [redacted] the Soviets told Finnish Communist Party officials last autumn that the CPSU Central Committee has issued a directive to its departments and embassies to collect information on "anti-Soviet phenomena" in West European countries for use in the propaganda battle over INF.

- The Soviets reportedly told leaders of the WPC in [redacted] to try to limit the effectiveness of a peace group that had criticized Soviet policies.

Direct Involvement in Peace Groups. Because of the urgency of their anti-INF campaign, the Soviets have risked discrediting some West European peace groups by directing diplomats and other Soviet officials abroad to undertake covert involvement in those groups' activities. For example:

- On 19 November the Dutch press reported that representatives of the Soviet Embassy and trade mission in the Netherlands had violated diplomatic rules by getting directly involved in the peace movement.

[redacted]

Influence Through Foreign Media and Disinformation. The Soviets routinely try to exploit the Western press to advance the USSR's peace movement objectives:

- The left-leaning West German magazine *Der Spiegel*, for example, is a leader in publishing interviews with the Soviets, particularly on arms control issues.

- The KGB, usually through front organizations, provides funding for West European media sympathetic to Soviet interests. For example, late last year it provided, via a Luxembourg-based East German front organization, the funding to finance the new printing installations of the pro-Soviet Greek Communist Party.

- The press organs of pro-Soviet European Communist parties, although they have limited circulation, provide sympathetic coverage of the USSR's policies and activities regarding antinuclear issues. This prevails even on the lowest level, as in the case of the local Communist party newspaper that reported daily on a Soviet peace delegation touring Denmark last November

Disinformation and forgeries are other "active measures" the Soviets and their allies are using in the campaign against INF basing:

- In May 1982 a forged letter, purportedly from former Secretary of State Haig to NATO Secretary General Luns regarding nuclear arms issues, was

circulated in Belgium and Luxembourg. It distorted NATO nuclear strategy and played on the fear of NATO use of nuclear weapons in a limited war.

- The West German Communist Party may have been involved in fabricating or disseminating a purportedly official notice that was posted in several areas of Bonn in mid-November alerting citizens to measures concerning the transport of nuclear and conventional weapons through the city. The forgery clearly was intended to increase public concern about a recent accident involving a Pershing I transporter and had no basis in fact.

Effectiveness of Soviet Efforts. It is difficult to evaluate the real effect of Soviet active measures in the West European peace movement. Clearly, not all opposition to NATO nuclear forces modernization is Soviet inspired. There is good evidence, however, that the Soviets have sought to exploit and manipulate the movement and that their covert support has enabled it to grow beyond its own capabilities. The most successful tactic employed by the Soviets to date, however, probably is the incessant emphasis in public and private meetings with West Europeans on the USSR's ostensible commitment to detente and arms control in contrast to the United States' alleged drive toward "military supremacy." This type of "political influence operation" is difficult to counter, because many West Europeans meet with Soviet officials and local Communists often, considering this to be a legitimate means of obtaining information.

There has, however, been a perceptible change recently in the attitude of some non-Communist peace groups toward Soviet and other Communist support:

- In the past six to eight months the Dutch Interchurch Peace Council (IKV) has distanced itself from the Soviet position and called more strongly for mutual disarmament by East and West.

- In June 1982 the West German "Greens" broke with the Communist Party over the issues of the need for disarmament by both superpowers, support for the peace movement in East Germany, and criticism of Soviet actions in Poland and Afghanistan.

- The British Campaign for Nuclear Disarmament (CND) reportedly will not support the WPC's "World Peace Assembly" scheduled to be held in Prague this June.

IV. Soviet Negotiating Options in Mid-to-Late 1983

Moscow will continue to assess NATO's deployment plans and the US stance in the current round of negotiations, which will probably last until late March. Although site preparation has been under way for some time, the first deliveries of INF equipment are scheduled to arrive in West Germany, the United Kingdom, and Italy between April and October. If by that time the Soviets conclude there has been insufficient movement in the NATO negotiating position and they are convinced that the INF equipment deliveries will be made, they probably will announce an end to the SS-20 moratorium [redacted]

[redacted]

During the summer round of the INF talks several options would be open to the Soviets. They could:

- Shift their tactics at the INF talks by expressing a willingness to trade off cruise and ballistic missiles currently under development against the GLCM and Pershing II.
- Call for a long suspension of the talks, blaming the United States for the stalemate.
- Walk out of the talks indefinitely, with no date set for resumption.
- Call for merging the INF talks with START.
- Propose to the West Europeans that they join the talks or suggest another venue for the talks, such as the Conference on Security and Cooperation in Europe (CSCE).

Trade-off. Probably the Soviets' most likely option [redacted] and one that they have suggested [redacted] is a proposal to trade off their future cruise and ballistic missiles against NATO's new systems. They currently have a number of such programs in development, some of which could be ready for deployment by late

1983. In his address on 21 December, Andropov stated that the USSR was testing a long-range cruise missile and would deploy it if the United States proceeded with plans for cruise missile deployment.

By matching their new systems against NATO's, the Soviets might seek to change the whole focus of the negotiations, so that the emphasis would be on limiting the new systems of both sides—while protecting their substantially deployed SS-20 force. That tactical shift could keep on the table their missile subceiling proposal, with its enticement of substantial reductions in the SS-20 force. They might argue then to NATO governments that European security would be better served by the missile subceiling proposal than by US INF deployments matched by Soviet counterdeployments.

The threat of such Soviet deployments, however, would not be well received in European capitals and might even increase Allied support for INF deployments. INF proponents would characterize the threat as a Soviet effort to divide Western Europe from the United States and would urge their governments to follow through with deployments. At the same time, however, the West European governments would urge the United States to persevere at the INF talks so that a deal might still be negotiated

Suspension. Of the above options, the second seems least likely, because the Soviets probably would feel that it would not be "tough" enough. With time running out before NATO deployment, they almost certainly would believe that more definitive measures were required to impress NATO with the gravity of the situation.

Walkout. If they chose to walk out, the Soviets might argue in justification that until the United States is interested in "bargaining seriously," there is no need to continue INF talks. In November they indicated[redacted] that the next round of negotiations (currently in session) would be a watershed. They also seemed to be laying the groundwork for an eventual public accounting of their "flexibility" throughout the negotiations, in contrast to US "intractability." At various times last fall Soviet INF delegates and party officials hinted at a walkout if the US position remained unchanged and Washington began INF deployments; but at the same time,[redacted] they indicated that they would continue negotiations even after the United States began such deployments.

Leaving the talks clearly would be risky to the Soviets: Western public opinion might blame them for the collapse of the negotiations. If they feared this possibility, they could stress their willingness to continue to negotiate at START but make it clear that no progress would be possible in that forum until INF questions were resolved.

Merger. The idea of negotiating INF in the START framework might be an option open to the Soviets, as Colonel General Chervov of the General Staff recently indicated in an interview with a West German newspaper. At present, Chervov opposes the idea because of the need to reach an INF settlement quickly and the likelihood that combining INF talks with START would delay an INF solution for many years. Nevertheless, the Soviets might consider this approach if they believed that it had West European support and could delay NATO's deployment plans.

Moscow would be in a good position if the talks were merged, because it has already linked the two in its negotiating approach. Its reduction proposal in START is contingent on no US deployment of new INF systems. The call to ban long-range cruise missiles and air-to-surface ballistic missiles is found in both its INF and its START proposals. Its objection to US proposals in both the INF talks and START is that Washington is not looking at the whole panoply of weapon systems comprehensively, but is interested in selectively limiting only Moscow's strengths, such as ICBMs and the SS-20

The Soviets might well see an advantage if all systems with a "strategic" mission—including US "forward-based" systems and British and French nuclear forces—were on the negotiating table. In their view this could open up opportunities for horse trading, such as occurred during SALT II, and could make more credible the Soviet argument that there is

overall strategic parity between East and West. If by late 1983 Moscow saw NATO deployment as a certainty and was still interested in a negotiated outcome, it might believe that this advantage would outweigh any disadvantage there might be in losing a separate forum for INF. (The separate forum has been useful in exerting leverage on the West Europeans, particularly the Germans.)

[redacted]

Broader Context. Another option open to the Soviets would be to invite the West Europeans to join the INF talks or propose that the talks take place within a broader European framework, such as the CSCE. They could argue that the negotiations are of paramount importance to Europe and that all major powers should be involved. There is no evidence to suggest such a move, but it would be consistent with the long-term Soviet strategy of capitalizing on differences of view among NATO countries. The Soviets would clearly recognize, however, the low likelihood of acceptance by the West Europeans, particularly the French and British, for the reason cited above.

V. Future Soviet Political Moves

The Soviets will continue vigorous efforts to influence the West German position, regardless of whether the elections result in a CDU victory or return the SPD to power. They may be more willing after the elections to offer specific inducements, such as eased emigration for ethnic Germans in the East, since they will no longer be constrained by reluctance to help the CDU in its campaign. At the same time, they may resort more openly to intimidation, particularly if the CDU is victorious. They might stress that West Germany would be more exposed than other West European countries to Soviet retaliation in the event of a nuclear exchange, because only West Germany would base Pershing IIs

Throughout Western Europe the Soviets will intensify their public campaign against US INF deployment. These efforts are likely to include:

- Stepping up contact with a broad spectrum of European politicians, media representatives, church leaders, and student groups, with the intention of purveying as widely as possible an image of Soviet reasonableness and a commitment to a negotiated INF solution.
- Employing propaganda to arouse public alarm over alleged US intentions of making Europe the "nuclear battlefield" of a US-Soviet conflict.
- Introducing new "peace" initiatives, such as their latest proposal for a tactical nuclear-free zone in Central Europe

VI. What Type of Agreement Might Moscow Accept?

Throughout the negotiations the Soviets have insisted that the United States forgo deployment of its new systems in an INF agreement. Privately, however, they have indicated that they expect Washington to proceed with deployment. While they have not provided any clues as to what level of NATO deployment they might ultimately accept,

[redacted]

Clearly the Soviets would like NATO's plan to fall through on its own, but they cannot be confident that this will happen. They probably would not welcome a situation in which NATO fully deployed its systems and they found it necessary to respond with hundreds of their own missiles. Between these extreme outcomes, they must have given considerable thought to an agreement in which NATO is permitted some level of deployment. Given their particular concern over the Pershing II, they might continue to call for a ban on it, while grudgingly accepting some level of GLCM deployment—albeit sharply reduced from the planned 464 launchers. In return, the Soviets probably would merely reiterate their missile subceiling proposal. In

fact, they could insist that any US GLCM deployment (augmenting the French and British missile launchers) be offset by deployments of additional Soviet missile launchers.

Moscow would view a negotiating outcome that killed the Pershing II program as a favorable initial step, but it still would be greatly concerned about limiting the US cruise missile threat. It could propose additional arms control measures that would severely limit air- and sea-launched cruise missiles. It might demand that ALCMs be quantitatively limited on heavy bombers (as they were in SALT II) and might call for a continuation of the ban on SLCM deployment that was negotiated in the now-expired SALT II Protocol. To get Washington more interested in such measures, Moscow might want to heighten the visibility of its own cruise missile systems (as Andropov did in his 21 December address)—particularly as those systems approach operational capability, perhaps as early as late this year. The Soviets probably would be willing to use either the INF talks or START to negotiate these measures.

VII. Possible Soviet Plans if Negotiations and Political Moves Fail

By late 1983 Moscow probably will be able to judge whether an agreement is possible and whether any of the negotiating options and political moves outlined above would be effective in postponing or derailing NATO's deployment plans. If the Soviets are convinced that the initial deployment will occur as scheduled in December, they almost certainly will take steps—for internal as well as foreign policy reasons—to implement whatever military response they have planned to make once NATO's deployment actually begins. This response was foreshadowed in Andropov's 21 December address and in March 1982, when Brezhnev threatened retaliatory measures that would put the United States and its allies "in an analogous position" if NATO deployed its new INF systems.

Military Options

The Soviets could, inter alia, field new cruise missiles and short-range ballistic missiles opposite Europe and deploy a larger SS-20 force.

- Station submarines with sea-launched cruise missiles near US coasts.
- Install nuclear-capable offensive weapon systems in Cuba, either overtly or covertly.

Last fall the Soviets hinted at the INF talks that they might respond with deployment of a long-range cruise missile or a new ballistic missile, or both. In his 21 December speech, Andropov highlighted the Soviet long-range cruise missile program as a counter to NATO's INF deployments, probably because the system is already at the flight test stage. The Soviets recently have modified a Y-class submarine and a number of Bear bombers, apparently to serve as platforms for a long-range cruise missile, which could be targeted against US territory. If they choose to develop a new IRBM for deployment opposite Europe, it probably will be a system more capable than the SS-20 in terms of payload and accuracy. Another Soviet option could be deployment of the SS-20 in the northeastern USSR, where it could target the northwestern United States. A Foreign Ministry official mentioned this possibility last August, and a Soviet discussed it in October

The above options seem more plausible than the emplacement of Soviet missiles in Cuba. Moscow no doubt understands that such an action could bring the superpowers to the brink of a nuclear confrontation. It probably would calculate that the political costs in Europe and the potential risk of military confrontation with the US administration—which has made initiatives in the Caribbean Basin a major element of its foreign policy—are not worth whatever increase in military or political leverage they think such a move might provide. Moscow probably also would believe that such an action would result in the collapse not only of the INF negotiations, but of START as well.

Nonetheless, the threat of missile emplacement in Cuba has been hinted at in This probably is part of an overall Soviet strategy to bring as much pressure as possible to bear on the United States and Europe to move off the zero option position.

Covert Measures. If the Soviets' current strategy fails, they probably will shift the focus of their active measures campaign. They will attempt to use covert means to complement military, diplomatic, and political moves, in an effort to slow the pace of deployment and to keep it at the lowest possible level. With the East-West atmosphere probably souring by that time, they might feel even less constraint against pursuing riskier measures—such as encouraging demonstrations and supporting radical peace groups, some of which might engage in sabotage at NATO facilities.

The Soviets also will use propaganda, disinformation, and support to Communist Party and front groups to increase the political costs to the governments of the basing countries. They will hope that this, in turn, will cause those countries to urge the United States to accede to an agreement that caps NATO deployments at a low level and minimizes reductions in Soviet forces.

In the Netherlands, the Soviets can be expected to intensify their active measures with the Communist Party and its fronts in the period leading up to a Dutch decision (scheduled for late 1983) on INF deployment. Soviet pressure on the Italian Communist Party to intensify support of the peace movement undoubtedly will increase as the initial GLCM equipment deliveries to Italy in October draw near. The Soviets are currently operating under a liability in Italy, however, since their public image there has suffered badly as a result of allegations of Soviet involvement in the attempted assassination of the Pope.

The Campaign for Nuclear Disarmament has been gaining political clout in the United Kingdom. The Soviets' ability to influence it appears to be extremely limited, but they will do what they can to support it, particularly as the projected GLCM deployment date (December) approaches. The Soviets can also be expected to attempt to persuade leftist groups to throw their support behind the END.

The Soviets probably will be careful, however, not to go too far with their active measures campaign. They are aware that strong antinuclear movements exist in all the INF-basing countries (except Italy), even without Soviet or Communist involvement. They also realize that, by treading carefully, they can profit from these movements, which have been aroused by heightened East-West tensions and greater public awareness of nuclear weapons programs affecting West European countries. For these reasons the Soviets probably will continue to rely more on overt political measures, which have proved to be their most effective activities.

Appendix

Significant INF-Related Events Scheduled for 1983

27 January	INF (Round IV) resumes
30 January–10 February	Vice President Bush's European trip begins in Bonn; includes a visit to INF and START negotiations
1 February	Session of the UN Committee on Disarmament begins in Geneva
14 February	Meeting of NATO's Special Consultative Group (SCG)
6 March	Elections in West Germany
March	NATO Nuclear Planning Group ministerial meeting in Portugal
March	Williamsburg summit
Late March	INF (Round IV) ends
March-April	CPSU Central Committee meets
April (?)	Votes on INF infrastructure funding to be held in Belgium, Denmark, and the Netherlands
April [illegible]	First GLCM equipment arrives in United Kingdom
9–10 June	NATO Foreign Ministers' meeting in Paris
June	INF (Round V) resumes
June	First Pershing II equipment arrives in West Germany
August	INF (Round V) ends
October	First GLCM equipment arrives in Italy
November	NATO Nuclear Planning Group ministerial meeting in Canada
4 December	SPD party congress in West Germany
December	NATO ministerial meetings
December	Scheduled initial operational capability for Pershing II in West Germany and GLCM in the United Kingdom

Senator COTTON. Director Pompeo, earlier this year, Dr. Roy Godson testified that he believed that Russia was using active measures and covert influence efforts to undermine our nuclear modernization efforts, our missile defense deployments, and the INF Treaty in keeping with these past practices.

To the best of your ability in this setting, would you agree with the assessment that Russia is likely using such active measures to undermine U.S. nuclear modernization efforts and missile defenses?

Director POMPEO. Yes.

Senator COTTON. Thank you.

As I mentioned earlier, the FY17 Intelligence Authorization Act included two unclassified provisions that I authored. One would be re-starting that old Active Measures Working Group. A second would require additional scrutiny of Russian embassy officials who travel more than the prescribed distance from their duty station, whether it's their embassy or a consulate around the United States.

In late 2016, when that bill was on the verge of passing, I personally received calls from high-ranking Obama administration officials asking me to withdraw them from the bill. I declined. The bill did not pass. It passed last week as part of the FY17 spending bill.

I did not receive any objection from Trump administration officials, to include from our intelligence community. Director Coats, are you aware of any objection that the Trump administration had to my two provisions?

Director COATS. No, I'm not aware of any objection.

Senator COTTON. Director Pompeo.

Director POMPEO. None.

Senator COTTON. Do you know why the Obama administration objected to those two provisions in late 2016, I would add, after the 2016 presidential election?

Director COATS. Well, it would be pure speculation. I don't—I couldn't read—I wasn't able to read the President's mind then and I don't think I can read it now.

Senator COTTON. Thank you.

I'd like to turn my attention to a very important provision of law I know that you've discussed earlier, Section 702. Director Rogers, it's my understanding that your agency is undertaking an effort to try to release some kind of unclassified estimate of the number of U.S. persons who might have been incidentally collected using 702 techniques. Is that correct?

Admiral ROGERS. Sir, we're looking to see if we can quantify something that's of value to people outside the organization.

Senator COTTON. Would that require you going in and conducting searches of incidental collection that have been previously unexamined?

Admiral ROGERS. That's part of the challenge, how do I generate insight that doesn't in the process of generating the insight violate the actual tenets that——

Senator COTTON. So you're trying to produce an estimate that is designed to protect privacy rights, but to produce that estimate you're going to have to violate privacy rights?

Admiral ROGERS. That is a potential part of all of this.

Senator COTTON. It seems hard to do.

Admiral ROGERS. Yes, sir. That's why it has taken us a period of time and that's why we're in the midst of a dialogue.

Senator COTTON. Is it going to be possible to produce that kind of estimate without some degree of inaccuracy or misleading information or infringing upon the privacy rights of Americans?

Admiral ROGERS. Probably not.

Senator COTTON. If anyone in your agency or, for that matter, Director McCabe, in yours, believes that there is misconduct or privacy rights are not being protected, they could, I believe under current law, come to your inspector general, come to your general counsel. I assume you have open door policies?

Admiral ROGERS. Whistleblower protections in addition, yes, sir, and they can come to you.

Senator COTTON. And they can come to this Committee.

Admiral ROGERS. They can come to the Committee.

Senator COTTON. So four—at least four different avenues—I'm probably missing some—if they believe there are any abuses in the Section 702 program.

Director MCCABE. And anyone in their chain of command.

Senator COTTON. I would ask that we proceed with caution before producing a report that might infringe on Americans' privacy rights needlessly and that might make it even that much harder to reauthorize a critical program, something that, Director McCabe, your predecessor last week just characterized, if I can paraphrase, as a must-have program, not a nice-to-have program.

Thank you.

Senator RISCH. Thank you, Senator Cotton.

Senator Harris.

Senator HARRIS. Thank you.

Acting Director McCabe, welcome. I know you've been in this position for only about 48 hours and I appreciate your candor with this Committee during the course of this open hearing.

Director MCCABE. Yes, ma'am.

Senator HARRIS. Until this point what was your role in the FBI's investigation into the Russian hacking of the 2016 election?

Director MCCABE. I've been the Deputy Director since February of 2016. So I've had an oversight role over all of our FBI operational activity, to include that investigation.

Senator HARRIS. And now that you're Acting Director, what will your role be in the investigation?

Director MCCABE. Very similar, senior oversight role to understand what our folks are doing and make sure they have the resources they need and are getting the direction and the guidance they need to go forward.

Senator HARRIS. Do you support the idea of a special prosecutor taking over the investigation in terms of oversight of the investigation, in addition to your role?

Director MCCABE. Ma'am, that is a question for the Department of Justice and it wouldn't be proper for me to comment on that.

Senator HARRIS. From your understanding, who at the Department of Justice is in charge of the investigation?

Director MCCABE. The Deputy Attorney General, who serves as Acting Attorney General for that investigation. He is in charge.

Senator HARRIS. And have you had conversations with him about the investigation since you've been in this role?

Director MCCABE. I have. Yes, ma'am.

Senator HARRIS. And when Director Comey was fired, my understanding is he was not present in his office. He was actually in California. So my question is: Who was in charge of securing his files and devices when that—when that information came down that he had been fired?

Director MCCABE. That's our responsibility, ma'am.

Senator HARRIS. And are you confident that his files and his devices have been secured in a way that we can maintain whatever information or evidence he has in connection with the investigation?

Director MCCABE. Yes, ma'am, I am.

Senator HARRIS. It's been widely reported, and you've mentioned this, that Director Comey asked Rosenstein for additional resources. And I understand that you're saying that you don't believe that you need any additional resources?

Director MCCABE. For the Russia investigation, ma'am, I think we are adequately resourced.

Senator HARRIS. And will you commit to this committee that if you do need resources, that you will come to us, understanding that we would make every effort to get you what you need?

Director MCCABE. I absolutely will.

Senator HARRIS. Has—I understand that you've said that the White House—that you have not talked with the White House about the Russia investigation. Is that correct?

Director MCCABE. That's correct.

Senator HARRIS. Have you talked with Jeff Sessions about the investigation?

Director MCCABE. No, ma'am.

Senator HARRIS. Have you talked with anyone other than Rod Rosenstein at the Department of Justice about the investigation?

Director MCCABE. I don't believe I have, not recently; obviously, not in that—not in this position.

Senator HARRIS. Not in the last 48 hours?

Director MCCABE. No, ma'am.

Senator HARRIS. Okay. What protections have been put in place to assure that the good men and women of the FBI understand that they will not be fired if they aggressively pursue this investigation?

Director MCCABE. Yes, ma'am. So we have very active lines of communication with the team that's—that's working on this issue. They have some exemplary and incredibly effective leaders that they work directly for. And I am confident that those—that they understand and are confident in their position moving forward on this investigation, as my investigators and analysts and professional staff are in everything we do every day.

Senator HARRIS. And I agree with you. I have no question about the commitment that the men and women of the FBI have to pursue their mission. But will you commit to me that you will directly communicate in some way—now that these occurrences have hap-

pened and Director Comey has been fired, will you commit to me that, given this changed circumstance, that you will find a way to directly communicate with those men and women to assure them that they will not be fired simply for aggressively pursuing this investigation?

Director MCCABE. Yes, ma'am.

Senator HARRIS. Thank you.

And how do you believe we need to handle, to the extent that it exists, any crisis of confidence in the leadership of the FBI, given the firing of Director Comey?

Director MCCABE. I don't believe there is a crisis of confidence in the leadership of the FBI. I suppose that's somewhat self-serving, and I apologize for that.

[Laughter.]

You know, it was completely within the President's authority to take the steps that he did. We all understand that. We expect that he and the Justice Department will work to find a suitable replacement and a permanent director, and we look forward to supporting whoever that person is, whether they begin as an interim director or a permanently selected director. This organization in its entirety will be completely committed to helping that person get off to a great start and do what they need to do.

Senator HARRIS. And do you believe that there will be any pause in the investigation during this interim period, where we have a number of people who are in acting positions of authority?

Director MCCABE. No, ma'am. That is my job right now, to ensure that the men and women who work for the FBI stay focused on the threats, stay focused on the issues that are of so much importance to this country, continue to protect the American people, and uphold the Constitution. And I will ensure that that happens.

Senator HARRIS. I appreciate that. Thank you.

Director MCCABE. Yes, ma'am.

Chairman BURR. Thank you.

Senator King. Second round, five minutes each.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

I want to go back to the question I asked you, Director Pompeo. And I went out and reviewed the response that you gave to me. And of course, what I'm concerned about is the Sally Yates warning to the White House that Michael Flynn could be blackmailed by the Russians.

And you said you didn't have any first-hand indication of it. Did you have any indication—second-hand, any sense at all that the national security adviser might be vulnerable to blackmail by the Russians? That is a yes or no question.

Director POMPEO. It's actually not a yes or no question, Senator. I can't answer yes or no. I regret that I'm unable to do so. You have to remember this is a counterintelligence investigation that was largely being conducted by the FBI and not by the CIA. We're a foreign intelligence organization.

And I'll add only this. I was not intending to be clever by using the term "first-hand." I had no second-hand or third-hand knowledge of that conversation either.

Senator WYDEN. So with respect to the CIA, were there any discussions with General Flynn at all?

Director POMPEO. With respect to what, sir? He was for a period of time the National Security Adviser.

Senator WYDEN. Topics that could have put at risk the security and the well-being of the American people. I mean, I'm just finding it very hard to swallow that you all had no discussions with the National Security Adviser.

Director POMPEO. I spoke with the National Security Adviser. He was the National Security Advisor. He was present for the daily brief on many occasions and we talked about all the topics we spoke to the President about.

Senator WYDEN. But nothing relating to matters that could have compromised the security of the United States?

Director POMPEO. Sir I can't recall every conversation that I had with General Flynn during that time period.

Senator WYDEN. We're going to ask more about it in closed session this afternoon.

Admiral Rogers, let me ask you about a technical question that I think is particularly troubling and that is the SS7 question and the technology threat. Last week the Department of Homeland Security published a lengthy study about the impact on the U.S. government of mobile phone security flaws. The report confirmed what I have been warning about for quite some time, which is the significance of cyber security vulnerabilities associated with a Signaling System 7.

The report says that the Department believes, and I quote, "that all U.S. carriers are vulnerable to these exploits, resulting in risks to national security, the economy, and the Federal Government's ability to reliably execute national security functions. These vulnerabilities can be exploited by criminals, terrorists, and nation-state actors and foreign intelligence organizations."

Do you all share the concerns of the Department of Human—the Homeland Security Department about the severity of these vulnerabilities and what ought to be done right now to get the government and the private sector to be working together more clearly and in a coherent plan to deal with these monumental risks. These are risks that we are going to face with terrorists and hackers and threats. And I think the Federal Communications Commission has been treading water on this and I'd like to see what you want to do to really take charge of this and deal with what is an enormous vulnerability to the security of this country?

Admiral ROGERS. Sure. I hear the concern. It's a widely deployed technology in the mobile segment. I share the concern. The Department of Homeland Security in their role kind of is the lead Federal agency associated with cyber and support from the Federal Government to the private sector, has overall responsibility here.

We are trying to provide at the National Security Agency our expertise to help generate insights about the nature of the vulnerability, the nature of the problem, partnering with DHS, talking to the private sector. There's a couple specific things from a technology standpoint that we're looking at in multiple forms that the government has created partnering with the private sector.

I'm not smart, I apologize, about all of the specifics of the DHS effort. I can take that for the record if you'd like.

Senator WYDEN. All right. I just want to respond before we break to Senator Cotton's comments with respect to Section 702. Mr. Director, glad to see my tax reform partner back in this role. You know, Mr. Director, that I think it's critical the American people know how many innocent law-abiding Americans are being swept up in the program.

The argument that producing an estimate of the number is in itself a violation of privacy is I think a far-fetched argument. It has been made for years. I and others who believe that we can have security and liberty, that they're not mutually exclusive, have always believed that this argument that you're going to be invading people's privacy doesn't add up.

We have to have that number. Are we going to get it? Are we going to get it in time so we can have a debate that shows that those of us who understand there are threats coming from overseas, and we support the effort to deal with those threats as part of 702, that we are not going to have Americans' privacy rights indiscriminately swept up.

We need that number. When will we get it?

Director COATS. Senator, as you recall, during my confirmation hearing we had this discussion. I promised to you that I would, if confirmed—and I was—go out to NSA, meet with Admiral Rogers, try to understand, better understand, why it was so difficult to come to a specific number. I did go out to NSA. I was hosted by Admiral Rogers. We spent significant time talking about that.

And I learned of the complexity of reaching that number. I think the statements that had been made by Senator Cotton are very relevant statements as to that. Clearly, what I have learned is that a breach of privacy has to be made—against American people, have to be made in order to determine whether or not they breached privacy. So, there is a anomaly there. There are issues of duplication.

I know that a—we're underway in terms of setting up a time with this Committee, I believe in June, as early as June, to address, get into that issue and to address that and talk through the complexity of why it's so difficult to say. This is specifically when we can get you the number and what the number is.

So we are committed to a special meeting with the Committee to try to go through this, this particular issue. But I cannot give you a date because—and number, because I understand the complexity of it now and why it's so difficult for Admiral Rogers to say this specific number is the number.

Senator WYDEN. I'm well over my time. The point really is privacy advocates and technologists say that it's possible to get the number. If they say it and the government is not saying it, something is really out of sync. You've got people who want to work with you. We must get on with this and to have a real debate about 702 that ensures that security and liberty are not mutually exclusive, we have to have that number.

Thank you, Mr. Chairman.

Senator RISCH. Thank you, Senator.

Senator King, I understand you have a question.

Senator KING. Thank you, Senator.

If this hearing had been held two weeks ago, we'd be spending the last two hours talking about North Korea. And I think we ought to pay some attention to that. Director Pompeo and Director Cardillo, could you give us an update on the North Korea situation, the nature of the threat, whether some of the pressure that we were feeling two and three and four weeks ago has relieved? Is there anything going on that should either concern or make us feel better about that situation?

Director Pompeo.

Director POMPEO. Senator, I don't see anything that should make any us feel any better about this threat. We have a threat from flashpoints that something could spark and have a conventional war, right, wholly apart from the issues we talk about with ICBMs and nuclear, just a well-armed adversary that our Department of Defense works hard to make sure and mitigate against. Those risks remain.

The leader continues to develop, test, attempt to verify, not only in the launches that we see, many of which have failed, but learned from each one, but continue to develop software that improves day by day. This threat is very real.

We should not all focus simply on the ICBMs either. American interests are held at risk today by shorter-range missiles in theater, enormous American assets.

Senator KING. Seoul is held at risk by artillery.

Director POMPEO. Seoul is held at risk. We have enormous American interests in and around the region in Seoul.

So, no, I wouldn't say that, in spite of the fact that it has fallen out of the headlines for the moment, that there's any decreased risk associated with the threat from Kim Jung Un.

Senator KING. There was some discussion after—again, about two weeks ago, of entering into some kind of discussions with the North Koreans. Has anything—can you report anything on that front?

Director POMPEO. Sir, there are none that I'm aware of related to trying to talk Kim Jung Un away from his nuclear missile program. We have taken actions at the Agency. I've stood up a Korean Mission Center to draw the best minds, the most innovative, creative people from across our Agency, and I'm sure we'll have others join in from across the intelligence community, to try and focus this effort so that we can get back on our front foot with respect to foreign intelligence collection against the North Koreans and the capacity to impact what Kim Jung Un is actually doing.

Senator KING. On that latter point, would you agree that the path to influence is through China?

Director POMPEO. I think it's among our most productive paths and one that I know the President's committed to working, as is Secretary Tillerson.

Senator KING. Thank you very much.

Admiral Rogers——

Director CARDILLO. Senator King——

Senator KING. Yes, please.

Director CARDILLO. May I just chime in? I was in front of you in closed session a couple of weeks ago giving you great detail about the threat you've just highlighted. What you'll hear this afternoon

is just the continuation of what I was briefing a couple of weeks ago.

So I would agree with the Director that this is—this threat has not only been sustained, it's continued to grow.

Senator KING. Because it's fallen out of the headlines doesn't mean it's not——

Director CARDILLO. That's correct. It's still our highest priority.

Senator KING. Thank you.

Director COATS. It is the highest priority, one of the highest, if not the highest, priority of the intelligence community at this time. A great deal of effort is being spent relative to how we can even better assess the situation and provide all the relevant intelligence to our policymakers.

Senator KING. Thank you.

Two final questions. Admiral Rogers, the reason I was late this morning, we had a very informative hearing in Armed Services on cyber with Jim Clapper and Admiral Stavridis and General Hayden. The upshot of that hearing was that we still don't have a doctrine. We still don't have a policy. We still don't really fully understand—you would concur, I assume, that cyber's one of the most serious threats we face?

Admiral ROGERS. Yes, sir.

Senator KING. And do we need to have a policy and a deterrent policy and something further than what we have now, which is kind of an ad hoc response to events?

Admiral ROGERS. Right, it tends to be a case-by-case basis. Yes, sir, I agree. And we spoke about that when I testified before the SASC last week, as a matter of fact.

Senator KING. And Senator McCain said what's the impediment? Why can't we get there? Is it the structure of our government? We've got too many people thinking about this? What is it going to take to get us to the point of having a doctrine that will guide us in this incredibly important era?

We are seeing the notion of warfare change before our eyes.

Admiral ROGERS. Sir, I don't have any easy answer for you. My role in life, not speaking now as the Director of NSA, but as the commander of the United States Cyber Commander, is to be operational commander. So I don't develop policy. I play a role on the doctrine side, trying to provide an operational perspective.

Senator KING. Well, I hope from your position, though, you would be——

Admiral ROGERS. Oh, yes, sir.

Senator KING [continuing]. Telling the Administration and everyone you can think of, because——

Admiral ROGERS. Yes, sir.

Senator KING [continuing]. I do not want to go home to Maine and say, well, we talked a lot about this but we didn't do anything, and when the electric system went down, you know, we might've been able to prevent it.

Admiral ROGERS. Yes, sir.

Senator KING. Director Pompeo, a final question. Do you think that Russian activity in the 2016 election was a one-off?

Director POMPEO. No, sir.

Senator KING. This is a continuing threat, is it not?

Director POMPEO. Yes, sir.

Senator KING. And things that they learned in this election they're going to apply in—in 2018, 2020, and beyond?

Director POMPEO. Yes, sir. And I hope we learn from it as well and we'll be able to more effectively defeat it.

Senator KING. And I believe that's why the work of this Committee and others is so important, because we've got to understand what they did, how they did it so that we can deal with it in the future. Would you agree?

Director POMPEO. Yes, Senator, I would.

Senator KING. Thank you very much.

Director COATS. Senator King, if I could just add to that. I think making this as transparent as possible, not only to our own public, but throughout democratic nations that are facing this threat. The more we inform our people of what the Russians are trying to do and how they're trying to impact our thinking and our decisions relative to how we want to be governed and what kind of democratic institutions that we want to preserve, the better.

So, my hope is the Russians have overstepped here to the point where people will say we absolutely have to do something about it and we have to put deterrent efforts in place as well as potentially offensive efforts.

Senator KING. Well, I think your point about open hearings and education is incredibly important. You and I were in the Ukraine and Poland just about a year ago and what they told us over there was that the best defense—they can't shut down their TV networks, they can't turn off the internet. The best defense is if the public knows what's happening and they say, oh, it's just the Russians again. And we have to reach that level of knowledge in this country. So I completely agree and hope that as much of our work as possible can be done in open hearing.

Thank you, Mr. Chairman.

Senator RISCH. Thank you, Senator King.

Gentlemen, thank you so much. Thank you all for your service. Thank you to all the men and women of all 17 agencies for the incredible service they provide to the people of the United States, keeping them safe, doing things that most people in America will never know nor be able to fully appreciate.

Mr. McCabe, a special thank you for stepping up to the battlefield promotion and representing your agency quite well here.

This part of the hearing will be adjourned. And gentlemen, you have about an hour and six minutes and we'll see at the other room. Thank you. Meeting's adjourned.

[Whereupon, at 12:24 p.m., the hearing was adjourned.]

Supplemental Material

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D. C. 20530

FEB 12 2018

The Honorable Richard M. Burr
Chairman
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance before the Committee of FBI Deputy Director Andrew McCabe on May 22, 2017, at a hearing concerning worldwide threats.

Thank you for the opportunity to present our views. Please do not hesitate to contact this office if we may be of additional assistance to you. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Stephen E. Boyd
Assistant Attorney General

Enclosure

RESPONSES OF
ANDREW MCCABE
DEPUTY DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

TO QUESTIONS FOR THE RECORD
ARISING FROM A HEARING
BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

CONCERNING
WORLDWIDE THREATS

MAY 22, 2017

Questions from Senator Harris:

(U) As you may be aware, it has been reported that when the FBI learned that the Democratic National Committee (DNC) was hacked, it failed to reach out to DNC leadership directly, and instead called the Committee's IT "help desk." (See, e.g. *The New York Times,* "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," Dec. 13, 2016).

1. **Is the press characterization accurate? If not, please characterize FBI's notification efforts and timeline accurately.**

Response:

(U//FOUO) The timeline and characterization of the FBI's notification efforts to the Democratic National Committee ("DNC") in the referenced *New York Times* article is incomplete. FBI began its notification efforts to the DNC on 06 August 2015 after FBI received reporting that the DNC was compromised by the advanced persistent threat actor referred to as CozyBear. After FBI requested to speak with the individual responsible for maintaining the IT systems, DNC referred the FBI to its Director of IT Yared Tamene. He was quickly identified to be the appropriate person to receive victim notifications on behalf of the DNC. The FBI was not initially aware that Tamene was a contract employee. His status as a contractor was not an issue because the DNC Chief Operating Officer Lindsey Reynolds, Technology Director Andrew Brown, DNC counsel Graham M. Wilson and DNC counsel Michael Sussmann were fully aware of the details of the compromise, and the fact that Tamene was the FBI's primary point of contact throughout the investigation. DNC executive management endorsed the FBI communicating technical details of the compromise with Tamene.

(U//FOUO) FBI provided DNC with two compromised IP addresses during this initial notification, indicated the DNC could potentially be a victim or a future victim of an ongoing

e-mail spear-phishing campaign, and advised the activity may be related to open source threat reporting under the names Miniduke and Minidionis. FBI had no reason to believe the information was not being handled appropriately, or that an in-person notification was warranted.

(U//FOUO) FBI's initial notification to DNC followed FBI's well-defined procedures for conducting expeditious notification to victims via the most reliable method available. FBI typically notifies the "individual, organization, or corporation that is the owner or operator of the computer at the point of compromise or intrusion" as they are in the best position to take immediate action on the information provided. On multiple occasions thereafter, FBI requested to be connected with the individual in charge of the IT systems at DNC, and was always directed to the same individual, Yared Tamene. Furthermore, once senior level DNC members became involved in the matter, DNC counsel confirmed that the FBI should continue to work through this individual.

(U//FOUO) FBI re-contacted DNC in December 2015 to advise that DNC systems were likely still compromised and to provide additional threat information. In January 2016, the FBI provided the DNC with an open source report titled *The Dukes: 7 Years of Russian cyberespionage*, which contained additional background on the threat actors. The FBI continued to notify the DNC when information was received that led FBI to believe that the DNC was still compromised. In February 2016, the FBI offered the use of a cyber response team to help identify the malicious traffic on DNC's network and offered to deploy a sensor on the network to help identify the malicious traffic; however, both offers were declined by the DNC.

(U//FOUO) In March 2016 FBI notified DNC about a spear-phishing campaign by a second adversary, referred to as FancyBear, against the DNC. FBI notified DNC again in April 2016 about a second set of FancyBear spear-phishing targets and identified users who clicked malicious links. FBI requested and received log files from DNC in April 2016. FBI continued to follow-up with DNC through June 2016, at which point a private security firm began providing mitigation services to the DNC, and the FBI began working directly with that firm.

2. Given the FBI's long-standing knowledge of Russia's influence efforts- including its use of cyberattacks to disrupt other countries' political processes- why wasn't the FBI's response more aggressive?

Response:

(U//FOUO) The cyber campaign in question targeted over 130 US victim companies and corporations, just one of which was the DNC. FBI exceeded standard procedures in its victim engagement with the DNC and believed the matter was being handled appropriately,

so there was no reason to further elevate the notification. Due to the size and scope of the malicious campaign in the summer of 2015, the most rapid and reliable method available for notification was direct telephonic notification. The FBI did recognize the high-profile nature of this victim, and acted accordingly.. The FBI had over 30 separate interactions with DNC IT and executive management. The FBI offered the use of a cyber response team to help identify the malicious traffic on their network and the FBI offered to deploy a sensor on the network to help identify the malicious traffic; however, both were declined. Instead, the DNC retained a private security firm to manage detection and remediation.

3. Why did the FBI wait until July 2016 to open an investigation into Russian interference in the 2016 U.S. election?

Response:

As described in part above, the FBI investigated malicious activity by Russian actors (both the theft and dissemination of information) as it learned of it, well-before the election (in 2015 and earlier) and continuing until after the election, in collaboration with various components of the Justice Department, including, after his appointment, the Special Counsel.

4. What has the FBI done to better assess and respond to these types of cyber intrusions?

Response:

(U//FOUO) The Department of Justice is currently conducting a review of the FBI's victim notification procedures. Although the review is still ongoing, the FBI believes the DNC notification was compliant with both 0395PG (internal notification policy) and PPD-41 (even though not in effect at the time of initial notification(s)). [Administrative note: PPD-41 was signed July 26, 2016, or approximately 45 days after the DNC data had been posted by online persona Guccifer2.0.] PPD-41 advises the private sector and Government agencies have a shared vital interest and complementary roles and responsibilities.

(U//FOUO) FBI has taken steps to increase its outreach efforts with sectors affected by the 2015/2016 election-related intrusions and intrusion attempts, and FBI continues to use unclassified bulletins to inform private sector entities about continuing advanced persistent threat activity and mitigation strategies.

(U//FOUO) In April 2016, FBI hosted a tabletop training exercise modeled on the actual CozyBear campaign from July 2015, which DNC attended. The purpose of the exercise was to familiarize participating organizations with spear-phishing campaigns, indicators of compromise, and to provide suggestions to improve information sharing between other

government agencies, the private sector, and FBI. The Republican National Committee (RNC) was also provided information from the exercise.

(U//FOUO) Between October 2016 and July 2017, FBI and/or Department of Homeland Security released five reports to the private sector regarding advanced persistent threat tactics, indicators, and recommended actions.

(U//FOUO) In April and May 2017, FBI Cyber Division re-engaged with voting systems companies and asked FBI field offices to have conversations with companies about the threat landscape and what, if any, threats they have seen since the 2016 election cycle. As of June, voting systems companies have not observed any targeting activity but communication lines remain open for information sharing and engagement. Additionally, FBI Cyber Division and related field offices are planning multiple tabletop training exercises for the 2018 election cycle.

(U//FOUO) On a larger scale, as far back as 2013, the FBI Cyber Division reorganized the manner in which it investigates state-sponsored computer intrusion activity. The Cyber Threat Team ("CTT") model established a standard to narrowly define, scope, and prioritize over 70 nation-state sponsored cyber threats. The traditional FBI investigative model focuses on the victim. If a crime occurs in a field office's geographic area of responsibility ("AOR"), then that field office opens an investigation. Due to the distributed nature of a cyber actor's victims, this created a situation where each field office was investigating dozens of computer intrusions. Numerous field offices would be investigating the same actor's criminal activity.

(U//FOUO) The CTT model shifted the focus to the nation-state actors, with a select group of field offices responsible for each cyber threat. Each threat is investigated by a team consisting of 2-6 field offices and a FBI Headquarters support team. This team is often times assisted by resources from other USIC agencies and allied foreign partners. This proved to be a far more efficient and effective use of the FBI's cyber resources. Approximately 80% of all field offices are assigned less than 3 threats, better distributing the workload and technical expertise of the FBI. A comprehensive threat picture is developed and owned by the designated CTT, thus enabling those assigned field offices to become the subject matter experts on the threat. The 70+ global nation-state cyber threats are banded for prioritization purposes. The top priorities are categorized as National Threat Priorities ("NTP"). Additional bands are groups 2-6. The actual categorization of various threats are classified and are not appropriate for this document.

(U//FOUO) In addition, also since approximately 2012, the FBI Cyber Division has worked closely with the Department of Justice's National Security Division and U.S. Attorney's Offices around the country to bring all legal tools (including but not limited to prosecution) to bear on the threats posed by state-sponsored hacking and other malicious activities (like influence operations) that might exploit it). Through these efforts, we have charged, arrested, and successfully prosecuted individuals working for (or for the benefit of) foreign states.

In doing so, DOJ and FBI seek to raise the costs of the activity, including by supporting the efforts of other departments and agencies, and to educate the American people about the threats we face (so they can better protect themselves and their networks).

5. **Are we better positioned today to prevent, detect, and respond to comparable cyber intrusions? If not, what should we be doing differently?**

Response:

(U//FOUO) The FBI can only respond to reports of computer intrusions and attacks that it learns of, and many victims prefer, for a variety of reasons, to remediate intrusions in-house or with the assistance of private security firms, rather than report the intrusion to the government and avail themselves of our assistance. Encouraging reporting by victims is one of the Department of Justice's priorities in its frequent outreach events to the private sector, and we would welcome reinforcement of that encouragement.

6. **From September 2015 to July 5, 2016, how was the assessment or preliminary investigation into hacking of computer systems belonging to the Democratic National Committee and the Republican National Committee (or state or local electoral boards) staffed? Please include an explanation of the number of agents assigned full-time to the investigation and the overall staffing plan.**

Response:

(U//FOUO) The FBI staffs all investigations with a combination of agent and analytical support. The exact number of personnel involved varies depending on the complexity and stage of the investigation.

7. **From July 6, 2016 to November 8, 2016, how was the investigation into Russian interference in the 2016 election staffed? Please include an explanation of the number of agents assigned full-time to the investigation and the overall staffing plan.**

Response:

(U//FOUO) *See* the response to the preceding question.

8. **How is the investigation into Russian interference into the 2016 election currently staffed? Please include an explanation of the number of agents assigned full-time to the investigation and the overall staffing plan.**

Response:

(U//FOUO) This question should be referred to the Special Counsel.

○