S. HRG. 115–40, PT. 2

DISINFORMATION: A PRIMER IN RUSSIAN ACTIVE MEASURES AND INFLUENCE CAMPAIGNS PANEL II

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

THURSDAY, MARCH 30, 2017

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE
25–998 PDF WASHINGTON : 2017

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

SELECT COMMITTEE ON INTELLIGENCE

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

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

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

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

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

Chris Joyner, *Staff Director*
Michael Casey, *Minority Staff Director*
Kelsey Stroud Bailey, *Chief Clerk*

CONTENTS

MARCH 30, 2017

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

DISINFORMATION: A PRIMER IN RUSSIAN ACTIVE MEASURES AND INFLUENCE CAMPAIGNS PANEL II

THURSDAY, MARCH 30, 2017

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

The Committee met, pursuant to notice, at 2:05 p.m. in Room SD–106, Dirksen Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

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

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

Chairman BURR. I'd like to call this hearing to order. This morning the committee examined the history and characteristics of the Russian active measures campaign as it led up to this, our second panel, which will examine the role cyber operations play in support of these activities.

I'd like to welcome our witnesses: Mr. Kevin Mandia, Chief Executive Officer of FireEye, a global cyber security company. Prior to founding the cyber security company Mandiant, which was acquired by FireEye in 2013, Mr. Mandia served in the United States Air Force as a computer security officer and later as a special agent in the Air Force Office of Special Investigations, where he worked as a cyber crime investigator.

Mr. Mandia, I thank you for being here today and, more importantly, thank you for your service.

General Keith Alexander is the CEO and President of IronNet Cybersecurity, another global cyber security firm on the forefront of our Nation's commercial efforts to mitigate cyber security threats. Prior to founding IronNet, General Alexander served for 40 years in our armed forces, culminating with his tenure as the Director of the National Security Agency from 2005 to 2014 and concurrent service as Director of U.S. Cyber Command from 2010 to 2014.

General, thank you for being here today and, more importantly, for your service to the country.

Also, Dr. Thomas Rid is a Professor of Security Studies at Kings College, London. He has studied and written extensively on cyber security issues. He has worked at Hebrew University in Jerusalem, John Hopkins School for Advanced International Studies, and the Rand Corporation.

Dr. Rid, thank you as well for your expertise and we look forward to your testimony, as well as we do the other two witnesses.

I'd like to note for the public and for my fellow members that the level of cyber expertise in front of us is truly remarkable. These witnesses will be able to provide at an unclassified level some extremely useful texture and detail to the discussion that we began this morning, and I feel certain—and I say this to all three of you—that the committee in a closed setting might want to reach out to you as we begin to dig a little deeper, so that we can get your thoughts and tap into your expertise in a setting that might be able to explore a little further than the open setting of this hearing.

So once again I'll say to members that for this hearing we will be recognized by order of seniority for five-minute rounds. I would note for members that we are targeted to have a vote somewhere between 4:00 and 4:30. It would be my hope that we could wrap up prior to that vote and not hold our witnesses open, and that way we would conclude Senate business for the week with that vote.

Vice Chairman.

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

Vice Chairman WARNER. Thank you, Mr. Chairman. I don't have any statement other than one to welcome all the witnesses and to point out that before Mr. Mandia's company was acquired by a California company he was based in Alexandria, Virginia, where he did great, great work. And we'd be happy to have you bring your company back, with all due deference to Senator Harris, back to Virginia.

Senator HARRIS. Stay in the sunshine.

Chairman BURR. With that, Kevin, I'm going to recognize you to start, and recognize there's a big difference between the tech company you ran and the tech company he claims that he ran.

[Laughter.]

STATEMENT OF KEVIN MANDIA, CHIEF EXECUTIVE OFFICER, FIREEYE, INC.

Mr. MANDIA. Thank you. I'd like to start by thanking the Chairman, thanking the Vice Chairman, and the whole Senate Intelligence Committee for this opportunity to share some of the experiences and observables I've had in cyberspace over the last 22 years. What I'm going to speak about today is the cyber capabilities and techniques attributed to Russian hackers, specifically the threat group that we refer to as APT28. I want to talk also about recommendations to prevent or mitigate the impact of these efforts to compromise.

Before I answer your questions, I want to give you a little bit of my background or the background of our company so you understand the context of my narrative. As I sit here right now, we have hundreds of employees responding to computer security breaches. We think it's critical to own that moment of responding to a breach, collecting the trace evidence, and analyzing that evidence.

So as I give you my narrative today, it's based on really three things. It's based on: one, what we are learning as we respond to hundreds of breaches a year. We're cataloguing that trace evidence and we're putting it into a linked database. Then we have over 150 threat analysts worldwide who speak 32 languages. They're in 32 countries, and they're trying to marry up what we're seeing in cyberspace to what we're seeing in the geopolitical world out there today.

Then the third source of my dialogue, the third source of evidence, is in fact we have 5,000-plus customers who are relying on our technology to protect them on a daily basis.

Let me first speak to the methodologies being used by APT Group 28. We attribute many intrusions to these folks. You might have heard about the Worldwide Antidoping Agency, the DNC breach, the DCC breach, the Ukrainian Central Election Commission, TV5Monde, and I can keep going on. I believe the Doctor will mention some more of these victims.

But all the breaches that we attribute to APT28 in the last two years involved the theft of internal data as well as the leaking of this data by some other party, potentially APT28, potentially some other arm of the organization, into the public.

During the course of our APT28 investigations, we've had a significant amount of evidence. We've looked at 550 or more pieces of custom malware. A lot of people will think, well, what's that mean? We don't see this malware publicly available. It's not available to any of you to download and use tomorrow. It's being crafted by somebody in a building somewhere. It's being shared by people in a closed loop and it's not widespread or available to anybody.

We've identified over 500 domains or IP addresses used by this group when they attack. To put that in perspective, almost every modern nation that develops an operational capability in cyberspace, the first thing they need to do is get an infrastructure they use to then attack the real site of their attacks, the real intent, the real target. So there's a huge infrastructure of compromised machines or false fronts or organizations that are used for these attacks, and we found over 500 of those.

We've analyzed over 70 lure documents written in many different languages. These are the documents that you receive during a spear phishing and they're armed documents if you open up and peruse them. What's interesting is when you assess the lure documents they're related to the subjects and interests of the people who are receiving these documents. So a lot of work is going into the backdrop or the background of the people that are being spear phished.

I can go on and on. I've got 40, 50 more pages of what they do. But I'll focus on a couple things that also help us attribute APT28's activities to the Russian government. In 2015 alone, we saw APT28 leverage five zero-days, at least based on our observables. A zero-day is an attack that does not have a patch available for it. It will work if received and you execute the file.

The best way to liken the value of a zero-day is, the minute it's used and it's been weaponized, its value goes down incredibly fast. So when you see these things, they're mostly in the—they're mostly in the toolbox of a nation-state at this point. Over the last ten years, the security industry has done a great job making the cost of zero-days go up and to the right, and we're seeing APT28 deploy zero-days as needed.

They're also extremely hard to detect once they're in your network, because they rely on the tools your system administrators rely on. So they're pretty—I always say they turn to ghosts almost. The minute they're in, you're likelihood of detecting them if you don't detect the initial breach goes down exponentially. So they have zero-day capability. They operate using your tools and they operate very hard to detect.

I want to share with you three observations that I saw emerge in 2014 that I did not see prior to responding to these state actors. I had the privilege of responding to them when I was in the Air Force, probably a different group, but a group that we attributed to the Russian government. Every time I responded to them on the front lines, if they knew we were watching them they would evaporate. We never got to observe the tools, tactics, and procedures of Russian state-sponsored intrusions in the late 1990s and early 2000s. They didn't let us do it.

For some reason, in August of 2014 we were responding to a breach at a government organization and during our response our front-line responder said: They know we're there, they know we're observing them, and they're still doing their activities. So I actually flew in, sat on the front lines. It's the first I have seen it.

To me that was big news because I had a 20-year run from 1993 to about 2014 where they never changed the rules of engagement. I'd say they changed in August or September 2014.

The second thing they did, they started operating at a scale and scope where you could easily detect them. We were observing and orienting on them. They were letting us do it, but their scale and scope became widely known to many security organizations, and we all started working together to get better visibility and fidelity into their tools, tactics, and procedures.

Lastly, something that I wouldn't have predicted, but we also witnessed for the first time in 2014, is a group that we'd attribute to the Russian government compromising organizations and then suddenly the documents were being leaked out in a public forum through hacktivist personas, which we have not seen.

In conclusion, today and into the foreseeable future it is our view that the United States is going to continue to see these things happen. While many organizations are actively trying to counter these attacks, there is such an asymmetry between offense and defense in cyberspace that it's really hard for any organization to modernize and prevent these intrusions from occurring when you have a state-sponsored attacker.

Therefore, we need to explore ways both within and outside of the cyber domain to help deter these attacks.

Lastly, I always say if I had five minutes to talk to the Senate, what would I say? Well, here it is. I think we have to first start with we've got to get attribution right. We've got to know who's hacking us so we can establish a deterrent, and this gives us a great opportunity to make sure we have the tools necessary and the international cooperation necessary to have attribution. When you have attribution right, then you can consider the proportional response and the other tools at your disposal as diplomats to make sure we have the deterrence we need.

Thank you very much for this opportunity.

[The prepared statement of Mr. Mandia follows:]

FireEye

Prepared Statement of Kevin Mandia, CEO of FireEye, Inc.
before the United States Senate Select Committee on Intelligence

March 30, 2017

Thank you, Mr. Chairman, Vice-Chairman Warner, and Members of the Senate Intelligence Committee, for the opportunity you have given me today to share our observations and our experiences regarding this important topic, as well as for your leadership on cybersecurity issues. As requested, I am going to discuss three topics here today: 1) the role of overt and covert cyber operations in support of Russian active measures, disinformation, and influence campaigns; 2) the cyber capabilities and techniques attributed to Russian state and non-state actors; and 3) recommendations to prevent and mitigate the threat posed by such cyber operations.

1. Background.

Before I turn to your specific questions, let me share some background on myself and my company to inform the context of my narrative. I have been working in cybersecurity for over two decades, since I was first stationed at the Pentagon at the outset of my career as a Computer Security Officer in 1993. During my time investigating computer intrusions while I was in the Air Force, I came to recognize that the biggest cyber threats to our infrastructure were intrusions from other countries, most notably Russia and China. I founded Mandiant in 2004 to create a company with that could effectively respond to these threats and innovate technologies to help detect and respond to advanced attacks. Fast forward a few years, Mandiant was bought by FireEye, and I became FireEye's CEO last June in 2016.

As I testify today, FireEye employees are on the front lines of the cyber battle, responding to active computer intrusions at dozens of the largest companies and organizations on a global scale, including incidents in cyber "hot zones" such as the Middle East and Southeast Asia. Over the last 13 years, we have responded to incidents at hundreds of companies around the world. During that time, we have investigated millions of systems, and we receive calls almost every single day from organizations that have suffered a cybersecurity breach.

In addition to the 300-plus security professionals responding to computer intrusions, FireEye has over 150 cyber-threat analysts on staff in 19 countries and speaking 32 different languages, to help us predict threats and better understand the adversary – often by considering the political and cultural environment of the threat actors. We have an enormous catalog of threat intelligence, and it continues to grow everyday coincident with the continually increasing attacks on organizations around the world.

The information I will share today, then, is derived from our experiences responding to computer security breaches, as well as intelligence derived from our experienced team of cyber threat analysts and collected from more than 5000 customers who use our products to detect intrusions into their networks and respond to these attacks.

2. The Role of Overt and Covert Cyber Operations in Support of Russian Active Measures, Disinformation, and Influence Campaigns.

The role of nation-state actors in cyber attacks was perhaps most widely revealed in February 2013 when Mandiant released the report, "APT1: Exposing One of China's Cyber Espionage Units," which detailed a professional cyber espionage group based in China.[1] Several months later in 2014 we released another report, this time regarding Russian cyber activities, entitled, "APT28: A Window into Russia's Cyber Espionage Operations?"[2] In that report, FireEye identified APT28 as a suspected Russian government-sponsored espionage actor, basing our conclusion on forensic details left in the malware employed since at least 2007. Since release of the initial report on APT28, we have continued to gather intelligence and collect data on the group's activities, and most recently, in January of this year, released "APT28: At the Center of the Storm"[3] which provides additional detail on the continued evolution of Russian cyber operations.

As shown in our most recent report, an analysis of the activities of APT28 indicates the group's interest in foreign governments and militaries, particularly those of Europe, as well as regional security organizations. In addition, our research indicates that APT28 network activity has likely supported information operations designed to influence the domestic politics of foreign nations. We provide an extensive listing of targets including the World Anti-Doping Agency (WADA), the U.S. Democratic National Committee, Mr. John Podesta, the U.S. Democratic Congressional Campaign Committee (DCCC), as well as TV5Monde and the Ukrainian Central Election Commission (CEC).

All of these breaches involved the theft of internal data – mostly emails – that was later strategically leaked through multiple forums and propagated in a manner almost certainly intended to advance particular Russian Government goals. We noted that the combination of network compromises and subsequent data leaks align closely with the Russian military's publicly stated intentions and capabilities. Russian strategic doctrine has for a long time included what the West terms 'information

[1] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[2] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

[3] https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf.

operations' which have been further developed, deployed and modernized. The recent activity in the United States is one of many instances of such operations conducted in support of Russian political objectives. I note that our conclusions were consistent with the U.S. Office of the Director of National Intelligence report released on January 7, 2017 in which this activity is described as "an influence campaign."[4]

3. Cyber Capabilities and Techniques Attributed to Russian State and Non-State Actors

So how was this done, and why do we assess that the Russian government was likely behind this activity? ***Let me first speak to the methodologies used.*** During the course of our APT28 investigations, we analyzed over 550 customer malware variants, identified approximately 500 domains, over 70 lure documents and dozens of spear phishing emails to help us understand their tools, techniques, and procedures. We find that APT28 continues to evolve its toolkit and refine its tactics in an effort to maintain its operational effectiveness in the face of heightened public exposure and scrutiny. In addition to the continued evolution of the group's first-stage tools, we have also noted that APT28 is:

1 - Leveraging at least five zero-day vulnerabilities in Adobe Flash Player, Java, and Windows in 2015 alone, including CVE-2015-1701, CVE-2015-2424, CVE-2015-2590, CVE-2015-3043, CVE-2016-7193, and CVE-2015-7645.
2 – Increasing its reliance on public code depositories, such as Carberp, PowerShell Empire, P.A.S. webshell, Metasploit modules, and others in a likely effort to accelerate their development cycle and provide plausible deniability.
3 - Obtaining credentials through fabricated Google App authorization and Oauth access requests that allow the group to bypass two-factor authentication (2FA) and other security measures, and
4 - Moving laterally through a network relying only on legitimate tools that already exist within victims' systems, at times forgoing their traditional toolset for the duration of the compromise.

Over the past two years we have witnessed an escalation of APT 28's overall activities and one notable change in its rules of engagement. Specifically, since 2014 we have seen APT28 in many instances compromise a victim organization, steal information, and subsequently leak the stolen data into the public. Many of these leaks have been conducted through the use of "false hacktivist personas", including, among others, "CyberCaliphate", "Guccifer 2.0", "DC Leaks", "Anonymous Poland", and "Fancy Bears' Hack Team". These "personas" appropriated pre-existing hacktivist or political brands likely to obfuscate their true identify, provide plausible deniability, and to create the perception of credibility.

[4] https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

Although we can link the collection activity to APT28, we have not been able to establish whether the APT28 operators themselves directly control the false personas that then leak material or if that responsibility instead resides with a separate entity. However, we do see similar patterns in infrastructure procurement between APT28 and some personas to suggest they played at least some role. For example, we believe that the actors behind the DCLeaks persona attempted to register the domain "electionleaks.com" one-week prior to "DCLeaks.com" in April 2016 – approximately two months prior to the first election-related leaks. These domains were registered using the service provider we have seen APT28 frequently use in the past to support cyber attacks. Thus, our intelligence indicates that APT28 likely operated with the knowledge that the data they stole during cyber intrusions would leverage these domains for public exposure of the data.

I include the following timeline and analysis to illustrate the use of these techniques over the last few years.

In June of 2014, Ukrainian officials revealed the investigation into the compromise of the Ukrainian Central Election Commission (CEC) internal network identified custom malware traced to APT28. During the May 2014 Ukrainian presidential election, purported pro-Russian hacktivists "CyberBerkut" conducted a series of malicious activities against the CEC, including a system compromise, data destruction, a data leak, a distributed denial-of- service (DDoS) attack, and an attempted defacement of the CEC website with fake election results.

In February of 2015, FireEye identified APT28 (CORESHELL) traffic beaconing from TV5Monde's network, revealing APT28 had compromised TV5Monde's network. In April 2015, alleged pro-ISIS hacktivist group CyberCaliphate defaced TV5Monde's websites and social media profiles and forced the company's 11 broadcast channels offline. We identified overlaps between the domain registration details of CyberCaliphate's website and APT28 infrastructure.

In July of 2016, the U.S. Democratic Congressional Campaign Committee (DCCC) announced that it was investigating an ongoing "cybersecurity incident" that the FBI believed was linked to the compromise of the DNC. House Speaker Nancy Pelosi later confirmed that the DCCC had suffered a network compromise. Investigators indicated that the actors may have gained access to DCCC systems as early as March. In August, the Guccifer 2.0 persona contacted reporters covering the U.S. House of Representative races to announce newly leaked documents from the DCCC pertaining to Democratic candidates. From August to October, Guccifer 2.0 posted several additional installments of what appear to be internal DCCC documents on its WordPress site.

Between March and October of 2016, investigators found that John Podesta, Hillary Clinton's presidential campaign chairman, was one of thousands of individuals targeted in a mass phishing scheme using shortened URLs that security researchers attributed to APT28. Throughout October and into early November, WikiLeaks published 34 batches of email correspondence stolen from Mr. Podesta's personal email account. Correspondence of other individuals targeted in the same phishing campaign, including former Secretary of State Colin Powell and Clinton campaign staffer William Rinehart, were published on the "DC Leaks" website.

In April through September, 2016, the U.S. Democratic National Committee (DNC) suffered a network compromise and a subsequent investigation found evidence of two breaches, attributed to APT28 and APT29. FireEye analyzed the malware found on DNC networks and determined that it was consistent with our previous observations of APT28 tools. In June 2016, shortly after the DNC's public announcement about the breach, the Guccifer 2.0 persona claimed responsibility for the DNC breach and leaked documents taken from the organization's network. Guccifer 2.0 continued to leak DNC documents through September of 2016.

And finally, in September of 2016, WADA confirmed that APT28 had compromised its networks and accessed athlete medical data. On Sept. 12, 2016, the "Fancy 'Bears' Hack Team" persona claimed to have compromised WADA and released athletes' medical records as "proof of American athletes taking doping."

Let me now turn to explaining ***why we assess that the Russian government was likely behind this activity***.

In order to make such an assessment, we reviewed and compared intrusion methodologies and tools, malware or authored exploits and use of shared personnel. We also examined forensic details that were left behind, such as the specific IP addresses or email addresses from spear phishing attacks, file names, MD5 hashes, timestamps, custom functions, encryption algorithms, or backdoors that may have command and control IP addresses or domain names embedded.

Targeting was also critical to our assessment. Knowing the types of organizations, individuals, or data that a threat group targets provided us with insight into the group's motivations and objectives. Gathering this type of data about a group typically requires visibility into the group's operational planning, their initial attacks or infection attempts, or into actual victim environments. We track all of the indicators and significant linkages associated with identified threat groups in a proprietary database that we have developed over many years comprised of millions of nodes and linkages between groups, and then analyze this information carefully in the context of the relevant political and cultural environment to develop our assessments.

Based on our extensive collected intelligence and analysis in this instance, we have determined that APT28's cyber operations are consistent with government sponsorship and control. Specifically, APT28 has relied upon a steady supply of sophisticated tools that would only have been available to a nation-state or state-protected contractor, pursued targets where Russian interests would be high, maintained a level of activity over several years requiring significant financial and personnel resources with no clear profit motive, and closely integrated its cyber attacks into broader propaganda efforts of benefit to a nation-state actor.

There are alternative explanations for APT28's sponsorship, however in our view these only appear plausible for explaining one incident at a time, and are not credible in the context of the totality of APT28's operations. By combining an increasingly wide range of technical intelligence, hands-on remediation of compromised systems, and an understanding of Russia's geopolitical aims based on its own public statements, our confidence in assessing Russian government sponsorship or control of APT28 has only grown since release of our initial report in 2014.

Moreover, the activities of APT28 are not consistent with any basic criminal activities to which we have responded, nor are they consistent with those perpetrated by a lone actor. The size of the infrastructure, the targeted information, the amount of malware and the totality of the sophistication, suggests a long-term, well-resourced espionage campaign in which Russia is the benefactor.

In summary, while we do not have pictures of a building, names of individuals, or a government agency to name, our assessment is supported by evidence of long-standing, focused operations that indicates a Russian government sponsor and government capability.

4. Recommendations to Prevent and Mitigate the Threat Posed by Such Cyber Operations.

Today, and into the foreseeable future, it is our view that the United States will face a motivated, technically sophisticated, and well-resourced adversary intent on accessing our private data, and potentially leaking it publicly. While many organizations are actively trying to counter these attacks, there currently exists a sizeable gap between what their safeguards can prevent and the ability of motivated attackers to circumvent those safeguards. Therefore, we will need to explore ways, both within and outside the cyber domain, to help deter these attacks.

Of course, all enterprises – private sector or government – should work to accurately assess their own risk profiles, and utilize updated technology and best practices to protect their networks and systems. However, organizations cannot buy, hire or train their way to perfect security and we must consider effective deterrence and proportional response outside of the cyber domain as well.

While diplomacy is not often cited as a primary tool in this arena, evidence collected regarding Chinese activity appears to reinforce its potential effectiveness. We conducted a comprehensive study of 182 compromised U.S. targets by 72 Chinese cyber threat groups going back to 2013, and we saw a sharp decline in these operations after September 2015 – when President Obama and President Xi met and specifically agreed to curtail cyber operations for commercial benefit. To be sure, Chinese cyber operations for traditional espionage remain, and US companies are still targeted for the security, political, economic, and military intelligence that Beijing seeks. However, it appears that the agreement had an impact, demonstrating that diplomacy can also be a useful tool for reducing the cyber threat both countries face, coupled with the public-private sector collaboration. This experience leaves me optimistic that with the combined efforts of both governments and the private sector, diplomatic engagement with Russia and other nations to restrict harmful cyber activity would be enforceable.

In addition to Russia, North Korea and Iran have been tied to a series of escalating attacks that go back several years. We have been surprised by the audacity of the sponsoring nation and their willingness to surpass "redlines" that we previously believed were established. It is entirely reasonable to suspect that these nations are emboldened by each other's behavior, and it is important to note that any response to the Russian cyber activities discussed today will likely be assessed by other countries.

Again, we applaud the leadership shown by this Committee to bring important issues such as those discussed today to light, and we in the private sector look forward to continuing to work with you to disseminate and support industry best practices and encourage adoption of comprehensive and effective cybersecurity programs across government and industry. I look forward to answering your questions today.

* * *

Chairman BURR. Thank you.

General, welcome.

STATEMENT OF GENERAL (Ret.) KEITH B. ALEXANDER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, IRONNET CYBERSPACE

General ALEXANDER. Chairman, Ranking Member, distinguished members of the committee: It's an honor to be here, I think. I want to pick up from where Kevin left off. I want to raise it up a strategic level.

I had the opportunity this morning to see on the news you and the Ranking Member talk about approaching this in a bipartisan way, approaching the solution in a bipartisan way. When you look at the problem and what we're facing, it's not a Republican problem, it's not a Democratic problem. This is an American problem and we all have to come together to solve it. I think that's very important.

If we step back and look at this, I want to cover several key areas to give my perspective on what's going on. First with respect to technology, communications is doubling every year. We're getting more devices attached to the network. This network is growing like crazy, and so are the vulnerabilities. Our wealth, our future, our country is stored in these devices. We've got to figure out how to secure them.

With those vulnerabilities, we've seen since 2007 attacks on countries like Estonia, Georgia, Ukraine, Saudi Arabia—a whole series of attacks, and then Crimea and others, and then the attacks on the power grid in the Ukraine. What's clear is this network and these tools have gone from interesting exploitation for governments and crime to elements of national power.

I think from my perspective, when we consider that this is now an element of national power, we have to step back and say: What's their objective? Sun-Tzu said: "Know yourself and know your enemy and you'll be successful in a thousand campaigns." What's Russia trying to do and why are they trying to do it?

From my perspective as I look at it from my background, it's clear it's not just trying to go after the Democratic National Convention or others. This is widespread and a campaign that they're looking at doing that will drive wedges between our own political parties and between our country and NATO and within NATO and within the European Union.

Why? I believe when you look at Russia and if you were to play out on a map what's happened over the last 25 or 30 years, they see the fall of the Soviet Union and the impacts on their near border and all these as impacts on them.

I bring all this up because one of the questions that's out in the press is: Do we engage the Russians or do we not? Every administration that I'm familiar with, including the Obama administration, started out with: We're going to engage them. In fact it was called "the reset button." While that didn't go far, I believe this Administration should do the same.

When I look at what's going on here, there's another opportunity that we have. When you look at the characteristics of leaders in this Administration, we have people with great business experience—the President and the Secretary of State—and great national security experience. In addressing the problem that we're now dealing with, this is a new area. We're seeing cyber as an element of national power. How do we now engage Russia and other countries and set the right framework?

I believe we have to engage and confront: engage them in those areas that we can, set up the right path, reach out, and cool this down, I really do. We've got to fix that.

At the same time, we've got to let them know what things they can't do and why they cannot do those—set those standards. I think what this group can do and what you are doing, Chairman and Vice Chairman, is make this a bipartisan approach: solve this for the good of the Nation.

We look at cyber security and what Kevin gave you in terms of what industry sees and what government sees. Over the last decade, we have jointly worked on coming up with cyber legislation, how industry and government works together. If we're going to address attribution and other issues, we also have to set up the way for our industry and sectors to work with the government so that that attribution of things that the government knows and those things that industry knows can be used for the common good.

It's interesting that sitting in the presidential commission, one of the things that came out when we looked at what's going on was, what's our strategy? At times people looked at this as it's a government issue and it's an industry issue. It's not. This is something that we need to look at as a common issue. "For the common defense," it's in the preamble to the Constitution and it's something that we should all look at. Then we should see, how do we extend that to our allies?

So I would step back and encourage, encourage you to step back and look at the strategy: What's Russia trying to do and why are they trying to do it, and how do we engage them? At the same time, we need to address our cyber security issues and go fix those and get on with that.

Thank you very much, Mr. Chairman.

[The prepared statement of General Alexander follows:]

Prepared Statement of GEN (Ret) Keith B. Alexander[*]
on
Disinformation: A Primer in Russian Active Measures and Influence Campaigns
before the
United States Senate Select Committee on Intelligence

March 30, 2017

Chairman Burr, Vice Chairman Warner, Members of the Committee: thank you for inviting me to discuss "*Disinformation: A Primer in Russian Active Measures and Influence Campaigns*" with you today, and specifically, how the ongoing revolution on how we create and communicate information, particularly in cyberspace, makes it easier for nations like Russia to undertake successful active measures campaigns, particularly in the realm of information operations, including overt and covert propaganda and disinformation efforts, in furtherance of national political goals. I would like to briefly touch on some of the things we ought do, working together, to combat such activities and to protect our nation—our government, our private sector, and our people—from these and other threats in cyberspace. In particular, I believe it is critical that our public and private sectors work more closely together. This Committee and the relevant agencies in the Executive Branch can play a key role in helping make that happen.

I want to thank both Chairman Burr and Vice Chairman Warner for your bipartisanship and for making cybersecurity and counterintelligence top priorities for this committee, including the Chairman's work on the Cybersecurity Information Sharing Act and Vice Chairman Warner's efforts with Senate Cybersecurity Caucus and on the Digital Security Commission Act. It is also worth noting that this committee has held more than 10 hearings and briefings over the last two years to examine the scale and scope of Russian activities,[1] and that as early as June 2016, this committee sought to require the establishment of a committee "[t]o counter active measures by Russia to exert covert influence over peoples and governments."[2]

Active measures have been utilized by Russia since the 1920s, perhaps most famously during the Cold War. Retired KGB Maj. Gen. Oleg Kalugin describes these "subversion" activities as "the heart and soul of the Soviet intelligence" that were specifically designed to "weaken the West, to drive wedges in the Western community alliances of all sorts, particularly

[*] Gen. (ret.) Keith B. Alexander is the former Director, National Security Agency and the Founding Commander, United States Cyber Command. Currently, he is the President and CEO of IronNet Cybersecurity and recently completed service as a member of the President's Commission on Enhancing National Cybersecurity.

[1] *See* Federal News Service, *Transcript: Full Committee Hearing on Russian Intelligence Activities*, Senate Select Committee on Intelligence (Jan. 10, 2017).

[2] *See* Intelligence Authorization Act for Fiscal Year 2017 § 501, *available online at* <https://www.intelligence.senate.gov/legislation/intelligence-authorization-act-fiscal-year-2017-reported-june-6-2016>.

NATO, [and] to sow discord among allies."[3] According to Kalugin, this "worldwide campaign...conducted and manipulated by the KGB," included "all sorts of forgeries and faked material...targeted at politicians, the academic community, [and the] public at large."[4] Likewise, Vasili Mitrokhin, a former senior KGB archivist, described the bulk of KGB active measures as "'influence operations' designed to discredit the [United States]...[through] disinformation fabricated by...the active measures branch of the [KGB]."[5] During the Cold War, these activities included efforts to undermine the FBI, the State Department, and civil rights leaders, as well as efforts to incite racial violence and hatred, including through the dissemination of false information about private organizations, individuals, and the government via false publications and materials misattributed to particular individuals or organizations, among other things.[6]

In many ways, this description of historic Soviet active measures is strikingly similar to what this committee described last year as Russian covert influence active measures, including the "[e]stablishment or funding of [] front group[s]...[c]overt broadcasting...[m]edia manipulation...[and] [d]isinformation and forgeries, funding agents of influence, incitement, and offensive counterintelligence, assassinations, or terrorist acts."[7] Director Clapper likewise indicated that "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" and that "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....[and] demonstrate[s] a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[8]

At the same time, it is certainly worth noting that aggressive efforts to collect intelligence on our elections are not new – indeed, ODNI has made clear that in 2008, the "foreign intelligence services...track[ed the] election cycle like no other" and "targeted the campaigns...[m]et with campaign contacts and staff[,] [u]sed human source networks for policy insights, [e]xploited technology to get otherwise sensitive data, [and] [e]ngaged in perception management to influence policy."[9] Indeed, Russia use of *kompromat* (compromising information), *maskirovka* (military deception), and proxy assets to disseminate propaganda (both official and unofficial) is likewise not new.

[3] *See* CNN, *Inside the KGB: An Interview with Maj. Gen. Oleg Kalugin* (Jan. 1998), *available online* at <https://web.archive.org/web/20070206020316/http:/www.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/>.

[4] *Id.*

[5] *Id.*

[6] *See, e.g., id.* at 234-39.

[7] *See* Intelligence Authorization Act for Fiscal Year 2017 § 501.

[8] *Id.*

[9] *See* ODNI, *Unlocking the Secrets: How to Use the Intelligence Community* (Dec. 10, 2008), at 12-13, available online at <https://icontherecord.tumblr.com/post/143906537893/new-freedom-of-information-act-request-documents>.

Efforts like these are empowered by the modern era of technology and, in particular, by the scale and scope of information traversing our networks. The amount of information circulating the globe via IP networks will reach 2.3 zettabytes by 2020, the "equivalent of all the movies ever made [] cross[ing] the global Internet every 2 minutes."[10] And it will be transmitted over 26.3 billion networked devices, more than three IP-connected devices per person worldwide.[11] At the same time, according to Pew Research, "a majority of U.S. adults – 62% – get news on social media," and given the penetration of some of these services, message targeting can be broad in scale yet highly focused. For example, Pew estimates up to 44% of the general population in the United States gets some measure of its news on Facebook.[12] And given the continued development and rapid iteration of technology and Internet-enabled platforms, these trends are likely to continue and even accelerate.

While this might not seem particularly troubling at first blush, it is worth evaluating in the context of potential efforts to manipulate information. Back in the Cold War era, if the Soviet Union sought to manipulate information flow, it would have to do so principally through its own propaganda outlets or through active measures that would generate specific news: planting of leaflets, inciting of violence, creation of other false materials and narratives. But the news itself was hard to manipulate because it would have required actual control of the organs of media, which took long-term efforts to penetrate. Today, however, because the clear majority of the information on social media sites is uncurated and there is a rapid proliferation of information sources and as other sites that can reinforce information, there is an increasing likelihood that the information available to average consumers may be inaccurate (whether intentionally or otherwise) and may be more easily manipulable than in prior eras. It is likewise easier to generate "buzz" and "hype" about particular events or storylines (again, whether accurate or inaccurate) because of the speed at which news is conveyed amongst the population.

These efforts also take place in the context of larger cyber efforts by our peer competitors, including the ongoing, massive theft of intellectual property from American companies and the use of actual destructive attacks on both public and private sector entities in the United States and abroad.[13] The reality is that as a free society, we have many vulnerabilities and leave ourselves open to threats—including propaganda and disinformation attacks—that more authoritarian nations may be more capable of combatting by limiting access to resources or restricting the freedom of their people. And it is worth noting that our enemies today need not attack our government to have a substantive strategic effect on our nation. Attacking civilian or

[10] *See* Cisco, *The Zettabyte Era—Trends and Analysis* (June 2016) at 1, 4, *available online at* <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf>

[11] *See Zettabyte Era*, n. 3 *supra* at 2.

[12] *Id.*

[13] These activities include destructive attacks against Saudi Aramco and Qatari RasGas in 2012, more recent attacks against the Saudi government, and destructive attacks conducted by nation-states against private institutions in the United States, including the Las Vegas Sands Corporation and Sony Corporation, not to mention massive disruptive attacks targeting American financial institutions. *See* Keith B. Alexander, *Prepared Statement on A Borderless Battle: Defending Against Cyber Threats*, U.S. House Committee on Homeland Security (March 22, 2017), at 2 & n. 1-3, available online at <http://docs house.gov/meetings/HM/HM00/20170322/105741/HHRG-115-HM00-Wstate-AlexanderK-20170322.pdf>.

economic targets, including through disinformation, may be a more effective approach in the modern era, particularly for asymmetric actors like terrorist groups. Moreover, as the number of nations that possess the capability to exploit and attack continues to grow, there is more of a chance that those with less of an incentive to act in line with appropriate state-to-state behavior will begin using cyber capabilities in a more aggressive way.

What all of this fundamentally means is that the future of warfare—including information operations—is here, and we need to structure and architect our nation to defend our country in cyberspace. Specifically, in my view, it is critical that as a nation, we fundamentally rethink how the government and the private sector relate to one another in cyberspace. We need to draw clear lines and make explicit certain responsibilities, capabilities, and authorities. And because the private sector controls the vast majority of the real estate in cyberspace, particularly when it comes to critical infrastructure and key resources,[14] there is no question that the government and private sector must collaborate. We need to recognize that neither the government nor the private sector can capably protect the systems and networks that our nation relies upon without extensive and close cooperation.

For the government to effectively work with the private sector to secure the nation in cyberspace, perhaps the single most important thing the government can do is to build real connectivity and interoperability with the private sector. This effort must be a two-way partnership between government and the private sector: the government can and must do more when it comes to partnering with the private sector, building trust, and sharing threat information—even highly classified threat information—at network speed, and in a form that can be actioned rapidly. Building out a cross-cutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to the air traffic control picture. Just as the air traffic control picture ensures our aviation safety and synchronizes government and civil aviation, the cyber common operational picture can be used to synchronize a common cyber defense for our nation, drive decision-making, and enable rapid response across our entire national cyber infrastructure. In my view, if properly implement, this could prove a critical defensive capability for the nation.

While much remains to be done to fully put our nation on a path to real security in cyberspace, I am strongly hopeful for our future. With your leadership, Mr. Chairman, and that of the Vice Chairman, working together collaboratively across the aisle and with the White House and key players in the private sector, as well as other key committees in Congress, I think we can achieve some real successes in the near future.

[14] *See, e.g.*, Office of the Director of National Intelligence, Office of the Program Manager-Information Sharing Environment, *Critical Infrastructure and Key Resources*, available online at <https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources> ("The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation's physical and economic security.").

Chairman BURR. Thank you, General.

Mr. Rid.

STATEMENT OF THOMAS RID, Ph.D., PROFESSOR OF SECURITY STUDIES, KING'S COLLEGE, LONDON

Dr. RID. Chairman Burr, Vice Chairman Warner, members of the committee: Thank you for giving me the opportunity to speak today about active measures.

Understanding cyber operations in the 21st century is impossible without first understanding intelligence operations in the 20th century. Attributing and countering disinformation today is therefore also impossible without first understanding how the United States and its allies attributed and countered hundreds of active measures throughout the Cold War.

Nobody summarized this dark art of disinformation better than Colonel Rolf Wagenbreth from the Stasi, who headed the Department X there. He said, and I quote: "A powerful adversary can only be defeated through a sophisticated, methodical, careful, and shrewd effort to exploit even the smallest cracks within our enemies and within their elites."

The tried and tested way of active measures is to use an adversary's existing weaknesses against himself, to drive wedges into preexisting cracks. The more polarized a society, the more vulnerable it is; and America in 2016, of course, was highly polarized, with lots of cracks to drive wedges into. But not all wedges; improved high-tech wedges that allowed the Kremlin's operatives to attack their target faster, more reactively, and at a far larger scale than ever before.

But the Russian operatives also left behind more clues and more traces than ever before, and assessing these clues and operations requires context. First, in the past 60 years—and we talked about this already this morning—active measures became the norm. The Cold War likely saw more than 10,000 active measures across the world. This is a remarkable figure. The lull in the 1990s and the 2000s I think was an exception.

Second, in the past 20 years aggressive Russian digital espionage campaigns—Kevin Mandia mentioned one of them—became the norm as well. The first major state-on-state campaign was called Moonlight Maze, and it started in 1996. In 2000 a shift in tactics became apparent, especially in Moscow's military intelligence agency, GRU. A once careful, risk-averse, and shrewd and stealthy espionage actor became more careless, risk-taking, and error-prone. One particularly revealing slip-up resulted in a highly granular view of just one slice of GRU targeting between March 2015 and May 2016 in the lead-up to the election. That slice contained more than 19,000 malicious links targeting nearly 7,000 individuals across the world, really.

Third, in the past two years now, coming closer to the present, Russian intelligence operations began to combine those two things, hacking and leaking. By early 2015, military intelligence was targeting defense and diplomatic entities at high tempo. Among the targets were the private accounts, for example, of the current Chairman of the Joint Chiefs of Staff, General Dunford, or current Assistant Secretary of the Air Force Daniel Ginsberg, or the current U.S. Ambassador to Russia John Tefft, and his predecessor Michael McFaul; a large number of diplomatic and military officials in Ukraine, Georgia, Turkey, Saudi Arabia, Afghanistan, and many countries bordering Russia, especially their defense attachés.

All, I add, are legitimate and predictable targets for a military intelligence agency. Russia intelligence, curiously, also targeted inside Russia, critics inside Russia, for example, the hacker group Shaltay Boltai. In early 2015, GRU breached successfully not just the German Parliament, but also the Italian military and the Saudi foreign ministry.

Between June 15 and November 16, at least six different front organizations appeared, very much Cold War style, to spread some of the stolen information to the public in a targeted way.

Finally, in the past year the timeline here in the U.S. election campaign began to align. Between March 10th and April 7, GRU targeted at least 109 full-time Clinton campaign staffers. These are only full-time core staffers, not their volunteers. These are not even counted here. Russian intelligence targeted Clinton's senior advisor Jake Sullivan in at least 14 different attempts beginning on 19 March. GRU targeted even Secretary Clinton's personal email account, but the data show that she did not fall for the trick and didn't actually reveal her password.

Military intelligence agency GRU also targeted DNC staffers between March 15 and April 11, the timing lines up nearly perfectly. About one week later, after the events that I just mentioned, the DCLeaks website was registered, getting ready to spread these data publicly. The overlap between individuals hacked by GRU and leaked on DCLeaks is nearly perfect. Out of 13 named leak victims, the available forensic evidence identifies 12 as targeted by GRU, with the exception of George Soros, by the way.

But a narrow technical analysis would miss the main political and ethical challenge. Soviet bloc disinformation specialists preferred the art of exploiting what was then called "unwitting agents." There is no contradiction in their reading between being an honest American patriot and at the same time furthering the cause of Russia. In the peace movement in the 1980s we saw that people were genuinely protesting, say, the NATO double track decision, but at the same time advancing Russian goals. There is no contradiction.

Three types of unwitting agents—and I would like to close with that—stand out: WikiLeaks; Twitter, the company itself, and I'm happy to expand later; and over-eager journalists aggressively covering the political leaks while neglecting or ignoring their provenance.

In 1965 the KGB's grandmaster of dezinformatsiya, General Ivan Agayants, inspected his active measures outpost in Prague, a particularly effective and aggressive one, and he said, quote: "Sometimes I am amazed how easy it is to play these games. If they did not have press freedom, we would have to invent it for them."

Later the Czech operative that he was speaking with in that very moment defected to the United States and testified in Congress, and I quote him to close. He said: "The press should be more cautious with anonymous leaks. Anonymity is a signal indicating that the Big Russian Bear might be involved."

Thank you.

[The prepared statement of Dr. Rid follows:]

DISINFORMATION

A PRIMER IN RUSSIAN ACTIVE MEASURES AND INFLUENCE CAMPAIGNS

HEARINGS

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

30 MARCH 2017, 2PM, HART OFFICE BUILDING

INTELLIGENCE.SENATE.GOV/HEARINGS/OPEN-HEARING-INTELLIGENCE-MATTERS-1

Thomas Rid[*]

Understanding "cyber operations" in the 21st century is impossible without first understanding intelligence operations in the 20th century. Attributing and countering disinformation operations today is therefore also impossible without first understanding how the US and its European allies attributed and countered thousands of active measures throughout the Cold War.

Active measures are semi-covert or covert intelligence operations to shape an adversary's political decisions. Almost always active measures conceal or falsify the *source*—intelligence operators try to hide behind

[*] Professor of Security Studies, King's College London. @RIDT

anonymity, or behind false flags. Active measures may also spread forged, or partly forged, *content*. The most concise description of disinformation as an intelligence discipline comes from one of its uncontested grandmasters, Colonel Rolf Wagenbreth, head of the East German Stasi's Active Measures Department X for over two decades:

> A powerful adversary can only be defeated through [...] a sophisticated, methodical, careful, and shrewd effort to exploit even the smallest 'cracks' between our enemies [...] and within their elites.[1]

The tried and tested way of active measures is to use an adversary's existing weaknesses against himself, to drive wedges into *pre-existing* cracks: the more polarized a society, the more vulnerable it is—America in 2016 was highly polarized, with myriad cracks and fissures to drive wedges into. Not old wedges, but improved high-tech wedges that allowed Moscow's operators to attack their target faster, more reactively, and at far larger scale than ever before.

Yet there was one big problem. The Russian disinformation operators also left behind more clues and traces than ever before. Thus the evidence implicating Russian intelligence in hacking-and-leaking operations over the past two years is also more granular than ever before. This digital forensic evidence can only adequately be assessed by looking at the wider picture of the 2016 influence campaign against the US election.

First: *in the past 60 years, active measures became the norm.* Russia's intelligence services pioneered *dezinformatsiya* in early twentieth century. By the mid-1960s, disinformation—or active measures—were well-resourced and nearly on a par with collection in the KGB, the Stasi's HVA, the Czechoslovak StB, and others. The Cold War saw more than 10,000 individual Soviet bloc disinformation operations.[2] The pace of Russian operations subsided during a short lull in the early 1970s, followed by an all-time high-water mark in the mid-1980s, and then a long intermission throughout the 1990s. Only in the late 2000s did disinformation begin to pick up speed again. By 2015 and especially 2016, the old playbook had been successfully adapted to a new technical environment.

Second, *in past 20 years, aggressive Russian digital espionage campaigns became the norm.* The first major state-on-state campaign was MOONLIGHT MAZE, which started in late 1996.[3] Ten years later American and European intelligence agencies and soon also an expanding number of private sector companies were tracking at least three different hacking groups linked to Russia's main intelligence agencies: tracking their implants and tools, their infrastructure, their evolving methods of operation, their targeting behavior, their evolving operational security, and—perhaps most importantly—the mistakes the Russian operators made again and again. In 2014 a shift in tactics became apparent especially in military intelligence: a once careful, risk-averse, and stealthy espionage actor became more and more careless, risk-taking, and error-prone. One particularly revealing operational security slip-up resulted in a highly granular view of just one slice of GRU[4] targeting between 16 March 2015 and 17 May 2016—that slice contained 19,300 malicious links, targeting around 6,730 individuals.[5] A high-resolution picture of Russia's digital espionage activities emerged.[6]

Third, *in past 2 years, Russian intelligence operators began to combine the two, hacking and leaking*—or digital espionage and active measures.

By early 2015, GRU was targeting military and diplomatic entities at high tempo, especially defense attachés world-wide. Among the targets are numerous senior US military officers and defense civilians, for example the private accounts of the current chairman of the Joint Chiefs of Staff, General Joseph F. Dunford; Generals Philip Breedlove, Wesley Clark, and Colin Powell; Navy Captain Carl Pistole, or current Assistant Secretary of the Air Force Daniel Ginsberg. Among the diplomatic targets were the current US ambassador to Russia, John F. Tefft; his predecessor Michael McFaul; former Permanent Representatives to NATO Ivo Daalder and Kurt Volker; and well-connected security experts Anthony Cordesman, Julianne Smith, and Harlan Ullman. The targets also included a large number of diplomatic and military officials in Ukraine, Georgia, Turkey, Saudi Arabia, Afghanistan, and many countries bordering Russia, especially their military attachés, all legitimate and predictable targets for a military intelligence agency. Russian intelligence also targeted well-known Russian critics, for example the author Masha Gessen, Garry Kasparov, and Alexei Navalny, as well as the Russia-based hacker group Shaltay Boltai. In early 2015, the same entity often referred to as APT28 or FANCYBEAR had successfully breached not just the German Parliament;[7] the Italian military;[8] but also Saudi Arabia's foreign ministry.

Then, in May and June 2015, the first publicly known large-scale disinformation operation, dubbed "Saudi Cables," tested an innovative tactic: hacking a target, exfiltrating compromising material (*kompromat*), setting up a dedicated leak website under false flag, and then passing files to Wikileaks for laundering and wide distribution.[9] Between June 2015 and November 2016, at least six front organizations sprung up as outlets for compromised files by GRU: Yemen Cyber Army, Cyber Berkut, Guccifer 2.0, DC Leaks, Fancy Bears Hack Team, and @ANPoland.

Finally, *in past year, the timeline of US-election operations began to align.* In early March, GRU began to train its well-established, semi-automated targeting tools from worldwide military and diplomatic targets to US political targets. Between 10 March and 7 April, GRU targeted at least 109 Clinton campaign staffers with 214 individual phishing emails (with 8 more attempts on 12 and 13 May). 36 times Clinton staffers clicked a malicious link (the success rate of actually breaching the account after a victim clicked this link is 1-in-7). Russian intelligence targeted Jake Sullivan in at least 14 different attempts beginning on 19 March, each time with a different malicious link against two of his email addresses. GRU targeted Hillary Clinton's personal email account at least two times in March, but the available data show that she did not fall for the password reset trick. The military intelligence agency also targeted DNC staffers with 16 emails between 15 March and 11 April, and 3 DNC staffers were tricked into clicking the treacherous "reset password" button on 6 April 2016.

Less than two weeks later, on 19 April, the front website DCLeaks.com was registered as a leak outlet for hacked files.[10] The overlap between individuals hacked by GRU and leaked by "DC Leaks" aligns nearly perfectly: out of 13 named leak victims,[11] the available forensic evidence identifies 12 as targeted by GRU, with a spike of activity in late March 2016 (all US victims except George Soros).[12] The Russian-orchestrated leak operation continued apace during the hot summer of 2016 using, often with small batches of files released in more than 80 individual leaks for the best publicity effect.

The *publicly available* evidence that implicates Russian intelligence agencies in the 2016 active measures campaign is extraordinarily strong. The DNC hack can be compared to a carefully executed physical break-in in which the intruders used uniquely identical listening devices; uniquely identical envelopes to carry the stolen files past security; and uniquely identical getaway vehicles.

Listening devices (*implants*): the DNC intruders reused implants that had been deployed in a very large number of Russian intrusions across many hundreds of targets in dozens of countries over the past decade.[13] The implants shared many common features, among them a specific communication protocol and other modular functionality—comparable to using the exact same listening device in different buildings without ever publishing the design plans for it.[14]

Getaway vehicle (*command-and-control infrastructure*): Russian intelligence agencies reused command-and-control sites—a common technique comparable to using the same getaway car with identical license plates in a burglary.[15] The infrastructure re-use is not easily forged, and allowed investigators to link the DNC breach to other breaches with high confidence, particularly to the German Bundestag hack, which the German government had already attributed to Russian military intelligence.

Envelopes (*encryption keys*): Russian operators also reused encryption keys across different targets, notably in targeting Ukrainian artillery units deployed against Russia-supported separatists as well as a Democratic organization in Washington, as well as in at least 75 other implants across a large number of targets world-wide.[16] This cryptographic overlap is an exceptionally strong forensic link, comparable to a human fingerprint.

But a narrow technical analysis would miss the main political and ethical challenges. Soviet bloc disinformation specialists perfected the art of exploiting *unwitting agents*.[17] In early 1980s, for example, there was no contradiction between being a genuine, honest, innocent peace activist against NATO's Double Track Decision—and at the same time being an unwitting agent for the Soviet cause. The internet has made unwitting agents more potent, more persistent, and more pervasive.

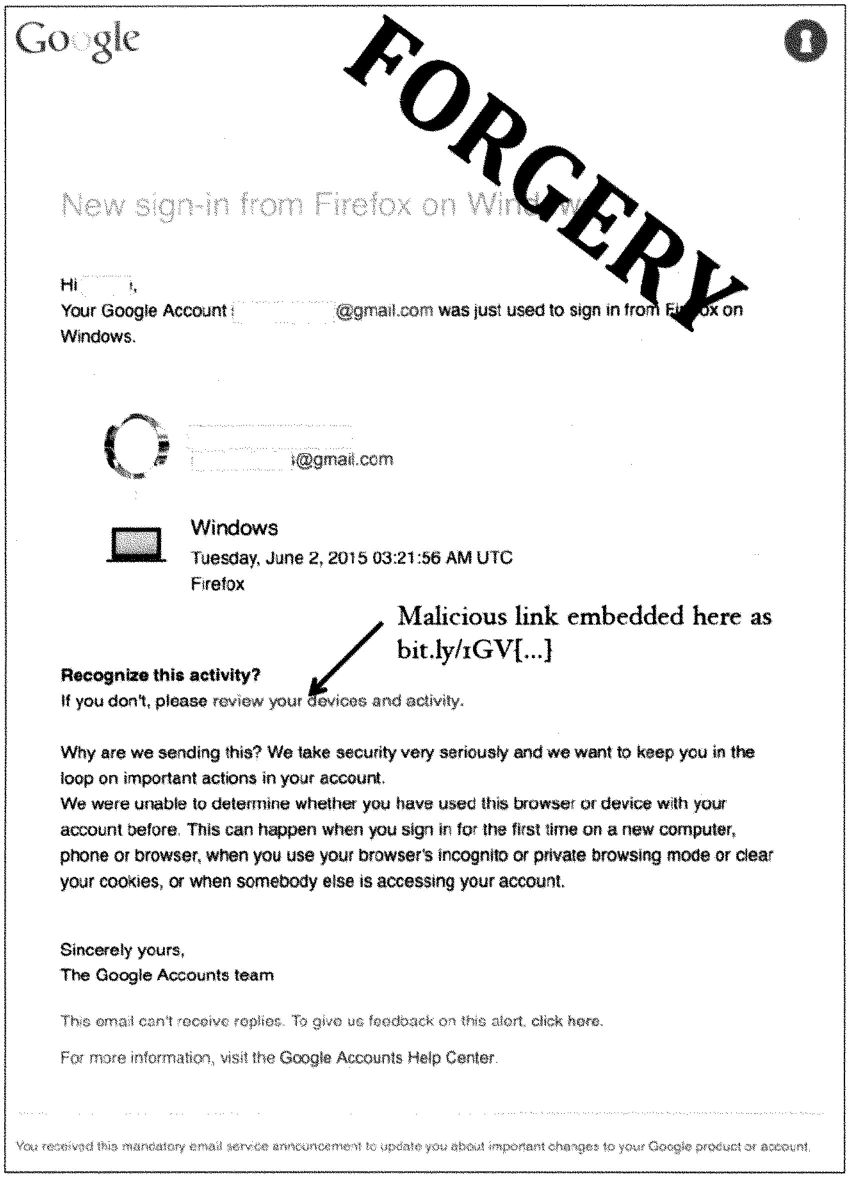
Three different types of unwitting agents stand out in the 2016 campaign. The first is Wikileaks. During the 2016 influence operation Russian intelligence agencies have abused anonymity tools for hacking[18]—and for leaking. Wikileaks was purpose-created to anonymize leaks. The controversial platform is a dream-come-true for active measures operators. Those Russian intelligence officers tasked with utilizing Wikileaks will likely play by their old playbook: any unwitting agent is more effective when left in the belief that they are genuinely holding the moral high-ground, not representing an authoritarian intelligence agency.

The second major unwitting agent has been Twitter, the social media platform most influential among opinion-leaders. Fully automated bots as well as semi-automated spam and trolling accounts make up a sizeable part of Twitter's active user base.[19] The company could easily generate statistics on how many accounts are automated bots or semi-automated to amplify disinformation or bully opponents; how many interactions and engagements with politically influential accounts during the 2016 campaign were actual human; and likely how many of those engagements were controlled from abroad or deliberately obfuscated. But the social media firm has a commercial incentive to hide or understate these figures, as they inflate the active user numbers, a precious measure for social media companies. The result is a platform practically purpose-built for active measures: easy exploitation—high impact.

The third group of unwitting agents of 2016 were those journalists who aggressively covered the political leaks while neglecting or ignoring their provenance. Soviet bloc active measures have skillfully fed forgeries and selected documents to journalists many hundreds of times. But doing so required handiwork and craftsmanship: preparing documents; writing cover letters; trust-building; or covert and cumbersome surfacing operations. Cold War disinformation was artisanal; today it is outsourced, at least in part—outsourced to the victim itself. American journalists would dig deep into large dumps, sifting gems, mining news, boosting ops.

"Sometimes I am amazed how easy it is to play these games," said the KGB's grandmaster of *dezinformatsiya*, General Ivan Agayants, during an inspection of the particularly aggressive active measures shop in Prague in 1965, "if they did not have press freedom, we would have to invent it for them."[20] — Three years later the operator Agayants was speaking with would defect to the US. In 1980 Ladislav Bittman testified on Russian Active Measures here in Congress. "The press should be more cautious with anonymous leaks," Bittman told the Permanent Select Committee on Intelligence, "Anonymity is a signal indicating that the Big Russian Bear might be involved."

Exhibit 1



Google

FORGERY

New sign-in from Firefox on Windows

Hi ,
Your Google Account @gmail.com was just used to sign in from Firefox on Windows.

@gmail.com

Windows
Tuesday, June 2, 2015 03:21:56 AM UTC
Firefox

Malicious link embedded here as bit.ly/1GV[...]

Recognize this activity?
If you don't, please review your devices and activity.

Why are we sending this? We take security very seriously and we want to keep you in the loop on important actions in your account.
We were unable to determine whether you have used this browser or device with your account before. This can happen when you sign in for the first time on a new computer, phone or browser, when you use your browser's incognito or private browsing mode or clear your cookies, or when somebody else is accessing your account.

Sincerely yours,
The Google Accounts team

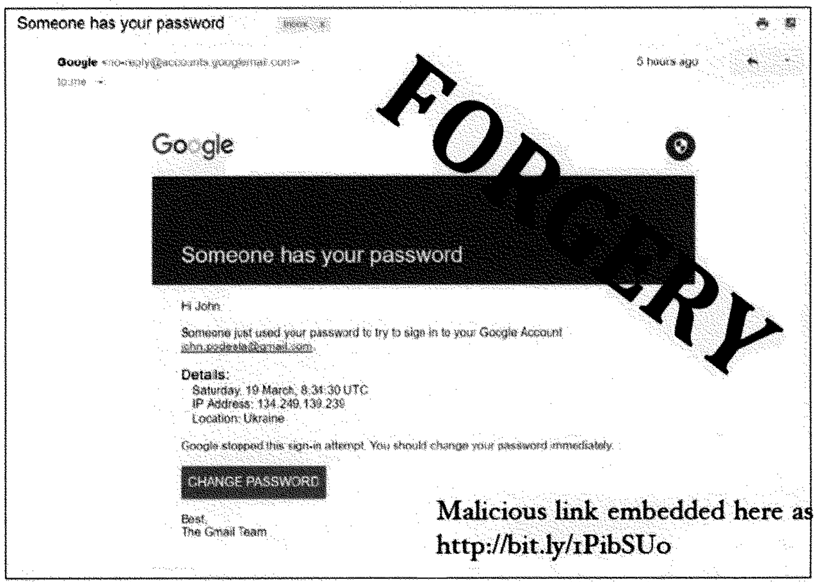
This email can't receive replies. To give us feedback on this alert, click here.

For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.

Sample GRU aka APT28/FANCYBEAR phishing email sent on 2 June 2015 (original).

Exhibit 2



Someone has your password

Google <no-reply@accounts.googlemail.com>

to me

5 hours ago

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:

Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

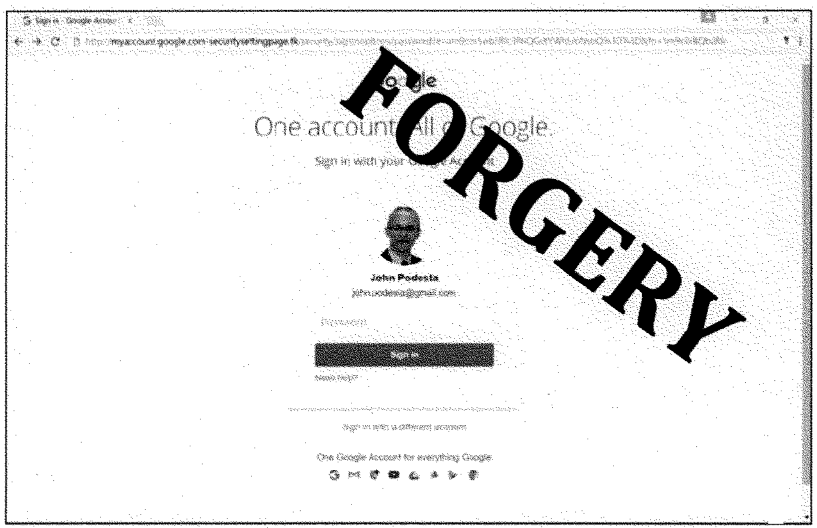
CHANGE PASSWORD

Best,
The Gmail Team

Malicious link embedded here as http://bit.ly/1PibSUo

Phishing email sent to John Podesta (reconstruction by Matt Tait). Note the tradecraft: the "o"s in "someone has your password" are unicode homoglyphs, presumably to evade Google's spam filters.

Exhibit 3



http://myaccount.google.com-securitysettingpage.tk

One account. All of Google.

Sign in with your Google Account

John Podesta

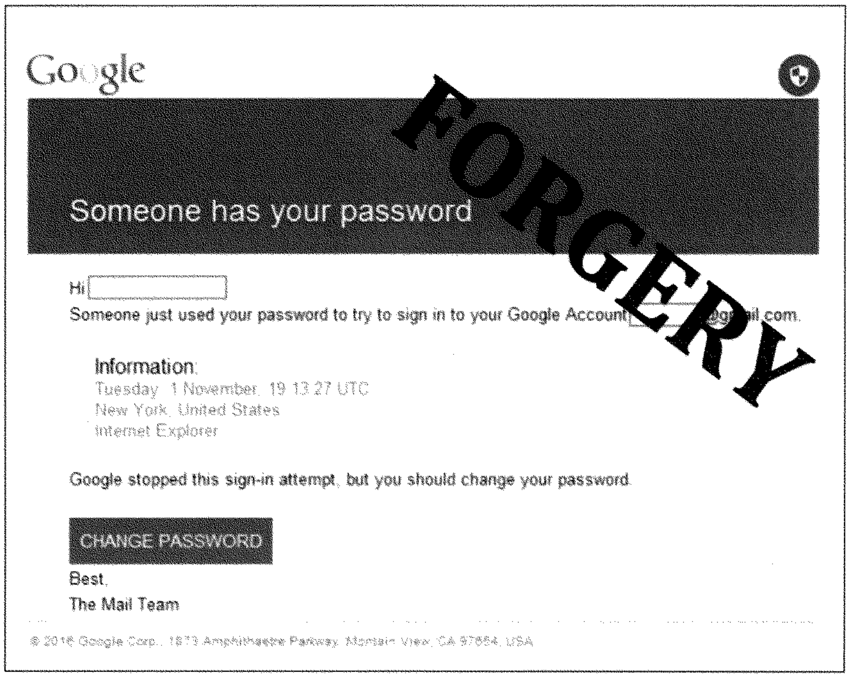
john.podesta@gmail.com

Sign in with a different account

One Google Account for everything Google

Password credential harnessing site, prefilled with John Podesta's picture, name, and email-address. Note the deceptive URL, with a dash, not a forward slash, after google.com, thus pointing to com-securitysettings.tk (reconstruction by Matt Tait).

Exhibit 4



Someone has your password

Hi

Someone just used your password to try to sign in to your Google Account gmail.com.

Information:
Tuesday, 1 November, 19:13:27 UTC
New York, United States
Internet Explorer

Google stopped this sign-in attempt, but you should change your password.

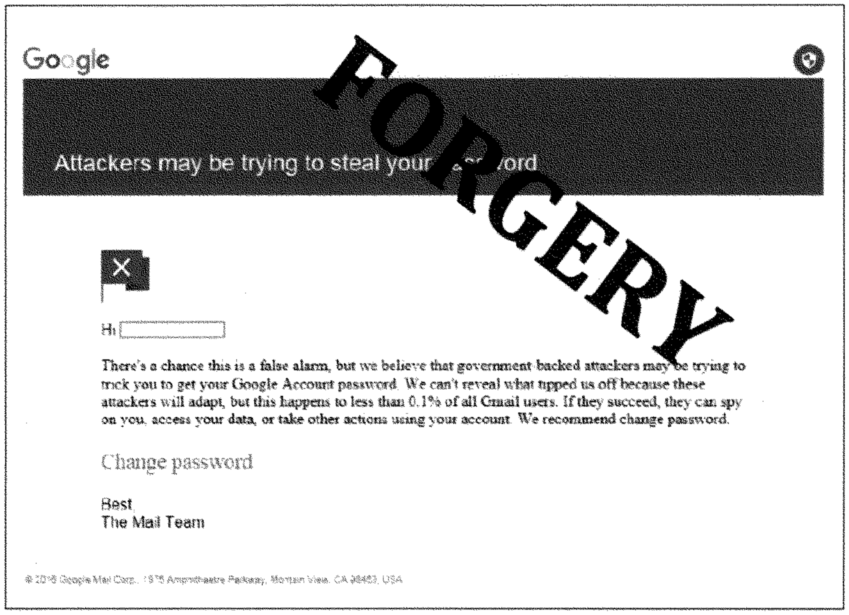
CHANGE PASSWORD

Best,
The Mail Team

© 2016 Google Corp., 1873 Amphitheatre Parkway, Montain View, CA 97654, USA

APT28/FANCYBEAR phishing email that fairly accurately represents legitimate warnings from Google. Note the flawed spelling in the address footer. This email was in fact sent from a yandex.com address but made to appear as a Google address. It included a TinyURL-shortened link on the "CHANGE PASSWORD" button (original).

Exhibit 5



Attackers may be trying to steal your password

Hi

There's a chance this is a false alarm, but we believe that government backed attackers may be trying to trick you to get your Google Account password. We can't reveal what tipped us off because these attackers will adapt, but this happens to less than 0.1% of all Gmail users. If they succeed, they can spy on you, access your data, or take other actions using your account. We recommend change password.

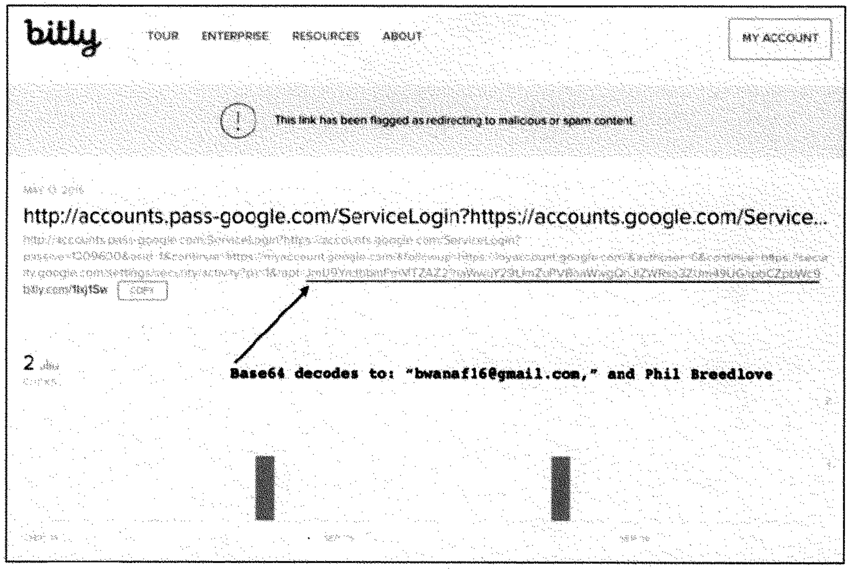
Change password

Best,
The Mail Team

© 2016 Google Mail Corp., 1575 Amphitheatre Parkway, Montain View, CA 94043, USA

Here APT28/FANCYBEAR, a state-backed attacker, sent a phishing email camouflaging as a state-backed attackers warning. Notably Google's legitimate message is only displayed in the Gmail user interface and never sent via email. This email was sent from a mail.com address, and included a TinyURL-shortened link on the "Change password" link (original).

Exhibit 6



This link has been flagged as redirecting to malicious or spam content.

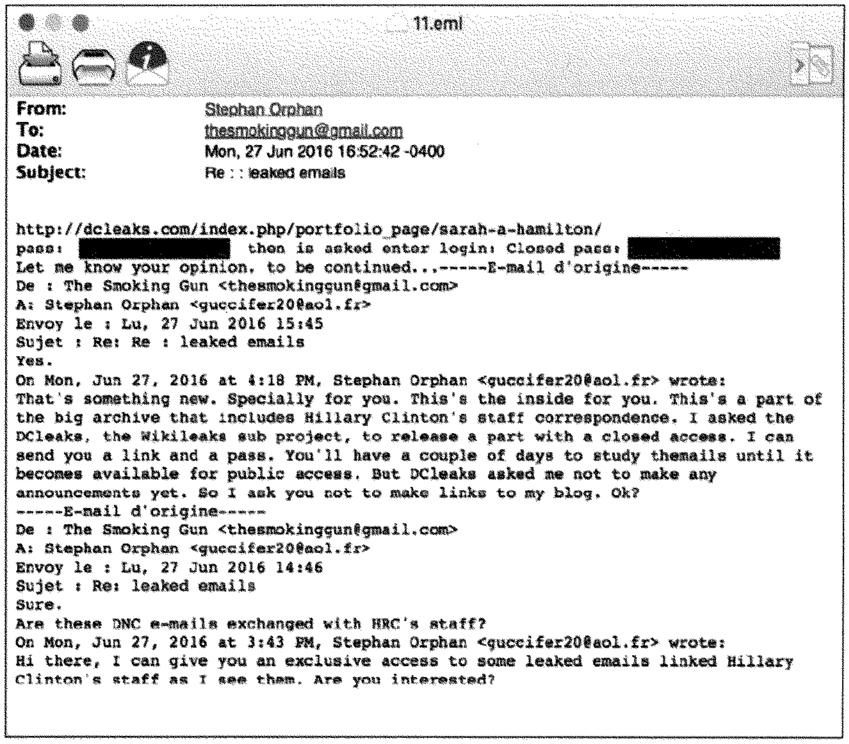
http://accounts.pass-google.com/ServiceLogin?https://accounts.google.com/Service...

http://accounts.pass-google.com/ServiceLogin?https://accounts.google.com/ServiceLogin?
passive=1209600&osid=1&continue=https://myaccount.google.com/&followup=https://myaccount.google.com/[illegible]
ity.google.com/settings/security/activity?pli=1&rapt=[illegible]
bitly.com/1lqj5w

Base64 decodes to: "bwanaf16@gmail.com," and Phil Breedlove

The Russian phishing URL with General Philip M. Breedlove's private email address and name encoded to pre-fill the forged login form. Breedlove was likely compromised in mid-May 2015, less than two weeks after ending his service as Supreme Allied Commander Europe. He became the first leak victim on DC Leaks in June 2016.

Exhibit 7

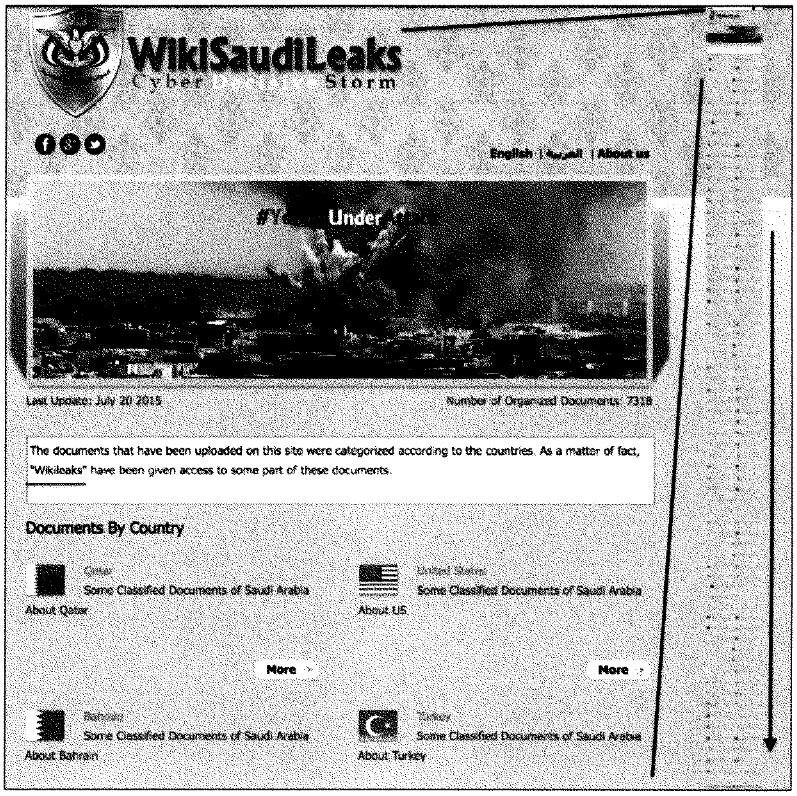


From: Stephan Orphan
To: thesmokinggun@gmail.com
Date: Mon, 27 Jun 2016 16:52:42 -0400
Subject: Re : : leaked emails

```
http://dcleaks.com/index.php/portfolio_page/sarah-a-hamilton/
pass: [redacted] then is asked enter login: Closed pass: [redacted]
Let me know your opinion. to be continued...-----E-mail d'origine-----
De : The Smoking Gun <thesmokinggun@gmail.com>
A: Stephan Orphan <guccifer20@aol.fr>
Envoy le : Lu, 27 Jun 2016 15:45
Sujet : Re: Re : leaked emails
Yes.
On Mon, Jun 27, 2016 at 4:18 PM, Stephan Orphan <guccifer20@aol.fr> wrote:
That's something new. Specially for you. This's the inside for you. This's a part of
the big archive that includes Hillary Clinton's staff correspondence. I asked the
DCleaks, the Wikileaks sub project, to release a part with a closed access. I can
send you a link and a pass. You'll have a couple of days to study themails until it
becomes available for public access. But DCleaks asked me not to make any
announcements yet. So I ask you not to make links to my blog. Ok?
-----E-mail d'origine-----
De : The Smoking Gun <thesmokinggun@gmail.com>
A: Stephan Orphan <guccifer20@aol.fr>
Envoy le : Lu, 27 Jun 2016 14:46
Sujet : Re: leaked emails
Sure.
Are these DNC e-mails exchanged with HRC's staff?
On Mon, Jun 27, 2016 at 3:43 PM, Stephan Orphan <guccifer20@aol.fr> wrote:
Hi there, I can give you an exclusive access to some leaked emails linked Hillary
Clinton's staff as I see them. Are you interested?
```

An operational security slip-up from 27 June 2016 in which one front account, Guccifer 2.0, offers non-public access credentials (password redacted) belonging to another front account, DC Leaks, to *The Smoking Gun*. The operators thus provided another forensic artifact to link the two fronts to each other, and to the wider Russian active measures campaign of 2016. Source: "Does a BEAR Leak in the Woods?" *ThreatConnect Research Team*, Arlington, VA: ThreatConnect, 12 August 2016.

Exhibit 8



WikiSaudiLeaks
Cyber Decisive Storm

Last Update: July 20 2015

Number of Organized Documents: 7318

The documents that have been uploaded on this site were categorized according to the countries. As a matter of fact, "Wikileaks" have been given access to some part of these documents.

Documents By Country

Qatar
Some Classified Documents of Saudi Arabia
About Qatar

United States
Some Classified Documents of Saudi Arabia
About US

Bahrain
Some Classified Documents of Saudi Arabia
About Bahrain

Turkey
Some Classified Documents of Saudi Arabia
About Turkey

The likely APT28/FANCYBEAR front website Wikisaleaks.com, captured on 10 August 2015, with the note that files had been provided to Wikileaks. The full-length site is depicted on the right. The captured version is at http://web.archive.org/web/20150810005744/http://www.wikisaleaks.com/

Endnotes

[1] Günter Bohnsack, Herbert Brehmer, *Auftrag Irreführung*, Carlsen, 1992, p. 16.

[2] Lawrence Martin (Ladislav Bittman), in interview with Thomas Rid, 25 March 2017, Rockport, MA. See also Bittman, Ladislav, *The Deception Game*, Syracuse University Research Corporation, 1972.

[3] Thomas Rid, *Rise of the Machines*, New York: Norton, 2016, last chapter.

[4] Three of the most potent Western intelligence communities agree with the APT28/FANCYBEAR attribution to Russian military intelligence: the United States; Germany; and the United Kingdom.

[5] SecureWorks shared the full dataset with the author. See also "Threat Group 4127 Targets Hillary Clinton Presidential Campaign," *SecureWorks Counter Threat Unit*, 16 June 2016, as well as "Threat Group-4127 Targets Google Accounts," *SecureWorks Counter Threat Unit*, 26 June 2016.

Out of 19,315 malicious links sent, 3,134 were clicked at least once—just above 16 percent. If the password harvesting success rate is 1-in-7, then the total number of compromised accounts in this set would be around 470, which would mean an overall success rate of 2.4 percent. This estimate is conservative, as the total number of clicks is understated for technical reasons.

[6] The number of private sector reports on the entity codenamed APT28, FANCYBEAR, Sofacy, Sednit, Pawn Storm, STRONTIUM is in the three digits, many of them unfortunately not publicly available. One of the first public reports was *APT28: A Window into Russia's Cyber Espionage Operations?* Milpitas, CA: Fireeye, 27 October 2014.

[7] See "Deutsche Beamte beschuldigen russischen Militärgeheimdienst," *Der Spiegel*, 30 January 2016. Also: "Nachrichtendienstlich gesteuerte elektronische Angriffe aus Russland," *BfV Newsletter*, Beitrag Spionageabewehr, January 2016.

[8] Stefano Maccaglia, "Evolving Threats: dissection of a Cyber- Espionage attack," Abu Dhabi: RSA Conference, November 2015.

[9] Brian Bartholomew and Juan Andrés Guerrero-Saade, "Wave your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks," *Virus Bullentin Conference*, 6 October 2016. (For a more extensive analysis: "TLP Amber" report from autumn 2015 by a major security company, https://www.us-cert.gov/tlp). The attribution of this Saudi operation is particularly difficult. I would assess with moderate confidence that "Wikisaleaks" was a Russian intelligence operation and that Yemen Cyber Army was a Russian front.

[10] For registration information, see http://whois.domaintools.com/dcleaks.com

[11] American victims whose personal emails were subsequently leaked on DC Leaks are Philip Breedlove, Sarah Hamilton, Brian Keller, Zachary Leighton, Capricia Marshall, Ian Mellul, Beanca Nicholson, Carl Pistole, Colin Powell, Sarah Stoll, William Rinehart, and John Podesta (where GRU used Wikileaks as an outlet).

[12] John Podesta was targeted on 19 March; Rinehart on the 22nd; Hamilton, Leighton, Nicholson, and Mellul on the 25th.

[13] Google reported that "Portions of the X-Agent code base can be found in malware dating back to at least 2004," see Neel Mehta, Billy Leonard, Shane Huntley, "Peering into the Aquarium," Palo Alto: Google Security Team, 5 September 2014, p. 20.

[14] The APT28/FANCYBEAR communication protocol is a strong forensic link between breaches against Washington-based political organizations, the compromised app used against Ukraine artillery units, the German Bundestag breach, and other operations. The full source code of the so-called X-Agent implant in question was not publicly available by 27 March 2017. Crowdstrike's Adam Myers, interview with author, Washington, DC, 27 March 2017. See Exhibit 1 for GRU's X-Agent communication protocol.

[15] One example is a re-used IP address, 176.31.112[.]10, which was hardcoded into two DNC implant samples:
4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976, and
40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f;
as well as in the Bundestag sample,
730a0e3daf0b54f065bdd2ca427fbe10e8d4e28646a5dc40cbcfb15e1702ed9a.

[16] The 50-bytes RC4 keys had a 46-bytes overlap. The keys were hardcoded into the X-Agent implants that were deployed against the Linux server of a Washington-based political organization—and against Android devices of Ukrainian artillery units in Eastern Ukraine. A member of the 55th Artillery Brigade developed a legitimate targeting app, named Попр-Д30.apk, in early 2013. By late April 2013 a rigged version of that app was offered for download on social media platforms used by the artillery units; this compromised app contained the implant with the similar RC4 key. Below the Linux 50-bytes key, followed by the Android key, with 46 bytes overlap (non-overlapping bytes in square brackets):

3B C6 73 0F 8B 07 85 C0 74 02 FF [D0 83] C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75
07 50 E8 B1 D1 [FF FF] 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35

3B C6 73 0F 8B 07 85 C0 74 02 FF [CC DE] C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75
07 50 E8 B1 D1 [FA FE] 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35

The RC4 keys strongly link at least 76 different samples in the Crowdstrike's intelligence library, all positively attributed to APT28/FANCYBEAR implants or loaders, aka GRU. The Ukrainian military's Android app may have been operationally less effective than initially portrayed. But the effectiveness of the app is an issue entirely unrelated to the targeting itself. The forensic significance of quality artifacts found in the implants is strong, especially the cryptographic overlap.

Myers, Adam, interview with Thomas Rid, Washington, DC, 27 March 2017; see also Crowdstrike, "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," Washington, 22 December 2016.

[17] Bittman, Ladislav, *The KGB and Soviet Disinformation. An Insider's View*. Washington: Pergamon-Brassey's, 1985, p. 50–51.

[18] Russian intelligence agencies evolve their tradecraft at a fast pace, making it hard for network defenders to keep up with. Just this week, news emerged that APT29 is abusing Tor Hidden Services for controlling attacks against that likely target US government and think tanks. See FBI, "Vulnerabilities and Post Exploitation IOCs for an Advanced Persistent Threat," Washington, DC: FBI Cyber Division, 11 May 2016, p. 3. For background, Eduard Kovacs, "OnionDuke APT Malware Distributed Via Malicious Tor Exit Node," *Security Week*, 14 November 2014. More recently: Matthew Dunwoody, "APT29 Domain Fronting With TOR," Fireeye, 27 March 2017.

[19] As many as 15 percent of Twitter accounts may be bots, which amounts to almost 50 million "users." One recent research project observed "a growing record of malicious applications of social bots." See Onur Varol et al, "Online Human-Bot Interactions: Detection, Estimation, and Characterization," Social and Information Networks, arXiv:1703.03107, 27 Mar 2017.

[20] Agayants, quoted in Bittman, *The KGB and Soviet Disinformation*, p. 70.

Chairman BURR. I want to thank all three of you for your testimony. I think it's safe to say that this is probably a foundational hearing for our investigation, to have three people with the knowledge that you do. I hope when you do get that second call or third call that you'll sit down with us as we have peeled back the onion and a little bit and we have technical questions. But we've got some technical expertise on the committee. You can look at a lot of gray hair and realize that my technology capabilities are very shallow and that many of us struggle to understand not just what they can do, but even the lingo that's used, the dark side of the web, the open side of the web. These things are amazing and would be shocking to most people.

I'm going to turn to the Vice Chairman for his questions.

Vice Chairman WARNER. Thank you, Mr. Chairman. Let me echo what you said. I think we've got an incredible panel of experts, and you're here because of that expertise.

I've got three questions that I'd like to try to get through, the first one hopefully fairly quickly. Based upon your expertise and knowledge, do you have, any of you, have any doubt that it was Russia and Russian agents that perpetrated during the 2016 presidential campaign the hacks of the DNC and the Podesta emails and the misinformation and disinformation campaign that took place during the election? A short answer will do. Do any of you have any doubt that it was Russia?

Mr. MANDIA. I think basically, from the observables we get at the victim sites you can't always connect the dots. We can't show you a picture of a building. We can't give you a list of names of people who did it. We have to look at a lot of other factors, some of which is incredible amounts of detail.

But we've got ten years of observation here. We've seen similar behaviors in the past. My best answer is it absolutely stretches credulity to think they were not involved.

Vice Chairman WARNER. General Alexander.

General ALEXANDER. I believe they were involved.

Vice Chairman WARNER. Dr. Rid.

Dr. RID. I believe they were involved as well.

Vice Chairman WARNER. Thank you.

It has been reported that some of the techniques—and I say to my good friend Richard Burr, I used to be technologically savvy up until about year 2000, 2001, which still puts me a decade ahead of some of my colleagues.

But it's been reported in the press and elsewhere that by using internet trolls and then the botnets and that exponential ability then to kind of flood the zone that in the misinformation and disinformation campaign they were, the Russians, were able to flood the zone, actually not in a broad-based, across the whole country, but literally target it down to precinct levels in certain states.

Is that capable to do, if you could have the botnet network that would in effect put out misinformation or disinformation and then all of the other accessory sites that would then gang up on that and target that down to a geographic location?

General ALEXANDER. I think it's technically possible. I don't know that you have—that I have enough information to say that was done at each one of those locations. But I think it's technically possible. If you put enough people on it, yes, you could do that.

Vice Chairman WARNER. Dr. Rid or Mr. Mandia.

Dr. RID. It's very technically possible. May I just make an important distinction here between a "botnet," which is usually remotely controlling somebody's computing resources and machine, and "bots," that is fake Twitter accounts that are automated.

Vice Chairman WARNER. But they both have the effect. Somebody's campaign—somebody's computer that is accessed or fake Twitter accounts, bots, they still have the same effect of pushing a news story higher on a news feed, for example, a Twitter news feed or a Facebook news feed?

Dr. RID. That is mostly done by bots within social media networks, that can be any social media network. Botnets are usually used for different purposes.

Vice Chairman WARNER. Kevin, do you want to?

Mr. MANDIA. Yes. Peeling back the question, there's a couple things. I think you can always try to get public perception to go certain ways based on the results of Google searches and things like that, and you can automate ways to up-level people's attention to things, with all the social media.

The good news is during the election a lot of states had the foresight to, let's do shields up and let's be very diligent, let's watch all the cyber traffic we can. And we didn't see any evidence, at least in the DDOS side or distributed denial of service attacks or attacks—we didn't see anything that harmed the actual election process.

Vice Chairman WARNER. That was not the—but the question of targeting in.

So here's the last question. I've heard and it's been reported that part of the misinformation-disinformation campaign that was launched was launched in three key states—Wisconsin, Michigan, and Pennsylvania—and it was launched, interestingly enough, not to reinforce Trump voters to go out, but actually targeted at potential Clinton voters with misinformation in the last week where they were not suddenly reading, if they got their news from Facebook or Twitter, Clinton and Trump back and forth, but stories about Clinton being sick and other things.

I guess my final point here is—and this may be beyond anybody's expertise, but my understanding is the Russians, although very good at some of this technology piece, they might not have been so good at being able to target to a precinct level American political turnout; that that would mean they might be actually receiving some information or alliance from some American political expertise to be able to figure out where to focus these efforts.

Dr. RID. I haven't seen a detailed analysis of the precinct-level targeting that would be good enough to substantiate this assumption. But this relates to a more fundamental problem. One different, separate entire group of actors and some completely legitimate within the campaign were taking advantage of social media. So it's really difficult to distinguish for researchers after the fact what actually is a fake account and what is a real account.

Ultimately, we need the cooperation of some of the social media companies to give us heuristics and visibility into the data that only they have.

General ALEXANDER. I would take it a step higher, that, Senator, I think what they were trying to do is to drive a wedge within the Democratic Party between the Clinton group and the Sanders group, and then within our Nation between Republicans and Democrats. I think what that does is it drives us further apart, that's in their best interest. And we see that elsewhere.

I'm not sure I could zone it down to a specific precinct, but I think what we would expect is for them to create divisions within the whole framework and destroy our unity. And you can see, actually, if you look back over the last year, we didn't need a lot of help in some of those areas.

So now the question is, and where I think you have the opportunity, is how do we build that back?

Chairman BURR. Let me say before I recognize Senator Rubio, I want to clarify what I said about Senator Warner's business. My reference meant that it was about 14 years ago, 15 years ago. And I think it was you, General Alexander, that came in front of the committee and said: In the future, people won't file technological patents because technology will change so quickly that you won't have a year and a half's time to go through the patent approval process before your technology is obsolete.

I think we have reached that point of technological explosion, that what we're talking about today we could have a hearing six months from now and probably talk about something different.

Vice Chairman WARNER. But I would say that the cell phones that I was involved with in the early 1980s have become a bit ubiquitous.

Chairman BURR. Well, we all wish we had flip phones again, I can tell you that.

[Laughter.]

Senator Rubio.

Senator RUBIO. Thank you, Mr. Chairman, and to the Ranking Member.

Before I get to my question, Mr. Chairman, in the first panel one of the individuals that appeared before us mentioned me in connection with efforts in the 2016 presidential primary. I am not prepared to comment on that and any information on that issue hopefully will be reflected in our report, if any.

I do think it is appropriate, however, to divulge to the committee, since a lot of this has taken a partisan tone, not in the committee but in the broader perspective, the following facts. In July of 2016, shortly after I announced that I would seek reelection to the United States Senate, former members of my presidential campaign team who had access to the internal information of my presidential campaign were targeted by IP addresses with an unknown location within Russia. That effort was unsuccessful.

I'd also inform the committee that within the last 24 hours, at 10:45 a.m. yesterday, a second attempt was made, again against former members of my presidential campaign team who had access to our internal information, again targeted from an IP address from an unknown location in Russia. That effort was also unsuccessful.

My question to all the panelists: I have heard a lot on the radio and on television an advertisement for a firm in the United States actively marketed in Best Buy and other places by the name of Kaspersky Labs. There have been open source reports which I can cite that basically say that Kaspersky Labs has a long history connecting them with the KGB's successor, the Russian security services. I have a Bloomberg article here and others.

I would ask the panelists: In your capacity as experts in information technology, would any of you ever put Kaspersky Labs on any device that you use, and do you think any of us here in this room should ever put Kaspersky Labs products on any of our devices or computers or IT material?

Mr. MANDIA. I think the way I'd address that is, generally people's products are better based on where they're most located and what attacks they defend against. For example, you think about Symantec or McAfee or my company and other companies. We are prominently used in the U.S., so we get to see the best attacks from China and cyber espionage campaigns in Russia. In the Middle East, it's already in massive escalation mode and we're all prominent there.

I think what we're starting to see is an alignment where Japan will let a U.S. company secure Japan, South Korea will let a U.S. company defend South Korea, the Middle East will let a U.S. company defend it, but you almost see lines being drawn.

There's no doubt the efficacy of Kaspersky's products. They probably get to see different things than we see, being this relevant here.

Senator RUBIO. My question was not about whether it's an effective tool. My question about it is whether you would ever put it on your computer.

Mr. MANDIA. My answer indirectly would be there would be better software probably available to you than Kaspersky to defend you here.

General ALEXANDER. I'll answer by, no, I wouldn't, and I wouldn't recommend that you do it either. There's better capabilities here that you can use, FireEye, for example, and I'm being credited now with that—no. There are other U.S. firms that answer and solve problems that will face you for the issues that you described earlier, Senator, that I think would be better at blocking them.

Dr. RID. I would, yes. I would also use a competing product at the same time. Always a bit of redundancy never harms.

But it's important to say that Kaspersky is not an arm of the Russian government if we look at the publicly available evidence. Kaspersky has published information about Russian cyber attack, cyber intrusion campaigns, digital espionage, about several different Russian campaigns. Name any American company that publishes information about American digital espionage?

Senator RUBIO. My second question to the panel in the time that I have remaining is: My concern in our debate here is that we're so focused on the hacking and the emails that we've lost—and I think others have used this terminology—we've focused on the trees and have lost sight of the forest.

The hacking is a tactic to gather information, for the broader goal of introducing information into the political environment, into the public discourse, to achieve an aim and a goal. It is the combination of information leaked to the media, which of course is always very interested in salacious things, as is their right in a free society. The public wants to read about that, too, sometimes.

But it's also part of this other effort of misinformation, fake news, and the like. Would you not advise this panel to look simply beyond the emails—that's an important part—to the broader effort in which the emails in the strategic placement of information in the press is one aspect of a much broader campaign?

General ALEXANDER. Senator, that was part of my point about bringing this up to a strategic level and saying that what's Russia trying to accomplish with respect to NATO, the European Union, and the U.S., and driving a wedge between those and creating tensions between those countries and ours.

If you were to go back and look at what's happened to Russia over the last 30 years and then play that forward and see what they're now doing, you can see a logic to their strategy. I think that's something that we now need to address. I do think we ought to address this with the Russians and get the Administration to do that. It's not something that we want to go to war on. It's something that we want to resolve by engagement and confrontation.

Dr. RID. How are active measures today different from in the Cold War? This is in answer to your question. In the Cold War, active measures were really artisanal—very quiet, craftsmanship, a lot of hard work, forging letters, doing research. It was a real undertaking. Today they're not artisanal; they're outsourced, outsourced in part to the victim, and especially to journalists, American journalists. They add the value to these active measures.

This is important because if we look at the operations in hindsight they appear a lot more sophisticated than they actually were. So we run the risk of overestimating Russian capabilities here.

Chairman BURR. Senator Feinstein.

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

Kevin Mandia, it's good to see you again. I want you to know how much your nation report was appreciated. You spoke before this committee and I think everybody very much appreciated it and I think it had some good results. So thank you very much.

General Alexander, this is the first time I've seen you out of uniform. Civilian clothing is becoming. I'd like to personally welcome you.

I don't know our third gentleman, but I want to address this to General Alexander. You were Cyber Command for a number of years. You spoke about the fact that the time has come for us to get tough. We have talked about that before. We have WikiLeaks and stream after stream after stream of release of classified information, which has done substantial harm to this Nation.

Yet we do nothing. And everybody says, well, we'd like to do something, but we don't quite know what it is. I never thought we would be in a situation where a country like Russia would use this kind of active measure in a presidential campaign. The size of this, the enormity of it, is just eclipsing everything else in my mind.

Yet there is no response. As you have left now and you've put the Cyber Command on your desk, what would you do? What would you recommend to this government?

General ALEXANDER. I think there are two broad objectives we ought to do. We ought to fix the defense between the public and private sector, between government and industry.

Senator FEINSTEIN. You've said that.

General ALEXANDER. We have to fix that, because much of what we're seeing is impacting the commercial—or the private sector. Yet the government can't really see that. So the government's not going to be able to help out and the ability to take actions to actively mitigate it therefore are nonexistent or after the fact.

If you think about Sony as an example and imagine that as the attack coming in, the government couldn't see that at network speed and so the government came in and did incident response. Everything could happen to Sony. What you really want the government to do is just stop a nation-state like North Korea or Russia from attacking us. But the government can't do that if it can't see it.

So we have to put this together. We have to come up with a way of sharing threat intelligence information at network speed and practicing what our government and industry do together and work that with our allies. I believe we can do this and protect civil liberties and privacy. I think we often combine those two, but we can actually separate and show that you can do both.

Senator FEINSTEIN. How?

General ALEXANDER. Well, for first, the information that we're talking about here doesn't involve our personally identifiable information. Think of this as looking at airplane traffic over the country. When you see radars looking at those airplanes that are going by—think of those as pieces of information—they aren't reading everybody in the airplane. They're seeing an airplane and they're passing it on to another controller, who sees a comprehensive picture.

What we see is what radar sees today. So we don't actually—we're not talking about reading threat information. We want to know what's that packet of information doing, why is it coming here, and can I or should I share the fact that a threat is coming to us.

Senator FEINSTEIN. I understand what you're saying. But what I'm asking you for is different. It is your expertise based on this, based on the fact that the Russian government, including two intelligence services, made a major cyber attack on a presidential election in this country, with a view of influencing the outcome.

What would you recommend?

General ALEXANDER. The first step was fix the defense, because if you take offense and you don't have a defense then the second step of going after the power or other sectors puts us at greater risk. So from a National Security Council perspective, what I would expect any administration to do is to look at the consequences of the actions that they take.

So when I said engage and confront, in this regard what I would do, what I would recommend, is first and foremost a quiet engagement with the Russian government about what we know and why we know it, without giving away our secrets, and say, that's got to stop. We need an engagement here.

If we're going to confront them, it would be: We know you're doing this right now; stop that. We had a channel in the Cold War for doing it. We need a channel to get that and build back the ability to stop things, from my perspective.

I would be against using cyber only as a tool against Russia when we have these vulnerabilities we haven't addressed here in our own country. I think it would be a mistake until we fix that. So that's why I say we have to do both.

I actually—and it was interesting. We were talking beforehand, and Thomas can add to this. One of the things that as you look at this—I don't believe Russia understood the impact their decisions would have in this area. It's far exceeded it. With all the discussion going on in our country today, I am sure that people in Russia are saying: Oops, we overdid this.

Now is the time for us to say: not only did you overdo it, we need to set a framework for how we're going to work in the future, and we need to set that now. That can only be done by engaging them face to face, and I think that's what has to be done.

Senator FEINSTEIN. Thank you. Very helpful.

Thank you, Mr. Chairman.

Chairman BURR. Senator Blunt.

Senator BLUNT. Let's start with General Alexander. I asked a question this morning, which was, after all the discussion of the long history of Russian involvement in European elections, of things that have happened for a long time and really in a significant way in the last 15 years, why do you think that we were not better prepared for this?

General Alexander, you just said that we needed to have a defense. Why wouldn't we have had a defense? What was this about this particular thing that had been so anticipated that the intelligence community, the U.S. Government, even the media, appears not to have had the defense you just mentioned we should have now?

General ALEXANDER. Senator, this has been a great discussion that you and the other House of Congress have talked about, and that's how do we put together our country's cyber legislation? Right now we do not have a way for industry and government to work together. So if you think about the DNC or the RNC or the electricity sector and others, when they're being attacked the ability for the government to see and do something on that doesn't exist.

Everybody recognizes that we need to do it. We talk about it. In fact, we had at the Armed Services Committee a discussion on it. But we haven't taken the steps to bind that together. We allow it, but we haven't created it.

I believe that's the most important thing that we could do on that one vector that Senator Feinstein brought up: fix the defense. The reason is the government's not tracking the RNC and the DNC. Now, industry sees it, and Kevin brought out some key points of what was going on and what they were seeing from an industry perspective. But the reality is we haven't brought these two great capabilities together.

The other part, it's my personal experience the government can help on attribution several times greater than what we see in industry. If you put those two together, we could act a lot better.

Senator BLUNT. Let's go to Mr. Rid. Mr. Rid, should we have—was there nothing we could have done here? Were we not paying the level of attention that we should have paid? Or is it just we just aren't ready because our structure doesn't allow us to anticipate what we know was happening in elections all over the world before 2015 and 2016 here? Particularly in Europe. Maybe "all over the world" might be a stretch, but all over Europe, not a stretch.

Dr. RID. There's a lot we can do in order to increase defenses here, as well as to minimize the effect of active measures that are already taking place. Let me name an example. Let's make this concrete. You as members of the legislative body are—and the same is true in Europe—the soft underbelly of the government of the wider administration and government, because—this is true for all parliaments—the IT security is notoriously bad.

The chip card that many of your staff members carry around their neck, the CAC card, as it's called, here in Congress, if my information is correct, doesn't actually have the proper chip. It has a picture of a chip. Try feeling. Try to feel the chip with your fingernail. There is no chip. It's only to prevent chip environment if you meet with other parts of the Executive Branch. That tells you that there's a very serious IT security problem. It should be mandatory—and potentially this is something you would think about as we move forward—it should be mandatory for all campaigns, just like you have to disclose financial records, it should be mandatory by default to have two-factor authentication. So not just a password, but actually a second thing, like a number that is generated by an app or a specific key.

Senator BLUNT. Thank you.

We had somebody this morning say it should be mandatory for the State Department to have a program to every day say what was true and what wasn't true. There are certain levels beyond what you can require people to do that really don't make that kind of sense.

Mr. Mandia—and I don't mean your comment didn't, but there are practical levels now. I also say the "soft underbelly" is one of the nicer things the Legislative Branch would be called these days. But your thoughts on why we didn't see this coming? The earlier panel had a more robust sense of where we should have been understanding what was going on than this one.

Mr. MANDIA. There's probably a lot of ways to answer that. I'll answer it this way. When it comes to cyber security, first off, I don't want to destroy anybody's hopes. When we say fix the problem, we've known about cancer for 4,000 years; we haven't cured it yet. The reality is this: when we fix the problem here, we're still going to have incidents, we're still going to have something of impact and consequence.

My experience is this: People get serious about cyber security when they have two things: either, A, a compliance driver and they take it seriously; or, B, they have the "oh, crap" moment, quite frankly, and they've been breached.

We published reports, my company did, in 2014 that had a lot of the allusions to what just happened. But sometimes you have to have it happen before you recognize that, wow, that was really on the table. I doubt it'll happen again, but now we're having the dialogue to make sure that it doesn't.

Senator BLUNT. Thank you, Chairman.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. I think it's been a very good panel.

I want to talk about one of our most significant vulnerabilities as it relates to cyber security. I have been working for some time now with Congressman Ted Lieu of California, who is a real expert in this field. One of the things that I'm particularly troubled by is our vulnerabilities in what's called "SS7," Signaling System 7. This essentially allows cellular networks to be able to talk to one another. We seem to have some very significant vulnerabilities that could allow a foreign actor, Russians and a variety of other interests hostile to our country, to hack, tap, or track an American's mobile phone. The hackers could be just about anybody, but certainly a foreign government, and the victim could be just about any American.

I think, Dr. Rid—and I welcome anyone who'd like to talk. But I think, Dr. Rid, you've done some serious analysis of these vulnerabilities in SS7 and I would be interested in hearing, A, how serious you think this is, and, B, what do you think our government ought to do about it, particularly in connection to the topic at hand, which is dealing with these Russian hacks?

Dr. RID. Thank you for this very specific question, although I have to say that I'm not an SS7 expert and I don't want to pretend to be one here. But the technology that you're referring to is certainly a weak point and can easily be exploited, ultimately because it is a trust-based system, a trust-based protocol. And if you have a landscape of a lot of mobile phone providers, it's relatively easy to undermine, that some one entity essentially undermines, can essentially exploit the trust here.

There are ways to remedy the problem, but I will just add one observation, that if—and I think many people in Congress will be doing this already—if you use an encrypted app for your communications, then you will most likely defeat some of that vulnerability there.

Senator WYDEN. I hope that's the case. I think the Congressman and I have been concerned that that may not be enough, because largely what has happened thus far is there have been self-regulatory approaches and that and other approaches weren't pursued. So we're going to continue this discussion. As I understood it, you had talked to some of our folks. You may not think yourself—you may not consider yourself an expert, but our folks thought you were very knowledgeable.

Dr. RID. Well, may I respond?

Senator WYDEN. Sure.

Dr. RID. I think we're looking in multiple ways at market failures here. So two-factor authentication, which I mentioned, we're looking at a market failure there because it's still an opt-in situation. If you have an opt-in situation, most people will not opt in and hence remain vulnerable.

The market, when we look at active measures—and this is one of the most fundamental ethical dilemmas here. The market favors disinformation today, and I can go into specifics on how we can remedy this if you like.

Senator WYDEN. Well, the Congressman and I feel that we ought to get the FCC, the Federal Communications Commission, off the dime, too, because it is clear that they have been slow-walking the various kinds of approaches that could provide an added measure of security.

Let me ask one other question and any of you three can get into it. In January the IC assessment, the intelligence community assessment, said that Russian intelligence accessed elements of multiple State or local electoral boards. So I asked the FBI Director then what exactly had been compromised and what was the nature and the extent of the compromise.

Director Comey responded that the Russians had attacked State voter registration databases and taken data from those databases. Can you add anything else to that? Any of you three are welcome to do it, because that sounds to me like pretty alarming stuff. The FBI Director in January—and I wish I'd had more time to get into it with him—essentially said that this was a problem, and I would be curious whether you knew anything more about this topic.

We can just go right down.

General ALEXANDER. I don't. I have talked to some of the—one of the Secretaries of State on just this and the issue that you brought up, the polling data, the registration data, is something that's at risk and something that the states are looking at. So I do think that's important.

Senator WYDEN. Great.

Thank you, Mr. Chairman.

Chairman BURR. Senator Cornyn.

Senator CORNYN. Thank you for being here and testifying.

I think maybe we assume that people know more about what we're talking about than maybe they actually do. So I'd like to kind of get basic maybe for my benefit and maybe some other people will learn some things as well. But I think we've referred to something that's called spear phishing. So I'd like to have one of you explain what that is.

Let me just tell you, by the way, that occasionally my junk email box on my personal email, I'll get emails that purport to be from the FBI Director or the Army Chief of Staff, Mark Milley, my friend from Fort Hood who's now the Army Chief of Staff, or maybe from Apple, telling me that I need to reset my password, or from Google saying I need to execute some sort of maneuver.

Then there's a link for me to click on. Is that what is commonly known as spear phishing, and once you click on that link then they basically could take over your machine?

Mr. MANDIA. Yes, you've basically got that right. Looking back at 2015 and 2016, we did nearly 1,000 investigations into computer intrusions, and we have a skewed vantage point because no one hires us to respond to an intrusion when they're five minutes behind the hack. They hire us when the hack and the breach is already at a scale and scope where they need help.

In 91 percent of those breaches, victim zero was in fact spear phishing, meaning that's how the Russian groups, the Chinese cyber espionage campaigns, and every capable hacking threat actor is breaking in. It is in fact a link that purports—it's a link or an attacked document that comes to you. It looks like it's coming from someone that knows you and it's got something relevant attached or the link is to something you consider relevant to what you do for a living.

That's what we were talking about earlier, is that's how we kind of know what the Russians were targeting, is they're doing very specific spear phishes to very specific people. But that is the number one way human trust is being exploited and that's how folks are breaking in.

Senator CORNYN. Would you be surprised if a member of Congress was being targeted by a Russian or a foreign government spear phishing?

Mr. MANDIA. I would not be, and I would expect every one of you is targeted on a near-daily basis.

Senator CORNYN. General Alexander, you were going to say something?

General ALEXANDER. Yes, I was going to add to what Kevin said. They're going to do research on you, know who your friends are, so they know you with Mark Milley from Texas, they know key things about you. Perhaps you golf and you have a friend that golfs, and they're going to send you something: Hey, how about this golfing thing? Click here or do this. And that's how they do it.

Spear phishing is targeted on an individual. They do research and understand more about you to go after you as a person.

Senator CORNYN. Well, Dr. Rid, you talked about the poor IT and cyber hygiene in the government space. I think some of this could be as simple as updating your antivirus software, scanning your machine periodically, and the like. But let me just mention the specific hack of the OPM, the Office of Personnel Management. I mentioned it at an earlier panel. 21 million Americans had their personal information stolen in government custody.

So even though they may have considered it private information, they were forced to give it to the government for security clearance or some other purpose, and now some foreign state actor through a cyber hack has access to 21 million private records, including more than 5 million sets of fingerprints.

Is that the kind of information that cyber actors, either criminals or espionage agents, foreign governments, would use to further collect espionage or to steal or to implant ransomware or something in a machine or in a business and then shake them down for money?

Dr. RID. Yes, absolutely. The more information, the more confidential information also, you have, the easier it is to craft a spear phishing, a targeted email, a deceptive email, a forged email so to speak. In my written testimony I included a number of samples, a number of exhibits——

Senator CORNYN. I saw that.

Dr. RID [continuing]. Including John Podesta's.

Senator CORNYN. Thank you. Thank you for doing that.

Well, we don't have control over everybody's private computer or what kind of software they use. But we do have something to say, I think, about what the United States Government does. And I think one of the things we need to be attentive to is to make sure that the United States Government networks are adequately protected.

I know, General Alexander, you had something to do about that at the NSA. But you didn't have the ability to protect all of this other information.

Let me just ask—I just have a couple of seconds and since you're here, General Alexander, we're going to have to take up the reauthorization of the Foreign Intelligence Surveillance Act, particularly Section 702. I just would like to ask you, since we have you here, a little bit about its importance to detecting and countering foreign cyber activity. And if you would also include in your answer the privacy protections that are a very, very important part of that and oversight that you got to see first-hand in your capacity as head of NSA and Cyber Command.

General ALEXANDER. I think that's the most important program that's out there, especially in counterterrorism. I can give you a real quick example. Najibullah Zazi in Denver was detected by that specific authorization. NSA saw that, provided it to the FBI, and Nazibullah Zazi was the individual in 2009 who was driving across the country to New York City when they arrested the individual in New York City based off of the other program and they found several backpacks in various states of readiness to attack the New York City subway—done by that program.

I think that's the most effective counterterrorism program we have, and I think it will be also effective in some areas for cyber security, although I don't have any examples off the top of my head here.

Senator CORNYN. Could you conclude your answer and talk a little about minimization and other privacy protections, because I think that's important to the American people, to know that we're very vigilant and diligent in that area as well?

General ALEXANDER. Yes. It's interesting because we did a series of presidential review groups on NSA after the Snowden leaks about these programs. At the time one of the board members of the ACLU, Geoffrey Stone, was on that panel. I was kind of skeptical about this individual being on there, and I'm sure he looked at me somewhat askance.

After five weeks of sitting down with our people and going through every one of those, he came up to me and he said: Your people have the greatest integrity of any agencies I've seen. And I said: Don't tell me; tell the American people; tell Congress; tell the people of NSA and tell the White House. And he did.

So there are some key statements by Geoffrey Stone that show that we can protect civil liberties and privacy. I think it's important to see some of his statements there, because what it did is—he also asked me to write an op-ed. So imagine an Army officer and a board member of the ACLU writing an op-ed on reauthorizing the metadata program, with some changes. And we did.

The reason—I asked him: Why are you doing that? And he said: The reason that I'm doing this is that if we don't have programs like this and we're attacked, we won't have civil liberties and privacy, and the mechanisms and the capabilities you have here to protect it are overseen by Congress, overseen by the courts, and overseen by the Administration. Everything has 100 percent review on it. And I think that's the best way to do it.

You know, he is right. If we do get another attack, they're going to ask Congress, they're going to ask the Administration, why we didn't stop those. I think this is exactly why we have to move down. I do think we have to be more transparent. I think as we bring cyber security in here, having a discussion like this open hearing about how we can protect these is absolutely critical for our country.

I have some statements, but I think your folks can pull those off the web, from Geoffrey Stone, with a "G". Thank you.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Let me start by saying that I guess I can take some comfort now knowing that Senator Rubio and Senator Cornyn and quite a few of us have had these sort of sophisticated targeting examples where you end up having to make sure that everything's in place, that your devices were not penetrated. I've certainly had staff targeted. I've had family members who have received these very sophisticated spear phishing and other kinds of approaches. Sometimes you know where the IP address is coming from because your provider literally tells you: Oh, by the way, if you didn't try to reset your account from Russia yesterday at 3:22 p.m., let us know.

And having been through that a few times, one of the things that I've certainly shared with my colleagues—and you mentioned this, Dr. Rid, is the importance of two-step authentication. I think it just can't be oversold to the public. Do you want to say just a couple more words about that and why that's so important?

Dr. RID. Had John Podesta had two-factor authentication the last month of the campaign, the last month of the campaign would have looked very different. I think that says it all.

Senator HEINRICH. That says it all. Yes, I could not agree more.

Given what we saw in 2016 and how easy it is to sometimes drive these wedges within our own society, what should we be expecting in 2018 and how should we be preparing for that? That's open-ended for any of the three of you if you want to share your thoughts.

Mr. MANDIA. It took about 18 years for me even to figure out as I responded to breaches they reflected geopolitical conditions, but they actually do. What I think we're going to observe in 2017 and 2018, the attacks will always exploit human trust. There will be clever ways to do it. There are ways to get around two-factor authentication, which we've seen Russians use as well as the Chinese government use.

I think it's going to be more what's fair game to espionage. I think that governments are going to start working on defining what are the industries that are fair game, what are the activities that are fair game and what aren't, because, quite frankly, every nation can get sucker-punched in cyber space, because we're exploiting human trust.

Senator HEINRICH. How do you send those signals about what is over the line and what the consequences of crossing that line might be?

Mr. MANDIA. Well, that's why we have diplomats. I think we're going to have doctrine. We're going to have things that we publish. We're going to have to let people know what we think are the right activities and are the wrong activities. The private sector will participate. Governments will participate. We'll get alignment with some nations and misalignment with others, and we'll adapt to that.

General ALEXANDER. Could I add to that?

Senator HEINRICH. Go ahead, General.

General ALEXANDER. I believe that one of the things that you could do and encourage is with the states setting up an exercise program between the State governments and the Federal Government about how you're actually going to improve the security of that and what they need to do, set the standards.

So I'd go beyond the National Institute of Standards and Technology. How do we know we're protecting voter registration databases, and what are the standards that we're holding them to and who's watching that, and setting the controls in place. I think that the states would greatly appreciate, so what are you going to do when we're being pummeled by a persistent? Now the government, the Federal Government, needs to step in. That's part of Senator Feinstein's question: How do you? Well, we haven't practiced that. We should practice that.

Senator HEINRICH. Dr. Rid.

Dr. RID. A very concrete suggestion that I think would actually make a difference. How many of the social media interactions, especially Twitter interactions, during the campaign of the most important Twitter accounts were created by bots?

Senator HEINRICH. Yes.

Dr. RID. Were created by automated scripts and not humans? The answer to that question—we don't know the answer to that question because Twitter and other social media networks have not provided the data. You could write a letter to these companies and ask them to provide the heuristics, to provide the data: How much of a problem is our bots?

Senator HEINRICH. That actually, that's very much in line with my next question that I was going to direct to you, which is: In addition to looking at the data, are there things that we should be doing working in concert with those social media companies to dampen the effectiveness of this feedback loop in the media cycle that is being exploited?

Dr. RID. Absolutely. You could, for instance, ask social media companies to provide detailed data, including a methodology of how they arrived at those data. It's very difficult for outsiders to get to the answer to these questions: How much of a problem are bots? I think it is a very significant problem.

When you sign up for a new Twitter account today, you can say—you know, the new accounts all have an egg face. You can say: I don't want any eggs, people who never change their account picture. No eggs is a good thing. You can say, I don't want eggs, but you can't say, I don't want bots. Bots are more of a problem than eggs, I believe.

So we should be in a position to, by default, move into an environment where we switch out abuse and bots out of our vision, if you like, as users.

Senator HEINRICH. Very helpful. Thank you all very much.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

General Alexander, first of all, it's nice to see you once again. Section 501 of the fiscal year 2017 intelligence authorization bill, which, regrettably, has not yet become law, requires the President to establish an interagency committee to counter active measures by Russia, including efforts to influence people and governments through covert and overt broadcasting.

The purpose of this committee would be to expose falsehoods, agents of influence, corruption, human rights abuses carried out by the Russian Federation or its proxies. Like the U.S. Information Agency, there once was an Active Measures Working Group that worked to counter covert disinformation from the Soviet Union, and that was disbanded.

Is this a recommendation, as we search for ways to counter the Russian attempts to spread propaganda, outright lies, influence our people—is this a recommendation that you believe should be implemented?

General ALEXANDER. I do. I think I would look at giving the Administration a suite of capabilities from diplomatic through cyber to what you just said, active measures, what we can do to expose that. I think we also need to give them the freedom to determine what's shared and what's not shared in terms of protecting the Nation in that regard, sharing it all with Congress of course, but how you publicize that if you know something is going on and you've got it through other means.

I think those things you'd want the Administration to at least be reasonable about, but I do think these are the kinds of things that should be put on the table. I would have to go back and look at all the tools that you're going to give them and say, does that meet the objectives of engaging Russia and confronting them when they cross the line on something? I think in this case this is something that would give them a tool, if they've crossed that line, to say, stop, here's what we know and here's the consequences.

Senator COLLINS. Because one of the aspects of this investigation that I found troubling that we've already learned is how weak our response is when we have a disinformation campaign. It seems to me that this working group could be useful. I realize it's a delicate issue in some ways because you don't want to sweep up legitimate—you don't want to be trying to set the rules for journalists, for example.

But that brings me to another issue for Professor Rid. That is, in your testimony you talked about how Russian disinformation specialized the act—specialists, I'm sorry, perfected the act of exploiting the unwitting agent. I assume by that you mean that individuals or entities who don't know or realize that they are being used by the Russians, but nevertheless are.

In your testimony you use examples of Twitter and journalists who cover political leaks without describing the origins of those leaks as examples of unwitting agents that were involved in the Russian influence campaign in 2016. You also list WikiLeaks. I would put WikiLeaks in a different category personally.

But what can we do about the unwitting agent? I mean the truly unwitting agent.

Dr. RID. Yes, I agree, in the case of WikiLeaks it's unclear whether they are unwitting indeed or just witting, so to speak.

Senator COLLINS. Right.

Dr. RID. But I think we are trained, the Western mind, if you like, is trained to think in contradictions. It's either this or that. But here I think we're looking at a situation—and this has been a pattern throughout the Cold War—where active measures operators recognize that unwitting agents—this could be journalists, politicians even; members of Parliament in the past have been the case—just because they're genuinely so passionate and engaged and activist in their outlook further the Russian cause.

So we have to recognize that this will continue to be a problem. We cannot simply get rid of that problem. It is something—for instance, we have documents from the Cold War time where disinformation active measures operators say they actually want conflict between the unwitting agent and the actual adversary, say WikiLeaks and the U.S. Government, conflict is good. So that's how far you can take. If the goal is driving wedges, then the unwitting agent is a trump card in your sleeve.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman BURR. Senator King.

Senator KING. Following up on that, it seems to me that the unwitting agent is a key part of this entire process, particularly where you're talking about disinformation. I think you make the point in your prepared statement that anonymity, anonymous leaks, there should be more work on where did it come from. Is that correct?

Dr. RID. Yes, absolutely. WikiLeaks was purpose-built to hide the source. That is the goal of the entire platform. Of course, I think—and I do take Julian Assange seriously when initially at least, historically, he was just an activist.

Senator KING. He was a clearinghouse, but now he's a selective leaker.

Dr. RID. That seems to be the case, yes.

Senator KING. General Alexander, we've been talking about this for at least four years. One of the problems—and you talked about this with Senator Collins—this country has no strategy or doctrine around cyber attacks; isn't that correct? And isn't that part of the problem? We need to have a doctrine and our adversaries need to know what it is.

General ALEXANDER. Absolutely, Senator, and I would add rules of engagement. We don't have—the consequence is if there were a massive attack we'd have to go back and get authority to act, where if it were missiles coming in we already have rules of engagement. So I think we need to step that up as well.

Senator KING. Ironically, part of that is transparency, because if we have a capability that would act as a deterrent but our adversaries don't know we have it, it doesn't act as a deterrent. Is that correct?

General ALEXANDER. That's correct. In fact, if I could, just to add something, because Thomas brought out another issue. I think it would be good also for the American people to release perhaps collectively the number of vulnerabilities our government has pushed out to industry, that has been identified by government, because often that's opaque. So what you wouldn't see is how much of that is actually being pushed to industry and how that's cleared. But you could get a collective summary from the departments and agencies that have pushed those out and see what's being shared. I think that's a good thing and it's a good way to start that dialogue.

Senator KING. That's a positive development, but I still believe that we need to develop a deterrence 2.0 to deal with the nature of the threats. And it doesn't have to be cyber for cyber. It could be sanctions or other. But there needs to be a certain response, a defined response and a timely response. Otherwise it's not going to have the deterrent effect.

General ALEXANDER. That's right, and we have to get the roles and responsibilities of the different agencies. Who's actually going to conduct that response? I think that has to be set straight and clear. We discussed that in the other hearing, but I think that's something that also means that if we had to react we wouldn't have the right people set up to react.

Senator KING. Mr. Mandia, one of the things—and I think this has been touched upon in the hearing—is the question of the vulnerability of our State election systems. We know that the Russians were poking around, if you will, in our State election systems. I learned recently that more than 30 states now allow internet voting and 5 have gone completely paperless. Doesn't this create a significant vulnerability?

Mr. MANDIA. It also creates an opportunity to do things even better. At the end of the day, when we look at—I go right to Estonia and what they do in their election process. I'm not totally intimate with it, but they have an identity management that's far better than our State, for our Nation.

When you have anonymity, it's really, really hard to secure the internet. Obviously, we're going to always have attacks on these areas. But what we're seeing is every election year—and I've responded to breaches every election year since 2004—both sides get targeted, things happen. We are still going up and to the right. I'm confident a modern nation—and probably others could speak better to this—would reserve the tool of tweaking electoral votes or ballots to the last resort. I've never seen evidence of that and I think we'll always have a natural risk profile to show great diligence in how we secure the election process and go forward.

Senator KING. My understanding of the intelligence is that it doesn't appear that they changed votes or vote tallies in this election.

Mr. MANDIA. No.

Senator KING. But they weren't going into those State election systems just for recreation. There was some purpose. I think one question, which I think any of you could answer, but you can answer: 2016 wasn't a one-off. This is a continuing ongoing and certainly future threat, is it not?

Mr. MANDIA. I think so. I think right now when you look at intelligence, it's been totally redefined by the internet. People are searching YouTube every day to see what operations are going on by ISIS. So the intelligence collection that we have today has never existed in the past. It's just that during this election we saw Russia break rules of engagement they had traditionally followed in that they added collections with computer intrusion, stealing documents and leaking them. But yes, I think this is a tool everybody's going to use.

Senator KING. Dr. Rid, do you want to respond?

Dr. RID. The great active measures campaign of 2016 will be studied in intelligence schools for decades to come, not just in Russia, of course, but in other countries as well.

Senator KING. So not only will it be studied; it will be attempts made to replicate it.

Dr. RID. That we can only assume, but it will certainly be studied.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Thank you, Mr. Chairman.

Let me ask you a question, Mr. Mandia. Your company has gone through an extensive amount of background to be able to look at the DNC hack and the exfiltration of their data. I want to repeat again what you have said orally and what is in your statement. Any other details that you can give us. You felt that this was Russian intelligence. You have answered that yes. But much of what you have put in your written statement seems to be a circumstantial look at it, that you were basically eliminating other things.

So let me ask you a question. Is this a process of elimination much like a doctor doing a diagnosis, saying it's not this, this, this, and it must be this? Or do you think there's something that zeroes in and says, no, that's really it and here's the evidence that links it?

Mr. MANDIA. I think that the intelligence available to the private sector is different for attribution than it is in the government. We can only take it so far. We're not going to fly people into Moscow and troll the streets trying to find a building. We have to do it by process of elimination. We have to do it by just deduction. But at the same timeframe, we hope the level of exactitude needed will come from the intelligence communities.

But we've done this with China. China, we just got lucky. Their operational security broke down so we could get an exact building and some people. Russia's operational security on the internet is better than that.

Senator LANKFORD. So let me ask: There has been conversation about Guccifer 2 being linked to the Russian government. Do you have any evidence of that or anything that would lead you to conclude that is true or lead you to at least disagree with the intelligence community on that?

Mr. MANDIA. I think it would be hard to think of any other—here's what we do know. I would attribute the Russian government to the breaches. We cannot connect all the dots from the breach, at least with the observables available to my company and our investigators. We can't go from breach and leaked data to suddenly Guccifer 2.0. We just don't have the means to do that.

Senator LANKFORD. But you think they're consistent?

Mr. MANDIA. I think it's remarkably consistent. APT28 intrusions are occurring and it's APT28 stolen data that's being leaked by DCLeaks, Guccifer, Anonymous Poland, and a bunch of other what we call fake personas or false personas.

Senator LANKFORD. Great, fair enough. So how confident are you that there's not any false flag operations that are involved in this?

Mr. MANDIA. We've observed this since 2007. I'm confident that APT28, the hacking group, is in fact sponsored by the government, the Russian government.

Senator LANKFORD. Fair enough. So let me ask you a question and it's the ongoing dialogue that we have here all the time. How do you define any difference in what's thrown around commonly as "We've had a cyber attack" or, as has been used in this conversation, "They've crossed the line"? We continue to talk about things like cyber doctrine, giving clear boundaries. We don't have any of those things. This has been an ongoing conversation for a while about who would set them, how they would be set. But at some point we have to have a clearer, a clear statement of what is crossing the line.

Earlier you made a statement it would depend on the State, it would depend on the situation and such. Can you give me an example—obviously, this is an example.

Mr. MANDIA. Right.

Senator LANKFORD. So other than this one, but give me an example of what it means to have a cyber attack that we can communicate to the American people, this is not just a nuisance hacker stealing information, this is an attack from a foreign government on our sovereignty?

Mr. MANDIA. First off, I go back to somebody made a comment once: It's hard to define pornography, but we know it when we see it. The reality is it's hard to delineate the cyber attack. I'll give you an example, though. I received a phone call once from one of our intrusion responders saying: We think North Korea hacked Sony Pictures. We went on site, we did the work, and we were as shocked as everyone that we even attributed it at, via our means, to most likely North Korea.

Then you start wondering, what levers do we have on North Korea to change their behaviors? That's why I think, A, attribution's critical. Got to know who did it. But I think the response will probably depend on our relations with those nations and their cooperation.

Senator LANKFORD. Talking to the difficulty of identifying who did it, as far as linking places when you get a chance to bounce and to be able to hide it different ways, is that becoming more difficult or easier based on the tools that we have or based on the tools that they have to be able to hide their location?

Mr. MANDIA. In the private sector, it's becoming more difficult for us to do attribution categorically. We used to have—we respond to hundreds of intrusions a year. By the end of 2010, six years of doing this, we only had 40 buckets of evidence. Every time we responded to a breach to figure out what happened and what to do about it, the trace evidence of what happened, cleanly into 40 buckets. Now we're into the thousands.

The TTPs and the malware's change, the infrastructure's changing. I would say actors are getting smarter about remaining anonymous in their attacks.

Senator LANKFORD. Mr. Rid, quickly I want to be able to ask you a question because you were alluding to this earlier. A matter of an attack is not just a matter of going and deleting files or creating chaos. It could be manipulating an existing file where you lose trust for it or adding a file that was never there, and suddenly there's something appearing on your computer that you never put there, someone else added to you.

So the threats of the attack that is out there, what could that look like?

Dr. RID. We have concrete examples. A recent one is a critic of President Putin in London was hacked and allegedly—and I think the evidence is quite good—illegal child abuse imagery was uploaded to his computer as an active measure to undermine his—to make him into a criminal in the U.K.

Senator LANKFORD. So they added child pornography onto his computer?

Dr. RID. You can just download something, as in the case of the DNC hack, where they uploaded something.

Senator LANKFORD. Thank you.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

Thank you all for your testimony today and helping us as much as you possibly can. We appreciate that. Let me ask this question. Could Russia have made a difference in the outcome if they wanted to? Did they get to the level that they could have gone further, but stopped and we fell into the trap?

Mr. Mandia.

Mr. MANDIA. In regards to the computers——

Senator MANCHIN. Basically, I'm understanding they were more aggressive than they've ever been and they got more involved than they ever got. Could they have done more and just stopped and we fell into the trap?

Mr. MANDIA. I don't know if we fell into the trap. I don't know what you mean by that.

Senator MANCHIN. The trap is basically what we're doing right now.

Mr. MANDIA. Could be. I can tell you this: I believe we probably know 90 percent of their cyber capability, maybe even only 80. They probably reserve their upper echelon for maybe——

Senator MANCHIN. Could they have basically changed the outcome of the election?

Mr. MANDIA. I have no idea. I don't know.

Chairman BURR. You don't know if they're capable of doing that?

Mr. MANDIA. I think—when I think of changing the outcome of an election, I'm an engineer; I think ones and zeroes kind of. I would say, could they have altered the votes? I think we would have seen that. I think we'll see the shot across the bow on some of the most severe attacks, things where we have lots of observation. I think we'd catch the shot across the bow.

Senator MANCHIN. Let me ask this question for anybody who wants to answer. How intense has their involvement been in other countries that we know in the past? Is it to the level they've gotten to with the United States in this past 2016 election? Are they that involved in France, Belgium, Germany?

Dr. Rid.

Dr. RID. It depends on how far you want to go back in history. The Stasi, we know that for a fact, affected the outcome of one vote of no confidence in the Bundestag, which kept Chancellor Brandt in power. So we have many, many historical precedents of elections.

Senator MANCHIN. How about in France going right now?

Dr. RID. Right now. We currently do not have a single example in Europe to my knowledge where a hack and a leak were combined in the way it would happen in the United States.

Senator MANCHIN. But their involvement in the election has shown a desire to get people that are more friendly toward the Russians?

Dr. RID. Yes. I mean, I'm not saying there's nothing going on. In fact, there are active measures under way. But they are of a different kind, it seems at this stage at least, than what we saw in 2016 here. They're more old-school, more forgeries, like the Lisa case that Senator Rubio mentioned earlier.

Senator MANCHIN. From the technology end of it, from the cyber end of it, do we have the ability to stop? And you're saying, what can we use? Is there going to be cyber warfare back to them? Is there something that we can do to a Russia that would stop this behavior or they would be concerned about we could intervene or interfere with their system?

Mr. MANDIA. I think General Alexander should comment on that, but I can tell you, at least on defense in the private sector, probably the best analogy I can give you is a hockey analogy. It's like going up against Gretzky on a penalty shot when the Russian government targets your organization. They have a good chance of putting the puck in the net.

General ALEXANDER. There's a couple of things, Senator, that I think we need to do. We talked about fix the defense. I think what we're doing right now with this committee and others is we have highlighted that we know they did this. They know that we know, and now the issue is they've been put on notice and now it's over to our government on the path forward.

We have an opportunity to engage and confront them on different issues. I think that in and of itself was something that perhaps they miscalculated. Now what we need to do is fix the defense and see what other actions we should take to defend our infrastructure, including the electoral infrastructure.

Senator MANCHIN. General, when Putin puts his statement out that he put out today claiming no responsibility, no knowledge whatsoever, and we know and the whole world should know—we've made it official. He seems to have a very high rating in Russia, so I don't think they're going to believe us. Do we have the ability to show from a technical aspect what was done?

General ALEXANDER. I think one of the benefits of his actual active campaign is it's had a great impact on his popularity in Russia. He's taken us on in these areas. I think saying "It wasn't us" is something that he would say ad infinitum. We saw this across the board, Thomas brought out, all the way back from Moonlight Maze and before Russian involvement, and they said it wasn't them. We knew it was.

Senator MANCHIN. Do any one of you three have what you would recommend as the greatest retaliation for Russia for this type of activity? Let's start right down the line if you will, Dr. Rid. What would you recommend? How would we retaliate, basically, to make sure that we harm them or hurt them to the point they will not continue this type of behavior?

Dr. RID. That's a tough question.

Senator MANCHIN. Militarily? Electronically?

Dr. RID. Certainly not militarily as there would be an escalation that is entirely inappropriate.

Senator MANCHIN. Economically?

Dr. RID. In I believe it was the DHS publication at the end of December, 29th, the then-Obama government pointed out, the Administration pointed out, RT as a major outlet of Russian active measures. At this stage RT has a license in the United States.

General ALEXANDER. I think we should step back, Senator, and say what is our objective with Russia? This was a single event. I think we should have—this is where the Administration from Secretary of State, Secretary of Defense, and others should get together—and we should give them the opportunity and time to do this—and say, what's our strategy going to be with Russia, which includes what you're asking? Because I don't think we want to do it tit for tat on these things and just retaliate.

What we really want to do is, how do we get an engagement with Russia that puts us and the world in a better place? I think it's part engagement and saying, here's what we want to do, we know this, and we've got to figure out how to stop, and here's what's going to happen if we don't, and put those on the table. But I think that needs to be done more in private than in public if we're going to have a chance of success.

You know, it's in our interests to address these problems now, when you look at what's going on in the Middle East, what's going on in Eastern Europe, and all the other problems we have. We've got to solve some of these by allowing the Administration to engage in that area. So I would push it over to the Administration. They have good people in this area.

Senator MANCHIN. My time—go ahead.

Mr. MANDIA. Yes, sir. A lot of comments here. I've got a very simple—there's a carrot or a stick. There's either money or the 82nd Airborne. I'd agree with everything the General said—not time for that.

I would caution the response if it's just in cyber space, the asymmetry. If all our tools work against them and all their tools worked against us in cyber space, Russia wins. So I don't think—there's too much asymmetry in cyber, based on our economy relying on it, our communications relying on it, our free press even. They can do an invasion on the privacy of everybody in this room. We can't really reciprocate that, hack Putin's email and post it and get the same results.

So I would just advise cyber-on-cyber just feels like we're in the glass house throwing rocks at a mud hut. We're not going to pan out very well there.

Senator MANCHIN. Thank you.

Chairman BURR. Senator Harris.

Senator HARRIS. Mr. Mandia, one main reason that we're doing this public hearing is so that the American public can actually understand what happened. So if we can just take a step back, because this is a fairly complex issue, and particularly when we start talking about bots and all these other things. Some people wonder, is it just a short form for a robot?

Let me ask you—Americans, I think many whom I've spoken with can't help but feel that they have been played if they made their decision in this election based on fake news. How can they know that they are receiving fake news? How can they detect it so that they can ultimately make decisions like who will be their President based on accurate information?

Mr. MANDIA. That goes beyond my expertise as a cyber security individual. I can just say as a lay person everybody's got to take everything they hear and vet it against multiple sources. But I simply don't have the right tools to be an expert on how do you determine fake from non-fake news.

Senator HARRIS. Do any of you feel experienced enough to answer that question?

Dr. RID. It's a simple answer. If it's in The New York Times or the Washington Post, it's not fake news. I mean, we have to believe in the center, so to speak. If we don't, if we can't trust the mainstream media any more, then we've lost.

General ALEXANDER. Could I add to that?

Senator HARRIS. Yes, please.

General ALEXANDER. I think part of it is we at times sensationalize and inflame, not inform. How do we get a more informed set of reports out to the American people on some of these issues? That's something I don't have an answer to, but that's part of the problem. We've got to figure out how to address that as we go into this next age of having all the information available at an instant.

We saw the attack on the White House, the theoretical attack about a year ago. It turned out to be fake news. I think we've got to take another few steps on that. That's where the news agencies, social media, and governments have to work together to help get the facts out there. Just the facts, ma'am.

Senator HARRIS. So tell me—I'm going to direct it—I'll start with Mr. Mandia, but whoever can answer this question if you feel you have an answer. How can we tell if Fox manipulated a Google search to elevate the placement of fake news in the 2016 elections, and what partnerships might we take with Google or any other search engine to avoid that happening in the future?

Mr. MANDIA. I think that's a great question. I think Google probably has the answer. Here's the reality even that's going to be difficult for them. There's a lot of ways. What you're describing is what we used to call astroturfing. It's the way to manipulate public opinion just based on the number of hits and influences behind that. It depends on the platform. It's actually a complex challenge for us to pierce anonymity behind, is that a bot or a human, because bots keep getting smarter, replicating us.

General ALEXANDER. I would just add, I think Google has some great folks in this area, and that may be something that you get the folks at Google, Facebook, Twitter together along with some of the other social media and ask them that question: How can we jointly solve some of these issues? I think it's a great question and one that they would take on.

Dr. RID. Social media companies are—the market assesses social media companies on the basis of active users, the active user base. Now, if a certain amount of the active users are simply bots. There's a commercial interest in not revealing the fact that a tenth, a third of your user base actually is machines.

Senator HARRIS. Thank you.

General Alexander, as a former General—I asked this question of the earlier panel. We invest in our military and our soldiers as part of our defense system and rightly. But Russia seems to be investing a great amount in its cyber security as a tool of warfare. What would you recommend we do in terms of the United States Government to meet those challenges in terms of how we're investing in infrastructure to be able to combat, both on the point of deterrence, but also resilience; after we do detect, when and if we do detect that we've been hacked, how we can step back up and pick back up as quickly as possible; and then obviously what we need to do in terms of any sort of retaliation?

General ALEXANDER. I think there are several key points that we have to do. One is we have to fix the relationship between industry and the government for sharing information so that they can be protected. We have to set up the rules of engagement and the rules of what each of the departments are going to do and they have to understand and agree to those. We have to rehearse that within the government and between government and industry.

Senator HARRIS. I only have a few seconds left, so I'd like you to direct your response—and I appreciate the points you made earlier on this, on this point. But we have a budget coming up. What would you advocate in terms of the budget that is going to be before us to vote on? It's called a skinny budget. There's a whole lot of discussion about where the limited resources and dollars are going to go. On this point, what would you advise us in terms of how we distribute those limited resources to meet these challenges, the challenges in terms of the Russian government and the finding by the FBI, NSA, and CIA that they hacked our systems?

General ALEXANDER. I think we definitely need to continue and increase the investment in what we have in our cyber capabilities, the forces and the infrastructure and the tools that we create. That's needed. I think we also have to look at—and one of the members over here brought out—government. Our IT in government is broke. We need to fix it, and we need to look at how we secure it. OPM was a great example that they used. I think that's something this Administration is already looking at, but we need to help them get there and figure out the best way to do that.

When you think about it, they don't have the IT resources or the cyber security professionals to actually defend them. The solution has got to look at what we do with the commercial sector and how we add that to government. I think those are the key things.

Senator HARRIS. I appreciate that. Thank you.

Chairman BURR. Do any other members seek additional questions?

Vice Chair.

Vice Chairman WARNER. I would just like to ask one quick one. I think this line of questioning we've heard about how we can react, very briefly because the Chairman hasn't asked his questions yet. But I do wonder. We saw the example that somebody did hack into former Prime Minister Medvedev's files, which showed lots and lots of luxury properties all over the world. In many ways that seemed to result in a series of protests across Russia, where unfortunately protesters were arrested.

But comment on that? Very briefly, since the Chairman hasn't had his questions.

Dr. RID. I'm not sure I understand the question properly. Are you implying that——

Vice Chairman WARNER. I'm inquiring whether the—I agree with Kevin on the notion of simply tit-for-tat actions in cyber because we're more technologically dependent. But there are activities kind of around active measures where Prime Minister, former President and now Prime Minister, Medvedev in Russia—maybe I'm mispronouncing the name—suddenly all his extensive property holdings became public, which caused great consternation in Russia and a series of protests.

Dr. RID. We know from publicly available information that President Putin, Vladimir Putin, believes the Panama Papers leak, which broke on the 3rd of April in 2016, so right in the middle of the ramped-up targeting—targeting on their side ramped up before Panama Papers broke as a story, but we have to assume they knew about Panama Papers, that it was coming.

Putin seems to believe Panama Papers was an American active measure against him. I don't think this was the case, but that puts the entire operation into a slightly different light and it's important to consider that.

Chairman BURR. Thank you, Vice Chairman.

Listen, we really are grateful to all three of you for making yourselves available. Keith, you're a guy that the committee has looked up to, not just because of the stars on your shoulder, but it's the knowledge in your head and how you have had a way for years to convey to the committee in a way that we could understand what the threat was, what our capabilities needed to be, the actions that we needed to take, why we needed to take them, and the objective of the effort.

I think what concerns me is that this thing's speeding so fast now, it's like you pulled the string on the top when we were kids, and over time the top slowed down, and it looks like now the top starts spinning faster and faster and faster once you've pulled the string.

So I want you to understand that we're probably going to invite you back in an informal setting, probably not a public setting, where some of the things we got into today we couldn't dig much deeper. And thank you for showing the constraint of doing that.

For that reason, I'm not going to include you in my other two questions, because it might put you on the spot.

I'm going to turn first to Dr. Rid. Do we have any idea how Russia transmitted emails to WikiLeaks? And if that's the process that everybody assumes happened, then how could WikiLeaks be, as you referred to, unwitting?

Dr. RID. That's a good question. Guccifer 2.0, the front that was created, tweeted that they gave emails to WikiLeaks. WikiLeaks tweeted that they received something from Guccifer 2.0 before this was attributed to Russia. So that's the only evidence that we have publicly and I think it's quite strong, or it's certainly notable.

Is WikiLeaks an unwitting agent? In truth, we can't answer the question because they haven't spoken on it. But we also can't just assume that they're not an unwitting agent. But ultimately it doesn't matter, because they are a very effective unwitting agent.

Chairman BURR. Kevin, do the forensics that you're able to have done suggest that WikiLeaks continues to hold additional emails that have not been released?

Mr. MANDIA. I can't answer that. I can tell you from all my experience what we've seen publicly released is probably under one percent of what we've attributed to the Russian government stealing.

Chairman BURR. We're trying as a committee to come up to speed on not just terminology, but what that terminology means. So I'd like to give you an opportunity to walk us through how you identify an actor like APT28?

Mr. MANDIA. Yes, and here comes the details. First, for the first time ever we started getting better software in place beforehand so we'd see keystroke by keystroke what they're doing. I think most Senators do not do command line execution, but there's different commands you can type, there's different letters that you type in different orders. You start getting to know the attackers when you get that command-level access to them.

Then it's the malware they've created, the IP addresses they use, the infrastructure they use to attack, the people that they actually target, the encryption algorithms they use, the pass phrases they use when they encrypt things, and the list goes on and on.

We tracked at one point—we created a scheme in about 2006 on how do you categorize the intelligence or the evidence, the forensics, from an intrusion investigation, and we had over 650 categories. I can't go into all of them today, but trust me, you observe a group for ten years or more; after a while, we got the bucket right. APT28 to us is a bucket. Every time we respond to them, there's enough criteria together that APT28 is our APT28, APT29 is our APT29, APT1 was PLA Unit 61398.

The link is we couldn't take 28 and 29 and say GRU or FSB. It just isn't available to us in the trace evidence when we respond to intrusions. But it's time-stamps, compilations.

I'll give you one last example because this is understandable. When you look at the malware that's been used in these attacks and their compile times, 98 percent or higher of it is compiled during business hours in Moscow or St. Petersburg. That's a pretty good clue. And whoever's doing it speaks Russian.

Chairman BURR. If you'd rather not answer this or don't know the answer, punt it and I'll forget it. Had the DNC decided to provide their system for FBI to do forensics on, would we have gotten more information?

Mr. MANDIA. I don't know. I can tell you—I can't speak specifically to that one, but over the last five to six years we respond to a lot of breaches now where the FBI is there, and they are there. And they're not the ones traditionally doing forensics. They are relying on a lot of the private sector forensicators. That's a made-up word. But we're doing our forensics. We're producing it. And the customers are choosing, our clients are choosing, to share that with the FBI.

I think the group that responded to the DNC is highly technical, highly capable. They got it right.

Chairman BURR. It was a diplomatic way of asking, do we have different capabilities than the private sector. And you said——

Mr. MANDIA. Yes. We've had tremendous help. When we respond and the FBI is in the room, it's fantastic help. Maybe they're cleansing intel from another agency or not. But there's been numerous cases where we're showing up and we know maybe three things to look for, and the FBI says: here's another 80; go look for those as well. So we are—and I've been doing this 20 years. It's more likely than not when we respond to intrusion the FBI is actually there and responding with us.

Chairman BURR. I sort of leave this hearing not having heard a word that I think we're going to use frequently based upon what's going on, and that's "dox." My understanding of the term "dox" is it's the 21st century term for "steal and leak." Am I going to hear "dox" a lot in the future?

Mr. MANDIA. It's an irritating word to hear, isn't it? But at the end of the day, yes, you'll probably hear it. That's the technique that, it looks like a state actor is using it. I can tell you the first time we saw North Korea delete things in the United States, that felt like it crossed a red line. Doxing appears to be the thing that crossed the line with the Russian activities.

Chairman BURR. Thomas.

Dr. RID. One sentence on what Kevin just said about the FBI there. Usually in an investigation of the kind he was describing, you would make a so-called image of the computer hard disk, and if the FBI has these images, which I understand they may have, then you don't actually have to physically be there. It's as good as being there physically.

But on the doxing observation, yes. Just to make another observation that may be personal for many of you here in this room, but the ethics rules in Congress may actually make members of Congress and in the Senate more vulnerable, because it forces you to use different devices, sometimes as many as three devices, I understand, to make different calls and different communications.

So even if the main work device is actually secured properly, then it would push you down into a more vulnerable area. That is a problem that possibly can also be fixed.

Chairman BURR. One last general statement, and I heed the advice you gave, General, and you backed up, Thomas, and I think, Kevin, you supported as well. Our response has to be well thought through, and it's not just what we do in reaction to, it's what we do as we set the course for some better defensive mechanism in the future.

But you can't neglect the fact that Russia over a period of time has done things outside of cyber—invasion of Ukraine, Moldova, presence in Syria, presence in Egypt. It continues on. We might look at this today in the rear view mirror and say: Boy, they miscalculated. The only way they miscalculated is to have taken our neglect of reaction to what they did as an opportunity to push a little harder on the accelerator.

Not being critical, but we've done nothing to Russia when they've made aggressive moves. And now all of a sudden this happened at home. It happened with elections. When you look at it from a standpoint of impact, I think the Ukrainian people would tell me what happened to them is much worse, and if it happened in the United States we would think that's much worse.

But the fact is that this is going to require a global response, because the globe is just as exposed as the United States. It was our election system in 2016. It is the French, the Germans—I won't get into the long list of them. But we're within 30 days of what is a primary election in France. It could be that the Russians have now done enough to make sure that a candidate that went to Russia recently and a socialist make the runoff and they end up with a pro-Russian government in France. They've won. That was their intent, I feel certain.

We're not sure what the effects are going to be in Germany, but we've actually seen them build up a party in Germany, not tear down but build up a party, and exploit things that were, when you look back on them, fake news, not that we created, but that was created within Germany, that never was news, but they used it, they exploited it. And look at what it's turned into.

So we may have been the first victim, but we may not have been victimized as much as others are going to be in the short term, and we certainly should heed the warning and not be an additional victim in 2018 or 2020.

Let me move to Senator King real quick.

Senator KING. Just a follow-up question to Dr. Rid. Tell me more about Guccifer 2.0. Is that a flesh-and-blood human being? Is it an office? Second question: is there any doubt that Guccifer 2.0 is an agent or somehow working for the Russian government?

Dr. RID. Guccifer 2.0 is—we know this from the evidence that's available, not all of it public, but only private sector sources and academic sources, I may say. Guccifer 2.0 is certainly not just one individual, because in private interactions with journalists we can literally see different types of humans at play. Some use it consistently at a specific time, lots of smileys and very informal. Others are more formal. All communicating through the same channel.

On the links, Guccifer 2.0 to others, APT28, as I mentioned and as I also lay out in my evidence in the written testimony, hacked 12 of the targets that were leaked, doxed, on DCLeaks. Guccifer 2.0 provided a password that was not publicly known, provided a password to DCLeaks to the smoking gun, the outlet. So that's a very strong forensic link there. The link I think—the docs can be connected.

Senator KING. But how about my second part of my question? Is Guccifer 2.0 an agent of the Russian government in some way, shape, or form?

Dr. RID. If you mean by "agent," an agency or sort of organization, it could be a subcontractor, it could be a team within an intelligence agency.

Senator KING. Affiliated or associated with the Russian government?

Dr. RID. I am confident that the answer is yes.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. I thank all the members, and I thank our panel today. You have provided us some incredible insight and knowledge. We're grateful to you.

This hearing is adjourned.

[Whereupon, at 4:02 p.m., the hearing was adjourned.]

Supplemental Material

Statement of Chairman Richard Burr

Russian Active Measures – OPEN HEARING – Panel 2
March 30, 2017

This morning the Committee examined the history and characteristics of Russian Active Measure campaigns as a lead up to this, our second panel, which will examine the role cyber operations play in support of those activities. I'd like to welcome our witnesses: Mr. Kevin Mandia, Chief Executive Officer of FireEye, a global cyber security company. Prior to founding the cyber security company Mandiant, which was acquired by FireEye in 2013, Mr. Mandia served in the United States Air Force as a computer security officer and later as a special agent in the Air Force Office of Special Investigations, where he worked as cybercrime investigator. I thank you for being here and thank you for your service. General Keith Alexander is the CEO and President of IronNet Cybersecurity, another global cybersecurity firm on the forefront of our nation's commercial efforts to mitigate cybersecurity threats. Prior to founding IronNet, General Alexander served for 40 years in our armed forces, culminating with his tenure as the Director of the National Security Agency from 2005 to 2014 and concurrent service as Director of U.S. Cyber Command from 2010 – 2014. General, thank you for being here and thank you for your many years of honorable service. Dr. Thomas Rid is a Professor of Security Studies at

King's College London. He has studied and written extensively on cybersecurity issues and worked at Hebrew University and Shalem in Jerusalem, Johns Hopkins' School for Advanced International Studies, and the RAND Corporation. Dr. Rid, thank you for being here today and I look forward to your testimony.

I'd like to note for the public and my fellow members that the level of cyber expertise in front of us is truly remarkable. These witnesses will be able to provide, at the unclassified level, some extremely useful texture and detail to the discussion we began this morning.