Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security

Richard Burr, Mark Warner,
Susan Collins, Martin Heinrich, James Lankford

Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security

Press Contact: Ben Khouri (Burr) 202-228-1616
Rachel Cohen (Warner) 202-228-6884
Annie Clark (Collins) 202-224-2523
Whitney Potter (Heinrich) 202-228-1578
D.J. Jordan (Lankford) 202-224-5754

Tuesday, May 08, 2018

WASHINGTON, D.C. – Today, Senator Richard Burr (R-NC), Chairman of the Senate Select Committee on Intelligence, Senator Mark Warner (D-VA), Vice Chairman of the Senate Select Committee on Intelligence, and Senators Susan Collins (R-ME), Martin Heinrich (D-NM), and James Lankford (R-OK), members of the Senate Select Committee on Intelligence, released the Committee's unclassified summary of the first installment of the Committee's Russia Report, including updated recommendations on election security and findings regarding Russian targeting of election infrastructure. In parallel, the Committee has prepared a comprehensive, classified report on threats to election infrastructure. The classified report will be submitted for declassification review, and the Committee anticipates releasing it to the public when that process is completed.

"I'm pleased to be able to release this summary of our findings and recommendations on election security to the American public," **said Senator Richard Burr**. "Today's primaries are the next step toward the 2018 midterms and another reminder of the urgency of securing our election systems. Our investigation has been a bipartisan effort from day one, and I look forward to completing the Committee's work and releasing as much of it as possible. We are

working tirelessly to give Americans a complete accounting of what happened in 2016 and to prevent any future interference with our democratic process."

"Elections at all levels are central to our democracy, to our institutions, and to our government's legitimacy, and I remain concerned that we as a country are still not fully prepared for the 2018 midterm elections. That's one reason why we, as a Committee, have decided that it is important to get out as much information as possible about the threat, so that governments at every level take it seriously and take the necessary steps to defend ourselves," **said Senator Mark Warner**. "I am proud of the bipartisan work our Committee members have done on this issue, and I look forward to continuing in a bipartisan way to investigate what happened in 2016, and prevent future interference in our elections."

"While our investigation remains ongoing, one conclusion is clear: the Russians were relentless in attempting to meddle in the 2016 election, and they will continue their efforts," **said Senator Susan Collins**. "The findings and recommendations we are releasing today are a major step forward in our effort to thwart any attempt to meddle in our elections. With the 2018 election fast approaching, the need to act now is urgent. We must provide states the assistance they need to strengthen the security of their voting systems."

"Our democracy hinges on Americans' ability to fairly choose our own leaders. With primary elections underway, and as we approach the midterm elections and the next presidential election cycle, we need to act quickly to protect the integrity of our voting process," **said Senator Martin Heinrich.** "I am proud of how our whole Committee, under the leadership of Chairman Burr and Vice Chairman Warner, has taken on the task of getting to the bottom of Russia's interference in our election. Until we set up stronger protections of our election systems and take the necessary steps to prevent future foreign intervention, our nation's democratic institutions will remain vulnerable to attack."

"During the 2016 election, Russian entities targeted presidential campaign accounts, launched cyber-attacks against at least 21 state election systems, and hacked a US voting systems software company," **said Senator James Lankford.** "We must proactively work to ensure the security of our election infrastructure for the possibility of interference from not just Russia, but possibly another adversary like Iran or North Korea or a hacktivist group. After 18 months of investigations and interviews, this bipartisan report underscores the importance of efforts to protect our democracy from foreign attacks on our elections."

The Committee's unclassified summary of this chapter of the Russia Report – Election Security Findings and Recommendations are embedded below:

Russian Targeting of Election Infrastructure During the 2016 Election:
Summary of Initial Findings and Recommendations

May 8, 2018

Overview

In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure. Russian actors scanned databases for vulnerabilities, attempted intrusions, and in a small number of cases successfully penetrated a voter registration database. This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.

- The Committee has limited information about whether, and to what extent, state and local officials carried out forensic or other examination of election infrastructure systems in order to confirm whether election-related systems were compromised. It is possible that additional activity occurred and has not yet been uncovered.

Summary of Initial Findings

- Cyber actors affiliated with the Russian government scanned state systems extensively throughout the 2016 election cycle. These cyber actors made attempts to access numerous state election systems, and in a small number of cases accessed voter registration databases.
    - At least 18 states had election systems targeted by Russian-affiliated cyber actors in some fashion.[1] Elements of the IC have varying levels of confidence about three additional states, for a possible total of at least 21. In addition, other states saw suspicious or malicious behavior the IC has been unable to attribute to Russia.
    - Almost all of the states that were targeted observed vulnerability scanning directed at their Secretary of State websites or voter registration infrastructure. Other scans were broader or less specific in their target.
    - In at least six states, the Russian-affiliated cyber actors went beyond scanning and conducted malicious access attempts on voting-related websites.[2]
    - In a small number of states, Russian-affiliated cyber actors were able to gain access to restricted elements of election infrastructure. In a small number of states, these cyber actors were in a position to, at a minimum, alter or delete voter registration data; however, they did not appear to be in a position to manipulate individual votes or aggregate vote totals.
- The Committee found that in addition to the cyber activity directed at state election infrastructure, Russia undertook a wide variety of intelligence-related activities targeting the U.S. voting process. These activities began at least as early as 2014, continued through Election Day 2016, and included traditional information gathering efforts as well as operations likely aimed at preparing to discredit the integrity of the U.S. voting process and election results.
- The Committee's assessments, as well as the assessments of the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), are based on self-reporting by the states. DHS has been clear in its representations to the Committee that the Department did not have perfect insight into these cyber activities. It is possible that more states were attacked, but the activity was not detected. In light of the technical challenges associated with

cyber forensic analysis, it is also possible that states may have overlooked some indicators of compromise.

- The Committee saw no evidence that votes were changed and found that, on balance, the diversity of our voting infrastructure is a strength. Because of the variety of systems and equipment, changing votes on a large scale would require an extensive, complex, and state or country-level campaign. However, the Committee notes that a small number of districts in key states can have a significant impact in a national election.

[1] These numbers only account for state or local government targets. DHS did not include states which may have witnessed attacks on political parties, political organizations, or NGOs. In addition, the numbers do not include any potential attacks on third-party vendors.

2 In the majority of these instances, Russian government-affiliated cyber actors used Structure Query Language (SQL) injection - a well-known technique for cyberattacks on public-facing websites.

Actors and Motive

- The Committee concurs with the IC that Russian government-affiliated actors were behind the cyber activity directed against state election infrastructure.
- While the full scope of Russian activity against the states remains unclear because of collection gaps, the Committee found ample evidence to conclude that the Russian government was developing capabilities to undermine confidence in our election infrastructure, including voter processes.
- The Committee does not know whether the Russian government-affiliated actors intended to exploit vulnerabilities during the 2016 elections and decided against taking action, or whether they were merely gathering information and testing capabilities for a future attack. Regardless, the Committee believes the activity indicates an intent to go beyond traditional intelligence collection.

DHS Efforts to Bolster Election Security

- The Committee found that DHS's initial response was inadequate to counter the threat. In the summer of 2016, as the threat to the election infrastructure emerged, DHS attempted outreach to the states, seeking to highlight the threat for information technology (IT) directors without divulging classified information. By the fall of 2016, as the threat became clearer, DHS attempted a more extensive outreach to the states with limited success.
    - At the outset, DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor.
    - In addition, members of the Obama administration were concerned that, by raising the alarm, they would create the very impression they were trying to avoid––calling into question the integrity of election systems.
- DHS and FBI alerts to the states in the summer and fall of 2016 were limited in substance and distribution. Although DHS provided warning to IT staff in the fall of 2016, notifications to

state elections officials were delayed by nearly a year. Therefore, states understood that there was a cyber threat, but did not appreciate the scope, seriousness, or implications of the particular threat they were facing.

  - Many state election officials reported hearing for the first time about the Russian attempts to scan and penetrate state systems from the press or from the public Committee hearing on June 21, 2017. DHS's notifications in the summer of 2016 and the public statement by DHS and the ODNI in October 2016 were not sufficient warning.
  - It was not until September of 2017, and only under significant pressure from this Committee and others, that DHS reached out directly to chief election officials in the targeted states to alert the appropriate election officials about the scanning activity and other attacks and the actor behind them. (However, the Committee notes that in the small number of cases where election-related systems had been compromised, the federal government was in contact with senior election officials at the time the intrusion was discovered.)

- The Committee found that DHS is engaging state election officials more effectively now than in the summer of 2016. Although early interactions between state election officials and DHS were strained, states now largely give DHS credit for making tremendous progress over the last six months.

  - States have signed up for many of the resources that DHS has to offer, and DHS has hosted meetings of the Government Coordinating Council and Sector Coordinating Council, as required under the critical infrastructure designation. Those interactions have begun to increase trust and communication between federal and state entities.
  - DHS hosted a classified briefing for state chief election officials and is working through providing security clearances for those officials.
  - An Election Infrastructure Information Sharing and Analysis Center has been established, focused on sharing network defense information with state and local election officials.

Ongoing Vulnerabilities

Despite the progress on communication and improvements to the security of our election process, the Committee remains concerned about a number of potential vulnerabilities in election infrastructure.

- Voting systems across the United States are outdated, and many do not have a paper record of votes as a backup counting system that can be reliably audited, should there be allegations of machine manipulation. In addition, the number of vendors selling machines is shrinking, raising concerns about supply chain vulnerability.

  - Paperless Direct Recording Electronic (DRE) voting machines––machines with electronic interfaces that electronically store votes (as opposed to paper ballots or optical scanners)––are used in jurisdictions in 30 states and are at highest risk for security flaws. Five states use DREs exclusively.

- Many aspects of election infrastructure systems are connected to and can be accessed over the internet. Furthermore, systems that are not connected to the internet, such as voting machines, may still be updated via software downloaded from the internet.
    - These potentially vulnerable systems include some of the core components of U.S. election infrastructure, including systems affiliated with voter registration databases, electronic poll books, vote casting, vote tallying, and unofficial election night reporting to the general public and the media. Risk-limiting audits are a best practice to mitigate risk.
- Vendors of election software and equipment play a critical role in the U.S. election system, and the Committee continues to be concerned that vendors represent an enticing target for malicious cyber actors. State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of many of these vendors, and while the Election Assistance Commission issues guidelines for security, abiding by those guidelines is currently voluntary.

Summary of SSCI Recommendations

The Senate Select Committee on Intelligence has examined evidence of Russian attempts to target election infrastructure during the 2016 U.S. elections. The Committee has reviewed the steps state and local election officials have taken to ensure the integrity of our elections and agrees that U.S. election infrastructure is fundamentally resilient. The Department of Homeland Security, the Election Assistance Commission, state and local governments, and other groups have already taken beneficial steps toward addressing the vulnerabilities exposed during the 2016 election cycle, including some of the measures listed below, but more needs to be done. The Committee recommends the following steps to better defend against a hostile nation-state who may seek to undermine our democracy:

1. **Reinforce States' Primacy in Running Elections**
    - States should remain firmly in the lead on running elections, and the Federal government should ensure they receive the necessary resources and information.
2. **Build a Stronger Defense, Part I: Create Effective Deterrence**
    - The U.S. Government should clearly communicate to adversaries that an attack on our election infrastructure is a hostile act, and we will respond accordingly.
    - The Federal government, in particular the State Department and Defense Department, should engage allies and partners to establish new international cyber norms.
3. **Build a Stronger Defense, Part II: Improve Information Sharing on Threats**
    - The Intelligence Community should put a high priority on attributing cyberattacks both quickly and accurately. Similarly, policymakers should make plans to operate prior to attribution.
    - DHS must create clear channels of communication between the Federal government and appropriate officials at the state and local levels. We recommend that state and

local governments reciprocate that communication.
- Election experts, security officials, cybersecurity experts, and the media should develop a common set of precise and well-defined election security terms to improve communication.
- DHS should expedite security clearances for appropriate state and local officials.
- The Intelligence Community should work to declassify information quickly, whenever possible, to provide warning to appropriate state and local officials.

4. **Build a Stronger Defense, Part III: Secure Election-Related Systems**

- Cybersecurity should be a high priority for those managing election systems.
- The Committee recommends State and Local officials prioritize the following:
    - Institute two-factor authentication for state databases.
    - Install monitoring sensors on state systems. One option is to further expand DHS's ALBERT network.
    - Identify the weak points in the network, including any under-resourced localities, and prioritize assistance towards those entities.
    - Update software in voter registration systems. Create backups, including paper copies, of state voter registration databases. Include voter registration database recovery in state continuity of operations plans.
    - Consider a voter education program to ensure voters check registration well prior to an election.
    - Undertake intensive security audits of state and local voter registration systems, ideally utilizing an outside entity.
    - Perform risk assessments for any current or potential third-party vendors to ensure they are meeting the necessary cyber security standards in protecting their election systems.

- The Committee recommends DHS take the following steps:
    - Working closely with election experts, develop a risk management framework that can be used in engagements with state and local election infrastructure owners to document and mitigate risks to all components of the electoral process.
    - Create voluntary guidelines on cybersecurity best practices and a public awareness campaign to promote election security awareness, working through the U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED).
    - Maintain and more aggressively promote the catalog of services DHS has available for states to help secure their systems, and update the catalog as DHS refines their understanding of what states need.
    - Expand capacity to reduce wait times for DHS cybersecurity services.
    - Work with GSA to establish a list of credible private sector vendors who can provide services similar to those provided by DHS.

5. **Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself**

- States should rapidly replace outdated and vulnerable voting systems. At a minimum, any machine purchased going forward should have a voter-verified paper trail and no WiFi capability. If use of paper ballots becomes more widespread, election officials should re-examine current practices for securing the chain of custody of all paper ballots and verify no opportunities exist for the introduction of fraudulent votes.
- States should consider implementing more widespread, statistically sound audits of election results. Risk-limiting audits, in particular, can be a cost-effective way to ensure that votes cast are votes counted.
- DHS should work with vendors to educate them about the potential vulnerabilities of both voting machines and the supply chains.

6. **Assistance for the States**

- States should use federal grant funds to improve cybersecurity by hiring additional Information Technology staff, updating software, and contracting vendors to provide cybersecurity services, among other steps. Funds should also be available to defray the costs of instituting audits.

###

[1] These numbers only account for state or local government targets. DHS did not include states which may have witnessed attacks on political parties, political organizations, or NGOs. In addition, the numbers do not include any potential attacks on third-party vendors.

[2] In the majority of these instances, Russian government-affiliated cyber actors used Structure Query Language (SQL) injection - a well-known technique for cyberattacks on public-facing websites.

Senate Intel Releases Election Security Findings in First Volume of Bipartisan Russia Report

Press Contact: Caitlin Carroll (Burr) (202) 228-1616

Rachel Cohen (Warner) (202) 228-6884

Thursday, July 25, 2019

Today, Senate Select Committee on Intelligence Chairman Richard Burr (R-NC) and Vice Chairman Mark Warner (D-VA) released "*Russian Efforts Against Election Infrastructure* ," the first volume in the Committee's bipartisan investigation into Russia's attempts to interfere with the 2016 U.S. elections.

Today's installment builds upon the unclassified summary findings on election security released by the Committee in May 2018. This was the first volume completed due to the fundamental importance and urgency of defending our democratic elections.

As part of its investigation, the Committee will also release final volumes examining the Intelligence Community Assessment (ICA) of Russian interference, the Obama Administration's response to Russian interference, the role of social media disinformation campaigns, and remaining counterintelligence questions. The Committee has submitted its volume on social media for declassification review and intends to release the remaining installments in fall 2019.

Over the last two and half years, the Committee's investigation has spanned more than 15 open hearings, more than 200 witness interviews, and nearly 400,000 documents.

Statement from Chairman Burr:

"In 2016, the U.S. was unprepared at all levels of government for a concerted attack from a determined foreign adversary on our election infrastructure. Since then, we have learned much more about the nature of Russia's cyber activities and better understand the real and urgent threat they pose. The Department of Homeland Security and state and local elections officials have dramatically changed how they approach election security, working together to bridge gaps in information sharing

and shore up vulnerabilities. The progress they've made over the last three years is a testament to what we can accomplish when we give people the opportunity to be part of a solution.

"There is still much work that remains to be done, however. I am grateful to the many states that provided their points of view, which helped inform our recommendations. It is my hope that the Senate Intelligence Committee's bipartisan report will provide the American people with valuable insight into the election security threats still facing our nation and the ways we can address them."

Statement from Vice Chairman Warner:

"When the Russians attacked elections systems in 2016, neither the federal government nor the states were adequately prepared. Our bipartisan investigation identified multiple problems and information gaps that hindered our ability to effectively respond and defend against the Russian attack in 2016. Since then – and in large part as a result of the bipartisan work done on this issue in our Committee – the intelligence community, DHS, the FBI, and the states have taken steps to ensure that our elections are far more secure today than they were in 2016. But there's still much more we can and must do to protect our elections. I hope the bipartisan findings and recommendations outlined in this report will underscore to the White House and all of our colleagues, regardless of political party, that this threat remains urgent, and we have a responsibility to defend our democracy against it."

You can read, "*Volume I: Russian Efforts Against Election Infrastructure*" here .

Key Findings and Recommendations:

- The Russian government directed extensive activity against U.S. election infrastructure. The Committee found the activity directed at the state and local level began in at least 2014 and carried into at least 2017. The Committee has seen no evidence that any votes were changed or that any voting machines were manipulated.
- Russian efforts exploited the seams between federal authorities and capabilities, and protection for the states. The Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) are, by design, limited in domestic cybersecurity authorities. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor.
- DHS and FBI warnings to the states in the late summer and fall of 2016 did not provide enough information or go to the appropriate people. The Committee found that while the alerts were actionable, they provided no clear reason for states to take the threat more seriously than other warnings.
- DHS has redoubled its efforts to build trust with the states and deploy resources to assist in securing elections. Since 2016, DHS has made great strides in learning

how election procedures vary across states and how to best assist those states. The Committee determined DHS's work to bolster states' cybersecurity has likely been effective but believes more needs to be done to coordinate efforts.

- Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure. Cybersecurity for electoral infrastructure at the state and local level was sorely lacking in 2016. Despite increased focus over the last three years, some of these vulnerabilities, including aging voting equipment, remain. As states look to replace machines that are now out of date, they should purchase more secure voting machines. At a minimum, any machine purchased going forward should have a voter-verified paper trail.
- Congress should evaluate the results of the $380 million in state election security grants allocated in 2018. States should be able to use grant funds provided under the Help America Vote Act (HAVA) to improve cybersecurity in a variety of ways, including hiring additional IT staff, updating software, and contracting vendors to provide cybersecurity services. When those funds are spent, Congress should evaluate the results and consider an additional appropriation to address remaining insecure voting machines and systems.
- DHS and other federal government entities remain respectful of the limits of federal involvement in state election systems. America's decentralized election system can be a strength against cybersecurity threats. However, the federal government and states should each be aware of their own cybersecurity limitations and know both how and when to obtain assistance. States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.
- The United States must create effective deterrence. The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act and respond accordingly. The U.S. government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator.

###

Senate Intel Committee Releases Bipartisan Report on Russia's Use of Social Media

Press Contact: Caitlin Carroll (Burr) (202) 228-1616

Rachel Cohen (Warner) (202) 228-6884

Tuesday, October 08, 2019

The second volume in the Committee's bipartisan Russia investigation outlines Russia's efforts to sow discord during 2016 U.S. presidential election

WASHINGTON, D.C. – Today, Senate Select Committee on Intelligence Chairman Richard Burr (R-NC) and Vice Chairman Mark Warner (D-VA) released a new report titled, "*Russia's Use of Social Media* ." It is the second volume released in the Committee's bipartisan investigation into Russia's attempts to interfere with the 2016 U.S. election.

The new report examines Russia's efforts to use social media to sow societal discord and influence the outcome of the 2016 election, led by the Kremlin-backed Internet Research Agency (IRA). The analysis draws on data provided to the Committee by social media companies and input from a Technical Advisory Group comprising experts in social media network analysis, disinformation campaigns, and the technical analysis of complex data sets and images to discern the dissemination of disinformation across social media platforms.

Statement from Chairman Burr:

"Russia is waging an information warfare campaign against the U.S. that didn't start and didn't end with the 2016 election. Their goal is broader: to sow societal discord and erode public confidence in the machinery of government. By flooding social media with false reports, conspiracy theories, and trolls, and by exploiting existing divisions, Russia is trying to breed distrust of our democratic institutions and our fellow Americans. While Russia may have been the first to hone the modern disinformation tactics outlined in this report, other adversaries, including China, North Korea, and Iran, are following suit.

"Any solution has to balance America's national security interests with our constitutionally-protected right to free speech. Social media companies, federal agencies, law enforcement, and Congress must work together to address these challenges, and I am grateful for the cooperation our Committee has gotten from both the Intelligence Community and the tech industry. My hope is that by continuing to shine a light on this issue, we will encourage more Americans to use social media responsibly, as discerning and informed consumers."

Statement from Vice Chairman Warner:

"The bipartisan work that this Committee has done to uncover and detail the extent of that effort has significantly advanced the public's understanding of how, in 2016, Russia took advantage of our openness and innovation, exploiting American-bred social media platforms to spread disinformation, divide the public, and undermine our democracy. Now, with the 2020 elections on the horizon, there's no doubt that bad actors will continue to try to weaponize the scale and reach of social media platforms to erode public confidence and foster chaos. The Russian playbook is out in the open for other foreign and domestic adversaries to expand upon – and their techniques will only get more sophisticated.

"As was made clear in 2016, we cannot expect social media companies to take adequate precautions on their own. Congress must step up and establish guardrails to protect the integrity of our democracy. At minimum, we need to demand transparency around social media to prevent our adversaries from hiding in its shadows. We also need to give Americans more control over their data and how it's used, and make sure that they know who's really bankrolling the political ads coming across their screens. Additionally, we need to take measures to guarantee that companies are identifying inauthentic user accounts and pages, and appropriately handling defamatory or synthetic content. It's our responsibility to listen to the warnings of our Intelligence Community and take steps to prevent future attacks from being waged on our own social media platforms."

The Committee has held five open hearings on Russia's use of social media, including a September 2018 open hearing with Facebook's Chief Operating Officer Sheryl Sandberg and Twitter's Chief Executive Officer Jack Dorsey. In December 2018, the Committee released two independent analyses of IRA activity, produced by New Knowledge and Graphika and the University of Oxford .

The Committee released the first volume of its Russia investigation in July 2019. You can read, "*Volume I: Russian Efforts Against Election Infrastructure*," here .

You can read, "*Volume II: Russia's Use of Social Media,*" here .

Key Findings and Recommendations:

- The Committee found that the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin. The Committee found that IRA social media

activity was overtly and almost invariably supportive of then-candidate Trump to the detriment of Secretary Clinton's campaign.

- The Internet Research Agency's (IRA) targeting of the 2016 U.S. election was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society. While the IRA exploited election-related content, the majority of its operations focused on exacerbating existing tensions on socially divisive issues, including race, immigration, and Second Amendment rights.
- The Committee found the IRA targeted African-Americans more than any other group or demographic. Through individual posts, location targeting, Facebook pages, Instagram accounts, and Twitter trends, the IRA focused much of its efforts on stoking divisions around hot-button issues with racial undertones.
- The IRA engaged with unwitting Americans to further its reach beyond the digital realm and into real-world activities. For example, IRA operatives targeting African-Americans convinced individuals to sign petitions, share personal information, and teach self-defense courses. Posing as U.S. political activists, operatives sought help from the Trump Campaign to procure campaign materials and to organize and promote rallies.
- The Committee found IRA activity increased, rather than decreased, after Election Day 2016. Analysis of IRA-associated accounts shows a significant spike in activity after the election, increasing across Instagram (238 percent), Facebook (59 percent), Twitter (52 percent), and YouTube (84 percent). Researchers continue to uncover IRA-associated accounts that spread malicious content.
- The Committee recommends social media companies work to facilitate greater information sharing between the public and private sector. Because information warfare campaigns are waged across a variety of platforms, communication between individual companies, government authorities, and law enforcement is essential for fully assessing and responding to them. Additionally, social media companies do not consistently provide a notification or guidance to users who have been exposed to inauthentic accounts.
- The Committee recommends Congress consider ways to facilitate productive coordination and cooperation between social media companies and relevant government agencies. Congress should consider whether any existing laws may hinder cooperation and whether information sharing should be formalized. The Committee also recommends Congress consider legislation to ensure Americans know the source behind online political advertisements, similar to existing requirements for television, radio, and satellite ads.
- The Committee recommends the Executive Branch publicly reinforce the danger of attempted foreign interference in the 2020 election. The Executive Branch should establish an interagency task force to monitor foreign nations' use of social media

platforms for democratic interference and develop a deterrence framework. A public initiative to increase media literacy and a public service announcement (PSA) campaign could also help inform voters.

- The Committee recommends candidates, campaigns, and other public figures scrutinize sourcing before sharing or promoting new content within their social media network. All Americans should approach social media responsibly to prevent giving “greater reach to those who seek to do our country harm.” The Committee recommends that media organizations establish clear guidelines for using social media accounts as sources to prevent the spread of state-sponsored disinformation.

Senate Intel Releases Bipartisan Report on Obama Admin Response to Russian Election Interference

Press Contact: Caitlin Carroll (Burr) (202) 228-1616

Rachel Cohen (Warner) (202) 228-6884

Thursday, February 06, 2020

WASHINGTON – Senate Select Committee on Intelligence Chairman Richard Burr (R-NC) and Vice Chairman Mark Warner (D-VA) today released the third volume in the Committee's bipartisan investigation into Russian election interference, "*U.S. Government Response to Russian Activities* ." The report examines the Obama Administration's reaction to initial reports of election interference and the steps officials took or did not take to deter Russia's activities.

Today's installment is the third of five volumes in the Committee's bipartisan investigation. The first volume, "*Russian Efforts Against Election Infrastructure* " was released in July 2019. The second, "*Russia's Use of Social Media* ," was released in September 2019. The two remaining installments will examine the 2017 Intelligence Community Assessment (ICA) on Russian interference and the Committee's final counterintelligence findings.

Statement from Chairman Burr:

"After discovering the existence, if not the full scope, of Russia's election interference efforts in late-2016, the Obama Administration struggled to determine the appropriate response. Frozen by 'paralysis of analysis,' hamstrung by constraints both real and perceived, Obama officials debated courses of action without truly taking one. Many of their concerns were understandable, including the fear that warning the public of the election threat would only alarm the American people and accomplish Russia's goal of undermining faith in our democratic institutions. In navigating those valid concerns, however, Obama officials made decisions that limited their options, including preventing internal information-sharing and siloing cyber and geopolitical threats.

"Thankfully, as we approach the 2020 presidential election we are in a better position to identify foreign interference efforts and address vulnerabilities Russia and other hostile foreign actors may seek to exploit. We must continue building on the lessons of 2016, including making sure we have strong response options at the ready. I hope this Committee's bipartisan report will help further the public's understanding of the threats we face and the current Administration's ability to respond to them."

Statement from Vice Chairman Warner:

"The 2016 Russian interference in our elections on behalf of Donald Trump was unprecedented in the history of our nation. This volume tries to describe how the Obama Administration grappled with this challenge as they began to learn the scope of the Russian assault on our democracy. I hope that the lessons we captured in this report will resonate with lawmakers, national security experts and the American public so that we might be better able to fight off future attacks.

"There were many flaws with the U.S. response to the 2016 attack, but it's worth noting that many of those were due to problems with our own system – problems that can and should be corrected. I am particularly concerned however, that a legitimate fear raised by the Obama Administration – that warning the public of the Russian attack could backfire politically – is still present in our hyper-partisan environment. All Americans, particularly those of us in government and public office, must work together to push back on foreign interference in our elections without regard for partisan advantage."

You can read "*Volume III: U.S. Government Response to Russian Activities*" **here** .

Key Findings and Recommendations:

- **The Committee found the U.S. government was not well-postured to counter Russian election interference activity with a full range of readily-available policy options.** While high-level warnings were delivered to Russian officials, those warnings may or may not have tempered Moscow's activity, and Russia continued disseminating stolen emails, conducting social media-based influence operations, and working to access state voting infrastructure through Election Day 2016.

- **The Committee found that the Obama Administration was constrained in its response by a number of external and internal concerns.** Those factors included the highly politicized environment, concern that public warnings would themselves undermine confidence in the election, and a delay in definitive attribution to Russia, among other issues.

- **The Committee found that the Obama Administration treated cyber and geopolitical aspects of the Russian active measures campaign as separate issues.** This bifurcated approach may have prevented the Administration from understanding the full extent of the threat Russia posed, limiting its ability to respond.

- **The Committee found that the decision to limit and delay information sharing about the foreign influence threat inadvertently constrained the Obama Administration's ability to respond.**

- **The Committee recommends the U.S. exert its leadership in creating international cyber norms.** The rules of cyber engagement are being written by hostile foreign actors, including Russia and China. U.S. leadership is necessary to establish any formalized international agreement on acceptable uses of cyber capabilities.

- **The Committee recommends the Executive Branch prepare for future attacks on U.S. elections.** Preparations should include the development of a range of standing options that can be rapidly executed in the event of a foreign influence campaign, as well as regular, apolitical threat assessments from the Director of National Intelligence. *The Intelligence Authorization Act* covering FY2020, which was passed last year, requires DNI to provide such assessments before regularly scheduled elections.

- **The Committee recommends an integrated response to cyber events.** Rather than treating cyber as an isolated domain separate from other geopolitical considerations, current and future Administrations should view cyber as an integral part of the foreign policy landscape.

- **The Committee recommends increased information sharing on foreign influence efforts, both within government and publicly.** Credible information should be shared as broadly as appropriate within the federal government, including Congress, while still protecting intelligence sources and methods. Information should also be shared with relevant private sector partners and state and local authorities. In the event that an active measures campaign is detected, the public should be informed as soon as possible with a clear and succinct statement of the threat.

###

Senate Intel Releases New Report on Intel Community Assessment of Russian Interference

Press Contact: Caitlin Carroll (Burr) (202) 228-1616

Rachel Cohen (Warner) (202) 228-6884

Tuesday, April 21, 2020

WASHINGTON – Today, Senate Select Committee on Intelligence Chairman Richard Burr (R-NC) and Vice Chairman Mark Warner (D-VA) released a new report, titled "*Review of the Intelligence Community Assessment*," the fourth and penultimate volume in the Committee's bipartisan Russia investigation.

The latest installment examines the sources, tradecraft, and analytic work behind the 2017 Intelligence Community Assessment (ICA) that determined Russia conducted an unprecedented, multi-faceted campaign to interfere with the 2016 U.S. presidential election. The installment builds upon the Committee's unclassified summary findings on the ICA issued in July 2018.

The ICA is informed by highly sensitive sources. In its review of that information, the Committee sought to protect the methods and means by which the U.S. Intelligence Community secured this information. In order to protect sources and methods, the vast majority of this chapter is redacted.

To date, the Committee has released four out of a total of five volumes in its comprehensive report on Russia's 2016 election interference. The previously released volumes examined U.S. election security, Russia's use of social media, and the Obama Administration's response to Russian interference. The fifth and final volume will examine the Committee's counterintelligence findings.

Statement from Chairman Burr:

"In reviewing the ICA, the Senate Intelligence Committee looked at two key questions: first, did the final product meet the initial task given by the President, and second, was the analysis supported by the intelligence presented? We found the ICA met both criteria. The ICA reflects strong tradecraft, sound analytical reasoning, and proper justification of disagreement in the one analytical line where it occurred.

"The Committee found no reason to dispute the Intelligence Community's conclusions.

"One of the ICA's most important conclusions was that Russia's aggressive interference efforts should be considered 'the new normal.' That warning has been borne out by the events of the last three years, as Russia and its imitators increasingly use information warfare to sow societal chaos and discord. With the 2020 presidential election approaching, it's more important than ever that we remain vigilant against the threat of interference from hostile foreign actors."

Statement from Vice Chairman Warner:

"The ICA summarizing intelligence concerning the 2016 election represented the kind of unbiased and professional work we expect and require from the Intelligence Community. The ICA correctly found the Russians interfered in our 2016 election to hurt Secretary Clinton and help the candidacy of Donald Trump. Our review of the highly classified ICA and underlying intelligence found that this and other conclusions were well-supported. There is certainly no reason to doubt that the Russians' success in 2016 is leading them to try again in 2020, and we must not be caught unprepared."

You can read, "*Volume IV: Review of Intelligence Community Assessment*" **here** .

Key Findings:

- **The Committee finds the Intelligence Community Assessment (ICA) presents a coherent and well-constructed intelligence basis for the case that Russia engaged in an attempt to interfere with the 2016 U.S. presidential election.** The Committee concludes that all analytic lines are supported with all-source intelligence, that the ICA reflects proper analytic tradecraft, and that differing levels of confidence on one analytic judgment are justified and properly represented. Additionally, interviews with those who drafted and prepared the ICA affirmed that analysts were under no political pressure to reach specific conclusions.

- **The Committee finds that the ICA reflects a proper representation of the intelligence collected and that this body of evidence supports the substance and body of the ICA.** While the Intelligence Community did not include information provided by Christopher Steele in the body of the ICA or to support any of its analytical judgments, it did include a summary of this material in an annex —largely at the insistence of FBI's senior leadership. A broader discussion of the Steele dossier will be included in the final volume of the Committee's report.

- **The Committee finds that the ICA makes a clear argument that the manner and aggressiveness of Russia's election interference was unprecedented.** However, the ICA does not include substantial representation of Russia's interference attempts in 2008 and 2012.

- **The Committee finds that the ICA did not include a set of policy recommendations for responding to Russia's interference attempts.** This omission was deliberate, reflecting the well-established norm that the role of the Intelligence Community is to provide insight and warning to policy makers, not to make policy itself.

- **The Committee finds the ICA would have benefited from a more comprehensive look at the role of Russian propaganda generated by state-owned platforms in the multi-pronged interference campaign.** Open source reporting on RT's and Sputnik's coverage of Wikileaks' release of information from the Democratic National Committee would have strengthened the ICA's examination of Russia's use of propaganda.

Read the Senate Intelligence Committee's previous reports:

"Volume I: Russian Efforts Against Election Infrastructure"

"Volume II: Russia's Use of Social Media"

"Volume III: U.S. Government Response to Russian Activities"

"Volume IV: Review of the Intelligence Community Assessment"

###

Senate Intel Releases Volume 5 of Bipartisan Russia Report

Press Contact: Dan Holler (Rubio), Nick Iacovella (Rubio) 202-224-3041

Tuesday, August 18, 2020

Miami, FL — U.S. Senate Select Committee on Intelligence Acting Chairman Marco Rubio (R-FL) and Vice Chairman Mark Warner (D-VA) released the fifth and final volume of the Committee's bipartisan Russia investigation titled, *"Volume 5: Counterintelligence Threats and Vulnerabilities ,"* which examines Russia's attempts to gain influence in the American political system during the 2016 elections.

The Committee's investigation totaled more than three years of investigative activity, more than 200 witness interviews, and more than a million pages of reviewed documents. All five volumes total more than 1300 pages.

You can read *"Volume 5: Counterintelligence Threats and Vulnerabilities"* here .

Read the Senate Intelligence Committee's previous reports :

- *"Volume I: Russian Efforts Against Election Infrastructure "*
- *"Volume II: Russia's Use of Social Media "*
- *"Volume III: U.S. Government Response to Russian Activities "*
- *"Volume IV: Review of the Intelligence Community Assessment "*
- Additional declassifications of *"Volume IV: Review of Intelligence Community Assessment"*

###

Rubio Statement on Senate Intel Release of Volume 5 of Bipartisan Russia Report

Press Contact: Dan Holler (Rubio), Nick Iacovella (Rubio) 202-224-3041

Tuesday, August 18, 2020

Miami, FL — U.S. Senate Select Committee on Intelligence Acting Chairman Marco Rubio (R-FL) and Vice Chairman Mark Warner (D-VA) released the fifth and final volume of the Committee's bipartisan Russia investigation titled, *"Volume 5: Counterintelligence Threats and Vulnerabilities ,"* which examines Russia's attempts to gain influence in the American political system during the 2016 elections.

Rubio released the following statement and a video message , which is available for download here :

"Over the last three years, the Senate Intelligence Committee conducted a bipartisan and thorough investigation into Russian efforts to influence the 2016 election and undermine our democracy. We interviewed over 200 witnesses and reviewed over one million pages of documents. No probe into this matter has been more exhaustive.

"We can say, without any hesitation, that the Committee found absolutely no evidence that then-candidate Donald Trump or his campaign colluded with the Russian government to meddle in the 2016 election.

"What the Committee did find however is very troubling. We found irrefutable evidence of Russian meddling. And we discovered deeply troubling actions taken by the Federal Bureau of Investigation, particularly their acceptance and willingness to rely on the 'Steele Dossier' without verifying its methodology or sourcing.

"Now, as we head towards the 2020 elections, China and Iran have joined Russia in attempts to disrupt our democracy, exacerbate societal divisions, and sow doubts about the legitimacy and integrity of our institutions, our electoral process and our republic.

"We must do better in 2020. The Committee's five reports detail the signs and symptoms of that interference and show us how to protect campaigns, state and local entities, our public discourse, and our democratic institutions. I join with Vice Chairman Warner in urging everyone — our colleagues, those in the Administration, state and local elections officials, the media, and the American public — to read them and take the recommendations seriously."

You can read *"Volume 5: Counterintelligence Threats and Vulnerabilities"* here .

Key Findings:

- The Committee found that the Russian government engaged in an aggressive, multi-faceted effort to influence, or attempt to influence, the outcome of the 2016 presidential election.

- WikiLeaks actively sought, and played, a key role in the Russian influence campaign and very likely knew it was assisting a Russian intelligence influence effort.

- The FBI gave the Steele Dossier unjustified credence, based on an incomplete understanding of Steele's past reporting record. The FBI used the dossier in a FISA application and renewals, and advocated for it to be included in the Intelligence Community Assessment before taking the necessary steps to validate assumptions about Steele's credibility.

- The FBI lacked a formal or considered process for escalating their warnings about the Democratic National Committee (DNC) hack within the organization of the DNC.

- The Committee assesses that at least two participants in a June 9, 2016, meeting with Trump Campaign officials, Natalia Veselnitskaya and Rinat Akhmetshin, have significant connections to the Russian government, including the Russian intelligence services. The Committee, however, found no reliable evidence that information of benefit to the Campaign was transmitted at the meeting, or that then-candidate Trump had foreknowledge of the meeting.

- The Committee found no evidence that anyone associated with the Trump Campaign had any substantive private conversations with Russian Ambassador Sergey Kislyak during the April 27, 2016, Trump speech held at the Mayflower Hotel.

- Paul Manafort's presence on the Trump Campaign and proximity to then-Candidate Trump created opportunities for Russian intelligence services to exert influence over, and acquire confidential information on, the Trump Campaign.

- George Papadopoulos was not a witting cooptee of the Russian intelligence services, but nonetheless presented a prime intelligence target and potential vector for malign Russian influence.

- Russia took advantage of members of the Transition Team's relative inexperience in government, opposition to Obama Administration policies, and Trump's desire to deepen ties with Russia to pursue unofficial channels through which Russia could conduct diplomacy.

Read the Senate Intelligence Committee's previous reports :

- *"Volume I: Russian Efforts Against Election Infrastructure "*
- *"Volume II: Russia's Use of Social Media "*
- *"Volume III: U.S. Government Response to Russian Activities "*
- *"Volume IV: Review of the Intelligence Community Assessment "*
- Additional declassifications of *"Volume IV: Review of Intelligence Community Assessment"*

###

Statement of Senate Intel Vice Chair Sen. Mark R. Warner

Press Contact: Rachel Cohen (Warner) 202 306 3278

Tuesday, August 18, 2020

~ On the release of Volume 5 of Senate Intelligence Committee's bipartisan Russia report ~

WASHINGTON – U.S. Sen. Mark R. Warner (D-VA), Vice Chairman of the Senate Select Committee on Intelligence, released the below statement on the release of the fifth and final volume of the Committee's bipartisan Russia investigation titled, "*Volume 5: Counterintelligence Threats and Vulnerabilities*":

"After more than three and a half years of work, millions of documents, and hundreds of witness interviews, I'm proud that the Committee's report speaks for itself.

"At nearly 1,000 pages, Volume 5 stands as the most comprehensive examination of ties between Russia and the 2016 Trump campaign to date – a breathtaking level of contacts between Trump officials and Russian government operatives that is a very real counterintelligence threat to our elections. I encourage all Americans to carefully review the documented evidence of the unprecedented and massive intervention campaign waged on behalf of then-candidate Donald Trump by Russians and their operatives and to reach their own independent conclusions.

"This cannot happen again. As we head into the heat of the 2020 campaign season, I strongly urge campaigns, the executive branch, Congress and the American people to heed the lessons of this report in order to protect our democracy."

###