AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–264

OPEN HEARING ON THE INTELLIGENCE COMMUNITY'S ASSESSMENT ON RUSSIAN ACTIVITIES AND INTENTIONS IN THE 2016 U.S. ELECTIONS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTENTH CONGRESS

FIRST SESSION

TUESDAY, JANUARY 10, 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

29–830 PDF WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

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

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

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

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

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

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
DESIREE THOMPSON-SAYLE, *Chief Clerk*

CONTENTS

JANUARY 10, 2017

OPENING STATEMENTS

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

WITNESS

James R. Clapper, Director of National Intelligence, Accompanied by: John Brennan, Director of the Central Intelligence Agency; James Comey, Director of the Federal Bureau of Investigation; and ADM. Michael Rogers, Director of the National Security Agency 5
Prepared statement 8

OPEN HEARING ON THE INTELLIGENCE COMMUNITY'S ASSESSMENT ON RUSSIAN ACTIVITIES AND INTENTIONS IN THE 2016 U.S. ELECTIONS

TUESDAY, JANUARY 10, 2017

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

The Committee met, pursuant to notice, at 1:03 p.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

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

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

Chairman BURR. I'd like to call this hearing to order. I'd like to welcome our witnesses: Jim Clapper, Director of National Intelligence; John Brennan, Director of the Central Intelligence Agency; Jim Comey, Director of the Federal Bureau of Investigation; and Admiral Mike Rogers, Director of the National Security Agency.

Directors Clapper and Brennan, while I've said this to you before in closed session, this is likely your last appearance before the Committee, at least in your current roles. I want to thank each of you, before you get out of here, for your many years of dedicated service both in uniform and out of uniform. Jim, John, in many different capacities, you have served your country in an unbelievable way, both of you. We want you to know how grateful we are to you and how grateful the Nation is to you for the service that you've provided.

We convene today to discuss the President's directed review of Russian activities and intentions in recent U.S. elections. While Russia and the Soviet Union have used active measures as tools of statecraft since the 1920s, recent actions by the Russian government represent, as you reported, a notable escalation.

I know that the public disclosure of these activities surprised many and the notion that another state would attempt to interfere in our elections is quite troubling. However, Russian active measures as a general topic is not new to the Members of this Committee. We've held more than 10 hearings and briefings over the last two years that have focused in whole or in part to better un-

derstand the scale and scope of these efforts and the intentions behind them.

Each of our witnesses has appeared before us in closed session to discuss this topic, and in response, on a bipartisan and bicameral basis, this Committee and its sister committee in the other body have put forward unclassified and classified proposals to address these activities. Some work has been done, but to effectively address this challenge to the integrity of our system of government will require a "whole of government" approach.

I look forward to hearing from our witnesses on the details of the intelligence community assessment. Intelligence reporting over the last few years, to include the classified and compartmented portions of this assessment, gives me no reason to doubt the findings contained within the product. That said, we owe it to our colleagues and the American people to do an independent and bipartisan review of the report and its conclusions.

I've therefore instructed Committee staff to carry out an assessment of the sourcing behind this report, and we will be asking each of our witnesses to provide the Committee access to the intelligence that contributed to this assessment. I want to assure my colleagues on this Committee and in this body that we will follow the intelligence wherever it leads and we will conduct this review in a nonpartisan manner. I also want to assure the witnesses before us today, as has long been our practice, the Committee will treat the protection of these sources with the level of security and professionalism required.

I'd also like to quickly thank the men and women of the intelligence community for their work in completing this review. To each of our witnesses: Please thank your respective staffs. I have no doubt that the President's directive, Jim, to you and to others ruined many's holiday plans.

While this moment in our history is critical and the testimony before this Committee in an open setting will, I hope, help the American people understand what Russia attempted to accomplish as part of its focus on our 2016 elections, I want to make this clear: Our democracy is not at risk. We can rest assured in the strength of the United States of America and have continued faith in the electoral process.

We must be alert, though, to the challenges that face us and the threats posed by those who seek to undermine Western democratic values, whether they are through interference in our elections or relentless propaganda and active measures targeting our friends and our allies abroad.

Our values are indeed under assault. The key differences between the efforts of the past and the attacks of today, however, is the tools being used to carry these out.

Gentlemen, thank you again for being here today. I look forward to your testimony, General Clapper, and to the opportunity to query questions to the rest.

I will now turn to the distinguished Vice Chairman, the Senator from Virginia.

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

Vice Chairman WARNER. Well, thank you, Mr. Chairman, and I want to echo, first of all, your comments in terms of commending all the witnesses, but particularly Director Clapper and Director Brennan, for your great service to our country.

I also want to acknowledge the new Members of our Committee, both new Members here, Senator Manchin and Senator Harris. I know Senator Cornyn will be joining us briefly and, while she's not here yet, I want to acknowledge the great role that Senator Feinstein has played, both as Chair and Vice Chair on this Committee.

We're here today to discuss the intelligence community's comprehensive review into Russian interference in our 2016 presidential election, for me one of the most serious events of my public life. Interference in American democracy and our electoral process by any outside power is unacceptable.

Now, much of the press reporting and conversation about Russian activities have focused on the hacks of the DNC and John Podesta. But, as the report pointed out, the Russians also hacked systems associated with the Republicans. They just chose not to release that material yet. There's nothing that prevents them from doing so at a time of their choosing in the future.

While the target of this campaign was Secretary Clinton, any of us, Democrats or Republicans, including members of this body, could easily be the next target.

What the Russians did was nothing less than an attack on our political system and democracy itself. We can simply not allow it to stand.

The IC assessment is more detailed, but is in line with the previous assessments from the intelligence community that Russian officials at the highest level, including President Putin, engaged in—in your words, not mine—"in an unprecedented level of interference in our election." It concludes that "these actions had the goal of harming the candidacy of Hillary Clinton and boosting the candidacy of President-elect Donald Trump."

We are not here to re-litigate the results of the election. At the same time, I am committed to ensuring that there is a thorough, bipartisan, and expeditious Congressional investigation of Russia's role. In my view, our Committee should focus on three broad areas: the Russian hacking and release of stolen information; Russia's use of state-owned media and other means to amplify real and fake news to further their goal; and contact between Russian government and its agents and associates of any campaign and candidate.

I, like you, Mr. Chairman, have written to all the witnesses here today asking them to cooperate with us in this investigation and turn over as many documents and as much evidence as quickly as possible. I, like you, am reiterating that call today. It is equally important that the incoming Administration and those folks who will take Director Clapper and Director Brennan's roles going forward will continue to cooperate in this effort.

Additionally, it's my hope, while we've made a first step, that we'll continue to try to declassify as much material as possible while again protecting sources and methods.

The American people deserve to know, as soon as possible, that their elected representatives have taken a close look at the intelligence report that we're considering today. They deserve to know whether we concur or not with its conclusions and that we're prepared to respond to the threats outlined in the assessment.

The actions that the President took recently in response to Russian activities were an appropriate first step. At the same time, I still have questions why the Obama Administration didn't act further and didn't act sooner.

But as we look forward, preventing future attempts to undermine our democracy and our position in the world will require a sustained response from the incoming Administration and from this Congress. I truly believe the strength of America's democracy will be measured in part on what actions we take to develop a robust and proactive cyber strategy.

Part of that strategy must include tools and capabilities to deter and effectively respond to future attempts by foreign actors to influence America's democratic process.

One of the things I've always valued about service on this Intelligence Committee is the tradition of leaving partisanship at the door oftentimes when we go into that SCIF. I look forward to working with you, Mr. Chairman, and all our Members to complete this investigation as quickly and expeditiously as possible.

Gentlemen, your agencies—the work that your agencies completed underscores the importance of the role the Nation's intelligence community plays and the men and women who quietly work every day to keep our country safe. This report represents the best analysis of the men and women of the intelligence community. These are professionals who have taken an oath of office to present the whole truth as they see it, faithfully to Republicans and Democratic administrations alike.

As a member of this Committee, I think all of us who've served for some time have seen first-hand the dedication of the men and women who work for you. I know that one of the most primary missions of the intelligence professionals is to render the best professional judgment, regardless of political considerations, and always be willing to speak truth to power. I support them for their work.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Vice Chairman.

For Members: Once Director Clapper has been recognized and completes his testimony, it is the intention of the Chair to recognize members based upon seniority for five-minute questions. There is a vote that's scheduled right now for 2:30. It's the intent of the Chair to complete our questions in open session by the conclusion of that vote, and it is the intent of the Chairman to then move to a closed session, which would start after the 2:30 vote. If there's need to adjust that, we'll make an adjustment on the way.

Having said that, a reminder to all members that we're in open session and that you should take that into account from the standpoint of the questions that you ask and realize that there are unclassified and classified reports.

With that, Director Clapper, the floor is yours.

STATEMENT OF HON. JAMES R. CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE, ACCOMPANIED BY: JOHN BRENNAN, DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY; JAMES COMEY, DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION; AND ADM. MICHAEL ROGERS, DIRECTOR OF THE NATIONAL SECURITY AGENCY

Director CLAPPER. Chairman Burr, Vice Chairman Warner, Members of the Committee: First, thank you for your gracious comments, particularly for John and me, as this should be our last hearing, although one never knows. There's still 10 days left. But more importantly, the comments about the work, the dedication and the patriotism of the women and men of the intelligence community. So we appreciate that.

We're here today to present the intelligence community's assessment of Russian activities and intentions during the recent U.S. presidential election. As you indicated, some aspects of our report involve very sensitive sources and methods that we can't discuss in this open televised hearing. So obviously we're asking for your support and understanding as we need to defer to a closed setting.

Our remarks today are based on a highly classified assessment that was produced by the three agencies represented here, the CIA, FBI, and NSA, at the request of President Obama, which we, as you also indicated, released publicly in a declassified version last Friday afternoon.

The report covers the motivation and scope of Moscow's intentions regarding the U.S. election and Russia's use of cyber tools and media to influence U.S. public opinion. I want to make clear that this report does not—repeat, does not—assess the impact of Russian activities on the actual outcome of the 2016 election or draw any conclusions in that regard one way or the other. The IC's role is to assess the intentions, capabilities, and actions of foreign actors, not to analyze U.S. political processes or U.S. public opinion. We can say that we did not see evidence of the Russians altering vote tallies.

We can't discuss the full range of classified information that supports our conclusions because of the extreme sensitivity of these sources. But the key judgments in the public and classified versions are the same. I can say that the report draws on intelligence collected by all three of these agencies represented here, some of which only came to light after Election Day.

When the IC says high confidence, we mean we have multiple high-quality sources of information that contribute to that assessment. The intelligence comes from a wide range of sources, including human sources, technical collection, and open source information. The key judgments are based on corroborating sources that are consistent with our understanding of historical and current Russian behavior.

While we cannot publicly disclose most of the information that backs up these judgments, we have briefed the report in detail to President Obama and his team, President-elect Trump and his team, and Congressional leadership, and this morning the House Permanent Select Committee for Intelligence. They have had the opportunity to explore the report and pose any questions they have had about the basis for our conclusions.

Both the classified and public versions of this report were written by seasoned, nonpartisan intelligence professionals, consistent with the highest standards of analytic objectivity and tradecraft that the IC has refined over the last 15 years or so to ensure we provide policymakers the most accurate insights that we can. I also need to add that this reflects the intelligence community's view, not that of the Administration.

Attributing cyber operations is difficult, but not impossible. Every cyber operation, malicious or not, leaves a trail. IC analysts use this trail and their constantly growing knowledge base of malicious actors and their tools and methods to trace operations back to their source and determine their connections to foreign governments. This is exactly what we did here.

Let me start with respect to the findings, to first address Russia's goals and intentions. We have high confidence that President Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. The goals of this campaign were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton and harm her electability and potential presidency.

Putin and the Russian government also developed a clear preference for President-elect Trump. Russia aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him.

Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of each of the candidates. When it appeared to Moscow that Secretary Clinton was likely to win, the Russian influence campaign began to focus more on undermining her future presidency.

Moscow's influence campaign blended covert intelligence operations with overt efforts by Russian government agencies, state-funded media, third party intermediaries, and paid social media users.

We're highly confident that the Russian intelligence services conducted cyber operations against people and organizations associated with the 2016 U.S. presidential election, including both major U.S. political parties. Russian military intelligence, or the GRU, compromised the email accounts of Democratic Party officials and publicly released victim data using the Guccifer 2.0 persona and DCLeaks.com and in exclusives to media outlets. They also relayed material to WikiLeaks.

Russia collected on some Republican-affiliated targets, but did not conduct a comparable disclosure campaign.

Russia's intelligence obtained and maintained access to elements of multiple U.S. State or local electoral boards. However, the Department of Homeland Security assesses these types of systems were not involved, not involved, in vote tallying.

Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging using Russian government-funded outlets, such as RT.

Moscow has long sought to undermine U.S.-led liberal democratic order. Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on U.S. presidential elections. They've used intelligence officers, influence agents, and

press placements to disparage candidates perceived as hostile to the Kremlin.

Moscow's behavior reflects Russia's more aggressive cyber posture in recent years, which poses a major threat to U.S. military, diplomatic, commercial, and critical infrastructure networks, as well as, as we've seen now, our elections. However, Russia's activities in 2016 demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. We assess Moscow will apply the lessons learned from the 2016 campaign aimed in the future to influence efforts worldwide, including against U.S. allies.

I'd like to wrap up by saying I've now got just 10 days left in my 53 years or so in the intel business, and I've seen the IC get things right and get things wrong. But I believe the level of professional tradecraft and cross-agency intelligence integration required to put this report together gives me great confidence that we've gotten it right here.

With that, we're open for your questions.

[The prepared statement of Director Clapper follows:]

Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution

6 January 2017

Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution

"Assessing Russian Activities and Intentions in Recent US Elections" is a declassified version of a highly classified assessment that has been provided to the President and to recipients approved by the President.

- The Intelligence Community rarely can publicly reveal the full extent of its knowledge or the precise bases for its assessments, as the release of such information would reveal sensitive sources or methods and imperil the ability to collect critical foreign intelligence in the future.
- Thus, while the conclusions in the report are all reflected in the classified assessment, the declassified report does not and cannot include the full supporting information, including specific intelligence and sources and methods.

The Analytic Process

The mission of the Intelligence Community is to seek to reduce the uncertainty surrounding foreign activities, capabilities, or leaders' intentions. This objective is difficult to achieve when seeking to understand complex issues on which foreign actors go to extraordinary lengths to hide or obfuscate their activities.

- On these issues of great importance to US national security, the goal of intelligence analysis is to provide assessments to decisionmakers that are intellectually rigorous, objective, timely, and useful, and that adhere to tradecraft standards.
- The tradecraft standards for analytic products have been refined over the past ten years. These standards include describing sources (including their reliability and access to the information they provide), clearly expressing uncertainty, distinguishing between underlying information and analysts' judgments and assumptions, exploring alternatives, demonstrating relevance to the customer, using strong and transparent logic, and explaining change or consistency in judgments over time.
- Applying these standards helps ensure that the Intelligence Community provides US policymakers, warfighters, and operators with the best and most accurate insight, warning, and context, as well as potential opportunities to advance US national security.

Intelligence Community analysts integrate information from a wide range of sources, including human sources, technical collection, and open source information, and apply specialized skills and structured analytic tools to draw inferences informed by the data available, relevant past activity, and logic and reasoning to provide insight into what is happening and the prospects for the future.

- A critical part of the analyst's task is to explain uncertainties associated with major judgments based on the quantity and quality of the source material, information gaps, and the complexity of the issue.
- When Intelligence Community analysts use words such as "we assess" or "we judge," they are conveying an analytic assessment or judgment.
- Some analytic judgments are based directly on collected information; others rest on previous judgments, which serve as building blocks in rigorous analysis. In either type of judgment, the tradecraft standards outlined above ensure that analysts have an appropriate basis for the judgment.

- Intelligence Community judgments often include two important elements: judgments of how likely it is that something has happened or will happen (using terms such as "likely" or "unlikely") and confidence levels in those judgments (low, moderate, and high) that refer to the evidentiary basis, logic and reasoning, and precedents that underpin the judgments.

Determining Attribution in Cyber Incidents

The nature of cyberspace makes attribution of cyber operations difficult but not impossible. Every kind of cyber operation—malicious or not—leaves a trail. US Intelligence Community analysts use this information, their constantly growing knowledge base of previous events and known malicious actors, and their knowledge of how these malicious actors work and the tools that they use, to attempt to trace these operations back to their source. In every case, they apply the same tradecraft standards described in the Analytic Process above.

- Analysts consider a series of questions to assess how the information compares with existing knowledge and adjust their confidence in their judgments as appropriate to account for any alternative hypotheses and ambiguities.

- An assessment of attribution usually is not a simple statement of who conducted an operation, but rather a series of judgments that describe whether it was an isolated incident, who was the likely perpetrator, that perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation.

This marks is a declassified version of a highly classified assessment. Its conclusions are identical for those in the highly classified assessment but this version does not include the full supporting information or key elements of the collection sensitive.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE · NATIONAL INTELLIGENCE COUNCIL

ICA

INTELLIGENCE COMMUNITY ASSESSMENT

Assessing Russian Activities and Intentions in Recent US Elections

ICA 2017-01D | 6 January 2017

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Scope and Sourcing

Information available as of 29 December 2016 was used in the preparation of this product.

Scope

This report includes an analytic assessment drafted and coordinated among The Central Intelligence Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), which draws on intelligence information collected and disseminated by those three agencies. It covers the motivation and scope of Moscow's intentions regarding US elections and Moscow's use of cyber tools and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the 2016 US presidential election and draws on our understanding of previous Russian influence operations. When we use the term "we" it refers to an assessment by all three agencies.

- This report is a declassified version of a highly classified assessment. This document's conclusions are identical to the highly classified assessment, but this document does not include the full supporting information, including specific intelligence on key elements of the influence campaign. Given the redactions, we made minor edits purely for readability and flow.

We did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election. The US Intelligence Community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze US political processes or US public opinion.

- New information continues to emerge, providing increased insight into Russian activities.

Sourcing

Many of the key judgments in this assessment rely on a body of reporting from multiple sources that are consistent with our understanding of Russian behavior. Insights into Russian efforts—including specific cyber operations—and Russian views of key US players derive from multiple corroborating sources.

Some of our judgments about Kremlin preferences and intent are drawn from the behavior of Kremlin-loyal political figures, state media, and pro-Kremlin social media actors, all of whom the Kremlin either directly uses to convey messages or who are answerable to the Kremlin. The Russian leadership invests significant resources in both foreign and domestic propaganda and places a premium on transmitting what it views as consistent, self-reinforcing narratives regarding its desires and redlines, whether on Ukraine, Syria, or relations with the United States.

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Assessing Russian Activities and Intentions in Recent US Elections

ICA 2017-01D
6 January 2017

Key Judgments

Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.

We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.

- **We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him.** All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

- Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency.

- Further information has come to light since Election Day that, when combined with Russian behavior since early November 2016, increases our confidence in our assessments of Russian motivations and goals.

Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls." Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.

- Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties.

- We assess with high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks.

- Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. **DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.**

- Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences.

We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes.

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Contents

Scope and Sourcing i
Key Judgments ii
Contents iv

CIA/FBI/NSA Assessment: Russia's Influence Campaign Targeting the 2016 US Presidential Election

Putin Ordered Campaign To Influence US Election 1

Russian Campaign Was Multifaceted 2

Influence Effort Was Boldest Yet in the US 5

Election Operation Signals "New Normal" in Russian Influence Efforts 5

Annexes

A: Russia—Kremlin's TV Seeks To Influence Politics, Fuel Discontent in US 6
B: Estimative Language 13

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Russia's Influence Campaign Targeting the 2016 US Presidential Election

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Russia's Influence Campaign Targeting the 2016 US Presidential Election

Putin Ordered Campaign To Influence US Election

We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign then focused on undermining her expected presidency.

- We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.
- In trying to influence the US election, we assess the Kremlin sought to advance its longstanding desire to undermine the US-led liberal democratic order, the promotion of which Putin and other senior Russian leaders view as a threat to Russia and Putin's regime.
- Putin publicly pointed to the Panama Papers disclosure and the Olympic doping scandal as US-directed efforts to defame Russia, suggesting he sought to use disclosures to discredit the image of the United States and cast it as hypocritical.
- Putin most likely wanted to discredit Secretary Clinton because he has publicly blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him.

We assess Putin, his advisers, and the Russian Government developed a clear preference for President-elect Trump over Secretary Clinton.

- Beginning in June, Putin's public comments about the US presidential race avoided directly praising President-elect Trump, probably because Kremlin officials thought that any praise from Putin personally would backfire in the United States. Nonetheless, Putin publicly indicated a preference for President-elect Trump's stated policy to work with Russia, and pro-Kremlin figures spoke highly about what they saw as his Russia-friendly positions on Syria and Ukraine. Putin publicly contrasted the President-elect's approach to Russia with Secretary Clinton's "aggressive rhetoric."
- Moscow also saw the election of President-elect Trump as a way to achieve an international counterterrorism coalition against the Islamic State in Iraq and the Levant (ISIL).
- Putin has had many positive experiences working with Western political leaders whose business interests made them more disposed to deal with Russia, such as former Italian Prime Minister Silvio Berlusconi and former German Chancellor Gerhard Schroeder.
- Putin, Russian officials, and other pro-Kremlin pundits stopped publicly criticizing the US election process as unfair almost immediately

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

after the election because Moscow probably assessed it would be counterproductive to building positive relations.

We assess the influence campaign aspired to help President-elect Trump's chances of victory when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to the President-elect. When it appeared to Moscow that Secretary Clinton was likely to win the presidency the Russian influence campaign focused more on undercutting Secretary Clinton's legitimacy and crippling her presidency from its start, including by impugning the fairness of the election.

- Before the election, Russian diplomats had publicly denounced the US electoral process and were prepared to publicly call into question the validity of the results. Pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity.

Russian Campaign Was Multifaceted

Moscow's use of disclosures during the US election was unprecedented, but its influence campaign otherwise followed a longstanding Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."

- We assess that influence campaigns are approved at the highest levels of the Russian Government—particularly those that would be politically sensitive.

- Moscow's campaign aimed at the US election reflected years of investment in its capabilities, which Moscow has honed in the former Soviet states.

- By their nature, Russian influence campaigns are multifaceted and designed to be deniable because they use a mix of agents of influence, cutouts, front organizations, and false-flag operations. Moscow demonstrated this during the Ukraine crisis in 2014, when Russia deployed forces and advisers to eastern Ukraine and denied it publicly.

The Kremlin's campaign aimed at the US election featured disclosures of data obtained through Russian cyber operations; intrusions into US state and local electoral boards; and overt propaganda. Russian intelligence collection both informed and enabled the influence campaign.

Cyber Espionage Against US Political Organizations. Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties.

We assess Russian intelligence services collected against the US primary campaigns, think tanks, and lobbying groups they viewed as likely to shape future US policies. In July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016.

- The General Staff Main Intelligence Directorate (GRU) probably began cyber operations aimed at the US election by March 2016. We assess that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political figures. By May, the GRU had exfiltrated large volumes of data from the DNC.

Public Disclosures of Russian-Collected Data. We assess with high confidence that the GRU used the Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks to release US victim data obtained in

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

cyber operations publicly and in exclusives to media outlets.

- Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his likely Russian identity throughout the election. Press reporting suggests more than one person claiming to be Guccifer 2.0 interacted with journalists.
- Content that we assess was taken from e-mail accounts targeted by the GRU in March 2016 appeared on DCLeaks.com starting in June.

We assess with high confidence that the GRU relayed material it acquired from the DNC and senior Democratic officials to WikiLeaks. Moscow most likely chose WikiLeaks because of its self-proclaimed reputation for authenticity. Disclosures through WikiLeaks did not contain any evident forgeries.

- In early September, Putin said publicly it was important the DNC data was exposed to WikiLeaks, calling the search for the source of the leaks a distraction and denying Russian "state-level" involvement.
- The Kremlin's principal international propaganda outlet RT (formerly Russia Today) has actively collaborated with WikiLeaks. RT's editor-in-chief visited WikiLeaks founder Julian Assange at the Ecuadorian Embassy in London in August 2013, where they discussed renewing his broadcast contract with RT, according to Russian and Western media. Russian media subsequently announced that RT had become "the only Russian media company" to partner with WikiLeaks and had received access to "new leaks of secret information." RT routinely gives Assange sympathetic coverage and provides him a platform to denounce the United States.

These election-related disclosures reflect a pattern of Russian intelligence using hacked information in targeted influence efforts against targets such as Olympic athletes and other foreign governments. Such efforts have included releasing or altering personal data, defacing websites, or releasing e-mails.

- A prominent target since the 2016 Summer Olympics has been the World Anti-Doping Agency (WADA), with leaks that we assess to have originated with the GRU and that have involved data on US athletes.

Russia collected on some Republican-affiliated targets but did not conduct a comparable disclosure campaign.

Russian Cyber Intrusions Into State and Local Electoral Boards. Russian intelligence accessed elements of multiple state or local electoral boards. Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment.

- DHS assesses that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying.

Russian Propaganda Efforts. Russia's state-run propaganda machine—comprised of its domestic media apparatus, outlets targeting global audiences such as RT and Sputnik, and a network of quasi-government trolls—contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences. State-owned Russian media made increasingly favorable comments about President-elect Trump as the 2016 US general and primary election campaigns progressed while consistently offering negative coverage of Secretary Clinton.

- Starting in March 2016, Russian Government–linked actors began openly supporting President-elect Trump's candidacy in media

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

aimed at English-speaking audiences. RT and Sputnik—another government-funded outlet producing pro-Kremlin radio and online content in a variety of languages for international audiences—consistently cast President-elect Trump as the target of unfair coverage from traditional US media outlets that they claimed were subservient to a corrupt political establishment.

- Russian media hailed President-elect Trump's victory as a vindication of Putin's advocacy of global populist movements—the theme of Putin's annual conference for Western academics in October 2016—and the latest example of Western liberalism's collapse.
- Putin's chief propagandist Dmitriy Kiselev used his flagship weekly newsmagazine program this fall to cast President-elect Trump as an outsider victimized by a corrupt political establishment and faulty democratic election process that aimed to prevent his election because of his desire to work with Moscow.
- Pro-Kremlin proxy Vladimir Zhirinovskiy, leader of the nationalist Liberal Democratic Party of Russia, proclaimed just before the election that if President-elect Trump won, Russia would "drink champagne" in anticipation of being able to advance its positions on Syria and Ukraine.

RT's coverage of Secretary Clinton throughout the US presidential campaign was consistently negative and focused on her leaked e-mails and accused her of corruption, poor physical and mental health, and ties to Islamic extremism. Some Russian officials echoed Russian lines for the influence campaign that Secretary Clinton's election could lead to a war between the United States and Russia.

- In August, Kremlin-linked political analysts suggested avenging negative Western reports on Putin by airing segments devoted to Secretary Clinton's alleged health problems.
- On 6 August, RT published an English-language video called "Julian Assange Special: Do WikiLeaks Have the E-mail That'll Put Clinton in Prison?" and an exclusive interview with Assange entitled "Clinton and ISIS Funded by the Same Money." RT's most popular video on Secretary Clinton, "How 100% of the Clintons' 'Charity' Went to...Themselves," had more than 9 million views on social media platforms. RT's most popular English language video about the President-elect, called "Trump Will Not Be Permitted To Win," featured Assange and had 2.2 million views.
- For more on Russia's past media efforts—including portraying the 2012 US electoral process as undemocratic—please see Annex A: Russia—Kremlin's TV Seeks To Influence Politics, Fuel Discontent in US.

Russia used trolls as well as RT as part of its influence efforts to denigrate Secretary Clinton. This effort amplified stories on scandals about Secretary Clinton and the role of WikiLeaks in the election campaign.

- The likely financier of the so-called Internet Research Agency of professional trolls located in Saint Petersburg is a close Putin ally with ties to Russian intelligence.
- A journalist who is a leading expert on the Internet Research Agency claimed that some social media accounts that appear to be tied to Russia's professional trolls—because they previously were devoted to supporting Russian actions in Ukraine—started to advocate for President-elect Trump as early as December 2015.

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Influence Effort Was Boldest Yet in the US

Russia's effort to influence the 2016 US presidential election represented a significant escalation in directness, level of activity, and scope of effort compared to previous operations aimed at US elections. We assess the 2016 influence campaign reflected the Kremlin's recognition of the worldwide effects that mass disclosures of US Government and other private data—such as those conducted by WikiLeaks and others—have achieved in recent years, and their understanding of the value of orchestrating such disclosures to maximize the impact of compromising information.

- During the Cold War, the Soviet Union used intelligence officers, influence agents, forgeries, and press placements to disparage candidates perceived as hostile to the Kremlin, according to a former KGB archivist.

Since the Cold War, Russian intelligence efforts related to US elections have primarily focused on foreign intelligence collection. For decades, Russian and Soviet intelligence services have sought to collect insider information from US political parties that could help Russian leaders understand a new US administration's plans and priorities.

- The Russian Foreign Intelligence Service (SVR) Directorate S (Illegals) officers arrested in the United States in 2010 reported to Moscow about the 2008 election.
- In the 1970s, the KGB recruited a Democratic Party activist who reported information about then-presidential hopeful Jimmy Carter's campaign and foreign policy plans, according to a former KGB archivist.

Election Operation Signals "New Normal" in Russian Influence Efforts

We assess Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide, including against US allies and their election processes. We assess the Russian intelligence services would have seen their election influence campaign as at least a qualified success because of their perceived ability to impact public discussion.

- Putin's public views of the disclosures suggest the Kremlin and the intelligence services will continue to consider using cyber-enabled disclosure operations because of their belief that these can accomplish Russian goals relatively easily without significant damage to Russian interests.
- Russia has sought to influence elections across Europe.

We assess Russian intelligence services will continue to develop capabilities to provide Putin with options to use against the United States, judging from past practice and current efforts. Immediately after Election Day, we assess Russian intelligence began a spearphishing campaign targeting US Government employees and individuals associated with US think tanks and NGOs in national security, defense, and foreign policy fields. This campaign could provide material for future influence efforts as well as foreign intelligence collection on the incoming administration's goals and plans.

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Annex A

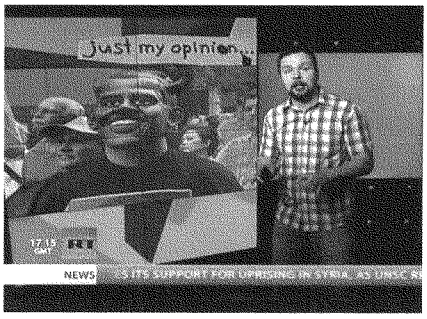
Russia* -- Kremlin's TV Seeks To Influence Politics, Fuel Discontent in US

RT America TV, a Kremlin-financed channel operated from within the United States, has substantially expanded its repertoire of programming that highlights criticism of alleged US shortcomings in democracy and civil liberties. The rapid expansion of RT's operations and budget and recent candid statements by RT's leadership point to the channel's importance to the Kremlin as a messaging tool and indicate a Kremlin-directed campaign to undermine faith in the US Government and fuel political protest. The Kremlin has committed significant resources to expanding the channel's reach, particularly its social media footprint. A reliable UK report states that RT recently was the most-watched foreign news channel in the UK. RT America has positioned itself as a domestic US channel and has deliberately sought to obscure any legal ties to the Russian Government.

In the runup to the 2012 US presidential election in November, English-language channel RT America -- created and financed by the Russian Government and part of Russian Government-sponsored RT TV (see textbox 1) -- intensified its usually critical coverage of the United States. The channel portrayed the US electoral process as undemocratic and featured calls by US protesters for the public to rise up and "take this government back."

- RT introduced two new shows -- "Breaking the Set" on 4 September and "Truthseeker" on 2 November -- both overwhelmingly focused on criticism of US and Western governments as well as the promotion of radical discontent.

- From August to November 2012, RT ran numerous reports on alleged US election fraud and voting machine vulnerabilities, contending that US election results cannot be trusted and do not reflect the popular will.



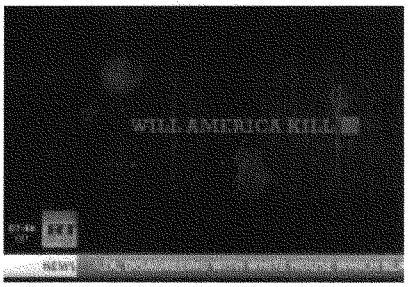
Messaging on RT prior to the US presidential election (RT, 3 November)

- In an effort to highlight the alleged "lack of democracy" in the United States, RT broadcast, hosted, and advertised third-party candidate debates and ran reporting supportive of the political agenda of these candidates. The RT hosts asserted that the US two-party system does not represent the views of at least one-third of the population and is a "sham."

* This annex was originally published on 11 December 2012 by the Open Source Center, now the Open Source Enterprise.

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

- RT aired a documentary about the Occupy Wall Street movement on 1, 2, and 4 November. RT framed the movement as a fight against "the ruling class" and described the current US political system as corrupt and dominated by corporations. RT advertising for the documentary featured Occupy movement calls to "take back" the government. The documentary claimed that the US system cannot be changed democratically, but only through "revolution." After the 6 November US presidential election, RT aired a documentary called "Cultures of Protest," about active and often violent political resistance (RT, 1-10 November).



RT new show "Truthseeker" (RT, 11 November)

RT Conducts Strategic Messaging for Russian Government

RT's criticism of the US election was the latest facet of its broader and longer-standing anti-US messaging likely aimed at undermining viewers' trust in US democratic procedures and undercutting US criticism of Russia's political system. RT Editor in Chief Margarita Simonyan recently declared that the United States itself lacks democracy and that it has "no moral right to teach the rest of the world" (*Kommersant*, 6 November).

- Simonyan has characterized RT's coverage of the Occupy Wall Street movement as "information warfare" that is aimed at promoting popular dissatisfaction with the US Government. RT created a *Facebook* app to connect Occupy Wall Street protesters via social media. In addition, RT featured its own hosts in Occupy rallies ("Minaev Live," 10 April; RT, 2, 12 June).

- RT's reports often characterize the United States as a "surveillance state" and allege widespread infringements of civil liberties, police brutality, and drone use (RT, 24, 28 October, 1-10 November).

Simonyan steps over the White House in the introduction from her short-lived domestic show on REN TV (REN TV, 26 December 2011)

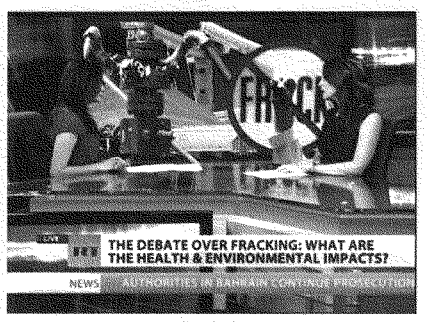
- RT has also focused on criticism of the US economic system, US currency policy, alleged Wall Street greed, and the US national debt. Some of RT's hosts have compared the United States to Imperial Rome and have predicted that government corruption and "corporate greed" will lead to US financial collapse (RT, 31 October, 4 November).

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

RT broadcasts support for other Russian interests in areas such as foreign and energy policy.

- RT runs anti-fracking programming, highlighting environmental issues and the impacts on public health. This is likely reflective of the Russian Government's concern about the impact of fracking and US natural gas production on the global energy market and the potential challenges to Gazprom's profitability (5 October).

- RT is a leading media voice opposing Western intervention in the Syrian conflict and blaming the West for waging "information wars" against the Syrian Government (RT, 10 October-9 November).



RT anti-fracking reporting (RT, 5 October)

- In an earlier example of RT's messaging in support of the Russian Government, during the Georgia-Russia military conflict the channel accused Georgians of killing civilians and organizing a genocide of the Ossetian people. According to Simonyan, when "the Ministry of Defense was at war with Georgia," RT was "waging an information war against the entire Western world" (*Kommersant*, 11 July).

In recent interviews, RT's leadership has candidly acknowledged its mission to expand its US audience and to expose it to Kremlin messaging. However, the leadership rejected claims that RT interferes in US domestic affairs.

- Simonyan claimed in popular arts magazine *Afisha* on 3 October: "It is important to have a channel that people get used to, and then, when needed, you show them what you need to show. In some sense, not having our own foreign broadcasting is the same as not having a ministry of defense. When there is no war, it looks like we don't need it. However, when there is a war, it is critical."

- According to Simonyan, "the word 'propaganda' has a very negative connotation, but indeed, there is not a single international foreign TV channel that is doing something other than promotion of the values of the country that it is broadcasting from." She added that "when Russia is at war, we are, of course, on Russia's side" (*Afisha*, 3 October; *Kommersant*, 4 July).

- TV-Novosti director Nikolov said on 4 October to the Association of Cable Television that RT builds on worldwide demand for "an alternative view of the entire world." Simonyan asserted on 3 October in *Afisha* that RT's goal is "to make an alternative channel that shares information unavailable elsewhere" in order to "conquer the audience" and expose it to Russian state messaging (*Afisha*, 3 October; *Kommersant*, 4 July).

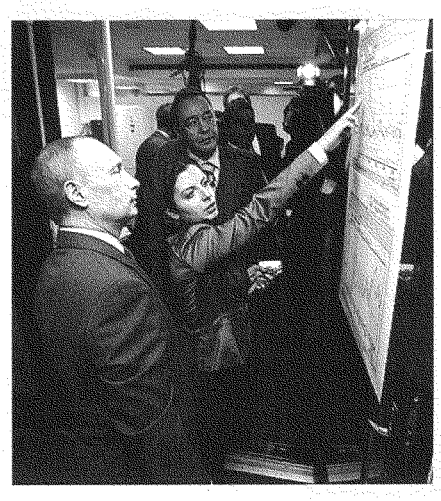
- On 26 May, Simonyan tweeted with irony: "Ambassador McFaul hints that our channel is interference with US domestic affairs. And we, sinful souls, were thinking that it is freedom of speech."

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

RT Leadership Closely Tied to, Controlled by Kremlin

RT Editor in Chief Margarita Simonyan has close ties to top Russian Government officials, especially Presidential Administration Deputy Chief of Staff Aleksey Gromov, who reportedly manages political TV coverage in Russia and is one of the founders of RT.

- Simonyan has claimed that Gromov shielded her from other officials and their requests to air certain reports. Russian media consider Simonyan to be Gromov's protege (*Kommersant*, 4 July; Dozhd TV, 11 July).
- Simonyan replaced Gromov on state-owned Channel One's Board of Directors. Government officials, including Gromov and Putin's Press Secretary Peskov were involved in creating RT and appointing Simonyan (*Afisha*, 3 October).
- According to Simonyan, Gromov oversees political coverage on TV, and he has periodic meetings with media managers where he shares classified information and discusses their coverage plans. Some opposition journalists, including Andrey Loshak, claim that he also ordered media attacks on opposition figures (*Kommersant*, 11 July).



*Simonyan shows RT facilities to then Prime Minister Putin. Simonyan was on Putin's 2012 presidential election campaign staff in Moscow (*Rospress, *22 September 2010,* Ria Novosti, *25 October 2012).*

The Kremlin staffs RT and closely supervises RT's coverage, recruiting people who can convey Russian strategic messaging because of their ideological beliefs.

- The head of RT's Arabic-language service, Aydar Aganin, was rotated from the diplomatic service to manage RT's Arabic-language expansion, suggesting a close relationship between RT and Russia's foreign policy apparatus. RT's London Bureau is managed by Darya Pushkova, the daughter of Aleksey Pushkov, the current chair of the Duma Russian Foreign Affairs Committee and a former Gorbachev speechwriter (*DXB*, 26 March 2009; *MK.ru*, 13 March 2006).
- According to Simonyan, the Russian Government sets rating and viewership requirements for RT and, "since RT receives budget from the state, it must complete tasks given by the state." According to Nikolov, RT news stories are written and edited "to become news" exclusively in RT's Moscow office (Dozhd TV, 11 July; *AKT*, 4 October).
- In her interview with pro-Kremlin journalist Sergey Minaev, Simonyan complimented RT staff in the United States for passionately defending Russian positions on the air and in social media. Simonyan said: "I wish you could see...how these guys, not just on air, but on their own social networks, *Twitter*, and when giving interviews, how they defend the positions that we stand on!" ("Minaev Live," 10 April).

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

RT Focuses on Social Media, Building Audience

RT aggressively advertises its social media accounts and has a significant and fast-growing social media footprint. In line with its efforts to present itself as anti-mainstream and to provide viewers alternative news content, RT is making its social media operations a top priority, both to avoid broadcast TV regulations and to expand its overall audience.

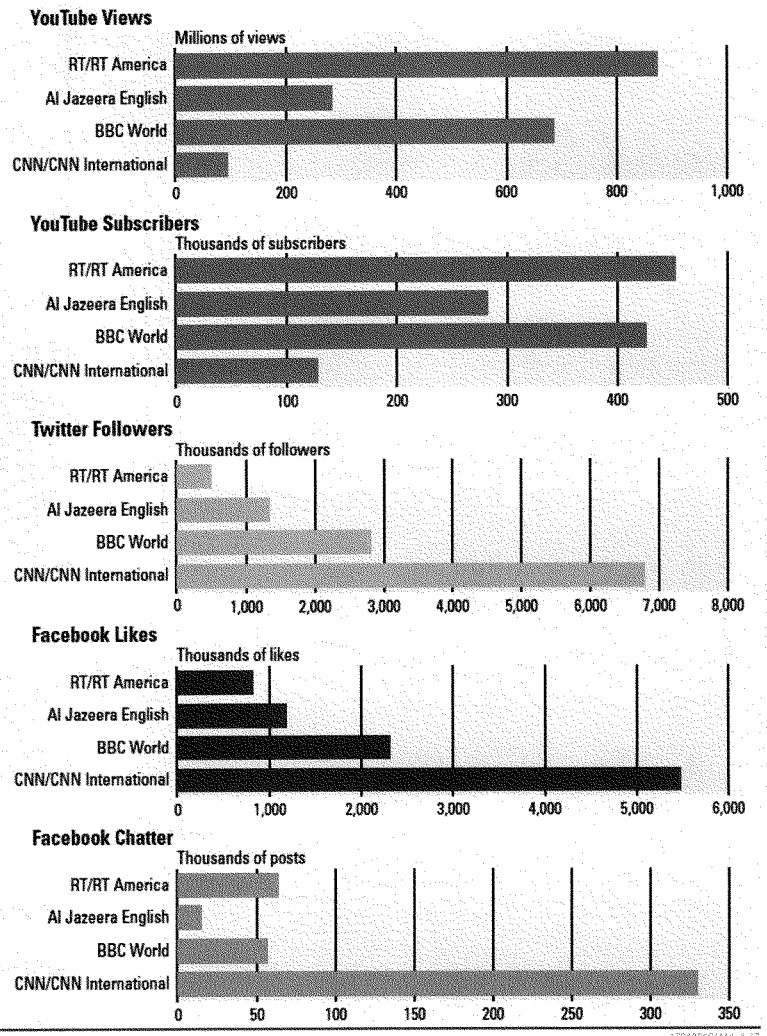
- According to RT management, RT's website receives at least 500,000 unique viewers every day. Since its inception in 2005, RT videos received more than 800 million views on *YouTube* (1 million views per day), which is the highest among news outlets (see graphics for comparison with other news channels) (*AKT*, 4 October).
- According to Simonyan, the TV audience worldwide is losing trust in traditional TV broadcasts and stations, while the popularity of "alternative channels" like RT or Al Jazeera grows. RT markets itself as an "alternative channel" that is available via the Internet everywhere in the world, and it encourages interaction and social networking (*Kommersant*, 29 September).
- According to Simonyan, RT uses social media to expand the reach of its political reporting and uses well-trained people to monitor public opinion in social media commentaries (*Kommersant*, 29 September).
- According to Nikolov, RT requires its hosts to have social media accounts, in part because social media allows the distribution of content that would not be allowed on television (*Newreporter.org*, 11 October).
- Simonyan claimed in her 3 October interview to independent TV channel Dozhd that Occupy Wall Street coverage gave RT a significant audience boost.

The Kremlin spends $190 million a year on the distribution and dissemination of RT programming, focusing on hotels and satellite, terrestrial, and cable broadcasting. The Kremlin is rapidly expanding RT's availability around the world and giving it a reach comparable to channels such as Al Jazeera English. According to Simonyan, the United Kingdom and the United States are RT's most successful markets. RT does not, however, publish audience information.

- According to market research company Nielsen, RT had the most rapid growth (40 percent) among all international news channels in the United States over the past year (2012). Its audience in New York tripled and in Washington DC grew by 60% (*Kommersant*, 4 July).
- RT claims that it is surpassing Al Jazeera in viewership in New York and Washington DC (*BARB*, 20 November; RT, 21 November).
- RT states on its website that it can reach more than 550 million people worldwide and 85 million people in the United States; however, it does not publicize its actual US audience numbers (RT, 10 December).

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

TV News Broadcasters: Comparative Social Media Footprint



This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Formal Disassociation From Kremlin Facilitates RT US Messaging

RT America formally disassociates itself from the Russian Government by using a Moscow-based autonomous nonprofit organization to finance its US operations. According to RT's leadership, this structure was set up to avoid the Foreign Agents Registration Act and to facilitate licensing abroad. In addition, RT rebranded itself in 2008 to deemphasize its Russian origin.

- According to Simonyan, RT America differs from other Russian state institutions in terms of ownership, but not in terms of financing. To disassociate RT from the Russian Government, the federal news agency RIA Novosti established a subsidiary autonomous nonprofit organization, TV-Novosti, using the formal independence of this company to establish and finance RT worldwide (Dozhd TV, 11 July).

- Nikolov claimed that RT is an "autonomous noncommercial entity," which is "well received by foreign regulators" and "simplifies getting a license." Simonyan said that RT America is not a "foreign agent" according to US law because it uses a US commercial organization for its broadcasts (*AKT*, 4 October; Dozhd TV, 11 July).

- Simonyan observed that RT's original Russia-centric news reporting did not generate sufficient audience, so RT switched to covering international and US domestic affairs and removed the words "Russia Today" from the logo "to stop scaring away the audience" (*Afisha*, 18 October; *Kommersant*, 4 July).

- RT hires or makes contractual agreements with Westerners with views that fit its agenda and airs them on RT. Simonyan said on the pro-Kremlin show "Minaev Live" on 10 April that RT has enough audience and money to be able to choose its hosts, and it chooses the hosts that "think like us," "are interested in working in the anti-mainstream," and defend RT's beliefs on social media. Some hosts and journalists do not present themselves as associated with RT when interviewing people, and many of them have affiliations to other media and activist organizations in the United States ("Minaev Live," 10 April).

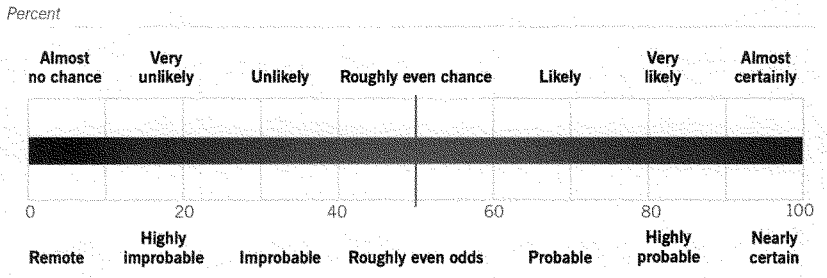
This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

Annex B

ESTIMATIVE LANGUAGE

Estimative language consists of two elements: judgments about the likelihood of developments or events occurring and levels of confidence in the sources and analytic reasoning supporting the judgments. Judgments are not intended to imply that we have proof that shows something to be a fact. Assessments are based on collected information, which is often incomplete or fragmentary, as well as logic, argumentation, and precedents.

Judgments of Likelihood. The chart below approximates how judgments of likelihood correlate with percentages. Unless otherwise stated, the Intelligence Community's judgments are not derived via statistical analysis. Phrases such as "we judge" and "we assess"—and terms such as "probable" and "likely"—convey analytical assessments.



Confidence in the Sources Supporting Judgments. Confidence levels provide assessments of the quality and quantity of the source information that supports judgments. Consequently, we ascribe high, moderate, or low levels of confidence to assessments:

- **High confidence** generally indicates that judgments are based on high-quality information from multiple sources. High confidence in a judgment does not imply that the assessment is a fact or a certainty; such judgments might be wrong.
- **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- **Low confidence** generally means that the information's credibility and/or plausibility is uncertain, that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that reliability of the sources is questionable.

Chairman BURR. Director, thank you for that thorough and concise testimony.

Director Clapper, as I stated in my opening statement, I've instructed a select group of Committee staff to complete an independent and bipartisan review of the reporting that underpins the intelligence community assessment before us today. Do I have your assurance that you will provide the access that they need to the reporting necessary to make their conclusions?

Director CLAPPER. Yes.

Chairman BURR. Director Comey, let me talk about forensics for just a minute, because the FBI has the expertise there. I know there's tremendous investigative value when the FBI is actually able to conduct their own forensics review on devices that have suffered cyber intrusions and attacks.

I believe there's some confusion, though, or at least some conflicting reporting as to whether the FBI requested access to the DNC's services, the Democratic Congressional Committee servers, and John Podesta's personal devices. Did the FBI request access to those devices to perform forensics on them?

Director COMEY. Yes, we did.

Chairman BURR. Would that access have provided intelligence or information helpful to your investigation and possibly to the findings included in the intelligence community assessments?

Director COMEY. Our forensics folks would always prefer to get access to the original device or server that's involved. So it's the best evidence.

Chairman BURR. Were you given access to do the forensics on those servers?

Director COMEY. We were not. A highly respected private company eventually got access and shared with us what they saw there.

Chairman BURR. But is that typically the way the FBI would prefer to do the forensics, or would your forensics unit rather see the servers and do the forensics themselves?

Director COMEY. We'd always prefer to have access hands-on ourselves if that's possible.

Chairman BURR. Do you know why you were denied access to those servers?

Director COMEY. I don't know for sure. I don't know for sure.

Chairman BURR. Was there one request or multiple requests?

Director COMEY. Multiple requests at different levels, and ultimately what was agreed to is the private company would share with us what they saw.

Chairman BURR. There has been much debate over the content released by WikiLeaks, Director Clapper—I should say DCLeaks—and what the intentions were behind those disclosures. Director Clapper, you made it perfectly clear in your testimony that the community feels that vote tallies were not altered.

Director CLAPPER. That's correct.

Chairman BURR. Do you believe there's any evidence that the DNC or the DCCC or the Podesta emails released publicly were altered in any way?

Director CLAPPER. We have no evidence of that.

Chairman BURR. Director Comey, do you have any intelligence that any Republican system that was targeted by these same groups was either successfully penetrated or, if penetrated and there was data exfiltrated, was there any exfiltration?

Director COMEY. There were successful penetrations of some groups and campaigns, particularly at the State level, on the Republican side of the aisle, and some limited penetration of old Republican National Committee domains.

Chairman BURR. Penetrations of those National Committee domains?

Director COMEY. Right, that were no longer in use.

Chairman BURR. From the standpoint of Republican candidates that were running for President, were those campaigns, any of those campaigns, targeted under this same effort by the Russians?

Director COMEY. The campaigns themselves, not to my knowledge.

Chairman BURR. Okay.

Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

Again, let me thank you, Director Clapper, for your report and the point that you continue to make, that it was not your job to analyze the effects in terms of the political campaign. I would add that any of us who are up here who've ever been through a close election, it means that any small item can be cause for harm.

I want to follow up on where the Chairman was headed. Director Comey, there was some information, though, that was taken from Republican-affiliated entities. There was a great deal of information taken from Democrats. There was selective leaking with, as the Director has indicated, with clear political intent in the process.

One of the things that I'm a little flabbergasted at is that somehow this is viewed by some as in their rear-view mirror. Don't the Russians have the capability of taking, even if it's old information about Republicans or other information about Democrats, and selectively leak that prospectively?

Director COMEY. Sure.

Vice Chairman WARNER. And could you describe—to my mind, this is not only one of the most significant items I've seen in my political life, but this is an ongoing threat to all of us and our electoral process. We have to be on guard, and could you speak for, or any other member of the panel speak to, the fact that—do you expect to see similar tactics used by Russians in terms of the upcoming elections in Germany, France, and The Netherlands?

Director CLAPPER. Yes, we do.

Vice Chairman WARNER. And are our allies taking what's happened in America with significant enough importance and are they putting up new defenses trying to guard against these activities?

Director CLAPPER. I can't say—at least I can't; maybe others can here—the extent to which they have reacted to this. But they are certainly aware. Europe has long been a target of Russian attempts to manipulate electoral processes. So they will continue with that. And certainly because of the controversy that's generated in our country, I think that will reinforce their desire to do that.

Vice Chairman WARNER. One of the things that actually another Member of the Committee raised is, certain Russian activities,

against just to note the seriousness, not only retrospectively but prospectively, that I believe there was a Russian dissident in London where Russian agents in effect planted false information in this individual's personal file and then called law enforcement and said: Look in this person's file, and there was child pornography placed there.

Could you anticipate at some time Russia trying, if we don't take more aggressive actions, trying those actions against American public officials?

Director CLAPPER. The Russians I think, while they have no compunction about using the full array of tools and techniques available in their kitbag. So I wouldn't put it past them to do that or any other tools they've used, such as paying people to participate in social media, for example.

Vice Chairman WARNER. This has been described as in effect the new normal for Russian doctrine; is that correct?

Director CLAPPER. I believe, yes.

Vice Chairman WARNER. And again, we've seen our system, your words, "a significant escalation." Before us we have people with service in the IC and the defense of our Nation for hundreds of years. I'd like to just go down the line. In any of your careers, have you ever seen this level of Russian interference in our political process? We'll start with Director Comey and just go down the line.

Director COMEY. No.

Director CLAPPER. I have not.

Director BRENNAN. No.

Admiral ROGERS. No.

Vice Chairman WARNER. I know we've got a lot of Members. Thank you, Mr. Chairman.

Chairman BURR. Senator Rubio.

Senator RUBIO. Thank you.

Let me begin by saying I don't believe this thing has anything to do with—well, let me just begin by saying, and I think the Chairman's already asked, it's clear that there was no hacking of voting machines and the changes of tallies. I would argue this has nothing even to—because this term "hacking" is thrown around and it makes it sound like some sort of cyber-specific situation.

That cyber tools were used as a means to an end. It isn't necessarily what we should be focused on here. What we're talking about here is active measures, the active measures taken by the government of Vladimir Putin to influence and to potentially manipulate American public opinion for the purpose of discrediting individual political figures, sowing chaos and division in our politics, sowing doubts about the legitimacy of our elections.

So if you look at the situation we now face, here's the aftermath: We had an election where, after some intrusions into some State databases, there was a leading—one nominee for President warning about fraud in the election. Then after the election we have some on the other side questioning the legitimacy of the President-elect because of Russian interference. And we have the President-elect questioning the credibility of the intelligence community because of its findings.

This sounds like a pretty effective and successful effort to sow chaos, to undermine credibility of our leaders and of our govern-

ment institutions. In essence, it sounds like they achieved what they wanted, to get us to fight against each other over whether our elections were legitimate and divide us in the way that it sows the sort of chaos that they sought to achieve.

My question is along the lines of what Senator Warner asked about a moment ago, because we've seen these active measures employed in the Baltic States, with Russian-speaking media outlets controlled by the Kremlin, in the Dutch referendum, in the Brexit vote, in the Italian referendum.

So let me lay out a hypothetical and you tell me if this is the kind of scenario we could face, because they don't limit this to elections. They target individual policymakers throughout many countries in Europe, particularly those in the former Soviet sphere. Hypothetically, imagine that there's a U.S. Senator or Congressman who adopts a policy position that the Kremlin does not agree with. So somehow through a phishing expedition they gain access to your personal computer network, and once they gain access to your personal computer network they use it to fabricate and/or actually conduct—you used the child pornography example; I'd say let's say money-laundering activity. Then they call law enforcement and tip them off: Congressman John So-and-So has been money laundering. And they go into your home, they seize your computer, and sure enough, it's sitting there on your network because someone got into it and did it. Now you're arrested and you're charged and you're removed from the public discourse.

Is this not what we have seen, the tactics that have been employed by Russian intelligence on behalf of the government of Vladimir Putin in other countries around the world? Is that not a tactic they have used to discredit individual political figures? And isn't it true that that could very well happen here in the United States?

Director CLAPPER. It is certainly well within both their technical competence and their potential intent to do things like that. The last two years running in my threat presentations, I've cited I think the next worrisome trend in the cyber business will be the compromise of the fidelity of information, and whether it's for a criminal purpose or a political purpose. So this is well within the realm, I think, of possibility.

Senator RUBIO. In the context of what their goals were, ultimately their ultimate goal—they may have or not—I don't get into the whole thing of who they wanted to see win. But in the end what they really wanted to see was Americans fighting against each other, bickering over these things, having questions about the legitimacy of the process, our leaders, etcetera.

Was that not their goal? And if it was, have they not largely achieved that, based on how this issue has been discussed since the aftermath of the election?

Director CLAPPER. I think in the first instance that was their goal. First, as I said in my prepared remarks, was to sow doubt about the efficacy of our system and to cast aspersions on our political system.

Senator RUBIO. To create doubt about the credibility of our elections, the legitimacy of our leaders, etcetera?

Director CLAPPER. All that, yes.

Senator RUBIO. So my last point is, the last time I checked Vladimir Putin is neither a registered Democrat nor a registered Republican. So what he is interested in is achieving these measures in the United States for his own strategic purposes. Therefore, there is literally—neither political party should take this lightly. This should not be a partisan issue. This involves whether or not we are going to allow someone to actively interfere in our political discourse and divide us as a Nation against each other.

Chairman BURR. Senator Wyden.

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

Gentlemen, the same to you. Let me, if I might, begin with you, Mr. Comey. After the election, as you know, the foreign minister, the Russian foreign minister, was quoted in various news reports saying that the Russians had had contacts with people associated with the Trump campaign. Now, that may or may not be true. There is, however, extensive press reporting on the relationships between the Russians and the individuals associated with both the Trump campaign and the incoming Administration.

My question for you, Director Comey, is: Has the FBI investigated these reported relationships and, if so, what are the agency's findings?

Director COMEY. Thank you, Senator. I would never comment on investigations, whether we have one or not, in an open forum like this. So I really can't answer it one way or another.

Senator WYDEN. Well, can you provide an unclassified response to these questions and release it to the American people prior to January 20th?

Director COMEY. I'm sorry? You said will I?

Senator WYDEN. Yes. Will you provide an unclassified response to the question I've asked? And as I've said, it's been reported widely. It's on the Reuters News Service, widely reported. Will you provide an unclassified response to the question I asked and release it to the American people prior to January 20?

Director COMEY. Sir, I'll answer any question you ask, but the answer will likely be the same as I just gave you: I can't talk about it.

Senator WYDEN. Well, I will tell you, I think the American people have a right to know this. And if there is delay in declassifying this information and relating it to the American people, releasing it to the American people, and it doesn't happen before January 20th, I'm not sure it's going to happen. That's why I'm troubled, and I hope that you will make a declassified statement with respect to the questions I've asked.

Now, let me ask one other question if I might. The report has a brief description of Russian cyber intrusions into State and local electoral boards. It reads, and I quote: "DHS assesses that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying."

My question to you—and I think I'd like to have you involved in this, too, Director Clapper. Director Comey, Director Clapper, what systems in your view were compromised by the Russians and what was the nature and extent of those compromises?

Director COMEY. There were intrusions and attempted intrusions at State-level voter registration databases. That is, not containing

the voting mechanism, but who's registered to vote and the address and the particulars of that sort. What the purpose was of those intrusions is not clear to us at this point. And we saw no activity on Election Day that reflected that anyone had messed with those voter registration databases. But there's no doubt that the Russians attacked, intruded, and took data from some of those systems.

Senator WYDEN. Director Clapper.

Director CLAPPER. I think that's the response. I don't have anything to add to that.

Senator WYDEN. I hope you will also tell us in the days ahead, Director Comey, more about the nature of those systems, because it is very clear, given what you found and reported in the declassified version, that we're going to be dealing with these issues coming up. And I think we need to know more specifics, maybe do it in a classified session, about the nature of those systems.

Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

First let me start by thanking Director Clapper and Director Brennan for your many years of service to your country. I also want to say that I appreciate the work that has been done by the intelligence community to produce this report, and I accept its findings.

I do think that it's important that we understand more fully the extent of Russian intrusions into the electoral process to try to shape public opinion. And it is important to underscore two points that have been brought out already, and that is that there is no evidence that voting totals were manipulated or changed or that emails that were released were manipulated or changed. Is that correct, Director Clapper?

Director CLAPPER. That's correct.

Senator COLLINS. The unclassified assessment states that Republican-affiliated web sites were hacked by the Russians, but the report does not go into detail about whether or not data were taken, stolen, from those systems and whether information came from networks used by Republican candidates, whether that included the Trump campaign.

Could you give us a fuller understanding of the hacking on the Republican side? Was the Trump campaign, for example, hacked by the Russians? Or if Mr. Comey is the better person for this.

Director COMEY. Thank you, Senator. I want to be thoughtful about what I say in an open setting. There was evidence that there was hacking directed at State-level organizations, State-level campaigns, and the RNC, but old domains of the RNC, that is email domains that they were no longer using, and that information was harvested from there, but it was old stuff. None of that was released.

We did not develop any evidence that the Trump campaign or the current RNC was successfully hacked.

Senator COLLINS. Does the IC's conclusion that the Russians sought to assist President-elect Trump's campaign depend upon an assessment, then, that the Russians covertly collected information from primarily Democratic sources, but some Republican sources as

well, but only chose to release the derogatory information from Democratic sources?

Director CLAPPER. That's correct.

Senator COLLINS. And I noticed, having looked at many IC assessments, that this one was produced by three agencies. Usually I'm used to seeing assessments where the entire intelligence community is involved. For example, the State Department's Bureau, which was the Bureau that was correct about the weapons of mass destruction, was not mentioned in the report.

Is there a reason why it was—did you only need the CIA, the FBI, and the NSA?

Director CLAPPER. It had a lot to do with the sensitivity of the sources and who could actually contribute to putting the assessment together. We can discuss all that in closed session.

Senator COLLINS. Thank you.

Finally, I just want to underscore your point that we have talked a lot about the Russians' attempt to mold public opinion for our campaign and, as Senator Rubio so eloquently said, sow the divisions and seeds of doubt that has everyone questioning and charges and countercharges, which are really not healthy in our democracy when a new administration is taking over.

But there's also an active Russian campaign to infiltrate, as you have said, military systems, defense contractor systems, critical infrastructure, commercial interests. Don't we need to take a broad look at all of the efforts by our adversaries to either control critical infrastructure, for example, or influence decision making in those arenas as well?

Director CLAPPER. Oh, I think if I understand your comment, Senator Collins, the point is valid that this is a multi-faceted activity. It began with a rather broad-gauged assault, if you will, attempt to infiltrate many entities across the board—military, commercial, governmental, party-related.

So yes, they think of this holistically and use many tools, as they did in this case. Hacking was just one of them.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Thank you, Mr. Chairman.

I want to thank Senator Collins for her continued focus on critical infrastructure, because that's something that, in light of what we've learned, I think we need to think through and realize what our exposures are.

I want to thank all of our witnesses. Attribution, obviously, of responsibility in cyber attacks is the first key step towards imposing a cost on those involved. Since a number of us wrote to the President in November asking that information on Russian interference in the presidential election be declassified, the four of you and your respective agencies have done some very important work in making as much of your findings public as possible. I want to say I'm very grateful for that. The public needs to understand what is at risk here.

To those who criticize these investigations as partisan, I would remind them that Russia didn't do this to help the Republican candidate. Russia did this to help Russia and to weaken America, and therein lies the heart of why this is so important, because in the

next election the shoe could easily be on the other foot and a foreign power could decide it wants the Democrat to win this time.

I think that both scenarios are deeply offensive, and foreign influence on our elections is intolerable no matter which party benefits in any given election. The ongoing efforts of Russia to impact U.S. elections threatens to undermine faith in our democratic systems, which is precisely their goal, and I think it's critical that they pay a price for their actions.

I want to return to the issue of the Russians being able to obtain access to parts of our electoral infrastructure, not the actual machines that count the votes, but the databases. We've had a couple of questions on this, but I want to ask, first of all, do we know if they would be able to manipulate the kinds of data that they had access to? So, for example, if you have a voter databases in a local county that was penetrated, would they be able to change the information within that database?

Director COMEY. Potentially, and that was our concern at the time we discovered this. We saw no indication of that, but that's a definite possibility.

Senator HEINRICH. If that had happened and, for example, the FBI or other elements of the intelligence community were not looking for that, would the electoral boards have had indications that that data had changed?

Director COMEY. Potentially not. They would have the indication. When chaos erupted on Election Day, when someone shows up to vote and your address is different or your middle initial is different or some particulars different, that creates delay, controversy, confusion.

Senator HEINRICH. So, unfortunately, I think this tells us that we are vulnerable to future attacks and manipulation in this case. I think that, obviously, you've laid out a scenario that would be very evident, but also we could have very subtle impacts to the elections. You could potentially have a scenario where someone's voter history, for example, was changed and if they haven't voted for a certain number of years maybe they get purged from the rolls.

Or many of us have had—we've seen flyers of our colleagues who've been criticized for missing a particular election. Maybe they didn't actually miss that election. So I think it begs the question what can we do in concert with those local, county, and State entities to make sure that we are protecting this data the way that we should.

Director CLAPPER. Well, part of our charge in this report was carried out jointly by—and I'll ask Director Comey to speak to this—the Department of Homeland Security and the FBI, to come up with a set of sort of best practices for inculcating greater degrees of cyber security.

DHS reached out in the run-up to the election to the states and I think ultimately about every State took advantage of the recommendations proffered by DHS.

Jim, do you want to add to that?

Director COMEY. No, I think that's the answer, is just understanding that they're a target and availing themselves of the expertise and technology to try to protect themselves, then we on the in-

telligence community side pushing to them indicators of the bad guys.

Senator HEINRICH. Director Clapper, I want to with my last question sort of change gears here for a moment. I asked you in the Armed Services Committee hearing last week about the role of Russian propaganda media outlets like RT. I saw a comment from General Flynn last August that sort of compared RT to CNN or MSNBC. Is that a fair analogy? Is there a structural difference between the way that RT exists within the media infrastructure and, say, a Fox News or MSNBC or CNN or CBS?

Director CLAPPER. To me, the major difference here is the bulk of funding for RT comes from the Russian government, and the Russian government gives editorial direction on what RT is supposed to broadcast. So I think that's a little bit different than CNN.

Senator HEINRICH. And they seem to exercise that discretion.

Director CLAPPER. Yes, they do.

Senator HEINRICH. Thank you.

Chairman BURR. Senator Blunt.

Senator BLUNT. Director Clapper, does RT get any of its broadcasts into the United States?

Director CLAPPER. Yes, it does, some.

Senator BLUNT. It does?

Director CLAPPER. It's very prevalent in Europe and lesser so—I think there's an RT channel here.

Senator BLUNT. And that would be a channel that would be accessible here to some number of people here?

Director CLAPPER. Yes.

Senator BLUNT. Let me——

Director CLAPPER. I don't know the audience size of RT.

Senator BLUNT. I doubt if it's very large, would be my guess. But I don't want to defend RT. I think it's a propaganda arm of a government that is definitely not on our side, and we need to be aware of that. We also need to be aware that—I think you said at one point that they—I think at that point you meant the Russians—think about this holistically and use many tools. We have lots of other countries, the Chinese particularly, that we also believe look holistically and use many tools. It's one of the topics, as you know, from our other meetings over the years, I'm very concerned about cyber generally.

I'm also concerned about our failure to secure Federal records. I think we could certainly give advice to states as to how to secure their records since we've had intrusions into our personnel system, since we've had hacking into the clearance process that a significant number of Americans, including all of you and most of us, have gone through, that are very detailed.

I was the State election official, chief election official in Missouri at one time, and those records, while could be confusing on Election Day, I don't believe there's any evidence of polling places where people had lines that were backed up because there were record changes that were out of the ordinary. I mean, often people show up and say, oh, I know I sent my voter transfer in, when they may or may not have.

But, Director Comey, we don't have any evidence of any disruption of the participation process because somebody got into local registration records; is that correct?

Director COMEY. That's correct, Senator.

Senator BLUNT. It's also my opinion that in any State I'm aware of there's nothing in those records that's not publicly available. You can go to the local registration office. You can often go directly into those records to access those records. Frankly, we have lost a lot more secure records at the Federal level than the relatively open voter registration records.

That doesn't mean that we don't want to help State and local officials secure their records in every way. But those are neither the most confidential records nor the hardest records to get into. And I guess for purposes of this discussion most importantly, there's no indication that any effort to get into those records impacted Election Day. I think you've all repeatedly said absolutely no indication that anything—that there was any intrusion into the vote-counting process.

I was a local election official when we first started counting ballots with computers and one of my concerns always was that the security for how you verify that system was only really protected by how many of those systems were going on all over the country. The diversity of the system itself makes it fairly hard to manipulate. I don't know that we benefit by trying to standardize it, either. But we would benefit by providing guidance on how to secure those important records.

No evidence, I think you said, Director Comey, that the Russians were able to get into Trump campaign email or other records or the current RNC records; is that right?

Director COMEY. That's correct.

Senator BLUNT. So since we don't believe they got in, the fact that they had nothing to release should not be a shock, on the records?

Director COMEY. Yes.

Senator BLUNT. And we do believe they tried to get in?

Director COMEY. We can't say with respect to the Trump campaign. With respect to the RNC, there's no doubt they hit an RNC domain. So it could be they were aiming at the current one and just missed it and hit an old one. But I can't say for sure sitting here.

Senator BLUNT. Well, I do know that the Chairman of the RNC, I heard him say over the weekend he thought they had done a better job securing their records. Whether that's true or not, I wouldn't know.

I think I did read in one, more than one published account, that the password to Mr. Podesta's email was "Password1," with a couple variations of spelling, of using capitals or something, and "password." So hopefully lots to be learned here, and thanks to all of you for your efforts to help us learn it.

Vice Chairman WARNER. Mr. Chairman, could I? For the Senator, and it was in the public report, in terms of YouTube views and YouTube subscribers, RT actually has a bigger presence in the United States than the BBC.

Senator BLUNT. And the BBC is also funded by the government, right?

Chairman BURR. Senator King.

Senator KING. Well, I'll just follow up on that point, because this is in the annex to the published report. RT America, millions of views on YouTube, 850 million; BBC, about two-thirds of that; CNN, significantly lower. The same thing in YouTube subscribers: RT America, 450 million.

So RT is a significant media presence. I think the important point with regard to RT is that we are talking about hacking. That's how this discussion is characterized. But this was a comprehensive strategy involving RT, trolls, paid bloggers, hacking, the whole package.

In fact, General Clapper, this is exactly what the Russians have done throughout Eastern Europe for some years; isn't that correct?

Director CLAPPER. That's correct. It's just as technology has progressed the Russians have taken advantage of it for this purpose.

Senator KING. I just want to be sure I heard correctly. Mr. Comey, did you answer Senator Wyden's question that there is an investigation under way as to connections between either of the political campaigns and the Russians?

Director COMEY. I didn't say one way or another.

Senator KING. You didn't say that——

Director COMEY. That was my intention at least.

Senator KING. You didn't way one way or another whether even there's an investigation under way?

Director COMEY. Correct. Especially in a public forum, we never confirm or deny a pending investigation.

Senator KING. The irony of your making that statement here I cannot avoid. But I'll move on.

Director COMEY. Well, we sometimes think differently about closed investigations. But you asked me if I had any pending investigations and we're not going to talk about that.

Senator KING. All right.

Is it my understanding that there are actually three reports—a highly classified that only went to certain individuals; classified, which this Committee has seen; and the public report—but that the conclusions of those three reports are identical? Is that correct?

Director CLAPPER. That's correct.

Senator KING. And the only issue, the difference between them, is sources and methods; is that correct?

Director CLAPPER. Largely.

Senator KING. And the reason you can't reveal sources and methods is that you would compromise future opportunities to gain information and also compromise fragile sources?

Director CLAPPER. Exactly.

Senator KING. It seems to me that trust is one of the issues. I mentioned in the Armed Services Committee, my folks in Maine tend to be skeptical: Prove it. Speak to me for a moment about the difficulty of proving what you've concluded pretty unequivocally, without revealing sources and methods? How do I convince my barber in Brunswick that this is for real?

Director CLAPPER. Well, that's why we have intelligence oversight committees, to represent the American people, with whom we

cannot share as fully and completely as we might like the evidentiary proof that we have and in which we're very confident.

So we're very dependent, given the nature of intelligence work to start with, very dependent on you as our overseers to look at that yourselves on behalf of the electorate.

Senator KING. But I think it is important to make the point to the public why sources and methods need to be protected.

Director CLAPPER. Well, we spend money that you the Congress appropriates. We literally spend billions of dollars gaining these accesses, which we would jeopardize. And of course, this then impairs the support that we can render to the oncoming administration and successive administrations. When we lose these accesses, it takes money and time to recover them, not to mention putting potentially assets who work for us lives at risk.

Senator KING. Was there any political influence brought to bear on any of the three of you in the preparation of this report? Did the President tell you what he wanted to find? Or was this somehow a politicized investigation?

Director CLAPPER. Absolutely not. The President asked us to compile all available information that we had, and when he was briefed on it he made the point once again that he was not—had not and was not going to give us any direction. That's why this is an IC product; it is not that of the current Administration.

Senator KING. Mr. Comey, would you affirm that as well?

Director COMEY. Yes. I hope I've demonstrated by now I'm tone deaf when it comes to politics, and that's the way it should be.

Senator KING. Thank you.

Director Brennan, the same conclusion?

Director BRENNAN. Yes, absolutely.

Senator KING. A final sort of technical question. I notice that the October 10th—sorry—the October 7th statement was the IC, the community itself, implying the entire community. This one was FBI, CIA, and DNI. Is there any difference? Why wasn't the report that was just released represent the entire 17-agency community?

Director CLAPPER. Again, because the three exclusive contributors to this are represented here and because of the sensitivity of many of the sources, we made a judgment to restrict it to these three agencies.

Senator KING. So there was no elimination of other views?

Director CLAPPER. No, there was none. But we felt, again because of the sensitivities, the sensitivity of the source, which we tried to protect even within the intelligence community, to cast the report as emanating from these three agencies.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Gentlemen, thank you. Thank you for your work and your service to the country and the leadership you've brought. I need to ask a couple of questions, some that you've heard before, just for quick review, and then I want to build on several things from the report.

Just to clarify again, does anyone know of any votes that were changed or an attempt to change votes in voting machines?

Director CLAPPER. As we stated in the report, we have no evidence of any manipulation of vote tallies whatsoever.

Senator LANKFORD. Voter rolls?

Director CLAPPER. No. There was reconnoitering, intrusion on certain voter rolls, but to the best of our knowledge no manipulation of them.

Senator LANKFORD. Give me a best guess: How many other countries is Russia currently or have, let's say in the last four years, tried to influence in their elections?

Director CLAPPER. I think one of the annexes portrays that, the number of countries that to one degree or another Russia has expended effort to try to influence political views or opinions.

Senator LANKFORD. 15 countries, 20? Give me a ballpark?

Director CLAPPER. A couple dozen maybe.

Senator LANKFORD. So maybe 20 or so.

You also make a comment in the report itself about previous U.S. elections and Russian engagement in previous U.S. elections, going all the way back to KGB putting a person—recruiting a Democratic Party volunteer or activist—you don't give the details on it—even on Jimmy Carter's campaign in the 1970s—moving forward.

Tell me about the differences in aggressiveness and style. If the Russians and then back to even the Soviets before have been involved in our elections since the 1970s and before, tell me the degree of difference in this one versus how they've been engaged in others?

Director CLAPPER. The history of this goes back to the sixties, when the Russians attempted to fund certain candidates, parlay certain lines of opinion or lines of view. And of course, you had the radio broadcasts and that sort of thing they would do. As the technology has increased and they've gotten more tools available to them, they've broadened the spectrum of things that they have done.

What is unique and what is disturbing, though, about this election, 2016, is the aggressiveness and the variety of tools they use and their activism in trying to convey information that they stole, in an effort to influence the outcome of the election. That's different than any previous case.

Senator LANKFORD. So additional tools, additional aggressiveness. They've been engaged in our elections before; this one's just at a much higher level?

Director CLAPPER. Yes.

Senator LANKFORD. You mentioned as well about the Russians trying to hack into both Democrats' computers and political operations and Republican, Democratic computer and political operations. Between the—let's just say DNC and RNC. We'll just use loose terms here. I understand there's multiple other entities that are connected there.

Between DNC and RNC, were they able to penetrate to the same level, to get the same quantity, quality, and type of materials? Or was there a difference between what they were able to glean from the Democratic DNC or the RNC?

Director COMEY. They got far deeper and wider into the DNC than the RNC.

Senator LANKFORD. Did they use similar methods with both? They were able to actually penetrate deeper or wider?

Director COMEY. Hard to say. Hard to say in this forum. Hard to say even in a closed forum. Because they didn't get into the RNC, it's harder to see. It makes it harder to answer. Similar techniques, the spear phishing techniques, were used in both cases. But there's no doubt they were more successful at DNC, deeper and wider, than at the RNC. They did hit some Republican-affiliated organizations, but not the current RNC itself; they didn't get in.

Senator LANKFORD. So they weren't getting to current information, basically?

Director COMEY. Not on the RNC. They got at the State-level current information, but not RNC current.

Senator LANKFORD. Okay. You also highlight several other ways that the Russians have been engaged in our Nation just as a whole. You mention not only the election and previous elections, but you also move and give two practical examples of how the Russians have been engaged in our political system. One was an anti-fracking campaign that the Russians seemed to be engaged in. Another one was the Occupy Wall Street movement that the Russians were engaged in as well.

Any additional highlights or any additional details that you can give on that? It was interesting that you highlighted those. Can we tell the nature of, for instance, with the Occupy Wall Street, the social media pages that were created to give communications capabilities to the Occupy protesters, how those were used and if they were used?

Director CLAPPER. We probably ought to take that one for the record, Senator, just to be for the sake of accuracy and just exactly what they did in those two campaigns. I don't have that on the top of my head.

Senator LANKFORD. It was just in the report. I thought it was interesting just as a way of illustration in the report that there was an illustration to say that they've also been engaged in some of the anti-fracking and some of the Occupy Wall Street movement as well.

I appreciate your work. Thank you.

Yield back.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman. I thank all of you for your service.

If I might ask, were there any disagreements on the involvement that Russia has had or attempts to have in this process of our elections by any of the intelligence community? Did any of you have different takes on this or have to collaborate in order to come to one conclusion?

Director CLAPPER. There was one aspect that there was a difference in confidence levels held by NSA versus the rest of us on one single aspect. I'd be more comfortable discussing that in a closed session.

Senator MANCHIN. Any other countries that have been hacking us from the standpoint that it brings the concern that you have with this? You're saying no one's ever done this to this level in our

political process, but when you look at espionage, sabotage, basically through military or industrial——

Director CLAPPER. Well, there's a lot of espionage, certainly, collecting and exfiltrating information. Obviously, the Chinese come to mind. But very much a contrast between the passive collection, passive exfiltration, as opposed to actively purloining information and then using it for a political end. That's the difference here. The Russians are unique.

Senator MANCHIN. Yes. I think all of us have been very much concerned that the outcome of the election was altered, and you have been very clear saying it has not been altered, nor would the outcome of this election have been any different.

Director CLAPPER. I have to clarify one aspect of what you just said, Senator. We did not assess the impact on the electorate. We did not do public opinion polls, because that's not our charter of the intelligence community to do that. So we just can't say about whether the release of the hacked information—how that changed any voters' opinion. We don't know.

Senator MANCHIN. Knowing that, then, what recommendations of sanctions would you have? What sanctions recommendation do you think would deter Russia or any other country from continuing hacking us?

Director CLAPPER. Well, that's clearly a policy call. We got into that last Thursday at the Senate Armed Services Committee, and there are a range of tools that we can use. I think Admiral Rogers and my view is that we should consider the whole range of tools, not necessarily do a cyber for cyber reaction, and look at all of them.

Senator MANCHIN. I'm thinking—what I'm trying to get to is, if hacking is so serious and the technology we have today can alter our lives relatively very quickly, if that's all capability and possibilities of happening, shouldn't we have a broad basically policy in the United States of America that any hacking internationally that's been confirmed and concurred by the intelligence community, once you all basically authorize that this happened, as you agreed right now this happened in our electoral process, that we should enforce sanctions on any country that does this, to deter them from doing it?

Director CLAPPER. Well, I think again the discussion we had in the Armed Services Committee Thursday was if you are conducting espionage then if we're going to punish, nation-states are going to punish each other for conducting espionage, which is a passive collection of information, that's a pretty heavy policy call which I don't think any of us want to make.

When it's an activist campaign as it was here, that's a different proposition. Again, I think it's not our call to decide what to do in response. Our only comment—and I will repeat it—was to consider the whole range of potential tools, instruments of power, national power, to respond.

The challenge you get into with cyber for cyber, of course, is you have to also consider the counter-retaliation to that. While we spend a lot of time agonizing over precision and being very surgical, the adversaries may not be quite as precise as we might be. So again, the bottom line: Consider all tools.

Senator MANCHIN. I'm just saying that when we now it's state-sponsored—Article 5 of the NATO Treaty specifies that all NATO members will defend the sovereignty and territorial integrity of other allies if they are attacked. Has NATO intervened at all? Have any of the other countries intervened in this, NATO allies?

Director CLAPPER. Well, I can't speak for each individual NATO member, what they may or may not have done to defend themselves or to retaliate against a perceived cyber attack.

Senator MANCHIN. Do we as the United States defend any of them when they've been attacked?

Director CLAPPER. Well, if the NATO alliance and member nation invokes Article 5—I believe that's the provision; I'm getting out of my lane here—that's where an attack against one is considered an attack against all. I don't know that that's ever been exercised, I don't think it has, in the cyber context.

Senator MANCHIN. Thank you, Mr. Chairman. My time has expired.

Chairman BURR. Senator Cotton.

Senator COTTON. I want to add my voice of gratitude to the many Members of this Committee who have expressed our gratitude for the men and women of our intelligence community. As President-elect Trump said on Friday, he has tremendous respect for those men and women, and I share that as well.

Second, those men and women have concluded that Russia hacked into the DNC and John Podesta's email. And while this Committee, as the Chairman said, will conduct a thorough inquiry into this matter, I have no reason to doubt those conclusions.

Third, I don't doubt it in part because Vladimir Putin is KGB, always has been, always will be. Back in the Cold War, Russian intelligence used to refer to the United States as "the main enemy," and they still do today. Vladimir Putin undermines the United States and our interests for the same reason the scorpion stings the frog as it crosses the river: It's in his nature. And he's done much worse for the last 18 years across numerous domains.

Seventh, Donald Trump won this election fair and square. Vladimir Putin didn't hack into Hillary Clinton's calendar and delete rallies in Michigan and Wisconsin, and didn't hack into a speech writer's computer and delete speeches that laid out a compelling vision for the working class. It's time to look into the mirror and say that Hillary Clinton lost this election, not because of Vladimir Putin or Jim Comey or fake news or the Electoral College, but because she ran a bad campaign.

That brings me to a conclusion in the report about the clear escalation, Director Clapper, of the scope of the activities: that Russia has conducted these kind of activities in recent years, but this was a clear escalation in the scope and the scale; is that correct?

Director CLAPPER. That's correct.

Senator COTTON. Why did they think they could get away with that kind of clear escalation against U.S. interests?

Director CLAPPER. I think the challenge, particularly in the cyber realm, I'll say, is that there's kind of an insidious progression of aggressiveness. I've certainly seen this over the last six years or so, where other countries get progressively more—as they develop

more capability, they also have an attendant willingness to try to use it.

We're seeing this particularly with kind of the second tier, meaning North Korea and Iran, who don't have the cyber capability, we don't believe, of the level of sophistication of certainly the Russians or the Chinese, but they are progressing. That's to me what's bothersome about this whole business of cyber and when do you draw the line to say enough's enough.

Senator COTTON. Let's move to the question of motive. The report states that at first Russia, in the assessment of the IC, had a desire to undermine U.S. democracy, to sow discord and confusion. Over time, though—as it viewed Hillary Clinton as the likely winner, to undermine her presidency. But over time it developed a "clear preference"—that's the language—for Donald Trump.

Can you tell us when Russia viewed Hillary Clinton as the likely winner?

Director CLAPPER. I think that was in the summer time frame, perhaps July–August or so.

Senator COTTON. Can you tell us when you believe that Vladimir Putin developed a clear preference for Donald Trump?

Director CLAPPER. Some time after that. I don't know that, certainly not in this setting, we can pick a date when he shifted gears, but he clearly did.

Senator COTTON. Did he or the intelligence services ever believe that Donald Trump was a likely winner?

Director CLAPPER. Initially, no. They thought that he was a fringe candidate and didn't think that at all.

Senator COTTON. A newspaper headline about the report over the weekend said something—I paraphrase—Russian cyber attack aims to install Putin in White House. Would a more accurate headline perhaps be "Russian cyber attack aims to undermine expected Clinton presidency"?

Director CLAPPER. I don't think you'll find a line like that in our report.

Senator COTTON. Your assessment of motive is based in part on the selective leaking and the relative levels of targeting Democratic material and Republican material on the one hand versus the other; is that correct? More democratic material was leaked, even though——

Director CLAPPER. Yes, clearly.

Senator COTTON. Is it possible that they just leaked the Democratic material because they thought Hillary Clinton was going to win and they wanted to undermine her and they didn't view it as profitable to leak Republican material?

Director CLAPPER. Well, that's—yes. I mean, that would seem to be the logical observation, that they favored the President-elect and they wished to denigrate as much as possible Hillary Clinton. And had she won, their plan was to try to undermine her presidency.

Senator COTTON. One final question about the leaks that have happened in this case, first in December before President Obama directed this review to occur, and then there were none until last Wednesday night when the Washington Post reported on what may be sensitive signals intelligence. Director Comey, have you received

a crimes report from anyone in the intelligence community about these leaks?

Director COMEY. I don't think yet as to the December leak or, obviously, anything this month, not yet.

Senator COTTON. Mr. Chairman, I suggest that we should include those leaks as part of our inquiry.

Chairman BURR. The Chair and the Vice Chair are working on that right now.

Senator Harris.

Senator HARRIS. Director Clapper, your report states that, quote, "We assess Russian intelligence services will continue to develop capabilities to provide Putin with options to use against the United States, judging from past practice and current efforts." You go on to write: "Immediately after Election Day, we assess Russian intelligence began a spear phishing campaign targeting U.S. Government employees and individuals associated with United States think tanks and NGOs in national security, defense, and foreign policy fields. This campaign could provide the material for future influence efforts." Then you indicate that the, quote, "election operation signals a new normal in Russian influence operations."

So indeed this is troubling. My question is, is the intelligence community supporting efforts to ensure that the computer networks and personal devices of the President-elect and his transition team are protected from continued influence?

Director CLAPPER. It's my understanding that they are very, very sensitive to this threat, and we've done what we can to educate the transition team about the pitfalls of mobile devices in secure areas and the like.

Senator HARRIS. Do you believe your education efforts have been successful?

Director CLAPPER. You'd have to ask them, I think.

Senator HARRIS. What about the President-elect's Twitter account, and in particular what is being done to safeguard his phone and account, given the potentially dire national security consequences of an infiltration?

Director CLAPPER. Probably best left to a closed environment to talk about that.

Senator HARRIS. Okay.

Director Comey, this is more of a comment than a question, but I wanted to echo the points made by Senators Wyden and King. I understand why the FBI could not disclose and comment on ongoing investigations. However, it seems that, despite past precedent, the new standard that was created over the summer and fall regarding the investigation into Secretary Clinton's email server was that there was a unique public interest in the transparency of that issue.

Particularly given the findings of your report, I am not sure I can think of an issue of more serious public interest than this one. This Committee needs to understand what the FBI does and does not know about campaign communications with Russia, and I hope that we can follow up on this in closed session to have more of an idea of what the FBI knows and what we might do to prevent any further harm.

Thank you.

Chairman BURR. Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman. And thanks to each of you for your service to the country and for the people you represent, who faithfully discharge their duties daily, many times unheralded.

I wanted to ask first of all, there seems to be a disparity between the RNC servers and the DNC servers in terms of their vulnerability. Admiral Rogers, this perhaps is a good question for you. Is good practice in terms of defenses important in terms of securing information like that that was stolen in these hacks?

Admiral ROGERS. Yes.

Senator CORNYN. Would this also be—would your concerns about the vulnerability of a private server also extend to government officials using private email servers and engaging in an exchange of classified information on those private email servers?

Admiral ROGERS. I would argue everyone needs to have an awareness of how they communicate, whether we're talking personal or at work. That's the nature of the world we find ourselves in.

Senator CORNYN. And to do so in compliance with the law, the protocol, etcetera, of the Federal Government.

When did the Russians first begin to hack U.S. networks, Admiral Rogers?

Admiral ROGERS. With respect to this particular issue?

Senator CORNYN. No. I'm just wondering, how long has this been going on?

Admiral ROGERS. Since the 1990s, off the top of my head.

Senator CORNYN. So while this has certainly become much more visible and focused, given the focus of the effort, this really is a longstanding effort by nation-states, including Russia, to hack into our networks, correct?

Admiral ROGERS. Yes, we have seen longstanding efforts to hack into our networks.

Senator CORNYN. This was perhaps unusual—maybe I should ask you—in that there was a coordination between the hacking and the propaganda efforts of Russia in order to try to undermine the legitimacy of the election process. Director Clapper, would you agree with that statement?

Director CLAPPER. Yes, orchestrated by the intelligence services.

Senator CORNYN. Is this the first time in your experience where you've seen that sort of multi-layered, multi-faceted coordination between propaganda efforts and hacking into our networks, or is this a new normal?

Director CLAPPER. Well, it's a progression of capabilities as they've acquired them and used them. They certainly have longstanding practices like that against European countries.

Senator CORNYN. What has the United States done since—the United States Government or—let's start with the U.S. Government. What have we done to respond to the hackings that have been occurring in U.S. networks since the 1990s in order to discourage or deter that sort of activity?

Director CLAPPER. Well, we've tried to up our game defensively. We have selectively responded. The Sony Picture attack comes to mind, and certainly there was a response to this, this case. But the

issue, as I said earlier, is if nation-states are conducting espionage against one another, which we do as well, as many other nation-states, that's—and if the standard is to punish because of the conduct of detected espionage, well, that's another policy call.

Senator CORNYN. As I recall, during the publicity about the Sony hack there was a lot of discussion as to how do you characterize this? Was this an act of war, was this a commercial—criminal activity involving a commercial enterprise? How do you think about that? Have we gotten better about characterizing the nature of the attack?

Director CLAPPER. Well, we in the intelligence community, particularly the Bureau, I think do an excellent job of attribution. Then of course the hard part is what, if anything, to do about it. Again, I would repeat what was said earlier about, against a cyber activity is the best response a counter-cyber activity or not? In the end, that wasn't the case with the Sony attack.

Senator CORNYN. Well, there could be multiple options, as I think you alluded to. It doesn't need to just be cyber for cyber. There are a multitude of retaliatory options, correct?

Director CLAPPER. Exactly, yes, sir. That was the point I think that Admiral Rogers and I made to the Senate Armed Services Committee when we had this discussion there Thursday.

Senator CORNYN. Perhaps this is heresy since I'm a new Member of the Intelligence Committee, but let me just give you my impression: that we have so fractured the jurisdiction of oversight of cyber issues that we need to figure out some better whole-of-government approach. I see Senator Reed smiling because, of course, the Armed Services Committee has some involvement in this; Homeland Security and Government Affairs.

But we need to figure out some way, I think, to deal with a whole-of-government approach so we are working as efficiently and effectively as possible. I know from what I read in the newspaper President-elect Trump has said he wants to commission a study to come back to him within 90 days, if I'm not mistaken, with some recommendations in that regard. We would certainly welcome your insight and advice.

Thank you.

Chairman BURR. Senator Reed.

Senator REED. Thank you, Mr. Chairman. Gentlemen, thank you for your dedicated service to the Nation for many, many, years.

The non-classified intelligence assessment which is available to the public concludes that, quote: "Putin, his advisers, and the Russian government developed a clear preference for President-elect Trump over Secretary Clinton," close quote, in part because, quote, "Putin has had many positive experiences working with Western political leaders whose business interests made them more disposed to deal with Russia, such as former Italian Prime Minister Silvio Berlusconi and former German Chancellor Gerhard Schroeder."

Either General Clapper or Director Comey, does the community have any intelligence that suggests that President-elect Trump or those close to him may have business interests that made them more disposed to deal with Russia?

Director CLAPPER. The Russians just believed or came to the conclusion that, because the President-elect is a businessman, that he would be easier to make deals with than the Democrats.

Senator REED. Thank you.

Director Clapper, at the Armed Services Committee hearing I asked you whether, given the scope and the difficulty of hiding all the different aspects of this comprehensive campaign, was this—first, was Putin advised that there was a significant chance of being discovered? And second, did he disregard that because he wanted to send a message as well as being disruptive of our process? And you deferred that response until after you had briefed the President and the President-elect. Can you add anything to that?

Director CLAPPER. I'm sorry, sir. Would you repeat the question?

Senator REED. Given the multiple aspects of this campaign—the hacking, the trolling, the social media—the idea that this could be done unnoticed—and given the scale and the intent—would be unnoticed, raises one question at least: Was he in any way advised that, you're taking a risk here? And second, did he disregard that risk, not only to be disruptive, but also to signal to the world that he is prepared to engage in this cyber operation and send us a signal?

Director CLAPPER. Well, I think, as we've seen, he I think always feels that, or felt, that he had deniability. And of course, that's what—both the Russian government and the Russian media are denying any culpability. And we're somewhat restricted because of our sources and methods concerns about showing our hand, showing our deck here, so to speak, and what led us to those conclusions that we feel so strongly about.

So he knows that. He's a professional intelligence officer and he probably understands our approach to the protection of sources and methods, and so he can just deny it and get away with it.

Senator REED. Let me just a final point here——

Director BRENNAN. If I could add, Senator.

Senator REED. Yes.

Director BRENNAN. When this started to break in the press in early August, I had a conversation with the director of the FSB, Alexander Bortnikov, and told him clearly that if Russia was doing this they were playing with fire and it would backfire and they would be roundly condemned by not only the U.S. Government, but also the American people.

And he said he would relay that to Mr. Putin at the time. He denied any activity along these lines, but I made it very clear to him that basically we were onto him.

Senator REED. A final point. Everyone has indicated and the report indicates that there was an effort made against the Democratic political campaigns and Republican political campaigns, but one was much more aggressive, frankly, than the other in terms of finding ways into the servers of not only the DNC, but the individual Democratic operatives.

Given what you posit as the goal of Putin, which was to discredit Secretary Clinton as much as possible, assuming she might be President, or in some way disrupting her campaign, it seems to me, at least to me, logical that they would devote those kind of resources to, one, to going after Democratic computers rather than

resources to Republicans. Is that borne out by your analysis, Director Clapper?

Director CLAPPER. Yes.

Senator REED. Thank you very much.

Thank you, Mr. Chairman.

Chairman BURR. Senator Risch.

Senator RISCH. Well, Mr. Chairman, let me say that, after sitting through this, to put this in perspective for the American people, those of us who are involved in intelligence matters at the dais here, for that matter at the table, I doubt there was anyone who was shocked or even mildly surprised when these facts came out.

This hacking business is ubiquitous and it has been since the internet was set up. The question was asked, when did Russia start this? I would expect it was the day that they hooked up to the internet. This goes on constantly, and as we've been sitting here there have been thousands of efforts against U.S. entities, U.S. computers, government, non-government, and that's just in the U.S. This has been going on all over the world.

Those of us who engage in this and have watched these things, most of which have never become public, on a scale of one to 10, we've seen a number of 10s. This one doesn't come close to a 10. But the interesting thing is, because it's been in the political—it's in the political spectrum, it has caught the fancy of the media, it's caught the fancy of the American people.

Russia is not in my judgment the most aggressive actor in this business. I think there are other actors that are much more aggressive, and indeed I think much more dangerous. It isn't limited to state actors. There's state actors, there's non-state actors, and there's combinations. They go after everything.

The criminal element is particularly troubling to a lot of people. I just heard Director Clapper. I think it's the first time I've ever heard an admission by an intelligence person that the U.S. does espionage. By that I think he's inferring, in the context we're in, that the U.S. does this. Now, I am not confirming that. I'll leave that to Mr. Clapper to do.

But nonetheless, the other interesting thing I've found is that I think I agree with Director Clapper entirely that you want to be careful here when you're talking about how you're going to respond to this. If it's responded to with a similar type of hacking, that escalates very, very quickly. We've sat through, actually gamed out what would happen in the situation where we had an actual hacking and then decided how we were going to respond to it, and if we did how the other side would respond to it.

The good that has come out of all of this is that finally I think the American people are getting a picture of how big this, how ubiquitous it is, how dangerous it is, and that something has to be done about it. Director Clapper I think is correct that our response has been to up our game as far as our defensive posture is concerned. Really, that is where the focus needs to be.

Again, one would hope we could find the silver bullet where you could stand up a defense and say: Look, it's there; this can never be penetrated; anything that happens behind this wall is just fine. I don't know if I'll live to see that day. I don't know if anybody will.

But in any event, it is good that we have this on the table. It's good that we're having the discussion about it. And I'm hoping that everyone will be patient with us and will be supportive as we do our best to up our game, to defend on these things, particularly in the realm of most of the challenges that the government generally and the public generally doesn't hear about, but the intelligence community does.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Senator Risch.

The vote has started. Senator Warner would like a question and a clarification. I have a clarification. Do any other members seek anything in this open session?

[No response.]

If not, I'll recognize Senator Warner.

Vice Chairman WARNER. My question is this. One, I'm intrigued by my colleague's comments. Many of us felt the conclusions were accurate. In many ways, it was the President-elect until Friday who was questioning these results.

I believe—and I would go back to my comments in my first line of questions, when all four of you, with literally hundreds of years of experience, said you have never seen anything in your career that approaches this level of Russian activities. We can debate who is the most serious threat, but anyone that underestimates the seriousness of this Russian threat I think does so at their own peril.

I want to ask you, Director Comey, and then I want to get a clarification. If a thief came up to the DNC and broke in and stole all of the most valuable information, and that same thief then drove up to the RNC and, because they had a better lock on the door, was only able to break in and get some old information, would both of those be crimes and would both of those be prosecuted?

Director COMEY. Sure, yes.

Vice Chairman WARNER. Director Clapper, one thing that I want to clarify, because I think, particularly with Senator Collins, there might have been some ambiguity. The conclusion you reached that the Russian government at its highest levels was targeting Clinton and favoring Putin was not the result simply of more—I'm sorry, favoring Trump and disfavoring Clinton—was not the result simply of more leakage on the Democratic side, but I believe, based upon page 1 of your unclassified report, is that Putin most likely wanted to discredit Clinton since he'd publicly blamed her since 2011 and then a series of other activities. That conclusion of favoring Trump and not favoring Clinton was not simply the result of disproportionate leaking on the Democratic side; is that correct? I just want to clarify that for the record.

Director CLAPPER. You mean just by virtue of the hacking?

Vice Chairman WARNER. My understanding, I was left with the impression that the reason you reached the conclusion that there was favoring of Trump over Clinton was because of the disproportionate releasing of information. I've seen in the non-classified report lots of evidence that it was ongoing concerns between Putin and Clinton.

Director CLAPPER. Clearly, one aspect of this. But we reviewed the totality of what they were doing. Whether by this means or by the multi-faceted propaganda campaign, the use of social media

tools, planting fake news, there was a campaign, all of which clearly seemed to favor, clearly favored——

Vice Chairman WARNER. Including after the election——

Director CLAPPER [continuing]. A preference for the President-elect over Secretary Clinton.

Vice Chairman WARNER. Including after the election, the fact that Russian efforts to discredit the electoral process in America stopped?

Director CLAPPER. Well, I think that was an overall objective throughout, to accomplish that objective, then as things moved on and progressed clearly a proclivity for the President-elect and an attempt to denigrate Secretary Clinton.

Director COMEY. If I might add, Senator, that's the challenge of the unclassified forum. There's more behind that conclusion. We just can't talk about it here.

Chairman BURR. Director Clapper, I think this is in the scope of an open session. You'll tell me if it's not. Is there any intelligence that Russian leadership, specifically Putin, directed the GRU or the SVR to penetrate these political organizations? Or was the leadership involvement in this process triggered by what they were able to exfiltrate and when the leadership saw the breadth of information they directed a disinformation campaign to happen?

Director CLAPPER. I think, as we said in our October statement, this came from the highest levels of the government, and I would assess that there was overall broad direction given, with execution carried out by the services.

Chairman BURR. So one can take the fact that this has been a continual fishing process on the part of the Russians that started in 2014, and from 2014 forward, that was all directed by the highest echelons of the Russian government?

Director CLAPPER. Yes. Again, I think it would be best to get into the details of that in a classified setting.

Chairman BURR. And we will do that.

There are a couple minutes left in a two-vote session. We will reconvene in the Committee room in closed session at the completion of that vote. This open hearing is adjourned.

[Whereupon, at 2:45 p.m., the hearing was adjourned.]

○