THE ROAD TO 2020: DEFENDING AGAINST ELECTION INTERFERENCE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

NOVEMBER 19, 2019

Serial No. 116–51

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

40–467 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

CEDRIC L. RICHMOND, Louisiana, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KATHLEEN M. RICE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
BENNIE G. THOMPSON, Mississippi *(ex officio)*

JOHN KATKO, New York, *Ranking Member*
MARK WALKER, North Carolina
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
MIKE ROGERS, Alabama *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
SARAH MOXLEY, *Minority Subcommittee Staff Director*

CONTENTS

THE ROAD TO 2020: DEFENDING AGAINST ELECTION INTERFERENCE

Tuesday, November 19, 2019

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:14 p.m., in room 310, Cannon House Office Building, Hon. Cedric L. Richmond (Chairman of the subcommittee) presiding.

Present: Representatives Richmond, Rice, Slotkin, Thompson; Katko, Walker, Taylor, and Joyce.

Mr. RICHMOND. The Committee on Cybersecurity, Infrastructure Protection, and Innovation will come to order. The subcommittee is meeting today to receive testimony on election security in a hearing titled, "The Road to 2020: Defending Against Election Interference."

Good afternoon. I want to welcome the witnesses to today's hearing on how we can secure the 2020 election against outside interference. Today we will take a broad look at election security issues, including efforts from the private sector to protect election infrastructure and political campaigns against malicious actors.

This threat is real, and it is personal. Yesterday it was reported that my State of Louisiana was the victim of a ransomware attack. The attack happened while the Secretary of State was awaiting certification of the recent election. While State officials activated the State's cybersecurity team in response to the attack, this incident highlights the exact scenario this committee is trying to prevent in the 2020 election.

It is an undisputable fact that in 2016 the Russian Government carried out a concerted, sophisticated operation to meddle in our Presidential election. The Kremlin leveraged sophisticated cyber capabilities to target our election infrastructure and amplify divisive, and at times, false rhetoric in an unprecedented way to sow discord, undermine the public's faith in democratic institutions, and ultimately damage the global leadership of the United States.

The Russian government's covert and malicious foreign interference campaign attacked every aspect of our elections. It involved engaging in conversations with personnel from a U.S. Presidential campaign, hacking a National political committee, conducting a phishing attack against a campaign chairman, targeting voter registration databases and other election infrastructure, and mobi-

lizing bots and fake on-line personas to carry out influence operations.

Today 2 other nation-state actors, China and Iran, are following suit, weaponizing new technologies to disrupt our democracy, distort the daily news, and compromise our election security.

As we move into the heart of the 2020 election cycle, we must set aside party politics and work together to improve election security and preserve the integrity of our democracy. To that end, I urge the White House to accept the intelligence community's unanimous conclusions about 2016 meddling, refrain from engaging in conspiracy theories ahead of the 2020 elections and show some needed leadership on election security. Failing to do so will further erode public confidence in our election process, and advance Vladimir Putin's goal of undermining the U.S.-led liberal democratic order.

For its part, Senate leadership must pass House-passed measures that would make election infrastructure more secure, and it should match the House's commitment to funding election security grants. Security vulnerabilities and an outdated, unsupported election infrastructure could jeopardize the accuracy of voter registration databases, or even the tally of votes cast. That is simply unacceptable. Voters deserve to know that they will be able to vote when they show up, and that their vote will be counted accurately.

To guard against covert, malicious, foreign influence campaigns, owners and operators of on-line platforms must understand and be candid with the public about how our adversaries use their platforms. Also, we need to educate the public so that they are informed and have the opportunity to distinguish between facts and disinformation. And our party organizations and campaigns must take cybersecurity seriously, monitor for disinformation, and refuse to take advantage of malicious disinformation circulated about their opponents.

Party and campaign organizations have tremendous power to counter efforts by foreign adversaries, simply by rejecting opportunities to take the cheap shots based on fake news. Together, those truly interested in defending our elections from foreign adversaries can make a real difference.

For example, despite a lack of leadership from the White House, the Department of Homeland Security is building relationships and providing a full suite of election security services to State and local election officials.

In addition, the Office of the Director of National Intelligence, Federal Bureau of Investigation, National Security Agency, and U.S. Cyber Command have teams to coordinate and integrate election security threat information.

The private sector is also stepping up. Cybersecurity researchers at non-profit and for-profit organizations are providing cybersecurity services to campaigns and election officials. I commend these efforts.

I look forward to hearing more from our distinguished panel on their efforts and yield back the balance of my time.

[The statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC L. RICHMOND

Today, we will take a broad look at election security issues, including efforts from the private sector to protect election infrastructure and political campaigns against malicious actors. It is an undisputable fact that, in 2016, the Russian government carried out a concerted, sophisticated operation to meddle in our Presidential election. The Kremlin leveraged sophisticated cyber capabilities to target our election infrastructure and amplify divisive—and at times false—rhetoric in an unprecedented way to sow discord, undermine the public's faith in democratic institutions, and ultimately damage the global leadership of the United States. The Russian government's covert malicious foreign interference campaign attacked every aspect of our elections.

It involved engaging in conversations with personnel from a U.S. Presidential campaign, hacking a National political committee, conducting a phishing attack against a campaign Chairman, targeting voter registration databases and other election infrastructure, and mobilizing bots and fake on-line personas to carry out influence operations. Today, 2 other nation-state actors, China and Iran, are following suit—weaponizing new technologies to disrupt our democracy, distort the daily news, and compromise our election security. As we move into the heart of the 2020 election cycle, we must set aside party politics and work together to improve election security and preserve the integrity of our democracy.

To that end, I urge the White House to accept the intelligence community's unanimous conclusions about 2016 meddling, refrain from engaging in conspiracy theories ahead of the 2020 elections, and show some needed leadership on election security. Failing to do so will further erode public confidence in our election process and advance Vladimir Putin's goal of undermining the U.S.-led liberal democratic order. For its part, Senate leadership must pass House-passed measures that would make election infrastructure more secure, and it should match the House's commitment to funding election security grants. Security vulnerabilities in outdated, unsupported election infrastructure could jeopardize the accuracy of voter registration databases or even the tally of votes cast. That is simply unacceptable.

Voters deserve to know that they will be able to vote when they show up, and that their vote will be counted accurately. To guard against covert malicious foreign influence campaigns, owners and operators of on-line platforms must understand and be candid with the public about how our adversaries use their platforms. Also, we need to educate the public so that they are informed and have the opportunity to distinguish between facts and disinformation. And our party organizations and campaigns must take cybersecurity seriously, monitor for disinformation, and refuse to take advantage of malicious disinformation circulated about their opponents. Party and campaign organizations have tremendous power to counter efforts by foreign adversaries simply by rejecting opportunities to take the cheap shots based on fake news.

Together, those truly interested in defending our elections from foreign adversaries can make real progress. For example, despite a lack of leadership from the White House, the Department of Homeland Security is building relationships and providing a full suite of election security services to State and local election officials. In addition, Office of the Director of National Intelligence, Federal Bureau of Investigation, National Security Agency, and U.S. Cyber Command have teams to coordinate and integrate election security threat information. The private sector is also stepping up. Cybersecurity researchers at non-profit and for-profit organizations are providing cybersecurity services to campaigns and election officials. I commend these efforts. I look forward to hearing more from our distinguished panel on their efforts.

Mr. RICHMOND. With that I now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Katko, for an opening statement.

Mr. KATKO. Thank you, Mr. Chairman. Thank you all for being here this afternoon on this very, very important topic.

Securing our elections remains one of the most pressing issues our country faces today. Secure voting systems and the accurate reporting of votes is foundational to our democracy. Americans should have full confidence in every aspect of our election process.

Unfortunately, our election systems have become the principal target of several adversaries. Disinformation campaigns engineered by Russia have sown political discord within our election process.

Social media has become a haven for false information regarding Election Day procedures and misinformation of candidates. Disinformation campaigns serve to confuse voters and undermine their confidence in the electoral process.

While foreign influence has had a measured effect on our discourse, election results have, fortunately, remained untouched. The success of the 2018 midterms demonstrated the progress that the Federal Government and our State and local partners have made together. I want to applaud election security efforts led by CISA and the partnerships with State and local governments that have resulted in a marked improvement of information sharing and cohesion.

Additionally, growing participation within the election infrastructure ISAC by local election officials has provided thousands of election offices with the cyber resources they need to maintain the reliability of their election infrastructure. Paper trails for voting systems are now in use in all but a few States, providing voters with a tangible, incorruptible record of their vote.

The continued development of auditing techniques confirms voting results where voter tallies may be called into question. These software independent techniques have become invaluable to protecting our election systems from cyber attacks. Software independence of our election infrastructure is absolutely essential for the integrity of our election systems.

This progress does not mean our election systems are secure. In my district we have seen multiple ransomware attacks affecting critical functions of the Syracuse City School District, for example, and the Onondaga County Library system. One can only imagine the effect of a similar targeted ransomware campaign aimed at voter registration databases before an election. Such an attack would hijack our election process and undermine all voter confidence in election results.

Furthermore, we must continue to develop our relationships with State and local partners to ensure Federal cybersecurity resources are being utilized. While participation in the alleged election infrastructure ISAC has improved since the 2016 elections, thousands of local election offices remain independent. Local election offices are not equipped to handle the cyber threats to their election infrastructure alone. It is imperative that the Federal Government makes available its cybersecurity resources to every local election office.

Election security has a history of bipartisan cooperation and support. Ensuring that our election process is uncompromised must remain a top priority for both sides of the aisle. I am confident that we can take the necessary and reasonable steps to continue to improve the integrity of our election systems.

I thank the witnesses for providing the committee with their testimony and look forward to hearing their ideas on how we can further improve the security of our election systems.

General Taylor, I must say it is nice to see you again, sir.

I want to thank all of you, and Chairman Richmond, and everyone here today for calling this important hearing. I yield back the balance my time.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

NOV. 19, 2019

Thank you, Mr. Chairman.

Securing our elections remains one of the most pressing issues our country faces. Secure voting systems and the accurate reporting of votes is foundational to our democracy. Americans should have full confidence in every aspect of our election process.

Unfortunately, our election systems have also become the principal target of several adversaries.

Disinformation campaigns engineered by Russia have sown political discord within our election process. Social media has become a haven for false information regarding election day procedures and misinformation of candidates. Disinformation campaigns serve to confuse voters and undermine their confidence in the electoral process.

While foreign influence has had a measured effect on our discourse, election results have fortunately remained untouched. The success of the 2018 midterms demonstrated the progress that the Federal Government and our State and local partners have made. I want to applaud election security efforts led by CISA and their partnerships with State and local governments that have resulted in a marked improvement of information sharing and cohesion. Additionally, growing participation within the Election Infrastructure ISAC by local election officials has provided thousands of election offices with the cyber resources they need to maintain the reliability of their election infrastructure.

Paper trails for voting systems are now in use in all but a few States, providing voters with an incorruptible record of their vote. The continued development of auditing techniques confirms voting results where voter tallies may be called into question. These software independent techniques have become invaluable to protecting our election systems from cyber attacks. Software independence of our election infrastructure is essential for the integrity of our election systems.

This progress does not mean our election systems are secure. In my district, we have seen multiple ransomware attacks affecting critical functions of the Syracuse City School District and Onondaga County Library System. One can imagine the effect of a similar targeted ransomware campaign aimed at voter registration database systems before an election. Such an attack would hijack our election process and undermine all voter confidence in election results.

Furthermore, we must continue to develop our relationships with State and local election partners to ensure Federal cybersecurity resources are being utilized. While participation in the Election Infrastructure ISAC has improved since the 2016 elections, thousands of local election offices remain independent. Local election offices are not equipped to handle the cyber threats to their election infrastructure alone. It is imperative the Federal Government makes available its cybersecurity resources to every local election office.

Election security has a history of bipartisan cooperation and support. Ensuring that our election process is uncompromised must remain a top priority for both sides of the aisle. I am confident that we can take the necessary reasonable steps to continually improve our election systems.

I thank the witnesses for providing the committee with their testimony and I look forward to hearing their ideas on how we can further improve the security of our election systems.

I want to thank Chairman Richmond for calling this important hearing and I yield back.

Mr. THOMPSON [presiding]. Thank you very much. The Chair recognizes himself for 5 minutes for an opening statement.

Good afternoon to our panel of witnesses. Thank you very much for being here.

Since 2016 officials throughout the intelligence community have described in disturbing detail the many ways the Russian government sought to meddle in our elections. For the 3 years that followed, heads of the Department of Homeland Security, the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency, among others, have warned that the Russian government will continue its efforts to sow discord and undermine confidence in our democracy.

More disturbing yet, Russia is not alone. According to the 2019 World-wide Threat Assessment, other adversaries, including China and Iran, will pursue opportunities to interfere in our elections. The intelligence community assesses that adversaries could exploit cyber means to target election infrastructure or engage in targeted influence campaigns to manipulate public opinion.

We also know that our adversaries will target political campaigns because they have done so in the past. Adversaries have hardly kept their desire to undermine the integrity of our elections a secret.

As Members of Congress, we have a duty to act. Today we are less than 1 year away from the 2020 Presidential election. The question everyone on this dais must ask themselves, is have we done enough to secure the 2020 elections from our adversaries?

Despite multiple efforts led by the House of Representatives, Congress has yet to send a single piece of comprehensive election security legislation to the President's desk. Instead, good pieces of legislation to provide additional resources to State and local elections officials and limit foreign interference have stalled in the Senate.

Moreover, despite multiple requests, the White House has failed to identify an official to coordinate the election security activities at various Federal agencies. In the mean time, with just a handful of legislative days left this year, and only a limited amount of time for legislative action next year, I will be interested to learn from our witnesses how they recommend Congress use that time to improve election security in advance of the 2020 elections.

Importantly, I am interested to know how academics and private sector can work with State and local election officials and campaigns to improve election security in the absence of Congressional action. The election security problems we face are shared, and we have a shared responsibility to solve them.

State and local election authorities, with help from the Federal Government, must invest in IT departments, train their employees, and upgrade and certify their election equipment.

The private sector, including voting system vendors, must take responsibility to secure their equipment, make it user-friendly, and demonstrate a willingness to admit weakness in their systems when examined by third-party cyber professionals.

Political campaigns must step up, too. They must implement robust cybersecurity policies to deprive our adversaries of information that can be twisted into a divisive narrative and serve as an extra check on disinformation.

Finally, the American public must also be vigilant and scrutinize the information presented to them carefully.

Before I close, I would also like to note that November is Critical Infrastructure Security and Resilience Month. I can think of no better way to observe it than to assess our preparedness for the 2020 Presidential elections.

I also thank Chairman Richmond for his steadfast leadership on election security, and I look forward to the hearing and witnesses' testimony today.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

NOVEMBER 19, 2019

I'd like to thank Chairman Richmond for calling today's hearing on election security. Since 2016, officials throughout the intelligence community have described in disturbing detail the many ways the Russian government sought to meddle in our elections. For the 3 years that followed, heads of the Department of Homeland Security, the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency, among others, have warned that the Russian government will continue its efforts to sow discord and undermine confidence in our democracy. More disturbing yet, Russia is not alone. According to the 2019 Worldwide Threat Assessment, other adversaries, including China and Iran, will pursue opportunities to interfere in our elections. The intelligence community assesses that adversaries could exploit cyber means to target election infrastructure or engage in targeted influence campaigns to manipulate public opinion. We also know that our adversaries will target political campaigns because they have done so in the past. Our adversaries have hardly kept their desire to undermine the integrity of our elections a secret. As Members of Congress, we have a duty to act.

Today, we are less than 1 year away from the 2020 Presidential election. The question everyone on this dais must ask themselves is: "Have we done enough to secure the 2020 elections from our adversaries?" Despite multiple efforts led by the House of Representatives, Congress has yet to send a single piece of comprehensive election security legislation to the President's desk. Instead, good pieces of legislation to provide additional resources to State and local election officials and limit foreign interference have stalled in the Senate. Moreover, despite multiple requests, the White House has failed to identify an official to coordinate the election security activities at various Federal agencies. In the mean time, we have just a handful of legislative days left this year, and only a limited amount of time for legislative action next year. I will be interested to learn from our witnesses how they recommend Congress use that time to improve election security in advance of the 2020 elections.

Importantly, I will be interested to know how academics and the private sector can work with State and local elections officials and campaigns to improve election security in the absence of Congressional action. The election security problems we face are shared, and we have a shared responsibility to solve them. State and local election authorities—with help from the Federal Government—must invest in IT departments, train their employees, and upgrade and certify their election equipment. The private sector, including voting system vendors, must take responsibility to secure their equipment, make it user-friendly, and demonstrate a willingness to admit weaknesses in their systems when examined by third-party cybersecurity professionals. Political campaigns must step up, too. They must implement robust cybersecurity policies to deprive our adversaries of information that can be twisted into a divisive narrative and serve as an extra check on disinformation.

Finally, the American public must also be vigilant, and scrutinize the information presented to them carefully. Before I close, I would also like to note that November is Critical Infrastructure Security and Resilience Month. I can think of no better way to observe it than to assess our preparedness for the 2020 Presidential elections.

Chairman THOMPSON. Other Members of the subcommittee are reminded that, under committee rules, opening statements will be submitted for the record.

[The statement of Honorable Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

Chairman Richmond and Ranking Member Katko, thank you for convening today's hearing on "The Road to 2020: Defending Against Election Interference."

I thank today's witnesses:

Panel I

General Frank Taylor (Ret.-U.S. Air Force), former under secretary for intelligence and analysis, U.S. Department of Homeland Security; executive director (pro tempore), US CyberDome;

The Hon. Richard Stengel, former under secretary for public diplomacy and public affairs, U.S. State Department;

Dr. Matt Blaze, McDevitt chair of computer science and law, Georgetown University; and

Ms. Ginny Badanes, director, Strategic Projects, Defending Democracy Program, Microsoft (Minority Witness).

I thank each of today's witnesses for bringing their expert view on state of election security as the 2020 elections approach.

The efforts to ensure that every eligible person can register to vote, and cast a vote in a public election have spanned generations.

I have been persistent in my efforts to protect the rights of disenfranchised communities in my district of inner-city Houston and across the Nation.

Throughout my tenure in Congress, I have cosponsored dozens of bills, amendments, and resolutions seeking to improve voters' rights at all stages and levels of the election process.

This includes legislation aimed at:

1. Increasing voter outreach and turnout;
2. Ensuring both early and same-day registration;
3. Standardizing physical and language accessibility at polling places;
4. Expanding early voting periods;
5. Decreasing voter wait times;
6. Guaranteeing absentee ballots, especially for displaced citizens;
7. Modernizing voting technologies and strengthening our voter record systems;
8. Establishing the Federal Election Day as a National holiday; and
9. Condemning and criminalizing deceptive practices, voter intimidation, and other suppression tactics;

Along with many of my colleagues in the CBC, I was an original cosponsor of H.R. 9, the Fannie Lou Hamer, Rosa Parks, and Coretta Scott King Voting Rights Act Reauthorization and Amendments Act, which became public law on July 27, 2006.

I also authored H.R. 745 in the 110th Congress, which added the legendary Barbara Jordan to the list of civil rights trailblazers whose names honor the Voting Rights Act Reauthorization and Amendments Act.

This bill strengthened the original Voting Rights Act by replacing Federal voting examiners with Federal voting observers—a significant distinction that made it easier to safeguard against racially-biased voter suppression tactics.

In the 114th Congress, I introduced H.R. 75, the Coretta Scott King Mid-Decade Redistricting Prohibition Act of 2015, which would prohibit States whose Congressional districts have been redistricted after a decennial census from redrawing their district lines until the next census.

The voting rights struggles of the 20th Century are now joined by voting rights threats posed by the 21st Century.

Russia an adversary of the United States engaged in repeated attempts to interfere in the 2016 Presidential election, which prompted an unprecedented all-of-Government effort to alert local and State election administrators to be aware of the threat.

Russia targeted our Presidential election according to the report, "Background to Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution," provided by the Office of the Director of National Intelligence's National Intelligence Council.

Russia used every cyber espionage tool available to influence the outcome of the Presidential election by using a multifaceted campaign that included theft of data; strategically-timed release of stolen information; production of fake news; and manipulation of facts to avoid blame.

The Russian General Staff Main Intelligence Directorate (GRU) is suspected by our intelligence agencies of having begun cyber operations targeting the United States election as early as March 2016.

They took on the persona of "Guccifer 2.0," "DCLeaks.com," and Wikileaks as the identities that would be reported as having involvement in the work they had under taken to undermine our Nation's Presidential election.

Russia is blamed for breaching 21 local and State election systems, which they studied extensively.

In February 2018, special counsel Robert Mueller released indictments of 13 Russians, at least one of whom has direct ties to Russian President Vladimir Putin.

The 37-page indictment details the actions taken to interfere with the U.S. political system, including the 2016 US. Presidential election.

Among the charges, which include charges for obstruction of justice, are several especially notable details.

The indictment states that 13 defendants posed as U.S. persons and created false U.S. personas and operated social media pages and groups designed to attract U.S. audiences.

The Russians are not deterred by these indictments and are poised to interfere in the 2020 election.

Russian interference in the 2016 election was a "calculated and brazen assault" on our democracy.

In September 2019, Acting Director of National Intelligence Joseph Maguire told Congress that "the greatest challenge that we do have is to make sure that we maintain the integrity of our election system.

"We know right now that there are foreign powers, not just Russia, that are trying to get us to question the validity on whether or not . . . our elections are valid."

Last month, a senior CISA official renewed the agency's warnings about threats to the 2020 elections.

Unfortunately, these warnings are being met with no response from current President and those who support him.

The current matter under consideration by the House Intelligence Committee alleges that the current President sought the assistance of a foreign leader to meddle in the 2020 election.

The committee must prepare the Nation to address the pending Russia threat to our Nation's election system, while also preparing to defend against threats to our election system posed by other nations.

The United States has enemies in other corners of the globe who would not hesitate to attack our election system if given the chance.

These foreign adversaries do not share our commitment to democracy, liberty, and human rights, or the precious freedoms we hold dear.

On January 6, 2017, Homeland Security Secretary Johnson, as one of his last official acts under the Obama administration, designated election systems as critical infrastructure, and created a new subsector under the existing Government Facilities Sector designation.

On January 29, 2019, the director of national intelligence testified before the Senate Select Committee on Intelligence that our adversaries "probably already are looking to the 2020 U.S. elections as an opportunity to advance their interests.

The House Committee on Homeland Security has the responsibility of providing for the cybersecurity of Federal civilian agencies as well as the security of the Nation's 16 critical infrastructure sectors from cyber and other threats.

The Election Infrastructure Subsector covers a wide range of physical and electronic assets such as storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of State and local governments.

The work to secure our Nation's election system from cyber threats is on-going, which is why this hearing is relevant.

The U.S. Department of Homeland Security's (DHS) mission in cybersecurity and infrastructure protection is focused on enhancing greater collaboration on cybersecurity across the 16 critical infrastructure sectors and the sharing of cyber threat information between the private sector and Federal, State, and local partners.

This committee will work hand-and-glove with the House Judiciary and House Administration Committees as well as the Senate Committees to ensure that the tools applied to the current threat to our elections is effectively and adequately addressed.

We know the threats that computing devices and systems face, which are almost too numerous to count:

- Internet of things-enabled devices;
- Ransom-ware;
- Mal-ware;
- Denial of Service Attacks;
- Distributed-Denial-of-Service Attacks;
- Pharming;
- Phishing;
- Data Theft;
- Data Breaches;
- SQL Injection;
- Man-in-the-middle attack.

This hyper cyber-threat environment poses risks to election systems because of the nature of Federal elections.

Elections are date- and time-sensitive, which means any disruption or interruption can have catastrophic implications.

During the 2016 election we learned of new threats from cyber space that go far beyond any that would have been considered in previous elections.

This Congress is poised to do the hard work of delving into the issue of Russian involvement in our National election and providing solutions.

The work today must focus on election recovery should a serious cyber incident occur during an election.

Vulnerabilities of computing systems are not limited to intentional attacks, but can include acts of nature, human error, or technology failing to perform as intended.

I am particularly concerned that so many jurisdictions rely on electronic poll books, to check-in voters before issuing them ballots, with no paper backups.

Finally, the use of untrustworthy paperless electronic voting machines without enough paper ballot options will come to an end when H.R. 1 becomes law.

The right and better approach to election cybersecurity is to be prepared and not need options for voters to cast ballots should voting systems fail, rather than being unprepared and needing options for voters to cast ballots during an election that are not available.

We must be steadfast in our resolve to have a strong shield to defend civilian and critical infrastructure networks for all threats foreign and domestic.

I look forward to the testimony of today's witnesses.

Thank you.

Chairman THOMPSON. I welcome our panel of witnesses. First, I am pleased to welcome back General Frank Taylor, United States Air Force, retired. He is a former under secretary for intelligence and analysis, and—at the Department of Homeland Security, and a board member of the U.S. CyberDome, a non-profit organization which provides cybersecurity at no cost to political parties, elected officials, and candidates across party lines.

Next, we have Mr. Richard Stengel. He is a former under secretary of state for public diplomacy and public affairs, where he created and oversaw the Global Engagement Center.

Next, we have Dr. Matt Blaze. He holds the McDevitt chair of computer science and law at Georgetown University. He works—his work focuses on technology, encryption, and, most importantly, election security.

Finally, we have this Ms. Ginny Badanes. Close? OK. She is the director of strategic projects at Microsoft's Defending Democracy Program, where she leads a team that works with political campaigns to protect against hacking and defend against disinformation campaigns.

Without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with General Taylor.

STATEMENT OF FRANCIS X. TAYLOR, GENERAL, U.S. AIR FORCE, RETIRED, FORMER UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY, BOARD MEMBER, US CYBERDOME

General TAYLOR. Thank you, Chairman Thompson, Ranking Member Katko. It is a pleasure to appear before this committee, this time as the acting executive director of US CyberDome, a non-profit organization dedicated to helping to secure Federal campaigns against undue influence. Thank you for the opportunity to appear and to discuss defending our election infrastructure.

You—both you, Chairman Thompson, and Mr. Katko—have outlined what the threat was from 2016. That threat continues to manifest itself, so I will not speak further to that.

But as the executive director of US CyberDome, I have talked with many other organizations who are helping campaigns with cybersecurity and to protect against disinformation. I have been engaged with personnel in the National party committees, the Federal campaign committees, as well as personnel who have worked for these types of committees in the recent past. The observations of this testimony come from those dialogs, my professional experience, and the experiences of US CyberDome founders and advisors.

US CyberDome is a 501(c)(4) non-profit organization. Our objective is to ensure the integrity of elections and confidence in their outcomes. We operate in full alignment with the Federal Election Commission Advisory Opinion 201(a)–12, to fund qualified vendors using US CyberDome donations. Initial US CyberDome activities have focused on the 2020 U.S. Presidential and Senatorial campaigns, but over time will apply to other campaigns.

We broker no-cost cybersecurity and disinformation protection services from qualified vendors to Federal campaign committees, National party committees, think tanks, and non-Governmental organizations. Using this cybersecurity framework as a measure of comprehensive cyber risk management, we have identified services for a multi-phase improvement initiative.

Perhaps not every campaign will need every service. However, our objective is to increase the overall level of protection across the campaign infrastructure, both within campaigns and in the National parties and services they depend on, envision services—ones that have a high probability of success within the campaigns, offer low disruption—and will offer low disruption to campaign workers, and offer the highest impact, and address the most urgent threats.

Our intent is to start with detection and response services, to include impostor website monitoring, social media, and dark web monitoring. These services are allowed per current Federal Election Commission advisory opinions. These services will hold the line. These services will hold a line against malicious actors. In later phases of our initiative we intend to broker more proactive and protective services, such as perimeter security management, distributed denial of service, and ransomware mitigation services. These will be enabled by an FEC opinion request that we are now staffing.

US CyberDome is comprised of cybersecurity experts who have trained and practiced the world's—at the world's largest accredited computer forensic and incident response institute in the world, the Defense Cyber Crime Center, which I am proud to also say I started in 1997, as the commander of OSI, and it continues to grow.

A special note: US CyberDome believes our role is to help ensure U.S. political discourse is free from foreign influence, but not participate in or affect that discourse.

Just a couple of observations about campaigns. Our assessment is campaigns are underprepared. Their focus is on getting their candidate elected, and the investment that is required to protect against the more sophisticated threats that the campaigns and our election infrastructure face are much more expensive than campaigns can afford. Our focus is to provide the campaigns with free-of-charge services to protect themselves as they pursue the election process.

With that, Mr. Chairman, I will yield my time.
[The prepared statement of General Taylor follows:]

PREPARED STATEMENT OF FRANCIS X. TAYLOR

NOVEMBER 19, 2019

INTRODUCTION

Chairman Richmond, Ranking Member Katko, and Members of the subcommittee, I am Frank Taylor, the executive director of US CyberDome, a non-profit dedicated to securing Federal campaigns against undue influence. Thank you for the opportunity to appear before you today to discuss defending against election interference.

US CYBERDOME'S ROLE IN DEFENDING AGAINST ELECTION INTERFERENCE

US CyberDome is a 501(c)(4) non-profit organization. Our objective is to ensure the integrity of elections and confidence in their outcomes. We broker no-cost cybersecurity and disinformation detection services from qualified vendors to Federal campaign committees, National party committees, think tanks, and non-governmental organizations. Initial US CyberDome activities are focused on the 2020 U.S. Presidential and Senatorial campaigns, and will apply to other campaigns over time. We operate in full alignment with the Federal Election Commission's Advisory Opinion 2018–12 to fund qualified vendors using US CyberDome donations.

US CyberDome is comprised of cybersecurity experts who have trained and practiced at the world's largest accredited computer forensics and incident response institute in the world, the Defense Cyber Crime Center, as well as the U.S. Department of Defense and National Institute of Standards and Technology. The team was formed by a group of cybersecurity experts who became alarmed by increasing cyber threats and the lack of protection for campaigns and voters. They formed the non-profit organization to absorb the extraordinary cost of providing cyber protection to campaigns by working with donors and charitable foundations.

Of special note, US CyberDome believes our role is to help ensure U.S. political discourse is free of foreign interference, but not to participate in or affect that discourse. For that reason, we are non-partisan in our approach. Our Board of Advisors represents a variety of political parties and beliefs to ensure we are guided in a balanced way. Additionally, our services are designed to be delivered fairly and equitably, regardless of political party or beliefs.

POLITICAL CAMPAIGNS IN 2019

Our freedom of speech and democracy are under attack by increasingly sophisticated and ever-evolving threats to the election process, including purposeful attacks and exploits from foreign governments, terrorists, organized crime, foreign corporate spies, and others.

The 2016 U.S. Presidential elections demonstrated that cyber attacks and disinformation can be used to manipulate the U.S. election. As set forth in the Bob Mueller's Report on the Investigation into Russian Interference in the 2016 Presidential Election, "the Russian government interfered in the 2016 Presidential election in sweeping and systematic fashion." They did so principally through 2 operations. First, a Russian entity conducted a sophisticated social media campaign, and second, a Russian intelligence service conducted computer-intrusion operations against campaign entities, employees, and volunteers, and then released stolen documents. Successful and public foreign interference in 2016 increased the likelihood that other nations will seek to influence in 2020 and beyond.

Other factors will very likely increase interference in the U.S. 2020 Presidential election. For instance, as the United States increases trade pressures around the world, cyber attacks from affected nations have increased. These, and potentially other factors, will likely lead to increased attacks on 2020 U.S. Presidential campaigns, and Federal campaigns in general.

In summary, I offer the affirmation of one US CyberDome Advisor, former Secretary of the U.S. Department of Homeland Security, Michael Chertoff. "Malign foreign actors continue their efforts to attack our democracy, including through the online penetration and disruption of our candidate and campaign organizations."

Even more insidious, some nation-states are busy gathering information about U.S. Presidential candidates, Senators, and Representatives, that may be used at a moment in time that is advantageous to that nation in the future; potentially far beyond 2020.

Not even the Government can guarantee a 100 percent success rate against every attack or exploit from malicious nations or nation-states. However, we can greatly increase success rates through diligence in detecting adversary activity, and expediency in responding to and reporting that activity.

As executive director for US CyberDome, I have talked with many other organizations who are helping campaigns with cybersecurity and disinformation. Organizations such as Microsoft and Area 1 Security who have received positive Advisory Opinions from the FEC and are supporting campaigns. Organizations such as the DigiDems who offer on-site technical personnel to campaigns and currently have over 80 personnel embedded in those campaigns. I have been engaged with personnel in National party committees and Federal campaign committees, as well as personnel who have worked for those types of committees in the recent past. The observations of this testimony come from those dialogs, my professional experiences, and the experiences of the US CyberDome founders and Advisors.

OBSERVATIONS ABOUT CAMPAIGNS

Campaigns are under-prepared.—They are not adequately resourced to defend against many expert, persistent, and well-funded threat actors such as nation-states. Most campaigns do not have enough technical expertise or historical experience against the myriad threats they face. Simply put, if they have not previously detected and responded to sophisticated threat actors, they will not be able to. Even campaigns with a very knowledgeable cybersecurity professional on-staff are hindered. One person cannot hold off the Korean People's Army or the Armed Forces of the Islamic Republic of Iran.

There are very few workplaces in the United States where campaigns can find someone with past experience defending against a wide variety of nation-state cyber attacks or disinformation. The intelligence community and Department of Defense have groups of such individuals. Also, the Defense Cyber Crime Center, an organization I commissioned while serving as the commander of the Air Force Office of Special Investigations also employs and trains some of these cyber specialists. Without this type of field-tested past experience, even well-skilled information technologists and cybersecurity professionals are ill-prepared to detect and respond to nation-state actors. Again, if they have not previously detected and responded to sophisticated threat actors, they likely will be unable to successfully do so.

Additionally, U.S. political campaigns are unlike any corporate or Government entity. They are essentially start-ups that can endure for weeks or years. The short tenure of personnel—both volunteers and employees—diminishes the effect of cybersecurity measures used successfully in corporate America. For instance, anti-phishing training has been demonstrated to reduce the effectiveness of phishing attacks in corporate America. Campaigns have less long-term effect from similar training, because their personnel are relatively short-tenure.

Campaigns are isolated.—Our democracy is rooted in the separation of powers—Executive, Legislative, Judicial. Our election process is a key component that must be independent. This very independence tends to isolate the election community from some of the core National security apparatus that it needs to protect it.

The United States Government has the best intelligence, law enforcement, National security, and cybersecurity capabilities in the world, but conditions isolate campaigns from U.S. Federal Government resources.

Campaign personnel may be concerned about the interests of for-profit organizations. Specifically, campaigns wonder how they can trust the advice of an organization that stands to profit on that advice. In particular, product vendors following common sales practice only represent their own products. This can inadvertently lead campaigns to a less-than-comprehensive cybersecurity solutions.

Campaigns focus.—Their singular focus is to get elected. Any effort not directly in support of getting elected, is not funded or underfunded. For election campaigns, every dollar spent on services like cybersecurity is a dollar that is not being spent on their core mission. Even proactive candidates may think twice about spending effort and money on cybersecurity, for fear this diversion of resources will result in less votes than their competitors. This results in a lack of incentive for campaigns to address cybersecurity more fully, despite the imminent threat.

Last mile cybersecurity.—In addition to the above campaign observations, I offer a technical one. We still struggle with the "last mile" of cybersecurity within our communities—getting actionable security intelligence in the hands of those who need to defend themselves. There are at least two aggravating circumstances. First, the classification level of threat information slows down the flow of actionable threat intelligence. Second, threat information is mainly conveyed in formats that cannot be automatically processed by computers. In cyber space, the pace of engagement

is extremely fast. It far outpaces the rate of de-classification and re-formatting threat intelligence. We are fighting an asymmetrical war on the cyber front, and we must adjust.

WHAT CAN WE DO

Capitalize on the non-profit model.—Non-profit organizations are uniquely positioned and scoped to support campaigns. Specifically, non-profits avoid misgivings campaigns may have about utilizing Federal Government and for-profit resources directly. When non-profits engage campaigns, it reduces risks they may face, and we all face, if those campaigns are isolated. Non-profits are not a part of the Executive branch of Government, therefore they are not affiliated with a competing candidate. Non-profits less prone to the financial conflicts of interest faced by a for-profit. At the same time, non-profits can still play an integral role in brokering the resources of the Federal Government and for-profit organizations. For instance, non-profits may offer an indirect way to disseminate cyber threat information (and do so in formats that can be immediately utilized by campaigns). For all of these reasons, I believe non-profit organizations are well-suited to support political committees and campaigns with on-going and proactive measures.

Specify minimum standards for campaign cybersecurity.—Campaigns may have greater incentive to spend effort and funds on cyber protections if they know their competitors are obligated to the same expenditures.

Here is a similar circumstance from recent history. In the past, US CyberDome personnel helped create the DoD-Defense Collaborative Information Sharing Environment (DCISE). The DCISE stemmed from the Comprehensive National Cybersecurity Initiative to be one of the first successful examples of "need to share" in America. The DCISE used specific methodologies and techniques to anonymously share intelligence and law enforcement information with the defense industrial base (DIB), and share that information with the Federal Government. In the DIB, there existed similar competitive pressures about the effort and time spent on participation in DCISE. Ultimately, the Defense Federal Acquisition Regulation incorporated requirements for DIB organizations to participate in the DCISE, thus "leveling the playing field" for all DIB organizations to participate. This propelled the DCISE to a well-utilized and effective solution for threat information sharing in the DIB. Similar requirements for Federal campaign committees would likely prove useful.

Focus on key technical challenges.—Congress should consider mandating that all U.S. Government threat intelligence be disseminated in computer-readable formats, in addition to prose. This simple requirement would go a long way to ensuring that action can be taken swiftly once threat intelligence information is received. I do not espouse a specific format. I would leave that up to the experts. Expressing all threat information in computer-readable formats will be a big step forward.

Challenges like de-classification are more complex to solve. Over-classification is something that intelligence organizations should evaluate for themselves. In other words, is it possible that certain aspects of the threat information never needed to be Classified to begin with? Accelerating de-classification should also be considered. We are living in an age where machine learning is broadly applied, and artificial intelligence is starting to be well-understood. These technologies hold significant promise to automate large portions of the de-classification process.

CONCLUSION

US CyberDome is defending against election interference by working with Federal campaign committees, National party committees, think tanks, and non-Governmental organizations. Our status as a non-profit affords us unique insights and opportunities to help the community. Thank you for the opportunity to testify. I am happy to answer any questions you may have.

Chairman THOMPSON. General Taylor, let me thank you for your testimony. I now recognize Mr. Stengel for his opening statement.

STATEMENT OF RICHARD STENGEL, FORMER UNDER SECRETARY OF STATE FOR PUBLIC DIPLOMACY AND PUBLIC AFFAIRS, U.S. STATE DEPARTMENT

Mr. STENGEL. Thank you, Mr. Chairman. I said thank you, Mr. Chairman. I feel very comfortable here today, because I spent so much time sitting next to General Taylor in Government.

So the consent of the governed, that is the basis of our democracy. If that consent is acquired through deception, the powers derived from it are not just. That is why disinformation is so dangerous to our democracy. Disinformation is deliberately false information designed to deceive or mislead. Misinformation is simply false information, whether deliberate or not. Disinformation is the much greater threat, because it is on the rise around the world and at home, particularly here at home.

Disinformation is asymmetric warfare. You might not be able to afford an F–35, but you can certainly hire some people with laptops who act as trolls. Yet it is often a weapon used by the strong against the weak, because authoritarian leaders have understood that they can repress free speech at home and spew disinformation on state media.

It is difficult to fight, because it is hidden in plain sight. It uses all the same principles of behavioral economics and the tools of the big social media companies to find a targeted audience. It is as old as humanity, but social media has made it exponentially easier to create, deliver, and instantly find large audiences.

I spent 3 years at the State Department, attempting to combat ISIS propaganda and Russian disinformation. In fact, we started the first counter-Russian group at the State Department, which eventually became the Global Engagement Center. I came to the State Department after 7 years as the editor of *Time,* where I understood media. What I found was that fighting ISIS was a lot more direct than fighting the Russians. ISIS at least said who they were. The Russians masqueraded as Americans to insert their poison into our digital bloodstream. We saw from the State Department the first wave of Russian disinformation around Putin's illegal invasion of Ukraine in 2014. Then the Russians took what they learned in the periphery and brought it here to our election in 2016.

But in attempting to counter Russian disinformation, I came to the conclusion that Government wasn't the answer. I saw that countering disinformation was often counter-productive. After all, we were the enemy. A tweet from the under secretary of state to someone was not going to change their mind.

Democracies aren't actually very good at combating disinformation. Why is that? In part, because our opponents use our freedoms against us. They exploit freedom of speech to create false speech, which is protected by the First Amendment. They use the same tools of microtargeting that advertisers use to sell us sneakers and phones, to sell us false narratives and conspiracy theories.

The truth is disinformation doesn't so much create division as amplify it. Even though I don't think Government has a direct role in countering disinformation through creating content or taking it down, I do think Government has a clear role in creating resilience to disinformation.

First, Congress can impose stricter regulations on the platforms that host all of this disinformation. Right now the law, the Communications and Decency Act, doesn't treat them as publishers, and they have complete immunity from liability for all this content on their platforms.

Take it from me. Not only are these companies publishers, they are the biggest publishers in the history of the world. To be sure, they can't have the same liability that I had when I was editor of *Time*. But they need to have some more liability for content that is on their platforms that is demonstrably false, that is created by robots, that attacks people on the basis of race, religion, ethnicity, gender, or sexual orientation, that is created by foreign actors to deceive American voters. They need to be much more accountable for making a good-faith effort to remove that content.

So as 2020 approaches, we see a host of new problems, deep fakes, data manipulation, where they—bad actors don't just steal data but manipulate it. The professionalization of interference, where private companies teach people how to do disinformation for profit, and the rise of home-grown disinformation and the recruitment of Americans as witting or unwitting agents of disinformation.

I actually think the platform companies need to embrace is what I call the five Ds of combating disinformation: Detection, demotion, deletion, disclosure, and digital literacy. They not only need to remove foreign influence; they need to publicize it.

I do think the one entity in Government that I mentioned before, the Global Engagement Center, which was created to combat global disinformation, can help with this election, too. I would urge the passing of the Honest Ads Act, which would bring a lot more transparency in political advertising.

As I have often said, we don't have a fake news problem, we have a media literacy problem. There was a poll this past week that showed that 47 percent of Americans say they find it difficult to evaluate whether the information they are getting is true. We need to teach deep media literacy and digital literacy in the schools. I can't think of anyone better to pay for that than the platform companies.

Ultimately, the problem of disinformation is not so much that people will come to believe what is false. The greatest problem is that they will doubt what is true.

I am honored to be here today, and I welcome your questions. Thank you very much.

[The prepared statement of Mr. Stengel follows:]

PREPARED STATEMENT OF RICHARD STENGEL

NOVEMBER 19, 2019

"Governments are instituted among men," the Declaration declares, "deriving their just powers from the consent of the governed." In a democracy, how do we obtain that consent? Through information, the Framers said, true information. The rise of disinformation is a threat to our democracy because it undermines our consent. If that consent is acquired through deception and disinformation, the powers derived from it are not just.

Disinformation is deliberately false information designed to deceive or mislead. Misinformation is simply false information that is not deliberate or designed to mislead. Disinformation is the much greater threat and it is on the rise around the world and at home. In the realm of politics, it is the promulgation of false narratives to undermine democracy.

Disinformation is asymmetric warfare: You might not be able to afford an F35, but you can always hire a few trolls with laptops. Yet it is often a weapon used by the strong against the weak: Authoritarian leaders have learned that they can repress free speech at home and spew disinformation on state media. That's a dangerous combination for the future of democracy. Disinformation is difficult to fight

because it is hidden in plain sight. It uses all the principles of behavioral economics—and the tools of the big social media companies—to find a targeted audience. Disinformation is as old as information, but social media has made it exponentially easier to create, deliver, and instantly find large and receptive audiences.

My book *Information Wars* is the story of how we attempted to fight Russian and ISIS disinformation from the State Department during the last 3 years of the Obama administration. I went into Government after 7 years as the editor of *TIME* and I thought I understood media. ISIS was something new in terrorism: A non-state actor as adept at social media as barbaric killings. But ISIS's digital jihadis did not pretend to be anyone else other than who they were—unlike the Russians, that is. The Russians adopted other identities and masqueraded as Americans to insert their poison into our digital bloodstream. From the State Department, we first saw Russia create a wave of social media disinformation in the Russian periphery around Putin's illegal invasion of Ukraine in 2014—and then the Russians took what they learned there and aimed it squarely at our election space in 2016.

What also makes disinformation effective is that there is often a kernel of truth in it. What united ISIS and Russian disinformation was what I called the weaponization of grievance. ISIS weaponized the grievances of Sunni Muslims who felt left out by modernity and repressed by their rulers. Putin weaponized the grievances of Russians who mourned the loss of the Soviet Union and never adapted to the modern world. If ISIS had a slogan, it was Make Islam Great Again. If Putin had a slogan, it would be Make Russia Great Again. They had their mantras long before we heard about making America great again. This global weaponization of grievance is the unified theory behind the rise of nationalism and right-wing strongmen across the globe.

But the ultimate threat is here at home. It's easier and more comfortable for us to see this problem as a threat from the outside, from foreign influence operations. And, indeed, they remain a grave National security threat. But the scale and range of domestic disinformation—created and spread by Americans to other Americans—dwarfs any foreign threat or troll factory. Our foreign adversaries seek to engage Americans and do so, but our home-grown disinformation overwhelms what our adversaries produce. Our internal challenge is far greater and more dangerous than any external one.

In attempting to counter Russian and ISIS disinformation I came to see that Government was not the answer. I saw that "countering" disinformation was often counter-productive. When we tried to create content ourselves, we very often played into our adversaries' hands. After all, we were the enemy. It's very hard for a tweet from the U.S. State Department to persuade someone of our point of view if we are seen as the cause of the problem. They see our efforts to rebut them as confirmation that they are right and that their strategy is working.

Democracies just aren't very good at combatting disinformation. Why is that? One reason is that our opponents not only use our freedoms against us, but our technology. They exploit freedom of speech to create dangerous and false speech, which is protected by the First Amendment. They utilize the same tools of micro-targeting that advertisers use to market sneakers and phones but they use them to sell us false narratives and conspiracy theories. Disinformation is hard to fight because it's not just a supply problem, it's a demand problem. People embrace it when it seems to confirm their beliefs. It's a missile that hits its target because the target welcomes it. The truth is, disinformation doesn't create divisions so much as widen them.

At the end of last year, the initial Senate Select Committee on Intelligence report on Russian interference in the 2016 election said the Internet Research Agency in St. Petersburg had created more than 10 million tweets—of which 6 million were original—across 4,000 accounts; more than 100,000 Instagram posts; and more than 50,000 Facebook posts. The second Senate Intelligence Committee report that came out last month reported that the Russians had done more since the election than they did before it. Now, as then, it's a whole-of-Government effort which includes Russian intelligence services, conventional Russian media, and even the foreign ministry. The Russians are shrewd about using our own biases against us. In 2016, they sought out groups who were afraid of immigrants and Muslims and stoked their fears. They targeted African American voters and told them voting was a waste of time. After Twitter and Facebook removed many on-line assets attributed to Russia in 2017, the Russians returned with a more tailored focus to activist communities who were susceptible to disinformation. With a focus on 2020, the Russians will again seek out cultural and social divisions and try to magnify them. As with 2016, they will often amplify both sides of divisive issues. Anything to create chaos and disunity and doubt about the integrity of our political process.

Even though I don't think Government has much of a role in countering disinformation through creating content or taking it down, I do think there is a clear Government role in raising awareness and creating resilience to disinformation. Combatting disinformation is a cross-cutting issue that has implications for a wide range of different agencies and committees. First, I think Government has a role in regulating the platforms that host disinformation. Currently, there is an alignment of economic interests between the disinformationists and the platforms: The social media companies make money when disinformation goes viral. Right now, the law doesn't treat the platform companies as publishers and they have complete immunity from liability for the content on their platforms. Not only are these companies publishers, they are the biggest publishers in the history of the world. No, they don't have human editors, but as a former editor I'm here to tell you that algorithms and content recommendation engines are editors—the fastest and most efficient editors in history.

To be sure, these companies cannot have the same liability that I used to have as editor of *TIME*. But they need to have some liability for content that is on their platform that is demonstrably false, that is created by robots, that attacks others on the basis of race, religion, ethnicity, gender or sexual orientation, that is created by foreign actors to deceive American voters. They need to be legally accountable for making a good-faith effort to remove such content from their platforms.

As the 2020 election approaches, there are a host of new problems: Deep fakes; data manipulation, where bad actors don't steal data but manipulate it; the professionalization of interference, as private companies hire out their services to create disinformation; the rise of domestic disinformation and the recruiting of Americans as witting or unwitting agents of disinformation.

Combatting these new efforts requires the detection and removal of foreign influence in our election, greater ad transparency, more accountability for the platform companies, and greater data protection. I would endorse the Senate Intelligence Committee's recommendations for fighting disinformation, and in particular the timely sharing of information between the private and public sector of real-time threats. I believe the tech companies would welcome that too. I'd also recommend the Five D's of combatting disinformation: Detection, demotion, deletion, disclosure, and digital literacy. The empowering of the Global Engagement Center, which was created at the end of 2016, to truly help fight all kinds of disinformation could be a vital effort of the Government. It is important to pass the Honest Ads Act, which would provide for more transparency in political advertising. All of this in addition to giving the content companies more liability for publishing proscribed content would help but not remedy the flood of disinformation. I've often said we don't have a fake news problem, we have a media literacy problem. Media and digital literacy need to be taught and the schools, and I can't think of a better source of that funding than the platform companies. We also need a privacy bill of rights that protects our information as part of a new digital social contract. The ownership of one's personal information is an unalienable right.

The disinformationists know that it's far easier to create confusion rather than clarity, to confuse rather than persuade. They want people to see empirical facts as an elitist conspiracy. Citizens have trouble discerning fact from fiction and we need to teach media and digital literacy in the schools from an early age. In a new poll from this past week, 47 percent of Americans say they find it difficult to know whether the information they encounter is true. The public needs to see that countering disinformation is a civic duty for which we all are responsible. Ultimately, the problem of disinformation is not so much that people will come to believe what is false. The greatest problem is that they it will cause them to question what is true.

Mr. RICHMOND [presiding]. Thank you. I will now recognize Dr. Blaze for 5 minutes to summarize his statement.

STATEMENT OF MATT BLAZE, PH.D., MC DEVITT CHAIR OF COMPUTER SCIENCE AND LAW, GEORGETOWN UNIVERSITY

Mr. BLAZE. Thank you, Chairman Thompson, Chairman Richmond, and Ranking Member Katko for convening this hearing on the vitally important topic of securing American elections against foreign interference.

I am here today as an academic and technologist who studies particularly election system security. As I know you are well

aware, the integrity of elections across the United States today depends heavily on the integrity of the computers and software systems embedded across our election infrastructure. Complex software lies at the heart of not just the vote-casting equipment used at polling places, but also the information systems used by local authorities to manage everything from voter registration records, to the tallying and reporting of election results, to the dissemination of authoritative information to voters.

Unfortunately, much of this information—much of this infrastructure has proven dangerously vulnerable to tampering and attack, in some cases in ways that can't easily be detected or corrected after the fact. These vulnerabilities create practical avenues for our adversaries to do everything from cause large-scale disruption on Election Day, disenfranchise large numbers of voters, create uncertainty as to the legitimate winners of election, or even to undetectably alter election outcomes.

Now, for the purpose of our discussion, it is helpful to consider voting machines and election management infrastructure separately. They have different properties and different mitigations. So let me begin with the voting equipment used at polling places first.

To be blunt, it is a widely recognized and indisputable fact that every piece of computerized voting equipment used at polling places today can be easily compromised in ways that have the potential to disrupt election operations, compromise the firmware and software in these devices, and alter vote tallies that get reported by county offices. Now, this is partly a consequence of poor design and implementation by equipment vendors, which is a notorious problem, but it is also ultimately a reflection of the nature of complex software.

It is simply beyond the state-of-the-art to build software systems that can reliably withstand a targeted attack by a determined adversary in a high-stakes environment like voting. The vulnerabilities are real. They are serious and, absent a surprising breakthrough in technology and computer science, probably inevitable for quite some time to come.

Now, fortunately, there is now also overwhelming consensus among experts who have studied this problem on how we can conduct reliable elections, despite the inherent unreliability of the underlying hardware and software that we use to cast our votes.

This requires 2 things, 2 properties of the equipment and processes.

The first is that the voting technology must retain a paper record that reliably reflects the voter's intended choices. Now, fortunately, equipment with this property already exists and is in use in many jurisdictions throughout the Nation. It has the added virtue of being relatively simple and inexpensive, compared to other alternative voting technologies that we use and have been using. I am referring here to paper ballots, preferably marked by hand, that are fed into optical scan ballot readers at the time that the vote is cast by the voter.

Now, paper ballots alone are not sufficient to accomplish reliable elections in the face of tampering, since the software in ballot scanners themselves all are vulnerable to tampering and to error. So there is a second requirement, and that is that the election be reli-

ably audited to ensure that the software is reporting the correct outcome of each race.

Now, there is a statistically rigorous technique recently invented called risk limiting audits that can accomplish this efficiently and quickly. But it must be done routinely after every election in order to provide meaningful assurance that election outcomes are correct.

Unfortunately, here and now, only a handful of States currently conduct risk limiting audits, although it is encouraging that more and more States are experimenting with them.

So the second technology at risk is the election management infrastructure that is used by local jurisdictions. While voting—vote casting equipment has justifiably gained a great deal of attention, there is more to this than just the voting machines. Each of the more than 5,000 local jurisdictions responsible for running elections has to maintain a number of critical information systems that are attractive targets for disruption by adversary. Most prominently are the voter registration databases that determine who is allowed to vote on Election Day.

Now, all of the 5,000 different local jurisdictions responsible for running these systems have different resources, practices, and regulations that govern them, but they have in common that they are targets of some of the world's most sophisticated intelligence services, and they are at the front line of our Nation's defense against election disruption.

There is no simple fix here, but—except the provisioning of significant additional resources to protect these systems. We don't expect the local sheriff to single-handedly defend against military ground invasions, and we should not expect county election IT managers to defend against cyber attacks by foreign intelligence agencies, yet that is what we effectively ask them to do.

So thank you again for your attention to these important issues.

[The prepared statement of Mr. Blaze follows:]

PREPARED STATEMENT OF MATT BLAZE [1]

NOVEMBER 19, 2019

INTRODUCTION

Thank you for the opportunity to offer testimony on the important questions raised by the security of the technology used for elections in the United States.

For more than 25 years, my research and scholarship has focused on security and privacy in computing and communications systems, especially as we rely on insecure platforms such as the internet for increasingly critical applications. My work has focused particularly on the intersection of this technology with public policy issues. For example, in 2007, I led several of the teams that evaluated the security of computerized election systems from several vendors on behalf of the States of California and Ohio.

I am currently the McDevitt chair of computer science and law at Georgetown University. From 2004 to 2018, I was a professor of computer and information science at the University of Pennsylvania. From 1992 to 2004, I was a research scientist at AT&T Bell Laboratories. I hold a PhD in computer science from Princeton University, an MS in computer science from Columbia University, and a BS from the City University of New York. This testimony is not offered on behalf of any organization or agency.

[1] Professor and McDevitt chair of computer science and law, Georgetown University, 600 New Jersey Ave NW, Washington, DC 20001. *mab497@georgetown.edu.* Affiliation for identification only.

In this testimony, I will give an overview of the security risks facing elections in the United States today, with emphasis on vulnerabilities inherent in electronic voting machines, as well as the exposure of our election infrastructure to disruption by National security adversaries. I have attempted, to the extent possible, to represent the current consensus of experts in the field, but space and time constraints limit my ability to be comprehensive or complete. An especially valuable resource, with comprehensive discussion and recommendations. is the recent National Academies "Securing the Vote" consensus study report.[2]

I offer 3 specific recommendations:

- Paperless ("DRE") voting machines should be phased out from U.S. elections immediately, and urgently replaced with precinct-counted optical scan ballots that leave a direct artifact of voters' choices.
- Statistically rigorous "risk-limiting audits" should be routinely conducted after every election, in every jurisdiction, to detect and correct software failures and attacks.
- State and local voting officials should receive access to significant additional resources, infrastructure, and training to help them protect their election management IT systems against increasingly sophisticated adversaries.

I. ELECTIONS AND SOFTWARE SECURITY

A consequence of our Federalist system is that U.S. elections are in practice highly decentralized, with each State responsible for setting its own standards and procedures for registering voters, casting ballots, and counting votes. The Federal Government has set only broad standards for such issues as accessibility, but has historically been largely uninvolved in day-to-day election operations. In most States, the majority of election management functions are delegated to local county and town governments, which are responsible for registering voters, procuring voting equipment, creating ballots, setting up and managing local polling places, counting votes, and reporting the results of each contest. Consequently, thousands of individual local election offices shoulder the burden of managing and securing the voting process for most of the American electorate.

Elections in the United States are among the most operationally and logistically complex in the world. Many jurisdictions have large numbers of geographically-dispersed voters, and most elections involve multiple ballot contests and referenda. Baseline election security must account for sophisticated adversaries, ballot secrecy, fair access to the polls, and accurate reporting of results, making secure election management one of the most formidable—and potentially fragile—information technology problems in government.

Computers and software play central roles in almost every aspect of our election process: Managing voter registration records, defining ballots, provisioning voting machines, tallying and reporting results, and controlling electronic voting machines used at polling places.[3] The integrity and security of our elections are thus inexorably tied to the integrity and security of the computers and software that we rely on for these many functions.

The passage of the Help America Vote Act (HAVA) in 2002 accelerated the computerization of voting systems, particularly with respect to the ways in which voters cast their ballots at local polling stations. HAVA provided funds for States to replace precinct voting equipment with "accessible" technology. As implemented, however, some of this new technology has had the unfortunate unintended consequence of increasing, rather than decreasing, the risk of our elections being compromised by malicious actors.

A. Election Software and Hardware

A typical[4] county election office today depends on computerized systems and software for virtually every aspect of registering voters and conducting elections. Generally, an election office workflow will include at least the following pre- and post-election functions:

Voter registration.—The on-going maintenance of an authoritative database of registered voters in the jurisdiction, including the precinct-by-precinct "poll books" of

---

[2] *https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy*.

[3] A typical election administration office is much like any modern enterprise, with local computer networks tying together desktop computers, printers, servers, and internet access. This increasing connectivity served as a critical avenue in 2016 for what U.S. intelligence agencies have identified as attacks by Russian military intelligence.

[4] The precise nature of the systems used and how they interact with one another will vary somewhat depending on the vendors from which the systems were purchased and the practices of the local jurisdiction.

voters (which might be on paper or in electronic form) that are used to check in voters at precinct polling stations.

Ballot definition.—The pre-election process of creating data files that list the various contests, candidates, and rules (e.g., number of permitted choices per race) that will appear on the ballot. The ballot definition is used to print paper ballots, to define what is displayed on touchscreen voting terminals, and to control the vote tallying and reporting software. Local races (such as school boards) may sometimes require that different ballot definitions be created for different precincts within a county in any given election.

Voting machine provisioning.—The pre-election process of configuring the individual precinct voting machines for an election. This typically includes resetting internal memory and loading the appropriate ballot definition for each precinct. Depending on the model of voting machine, provisioning typically involves using a computer to write removable memory cards that are installed in each machine.

Absentee and early voting ballot processing.—The process of reading and tabulating ballots received by mail and from early voting polling places. Mail votes are typically processed in bulk by high-volume optical scan ballot reading equipment.

Tallying and reporting.—The post-election process of tabulating the results for each race received from each precinct and reporting the overall election outcomes. This process typically involves using a computer to read memory card media retrieved from precinct voting machines.

Each of the above "back end" functions employs specialized election management software running on computers. Depending on the size and practices of the county, the same computers may be used for more than one function (e.g., the ballot definition computer might also serve as the tallying and reporting computer). These computers are typically off-the-shelf desktop machines running a standard operating system (such as Microsoft Windows), often equipped with electronic mail and web browser software along with the specialized voting software. Election office computers are typically connected to one another via a wired or wireless local area network, which may have a direct or indirect connection (sometimes via a firewall) to the internet.

In some jurisdictions, some of these election management functions (most often those concerned with voter registration databases and ballot definition), may be outsourced by a county or State to an election services contractor. These contractors provide jurisdictions with specialized assistance with such tasks as creating ballots in the correct format, managing voter registration databases, creating precinct poll books, and maintaining voting machines. The degree to which jurisdictions rely on outside contractors varies widely across the Nation.

Much of the voting equipment used at precincts is computerized as well, although it is generally packaged in specialized hardware. This equipment includes:

Direct Recording Electronic (DRE) Voting Machines.—DRE machines are special-purpose computers that display ballot choices to the voter (based on the ballot definition) and record voter choices. Both the ballot definition configuration and the vote count are typically stored on removable memory media.[5]

Optical Scan Ballot Readers.—Optical scan ballot readers are specialized computers that read voter-marked paper ballots. The ballot is read according to the ballot definition configuration (typically on removable memory media), and a tally is maintained in memory (also typically on removable media). The machine also captures the scanned ballots and stores them in a mechanically-secured ballot box.

Ballot-Marking Devices (BMDs).—Ballot-marking devices are an assistive technology used in optical scan systems to allow visually or mobility impaired voters to create ballots for subsequent scanning. BMDs are similar in appearance to DRE machines in that they display (or read aloud) the ballot electronically, based on a ballot definition configuration, and accept voter choices for each race. However, instead of recording those choices in computer memory as DREs do, BMDs print a marked paper ballot that can then be submitted through an optical scan ballot reader.

Electronic Poll Books.—These devices are typically tablet-style computers that contain an authoritative copy of the database of registered voters at each precinct. Electronic poll books are not used directly by voters, but rather by precinct poll workers as voters are checked in at their polling place. They are not used in all jurisdictions.

---

[5] Some models of DRE can be equipped with a Voter Verified Paper Audit Trail (VVPAT) option in which the voters' selections are printed on a paper tape roll that is visible to the voter. VVPATs can assist with determining the voter's intent during a recount, but their efficacy depends on each voter's diligence in confirming that their choices are correctly recorded on the paper tape before they leave the voting booth. Research consistently suggests that, in practice, very few voters successfully perform this confirmation step.

B. Software and Election Security

Securing complex software systems is notoriously difficult, and those that perform the various functions described above are no exception.[6] There are several avenues of vulnerability in such systems. Common software "bugs" often introduce vulnerabilities that can be exploited by an adversary to silently compromise the integrity of data or make unauthorized (and difficult to detect) changes to the behavior of systems. Configuration and system management errors (such as the use of vulnerable out-of-date platforms and weak passwords) can further compromise security. Computer networks (which are not generally used by precinct voting machines themselves but are commonly connected to back end systems in election offices) compound these risks by introducing the possibility of remote attack over the internet.

The integrity of the vote today thus increasingly depends on the integrity of the software systems—running on voting machines and on county election office networks—over which elections are conducted. Any security weakness in any component of any of these systems can serve as a "weak link" that can allow a malicious actor to disrupt election operations, alter tally results, or disenfranchise voters.

In many electronic voting systems used today, a successful attack that exploits a software flaw might leave behind little or no forensic evidence. This can make it effectively impossible to determine the true outcome of an election or even that a compromise has occurred.

Unfortunately, these risks are not merely hypothetical or speculative. Many of the software and hardware technologies that support U.S. elections today have been shown to suffer from serious and easily exploitable security vulnerabilities that could be used by an adversary to alter vote tallies or cast doubt on the integrity of election results.

II. CURRENT ELECTRONIC VOTING SYSTEMS HAVE PROVEN VULNERABLE TO A RANGE OF KNOWN, EXPLOITABLE SECURITY FLAWS

A. Risks in Various Election Components

Security concerns about computerized voting systems have been raised from almost the moment such systems were first proposed. Most of these concerns have focused on electronic voting equipment used at polling stations, although the "back end" election management software used to manage voter registration, provision voting machines, and tally are at least equally critical to the integrity of the vote.

To be clear, all electronic voting technology can and does suffer from security vulnerabilities. The consequences of these vulnerabilities being successfully exploited, however, depends on the particular class of device and whether the technology permits effective post-election auditing to validate or recover correct election results.

1. Election Management IT Systems

As noted above, local jurisdictions rely on computers for almost every aspect of election administration. Official information for voters is distributed on public-facing websites. Voter registration records, used on election day to determine who is permitted to vote, are maintained in computerized databases. Ballots forms are created and edited on computers. Absentee ballot mailings are managed by computer. Preliminary and official election results are maintained and disseminated by computer. Specialized "Election Management" software (generally provided by the vendor of the voting equipment) is used to configure ballots and read results from precienct voting machines.

In most cases, the computers used for election administration employ the same hardware, operating systems, and networking platforms employed by other enterprises, and are connected, directly or indirectly, to the internet. Election management systems are exposed to the same risks of compromise by malicious actors that cause the commonplace "data breaches" in other private- and public-sector domains that have become regular fixtures of on-line life.

Many jurisdictions outsource some of their election management tasks to outside vendors or contractors. This further amplifies the exposure of local election systems to external tampering.

Disruption or compromise of any local election administration functions can have grave and often non-recoverable consequences for the integrity of elections. Com-

[6] The fact that software systems can be, and often are, vulnerable to attack is not unique to election systems, of course. Serious data breaches are literally daily events across the public and private sectors, and cybersecurity is widely recognized to be a serious law enforcement and National security problem. To the extent that elections depend on software or are administered by networked computing systems, they are subject to all the same risks.

promise of voter registration databases can be exploited by adversaries to cause long lines at polling places (forcing large numbers of voters to cast provisional ballots) and can selectively disenfranchise voters to favor particular candidates. Provisioning of voting machines with incorrect ballot definitions can prevent correct ballots from being cast. Errors in in unofficial or final tallies can cast doubt on the legitimacy of entire elections. In some cases, successful attacks may not be discovered until long after polls have closed, or may never be discovered at all.

The IT and security administration of election management computers varies widely from jurisdiction to jurisdiction. In the best cases, there may be a full-time staff devoted to securing and managing election computers and networks. In a more typical case, computer security is relegated to the general county IT staff, which may have only limited resources relative to the threat. In all cases, however, even the best defensive cybersecurity resources of a local county are of only limited value against a foreign state adversary.

Local election management computers and networks are especially attractive targets for foreign tampering and interference. They can often be attacked remotely, without the need for physical presence in the targeted jurisdiction, and successful attacks may be rewarded with partial or complete control over a county's voter registration databases, voting machine configuration, and results reporting infrastructure.

2. Electronic Poll Books

Electronic poll books, which are not used in every jurisdiction, perform the initial voter "check-in" function at polling places on election day. They must, by nature of their function, have reliable access to an authoritative list of the voters registered to vote at each polling places. This may be accomplished either with an internal copy of the voter registration database or by on-line remote access to a central computer. In either configuration, electronic poll books perform an essential election function and must be reliably secured against tampering. If poll books are unavailable or if their databases are corrupted, voters will not be able to cast ballots (except by provisional ballot, to the extent that is a viable option).

Electronic poll books have received much less scrutiny than other precinct voting equipment, but are subject to all the same risks and attack vectors as other electronic devices. In many jurisdictions, they are largely unregulated and require little or no outside certification or audit.

3. Optical Scan Ballot Readers

Optical scan ballot readers are specialized computers that scan and retain printed ballots and record on electronic storage media the tally of votes cast in each race. They depend on the integrity of their software and hardware for their ability to correctly interpret ballots and to correctly record votes. They are exposed to physical access by poll workers, and, in many cases, individual voters.

Ballot scanners can be compromised in a number of practical ways, any one of which can compromise the recorded vote tally. However, because they retain the physical paper ballots marked by voters, it is possible to recover from such a compromise if it is detected. A technique called "risk-limiting audits" can reliably detect and recover from defective or compromised ballot scanners and is discussed in the sections that follow.

4. Ballot Marking Devices

Originally, Ballot Marking Devices (BMDs) were conceived of narrowly, as an assistive technology for use by voters with disabilities to assist them in marking optical scan paper ballots, (bringing such systems into compliance with Help America Vote Act (HAVA) requirements for accessible voting). However, certain recent voting products greatly expand the use of BMD technology by integrating a BMD into the voting process for all voters, whether they require assistive technology or not.

BMD-based voting systems are controversial, since, by virtue of their design, the correctness of their behavior cannot be effectively audited except by every individual voter carefully verifying his or her printed ballot before it is cast. A maliciously compromised BMD could subtly mismark candidate selections on ballots in a way that might not be noticed by most voters. If BMDs fail or must be rebooted at a polling place, there may be no way for voters to create marked ballots, making BMDs a potential bottleneck or single point of failure on election day.

As a relatively new technology, BMD-based systems have not yet been widely examined by independent researchers and have been largely absent from practical election security research studies. However, even with relatively little scrutiny, exploitable weaknesses and usability flaws have been found in these systems, This underscores the need for more comprehensive studies and for caution before these systems are purchased by local jurisdictions or widely deployed.

5. Direct Recording Electronic (DRE) Voting Machines

From a security perspective, by far the most problematic and risky class of electronic voting systems are those that employ Direct Recording-Electronic (DRE) machines. DRE machines are special purpose computers programmed to present the ballot to the voter and record the voter's choices on an internal digital medium such as a memory card. At the end of the election day, the memory card containing the vote tallies for each race is generally removed or electronically read from the machine and delivered to the county election office, where the tallies from each precinct are recorded by the county tallying software. DRE machines are sometimes informally called "touchscreen" voting machines, although not all DRE models use actual touchscreen displays (nor are all election devices that employ touchscreens DREs).

The design of DREs makes them inherently difficult to secure and yet also makes it especially imperative that they be secure. This is because the accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data. Every aspect of a DRE's behavior, from the ballot displayed to the voter to the recording and reporting of votes, is under control of the DRE hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or re-load new and maliciously behaving) software running on the machine, not only has the potential to alter the vote tally, but can make it impossible to conduct a meaningful recount (or even to detect that an attack has occurred) after the fact. If a DRE is compromised at any time before or during an election, any votes cast on it are irreparably compromised as well.

DRE-based systems introduce several avenues for attack that are generally not present (or are not as security-critical) in other voting technologies:

- Alteration or deletion of vote tallies stored in internal memory or removable media
- Alteration or deletion of ballot definition parameters displayed to voters [7]
- Alteration or deletion of electronic log files used for post-election audits and detecting unauthorized tampering.

Attacks might be carried out in any of several ways, each of which must be reliably defended against by the DRE hardware and software:

- Direct tampering with data files stored on memory cards or accessible through external interface ports
- Surreptitious replacement of the certified software running on the device with a maliciously altered version
- Exploitation of a pre-existing vulnerability in the certified software.

Successfully exploiting just one of these avenues of attack can be sufficient to undetectably compromise an election. The design of DREs makes it necessary not only that their hardware be highly secure against unauthorized tampering, but that the software running on them not suffer from any vulnerabilities that could be exploited by a malicious actor. This makes the security requirements for DREs more stringent—and also more easily defeated—than for any other currently-deployed election technology.

Unfortunately, the DRE-based systems purchased by and used in various States under HAVA have repeatedly been found to suffer from exactly these kinds of exploitable hardware and software vulnerabilities.

B. The 2007 California and Ohio Studies

To date, the most extensive independent studies of the security of electronic voting systems were commissioned 10 years ago by the Secretaries of State of California and Ohio. Expert review teams were given access to the voting machine hardware and software source code of every system certified for use in those States. The systems used in California and Ohio were also certified for use in most of the rest of the country, so these studies effectively covered a large fraction of available electronic voting equipment and software. I led the teams that reviewed the Sequoia products (for the State of California) and the ES&S products (for the State of Ohio);

---

[7] An incorrect (or maliciously altered) DRE ballot definition can make it impossible to determine the true election results even without any malicious software exploitation. For example, in York County, PA, a DRE ballot definition programming error in the 2017 general election appears to have allowed candidates in some local races to be voted for twice, with the possible consequence that the election will have to be invalidated and redone. See *http://www.ydr.com/story/news/2017/11/08/voting-machine-problems-what-york-countys-options/843423001/*. Paper-based systems, in contrast, are more robust against such errors. For example, the 2000 general election in Bernalillo County, NM had a similar error in their punch card-counting software, but was later able to correct the error without a new election; see *https://www.wsj.com/articles/SB976838091124686673*.

other teams in these studies reviewed the Diebold/Premier and Hart InterCivic products.[8]

In both studies, every team found and reported serious exploitable vulnerabilities in almost every component examined. In most cases, these vulnerabilities could be exploited by a single individual, who would need no more access than an ordinary poll worker or voter. Such an attacker would be able to alter vote tallies, load malicious software, or erase audit logs. Some of the vulnerabilities found were the consequence of software bugs, while others were caused by fundamental architectural properties of the system architecture and design. In some cases, compromise of a single system component (such as a precinct voting machine) was sufficient to compromise not just the vote tally on that machine, but to compromise the entire county back-end system.

In response, California and Ohio ordered some equipment decertified and some election-day procedures modified. However, all the vulnerable equipment and software remained certified for use in at least some other States.

Some equipment vendors and local voting officials claimed at the time that the findings of the California and Ohio studies were irrelevant or overstated, that any problems identified could be easily fixed, and that it would be difficult or impossible for anyone but an expert with extensive experience and access to privileged information (such as source code) to exploit vulnerabilities in practice. However, as exercises such as the DEFCON Voting Village (described below) have demonstrated, not only do these systems remain vulnerable, but they can be readily exploited by people with no more than ordinary computer science experience and expertise and without access to any secret or proprietary information.

C. The DEFCON Voting Village Exercise

The DEFCON conference is one of the world's largest and best-known computer security "hacker" conferences. This year's DEFCON was held August 8–10, 2019, in Las Vegas, NV, and drew more than 25,000 participants from around the world. DEFCON participants have broad interest in technology, and include security researchers from industry, Government, and academia, as well as individual hobbyists.

For the last 3 years, DEFCON has featured a Voting Machine Hacking Village ("Voting Village") to give participants an opportunity to examine and get hands-on experience with the security technology used in U.S. elections, including voting machines, voter registration databases, and election office networks. I am one of the organizers of the Voting Village.[9]

The voting machines available in the Voting Village included a variety of DRE, optical scan readers, ballot marking devices and electronic poll books from a range of commercial vendors. We acquired (from the surplus market) and made available to participants a sampling of different pieces of election hardware, including both DRE and optical scan voting machines as well as "poll book" devices used by used by precinct workers to verify and check in voters at polling places. Every model machine currently at the Voting Village is still certified for use in U.S. elections in at least one jurisdiction today.

The DEFCON Voting Village is not intended to be a formal security assessment or test, but rather an opportunity for a general audience of technologists to examine election equipment and systems. However, participants are encouraged to critically examine and probe the equipment and software for vulnerabilities, and to seek practical ways to compromise security mechanisms. No proprietary information or computer source code is made available.

The results of the Voting Village are summarized each year in detail in a report.[10] It is notable that participants, who overwhelmingly do not have any previous special expertise in voting machines or access to any proprietary information about them, have been very quickly able to find ways to compromise every piece of equipment in the Village by the end of the weekend. Depending on the individual model of machine, participants have found ways to load malicious software, gain access to administrator passwords, compromise recorded votes and audit logs, or cause equip-

---

[8] The various final reports of the California "Top-To-Bottom Review" studies can be found at *http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/*. The final report of the Ohio "Project EVEREST" study can be found at *https://www.eac.gov/assets/1/28/EVEREST.pdf*.

[9] Organizers of the DEFCON Voting Village include the author as well as Harri Hursti, Margaret MacAlpine, and Jeff Moss.

[10] The current Voting Village final report is available at: *https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf*.

ment to fail. In most cases, these attacks could be carried out from the ordinary interfaces that are exposed to voters and precinct poll workers.

The ease with which participants compromise equipment in the Voting Village should be regarded as at once alarming and yet also unsurprising. It is alarming because the very same equipment is in use in polling places around the United States, relied on for the integrity of real elections. But it is also ultimately unsurprising. Versions of many of the machines at DEFCON had been examined in the 2007 studies and found to suffer from basic, exploitable security vulnerabilities. It should not come as any surprise that, given access and motivation, people of ordinary skill in computer security would be able to replicate and expand on these results. It is, in fact, precisely what the previous studies of these devices warned would happen.

In summary, the DEFCON Voting Village demonstrates that much of the voting technology used in the United States is vulnerable not just to hypothetical expert attack in a laboratory environment, but also to practical analysis, manipulation, and exploitation by non-specialists with only very modest resources.

III. US ELECTION SYSTEMS ARE NOT ENGINEERED TO RESIST NATIONAL ADVERSARIES

The traditional "threat model" against which electronic voting systems have been evaluated has been largely focused on resisting traditional election fraud, in which domestic conspirators, perhaps assisted by corrupt poll workers or election officials, attempt to "rig" an election to favor a preferred candidate in a local, State, or National contest. Fraud might be accomplished by altering votes, adding favorable votes, deleting unfavorable votes, or otherwise compromising the security mechanisms that protect the ballot and tally.

While virtually every study of electronic voting technology has raised questions about the ability of current systems to resist serious efforts at fraud, traditional election fraud is not the only kind of threat, or even the most serious threat, that a voting systems must resist today.

Electronic voting systems must resist not only fraud from corrupt candidates and supporters, but also election disruption from hostile nation-state adversaries. This is a much more formidable threat, and one that current systems are far less equipped to resist.

The most obvious difference between traditional election fraud by corrupt domestic actors and disruption by hostile state actors is the expected resources and capabilities available to each. The intelligence services of even small nations can marshal far greater financial, technical, and operational resources than would be available to even highly sophisticated criminal conspiracies. For example, intelligence services can feasibly conduct advance operations against the voting system supply chain. In such operations, the aim might be to obtain confidential source code or to secure surreptitious access to equipment before it is even shipped to local election officials. Hostile intelligence services can exploit information and other assets developed broadly over extended periods of time, often starting well before any specific operation or attack has been planned.

But their greater resources are not the most important way that hostile state actors can be a more formidable threat than corrupt candidates or poll workers. They also enjoy easier goals. The aim of traditional "retail" election fraud is to tilt the outcome in favor of a particular candidate. That is, to succeed, the attacker must generally alter the reported vote count or add, change, or delete votes. But a hostile state actor—via an intelligence service such as Russia's GRU—might be satisfied with merely disrupting an election or calling into question the legitimacy of the official outcome. With election systems so heavily dependent on demonstrably insecure software and voting equipment, this kind of disruption could be comparatively simple to accomplish, even at a National scale.

A hostile state actor who can compromise even a handful of county networks might not need to alter any actual votes to create widespread uncertainty about an election outcome's legitimacy. It may be sufficient to simply plant suspicious (and detectable) malicious software on a few voting machines or election management computers, create some suspicious audit logs, delete registered voters from the rolls, or add some obviously spurious names to the voter rolls. If the preferred candidate wins, they can simply do nothing (or, ideally, use their previously-arranged access to restore the compromised networks to their original states, erasing any evidence of compromise). If the "wrong" candidate wins, however, they could covertly reveal evidence that county election systems had been compromised, creating public doubt about whether the election had been "rigged". This could easily impair the ability of the true winner to effectively govern, at least for a period of time.

Electronic voting machines and vote tallies are not the only potential targets for such attacks. Of particular concern are the back-end systems that manage voter registration, ballot definition, and other election management tasks. Compromising any of these systems (which are often connected, directly or indirectly, to the internet and therefore potentially remotely accessible) can be sufficient to disrupt an election while the polls are open or cast doubt on the legitimacy of the reported result. The decentralization of election operations, managed by thousands of individual local offices throughout the Nation (with widely-varying resources) is sometimes cited as a strength of our electoral process. However, this decentralization can be turned to the adversary's advantage. An attacker can choose arbitrarily from among whatever counties have the weakest systems—those with the least secure software or most poorly defended networks and procedures—to target.

It is beyond the scope of my testimony to speculate on specific intrusions that occurred against State and local election management systems in the 2016 U.S. general election, much of which remains Classified or under investigation. It has been reported that voter registration management systems in at least several States were targeted for exploitation and access. It is unclear whether voting machines or tallying systems were also targeted. However, targeting and exploiting such systems would have been well within the capability of any major rival intelligence service.[11]

In summary, the architecture of many current electronic voting systems, especially those that employ DRE voting machines, makes disruption attacks an especially attractive option for our foreign adversaries—and especially difficult one to effectively defend against. These systems can give hostile actors interested in disruption an even easier task than that facing corrupt candidates seeking to steal even a small local office. And the consequences of election disruption strike at the very heart of our National democracy.

IV. RECOMMENDATIONS: ALL U.S. ELECTIONS SHOULD EMPLOY PAPER BALLOTS AND RISK-LIMITING AUDITS

It is perhaps tempting to conclude pessimistically that election technology in the United States is fatally flawed, leaving our Nation irreparably vulnerable to election fraud and foreign meddling. But while it is true that the current situation exposes us to significant risk, it is by no means hopeless or beyond repair. Relatively simple, and available, technologies can be deployed that render our elections significantly more robust against attack.

While electronic voting machines do indeed suffer demonstrably fundamental weaknesses, some electronic voting technologies are significantly more resilient in the face of compromise than others. The most important feature required is that there be a reliable record of each voter's true ballot selections that can be used as the basis for a post-election audit to detect and recover from failure or compromise of the software or hardware.

Among currently available, HAVA-compliant voting products, the only systems that meet this requirement are those that employ optical scan paper ballot technology. In such systems, the voter fills out a machine-readable paper ballot form (possibly with the aid of an assistive ballot marking device for language-, visually- and mobility-impaired voters), that is then deposited into a ballot scanning device that reads the ballot choices, maintains an electronic tally, and retains and secures the marked paper ballots for subsequent audit. After the polls close, the electronic tally records are read from each ballot scanner and preliminary results calculated.

The paper records of votes that precinct-counted optical-scan systems provide are a necessary, but not by themselves sufficient, safeguard against software. As noted above, even non-DRE systems can suffer from flaws and exploitable vulnerabilities in the voting machine and back-end software. The second essential safeguard is a systematic and reliable process for detecting whether the software has reported incorrect results, and to recover the true results if so.

The most reliable and well-understood method to achieve this is through an approach called risk-limiting audits.[12] In a risk-limiting audit, a statistically significant randomized sample of ballots are manually checked by hand and the results compared with the electronic tally. (This must be done for every contest, not just those with close results that might otherwise call for a traditional "recount".) If discrepancies are discovered between the manual and electronic tallies, additional

[11] For a comprehensive discussion of technical attacks against our election infrastructure in 2016, see the Report of the Select Committee on Intelligence, US Senate on Russian Active Measures in the 2016 US Election, Vol 1. *https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf*

[12] A good introduction to the theory and practice of risk-limiting audits in elections can be found at *https://www.stat.berkeley.edu/?stark/Preprints/RLAwhitepaper12.pdf.*

manual counts are conducted. The effect of risk-limiting audits is not to eliminate software vulnerabilities, but to ensure that the integrity of the election outcome does not depend on the herculean task of securing every software component in the system. This important property is called strong software independence.[13]

Optical scan paper ballots and risk-limiting audits comprise a critical, and readily deployable, safeguard against both traditional election fraud and nation-state disruption. Taken together, they permit us to more safely enjoy the benefits of computerized election management, without introducing significant new costs or requiring the development of speculative new technology. The technology required for this is available today, from multiple vendors, and is already in use in many States.

As important as paper ballots and risk-limiting audits are, however, they are not panaceas that solve every threat to our elections. It is also critical that the State and county back-end computer networks and systems used for election management and voter registration be vigilantly protected against compromise. As we saw in 2016, hostile adversaries might attempt to breach not just voting machines, but also back-end election management systems and voter registration database systems, which are often connected, directly or indirectly, to the internet.

It is no exaggeration to observe that State and local election officials serve on the front lines of our National cybersecurity defense. They must be given sufficient resources, infrastructure, and training to help them effectively defend their systems against an increasingly sophisticated—and increasingly aggressive—threat environment. It is notable that the budgets for election administration often must compete for resources with essential local services such as fire protection and road maintenance. Election management represents only a miniscule fraction of the total National spending on political campaigns. Additional investment here will pay significant dividends for our security.

By analogy, we do not make the county sheriff responsible for defending against ground invasions by foreign military forces. Yet that is precisely the role into which we have placed our local county IT administrations in defending our election infrastructure against electronic attacks. Just by doing so, we have set them up for failure.

Simply put, much of our election infrastructure remains vulnerable to practical attack, with threats that range from traditional election tampering in local races to large-scale disruption by National adversaries. We should take no comfort if such attacks have not yet been widely detected. At best, it is only because, for whatever reason, serious attempts have not yet been made. Given the potential rewards to our adversaries, it is only a matter of time before they will.

National-level investment in safeguards such as those described above serve our democracy in critically important ways. They can provide a significant improvement to election security, both in our ability to resist attack and in our ability to recover from attacks when they occur. Perhaps most importantly, they provide meaningful assurance to voters that their ballots truly count and that their elected officials are governing truly legitimately. Our republic cannot long survive without the confidence that comes from that assurance.

Mr. RICHMOND. Thank you, Dr. Blaze.

We have votes that have been called. There is a minute and 48 seconds left on us to vote. There is still 282 people who have not voted.

But what we will do is we will go into recess right now; we will go vote. There is probably going to be 1 vote—at most, 2 votes. So we will come back and resume immediately when votes are over.

So with that we will stand in recess.

[Recess.]

Mr. RICHMOND. I will now call the committee back to order, and I will recognize Ms. Badanes for 5 minutes to summarize her testimony.

Thank you for your patience.

---

[13] See Ron Rivest. "On the notion of 'software independence' in voting systems". *Phil. Trans Royal Society A.* Volume 366 Issue 1881. October 28, 2008. *http://rsta.royalsocietypublishing.org/content/366/1881/3759.*

STATEMENT OF GINNY BADANES, DIRECTOR, STRATEGIC PROJECTS, DEFENDING DEMOCRACY PROGRAM, MICROSOFT

Ms. BADANES. Absolutely. Chairman Richmond, Ranking Member Katko, and Members of the subcommittee, thank you for the opportunity to testify today on the important topic of campaign security. My name is Ginny Badanes, and I am the director of strategic projects for Microsoft's Defending Democracy Program.

Our team works globally with a variety of stakeholders to preserve and protect electoral processes, protect campaign organizations from cyber-enabled threats, and defend against disinformation campaigns.

Microsoft has several initiatives to achieve these goals. But my testimony today will focus on our efforts to increase the cybersecurity and resilience of campaign organizations.

To address how campaigns can protect themselves, it is helpful to first understand the threats that they are up against. Campaigns face a unique challenge when it comes to securing themselves. Most campaigns have limited budgets, and even more limited cybersecurity expertise. Yet they can face outsize threats and a symmetry that can harm our democratic process.

Microsoft's work to protect campaign organizations builds upon our broader experience in assessing and tracking cybersecurity threats. The Microsoft Threat Intelligence Center, known as MSTIC, has focused on tracking nation-state adversaries for more than a decade. We provide notification to customers when an online service account has been targeted or compromised by a nation-state actor that we are tracking.

As a technology provider with many customers in this space, we believe we have an obligation to do more to support campaign's efforts to protect themselves. For that reason, we now offer services specifically designed to assist the campaign community.

In August of last year we began offering a free service called Account Guard, which provides campaign customers of our email and productivity tools with additional security support. We did this for 2 reasons.

First, we wanted to address the reality that threat actors do not only attack the enterprise accounts of their targets. They go after personal accounts of staff, as well. For that reason, Account Guard customers have the option to also enroll their personal Microsoft email accounts, such as Hotmail or Outlook. This optional enrollment provides our threat monitoring team with valuable information about what might otherwise appear to be a standard consumer account. More importantly, it allows us to notify the individual and the organization quickly if we identify a threat actor targeting that personal account.

Second, we recognize that campaigns might not be equipped to receive a nation-state attack notification. While the information can be very valuable, it doesn't serve much purpose if the recipient isn't sure what to do with the information that they receive. For that reason, in addition to informing the customer about an attack, we also include information about what to do next, especially if the attack resulted in a breach. This additional communication ensures that notifications reach the right person within the organization, and that they can turn that information into action.

We have also created a new version of our email and productivity tools just for campaigns. We did this based on feedback that sophisticated security tools aren't realistic on a campaign budget, and that setting them up was too difficult for the typical campaign IT staff. So we made Microsoft 365 for Campaigns available this past summer. This allows campaigns to access security tools at a much lower cost, and provides non-technical users with, essentially, an easy button to turn on key security features.

While new tools and free services are helpful, they don't address the most impactful thing that campaigns can do to protect themselves, and that is to educate their team about cybersecurity hygiene. That is why we provide a variety of cybersecurity trainings in person, as well as on-line, tailored to the specific needs of the campaign community. We encourage campaigns to do the basics, such as turn on two-factor authentication, use better password management, use a cloud service provider, and use secure communication platforms.

In conclusion, Congress plays a critical role in securing our campaign organizations and elections. In addition to the recommendations made by my fellow witnesses, Congress also can contribute to a multi-stakeholder approach that addresses the threats themselves. We believe that combating attacks at the root will require a joint effort, from private-sector actors such as Microsoft, as well as State, local, and Federal Governments, civil society, academia, and campaign organizations themselves.

Campaigns face the threat of capable, well-funded, and agile adversaries. While there is much they can do to protect themselves, we have seen first-hand that they benefit from assistance from the private sector, and they would certainly benefit from Congressional and Executive branch leadership and multi-stakeholder engagement, especially around establishing international norms to discourage nation-state attacks against our democratic institutions.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Badanes follows:]

PREPARED STATEMENT OF GINNY BADANES

NOVEMBER 19, 2019

Chairman Richmond, Ranking Member Katko, Members of the subcommittee, thank you for the opportunity to testify today on the important topic of campaign security.

My name is Ginny Badanes and I am the director of strategic projects for Microsoft's Defending Democracy program. We focus on advocating for and contributing to the stability and security of democratic institutions globally. In a non-partisan manner, our team works with a variety of governmental and non-governmental stakeholders in democratic countries to achieve the following goals:

- Explore technological solutions to preserve and protect electoral processes and engage with Federal, State, and local officials to identify and remediate cyber threats;
- Protect campaign organizations from hacking through increased cyber resilience measures, accessible and affordable security tools, and incident response capabilities; and,
- Defend against disinformation campaigns in partnership with leading academic institutions and think tanks dedicated to countering state-sponsored digital propaganda and falsehoods.

Though the Defending Democracy team undertakes several initiatives in pursuit of these goals, my testimony today will focus on our efforts to increase the cybersecurity and resilience of campaign organizations.

THREATS TO CAMPAIGN ORGANIZATIONS

To address how campaign organizations can protect themselves, it is helpful to first understand the threats that they are up against. Campaign organizations face uniquely challenging circumstances when it comes to securing themselves. Outside of a handful of Presidential campaigns, many campaign organizations often have limited technology budgets and usually even more limited cybersecurity expertise. Yet, they can face outsized threats, an asymmetry that can have detrimental effects on our democratic processes. Campaign organizations are like technology startups with enterprise cybersecurity needs.

Microsoft's work to protect campaign organizations and democratic institutions broadly builds upon the company's experience in assessing and tracking cybersecurity threats. The Microsoft Threat Intelligence Center (MSTIC) has focused on tracking nation-state actors for more than a decade. We provide notification to customers, including election-sensitive customers, when an on-line service account has been targeted or compromised by a nation-state actor that we are tracking. We continuously track these global threats, building this intelligence into our security products to protect customers and using it in support of our efforts to disrupt threat actor activities through direct legal action or in collaboration with law enforcement. But let's be clear—cyber attacks continue to be a significant weapon wielded in cyber space. In some instances, those attacks appear to be related to on-going efforts to attack the democratic process.

In the past year, Microsoft notified nearly 10,000 customers, including campaign organizations,[1] that they have been targeted or compromised by nation-state attacks. About 84 percent of these attacks targeted our enterprise customers, and about 16 percent targeted consumer personal email accounts. This data demonstrates the significant extent to which nation-states continue to rely on cyber attacks as a tool to gain intelligence, influence geopolitics, or achieve other objectives.

Based upon the threats we are tracking, most of the nation-state activity in recent months originated from actors in 3 countries—Iran,[2] North Korea, and Russia.[3] We have also seen activity by actors operating from China, but not at the same volume as the actors in these 3 nations. These actors have targeted a variety of industries including a number of stakeholders that are important to political dialog and democratic processes, including think tanks, universities, diplomatic entities, journalists, current and former Government officials, and campaign staff.

MICROSOFT & CAMPAIGN SECURITY

Recognizing the unique needs of campaign organizations, Microsoft offers services to help them increase their cybersecurity and resilience.

- On-line account security protection
- Security guidance, on-going education, and training
- Microsoft 365 for Campaigns

ON-LINE ACCOUNT SECURITY PROTECTION

In August 2018, Microsoft instituted enhanced cybersecurity services for campaign users of Office 365 and free consumer email services. With more than 60 million users of its paid Office365 (O365) cloud-based productivity software and free Outlook.com and Hotmail.com web-based e-mail services, Microsoft found itself in a unique position to protect election-sensitive users of its products against such hacking. To that end, Microsoft requested and received an advisory opinion from the Federal Election Commission (FEC) confirming that Microsoft may offer a package of free enhanced on-line account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers. The Advisory Opinion concluded that the provision of such services is not a prohibited in-kind contribution under campaign finance law.[4]

Until this advisory opinion, the FEC had not robustly addressed the provision of cybersecurity services to political campaigns and National committees. In response,

---

[1] New Cybersecurity Threats require new ways to protect democracy. *https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/*.

[2] Recent Cyberattacks Require Us All To Be Vigilant. *https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/*.

[3] New Cyberattacks Targeting Sporting and Anti-Doping Organizations. *https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/*.

[4] FEC Advisory Opinion 2018–11, *https://www.fec.gov/files/legal/aos/2018-11/2018-11.pdf*.

this advisory opinion sparked a series of similar requests for approval[5] from cybersecurity firms to provide cybersecurity services to Members of Congress, political campaigns, and National committees at reduced costs or at no cost at all.

The Microsoft service is called AccountGuard,[6] and it serves 2 primary functions.

(1) Cross-Account Notifications.—We recognize that threat actors do not only attack the enterprise accounts of their targets, they go after the target's personal accounts as well. We provide AccountGuard customers with the ability to enroll the personal Microsoft email accounts (Hotmail.com, Outlook.com) of staff and other affiliates of their organization. This optional enrollment provides our threat monitoring team with valuable information about what might otherwise appear to be a typical consumer account. More importantly, it allows us to notify the individual and organization quickly if we identify a threat-actor targeting that personal account.

(2) Nation-State Attack Enhanced Monitoring.—If an AccountGuard customer is targeted by a nation-state actor that we track, the team provides customers with additional services and notification. In addition to informing them about the attack, we include information about what to do next, especially if the attack resulted in a breach. This additional communication ensures that notifications reach the right person within an organization.

Since the launch of AccountGuard we have uncovered attacks specifically targeting organizations that are fundamental to democracy. We have steadily expanded AccountGuard to political campaigns, political parties, think tanks, and democracy-focused non-governmental organizations (NGO's), in 26 countries across 4 continents. While this service is relatively new, we've already made over 900 notifications of nation-state attacks targeting organizations participating in AccountGuard. This data shows that democracy-focused organizations in the United States should be particularly concerned as 95 percent of these attacks have targeted U.S.-based organizations. By nature, these organizations are critical to society but have fewer resources to protect against cyber attacks than large enterprises.

Many of the democracy-focused attacks we've seen recently target NGO's and think tanks and reflect a pattern that we also observed in the early stages of some previous elections. In that pattern, a spike in attacks on NGO's and think tanks that work closely with candidates and political parties, or work on issues central to their campaigns, typically serves as a precursor to direct attacks on campaign organizations and election systems themselves. Similar attacks occurred in the U.S. Presidential election in 2016 and in the last French Presidential election. In 2018 we detected attacks targeting, among others, U.S. Senate offices, and think tanks associated with key issues at the time.[7] Earlier this year we saw attacks targeting democracy-focused NGO's in Europe close to European elections.[8] As we head into the 2020 elections, given both the broad reliance on cyber attacks by nation-states and the use of cyber attacks to specifically target democratic processes, we anticipate potential attacks targeting U.S. election systems, campaign organizations, or NGO's that work closely with campaign organizations.

Our adversaries have a stated goal of seeking to diminish the confidence of our citizens in the processes that are at the very core of our democracy. We should anticipate that we will see more attacks on our election processes in 2020 in furtherance of this goal.

SECURITY GUIDANCE, ON-GOING EDUCATION & TRAINING

Informed by our observations about campaign challenges, Microsoft provides in-person cybersecurity trainings tailored to the specific needs of the campaign community regardless of whether there is any formal relationship with Microsoft.[9] These

---

[5] FEC Advisory Opinion 2018–15 (approving Senator Wyden's request to use campaign funds for cybersecurity expenses), *https://www.fec.gov/data/legal/advisory-opinions/2018-15/;* FEC Advisory Opinion 2018–12 (approving the provision of free cybersecurity resources to candidates and political party committees, by nonprofit corporation and its private-sector sponsors and partners), *https://www.fec.gov/files/legal/aos/2018–12/2018–12.pdf.*

[6] Microsoft AccountGuard, *https://www.microsoftaccountguard.com/en-us/*.

[7] "Microsoft Says It Stopped Cyberattacks on Three 2018 Congressional Candidates", Time, July 19, 2018: *https://time.com/5343585/microsoft-candidate-cyberattacks/*.

[8] "New steps to protect Europe from continued cyber threats", Feb. 20, 2019, *https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/*.

[9] We acknowledge these security solutions and on-going trainings depend on the campaign organizations and individuals having access to a smart phone or to broadband connectivity. Microsoft notes that broadband connectivity is also an urgent National problem that we are committed to helping solve. We've contributed to this effort through our Microsoft Airband Initiative, a 5-year commitment to bring broadband access to 3 million unserved Americans living in

Continued

trainings cover the basics of cybersecurity hygiene and highlight many of the best practices recommended by our partners at Harvard Belfer Center in their Cybersecurity Campaign Playbook.[10] To date, we've trained over 1,000 political professionals in 13 countries with our security workshop trainings.

In addition to the in-person trainings, we conduct webinars focused on specific cybersecurity topics of interest to campaign organizations. Just this week, for example, Microsoft security experts are hosting 2 webinars representative of our training efforts in this area. One helps non-technical election-sensitive customers learn how to protect their user accounts. We will cover topics such as common attack vectors, multi-factor authentication, credential hygiene, and identity best practices. The other webinar helps information technology (IT) professionals in the election-sensitive space learn technical best practices and tools available to them to secure their organization's environment.

Finally, all our AccountGuard customers receive monthly guidance from us. This guidance highlights stories of relevance, provides best practices, and promotes better cybersecurity hygiene across their organization.

MICROSOFT 365 FOR CAMPAIGNS

Campaign organizations are fast-moving environments that face significant security threats from nation-state actors and criminal scammers—much like large enterprises. However, unlike enterprises, campaign organizations often must ramp up and down quickly, vary in their ability to hire dedicated and experienced IT staff, and have unpredictable budgets.

While the AccountGuard service is a step in the right direction to help protect campaign organizations facing these challenges, we recognized that we could do more to provide this community with access to secure, reliable, accessible, and affordable software. For those reasons, Microsoft recently announced the availability of Microsoft 365 for Campaigns.[11]

First, to address the constrained budgets of campaign organizations, we have used our non-profit pricing model for this offering so campaign organizations can get access to software at a significantly reduced rate.

Second, to address the problem of ease of use for non-technical users, we have streamlined the configuration and set-up of high-impact security settings. With only a click or two, customers can now turn on recommended security features to create a secure baseline from which to operate their campaign organization.

Just a few examples of the settings that can now be automated—

- *Enabling multi-factor authentication*.—A second layer of security for sign-ins.
- *Turning on Office 365 Advanced Threat Protection*.—A service that protects emails, links, and files from phishing and malware attacks.
- *Providing device protection*.—Secures access to sensitive data on mobile devices using a service called Microsoft Intune.[12]

This offering derives from our Microsoft 365 Business product, which is tailored to small and medium businesses. That means campaign customers can now access the high-end security capabilities typically leveraged by enterprise customers, enjoy easier deployment of those features, and do so at an affordable rate.

OTHER WAYS CAMPAIGN ORGANIZATIONS CAN PROTECT THEMSELVES

While we encourage innovation in this area, campaign organizations can best protect themselves by employing basic hygiene.[13] A few examples of how that can be achieved:

- *Password management*.—In 2016, Microsoft saw over 10 million username/password pair attacks every day. This gives us a unique vantage point to understand the role of passwords in account takeovers.[14] Despite general awareness

---

rural communities by July 2022. Microsoft is partnering with a number of local providers across the United States to offer new broadband services where there is no option or affordable alternative.

[10] Cybersecurity Campaign Playbook, *https://www.hks.harvard.edu/publications/cybersecurity-campaign-playbook*.

[11] "Protecting political campaigns from hacking", May 6, 2019: *https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-political-campaigns-from-hacking/*.

[12] Microsoft InTune, *https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/microsoft-intune*.

[13] Your Pa$$word Doesn't Matter. *https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984.*

[14] Microsoft Password Guidance by the Microsoft Identity Protection Team. *https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft__Password__Guidance-1.pdf.*

of the importance of using unique passwords to secure data, users admitted to reusing the same password 62 percent of the time for multiple accounts as recently as a year ago.[15] As a result, we train campaign organizations to use strong unique passwords and more importantly, to use password managers to generate them.

- *Two-factor authentication*.—We encourage campaign organizations to use a 2-step authentication source like a phone app or a physical key for all accounts.
- *Using a cloud service provider*.—We encourage campaign organizations to leverage cloud services for email, documents, and infrastructure and avoid public or anonymous sharing.
- *Using a secure communications platform*.—For sensitive data, Microsoft encourages campaign organizations to use encrypted communications channels and avoid using public Wireless Fidelity (Wi-Fi) channels for accessing sensitive information.

EMERGING THREATS

Earlier this fall, director of the Cybersecurity and Infrastructure Security Agency (CISA), Chris Krebs drew attention to the threat of ransomware attacks against our local governments and the impact that could have on our elections if executed against voter registration systems close to, or on, election day.[16] We agree this is a risk that deserves attention from all election security stakeholders. Voter registration databases (some of the same systems targeted in 2016), are vulnerable because they are some of the only election sensitive systems that are regularly connected to the internet. We are currently exploring how we can work with Government and others in the tech community to continue to raise awareness of this threat while also providing additional solutions to protect against ransomware. Basic security recommendations in this context include using modern technology, setting up two-factor authentication for all relevant accounts, creating secure back-ups, and engaging in exercises to ensure rapid restoration of data in the event of an attack.

An additional emerging threat is the increased potential for bad actors to use artificial intelligence to create malicious synthetic media, better known as "Deepfakes". Advances in synthetic media have created clear benefits; for example, synthetic voice can be a powerful accessibility technology, and synthetic video can be used in film production, criminal forensics, and artistic expression. However, as access to synthetic media technology increases, so too does the risk of exploitation. Deepfakes can be used to damage reputations, fabricate evidence, and undermine trust in our democratic institutions. To help guard against this challenge, Microsoft has established clear principles that govern its use and deployment of synthetic media and other artificial intelligence, including fairness, inclusiveness, reliability & safety, transparency, privacy & security, and accountability. Furthermore, Microsoft has engaged with partners in academia, civil society, and industry to work together to advance best practices for the ethical use of AI. One such effort includes a recent "Deepfakes Detection Challenge" we helped launch together with Facebook and the Partnership on AI, a technology industry consortium focused on best practices for AI systems, which invites researchers to build new technologies that can help detect deepfakes and manipulated media.

WHAT CONGRESS CAN DO

When conducting trainings for political parties and campaign organizations in democracies around the world, we always encourage leadership of those organizations to attend the sessions alongside their teams. While leaders may not have a technical background, they play an incredibly important role when it comes to their organization's cyber health: Setting the culture.

Similarly, Congress plays a critical role in securing our campaign organizations and elections. By holding this hearing on the cybersecurity health of campaign organizations and the election space more broadly, the committee is contributing to the culture of security that is necessary to ensure a more secure environment.

Beyond culture-setting, Congress also can contribute to a multi-stakeholder approach to addressing the threats themselves. We believe that combatting attacks will require a joint effort from private-sector actors such as Microsoft, as well as

---

[15] See eg. Passwords Reuse Abound Recent Survey Shows. *https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689.*

[16] "CISA Director's Outlook on Ransomware", Aug 23, 2019: *https://www.politico.com/newsletters/morning-cybersecurity/2019/08/23/cisa-directors-outlook-on-ransomware-5g-more-727286.*

State, local, and Federal Governments, civil society, academia, and campaign organizations themselves.

Cyber attacks, especially ransomware attacks, are increasingly targeting State and local authorities, including for example, Atlanta (GA), Baltimore (MD), Cleveland (OH), Greenville (NC), Imperial County (CA), Stuart (FL), Augusta (ME), Lynn (MA), Cartersville (GA). Most recently there was an attack on over 20 government entities in Texas. Overall, we can reasonably expect that the situation will only get worse. Importantly, these and other attacks are increasingly leveraging sophisticated tools that are developed by governments, creating a dangerous ecosystem of cyber weapons and requiring adoption of international norms for responsible behavior on-line. Microsoft advances support for the adoption and observance of such norms.

Microsoft supports the multi-stakeholder approach taken by the Paris Call for Trust and Security in Cyber Space.[17] It reaffirms a number of norms and principles established in other forums, including at the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN–GGE), and at the G7 and G20, respectively. Importantly, the Paris Call includes a comparatively new principle to protect electoral processes from foreign interference—"Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities."

However, what truly distinguishes the Paris Call is that it recognizes that a multi-stakeholder approach is essential to achieve success. The Call has so far been endorsed by over 1,000 signatories, the largest coalition of signatories ever in support of a cybersecurity document: 74 governments, 357 civil society and public sector organizations, and 607 industry members all agreeing to 9 core principles to govern conduct in cyber space. Microsoft was one of the private-sector signatories and we will continue to advocate that all governments agree to observe the 9 principles of the Call.

While we are here today to discuss campaign organizations, we'd be remiss not to address other ways Congress can support securing our elections. In our discussions with voting officials around the country we have learned that consistent and reliable funding over time will best enable election officials to plan ahead, purchase new equipment rather than letting outdated systems remain active, and invest in the kind of cybersecurity training and staffing that we expect of all critical infrastructure owners and operators. Our adversaries are relentless and well-resourced. To ensure we can maintain defenses, our State and local voting officials need a durable source of Federal financial support so that the most secure technology can be deployed rapidly to ensure our vote is protected. The stewardship of our democracy demands nothing less.

CONCLUSION

Campaign organizations face the threat of capable, well-funded, and agile adversaries. Organizations of any size would struggle to be prepared for these challenges, but the size and nature of campaign organizations makes them especially vulnerable. There is a lot that campaign organizations can do to protect themselves. They can create a culture of cyber awareness, encourage everyone associated with the campaign organization to turn on two-factor authentication on all their accounts (personal as well as organizational), and be aware of phishing campaigns. These are the most important actions campaign organizations can take to protect themselves. But they need additional help. They will benefit from industry partners providing access to tools that support these efforts. They will benefit from NGO's like Defending Digital Campaigns and Cyberdome who can help filter and provide tools at affordable rates. And finally, they would benefit from Congressional and Executive branch leadership in multi-stakeholder engagement, especially around establishing international norms to discourage nation-state attacks against our democratic institutions.

Mr. RICHMOND. The gentlelady yields back. Thank—I want to thank the witnesses for your testimony.

I will remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for opening questions.

[17] Paris Call for Trust & Security in Cyber Space: *https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in*.

Let me start where we just finished, with Ms. Badanes. You heard me mention the Louisiana ransomware attack on our secretary of state, and it appears it was the business side of that office, as opposed to the election side.

But you mentioned in your testimony that ransomware attacks against election infrastructure—how has Microsoft seen this threat grow, No. 1?

No. 2, how can the private sector assist our local governments in securing sensitive election systems?

You mentioned the campaign, so—the infrastructure.

Ms. BADANES. Thank you for the question. This is a topic that Microsoft has been aware of for a long time, ransomware, generally, an issue. We tend to agree with Director Krebs of CISA, who has pointed out recently that ransomware attacks, if timed a couple weeks before an election or, indeed, the week of an election, could have dramatic effects on the results of the election.

As you discussed in your opening statements, it could do things like tying up the voter registration database, sowing chaos when people go to try and vote. It could also, depending on the timing, make it difficult or impossible to deliver ballots, or the ballot formats in the right—at the right time. So it is a real concern.

The reason that we address it—and why I believe Director Krebs has, as well—as a potential emerging threat, is because we have seen it happen in large and small cities in the recent past. So clearly, we have seen this in Baltimore and Atlanta, and lots of other places. Then, of course, the information that just came out this morning about what was happening in Louisiana.

So it is a big concern. It is one that we are working with our partners in Government, DHS in particular, to think through what steps can be taken to form a resilient response. Because the reality is these systems will remain vulnerable, as long as there are people trying to attack it. But if they have resilient plans in place, they can respond accordingly.

Mr. RICHMOND. Thank you.

General Taylor, over the last couple years, since 2016, we have put an enormous amount of time from this committee into looking at our election infrastructure. We learned in 2016 that our adversaries can exploit cybersecurity vulnerabilities in campaign organizations to steal information and spin a divisive narrative.

How can campaigns help serve as a line of defense against foreign influence in our elections?

General TAYLOR. Well, thank you for the question, Mr. Chairman.

I think the important thing is recognizing that they are a target, first, and that they need to invest in cybersecurity. Part of what U.S. CyberDome is attempting to provide to them free of charge is expert-level capability to protect themselves.

As I mentioned in my remarks, campaigns are not built to—with cybersecurity expertise. They—and the nature of the threat that is coming at them requires a very sophisticated understanding of how that threat is manifesting itself. That can only be done by security experts, cybersecurity experts, and campaigns just don't have those kinds of people, routinely. They are startups only together for 1 or 2 years, at most, and can't invest in those kinds of capabilities.

Mr. RICHMOND. Thank you. Mr. Stengel, in the beginning of your book you stated that disinformation doesn't create divisions, it amplifies them. We know the Russians' influence of campaigns fed off of conflict, manipulating discussions on race relations, gun control, global warming, among others, to turn Americans against each other.

How do we equip voters to understand when public debate is being manipulated by the Russians or some other adversary to undermine U.S. interests?

Then the second part of that would be how can we de-politicize the conversation about disinformation and foreign-influenced campaigns all together?

Mr. STENGEL. Thank you for that question, Mr. Chairman. In my book I talk about what the Internet Research Agency did in the last few weeks, in particular before the election, where they focused on African American voters.

What I meant about that disinformation doesn't create division, it amplifies it, they were trying to get African American voters not to vote. There was a bunch of tweets to people who followed the site that they created, called Blacktivist, which was created, of course, from St. Petersburg, to black voters saying, "Don't wait in line to vote, vote at home." They were trying to get black voters not to vote. They were trying to get voters to vote for minority candidates. Joel Stein, for example.

So they can suppress people's votes, they can increase enthusiasm or decrease it. They are not really going to change people's minds.

Again, the issue of disinformation is one that people have to be aware of. The first line of defense is the fact that we are actually talking about it now, and that people have to be skeptical of the information that they get, and they need to have some kind of media literacy, where they check the information against other sources. Ultimately, that is what the Russians try to do, not so much get people to believe their point of view, which they don't have, but to make them doubt the voracity of everybody else.

Mr. RICHMOND. Thank you. My time is up. I will yield back, and I will now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Katko.

Mr. KATKO. Thank you, Mr. Chairman, and thank you all. I have about 30 minutes of questions, but I know I only have 5, so I will get through as much as I can.

Ms. Badanes, a lot of questions I would like to ask you, but first of all, on your computer laptop you have a sticker that says, "Protect 2020." Could you briefly explain what that represents? Because I know what it does. What was Microsoft's interaction with 2020, if anything?

Ms. BADANES. Sure. Well, I have a couple stickers here that were actually produced by DHS with CISA. Protect 2020 represents an initiative by lots of different stakeholders. To protect our elections we need participation from governments, private sector, academics. It is really going to be a collaborative effort.

So they are very generous with giving out their stickers, so that all of us who are part of that effort can display how much we care about this.

Mr. KATKO. What is Microsoft's role in that effort?

Ms. BADANES. We have a variety of initiatives. We have some security initiatives, obviously, for campaigns, as I mentioned in my opening statement. But we also do work around election security. We actually have an open source software development kit, where we are inviting people to come in and use it in their elections, to ensure that a voter's vote makes it all the way through. So we have several initiatives that we are doing.

We try and identify places where Microsoft fits, where our resources and our knowledge and people are a good fit to fill some gaps.

Mr. KATKO. It is a free tool that local election officials can use. But is it fair to say we only have about 25 percent of the local official agency—election agencies using that tool?

Ms. BADANES. Currently, it is not used by anyone. It is an open source, and we want to have some pilots.

Mr. KATKO. I am thinking of something else, then, I am sorry.

Ms. BADANES. OK.

Mr. KATKO. Whatever it is. But I know something with CISA, where 25 percent of the people are not taking up with CISA's free assistance——

Ms. BADANES. Oh——

Mr. KATKO [continuing]. To give them assistance with their local elections. That—I am concerned that—why they wouldn't be taking up—it is a free advice, and they get free notification updates as to security vulnerabilities, and they are not using them. I just—for the life of me, I can't understand why.

Ms. BADANES. I am not sure.

Mr. KATKO. Yes, OK. Well, Mr. Blaze, I know we have had some discussions with you in the past, and you have described the election security vulnerabilities as follows. Basically, no matter what we do, it is never going to be perfectly secure, but there is ways you can minimize the risks.

So obviously, making sure the machines that actually do the tabulation are off-line, and they have a separate, verifiable way—usually it is through paper, but maybe some other ways, as well, but generally through paper—so we have a recording of the actual vote.

Then, you want—I think you said in your testimony, and I have heard you say it before—the risk-limiting audit is a great tool to go back and do. Now, the concern I have is something General Taylor mentioned, and some others alluded to. A lot of these local election agencies don't have the funding to do what we need them to do. So I would like to hear from you all as to what we should be doing in that regard, because whether it is a risk-limiting audit or other types of audits you can do afterward, having the paper trail and going back and doing the spot checks, to me, is the only way to really ensure the integrity of the numbers and the tabulations.

Some jurisdictions are better than others. But again, a lot of them do not participate—are not able to do this. So what can we do to fill that gap? I would like to hear from any of you.

Mr. BLAZE. So I will start off by saying that I agree with you completely, and there is wide variance among the thousands of election administrators throughout the country in capability and funding and interest.

You know, one thing that we can do is, you know, infuse funding specifically to replace voting equipment with those that use paper ballots to conduct risk-limiting audits, to share experience——

Mr. KATKO. The problem is, I think—I don't want to interrupt you, because we are short on time, but—a lot of jurisdictions will get the funding, but they will choose not to do risk-limiting audits, they will put it into hardware.

So what—just briefly, if you can, I want to give the others an opportunity, as well—what can we do?

Mr. BLAZE. Right.

Mr. KATKO. What should we be doing?

Mr. BLAZE. Well, we have to recognize in any funding initiative that the audit step is at least equally important.

Mr. KATKO. OK, OK.

Mr. BLAZE. That is absolutely critical.

Mr. KATKO. OK. Mr. Stengel, General? Anybody want to add anything to that?

Mr. STENGEL. No, go ahead.

General TAYLOR. You know, I think of this, Mr. Katko, as—I look at the defense industrial base and how long it took that organization, those organizations to really kind-of realize what the threat is. I don't think—I think this is a long-term strategy. I think the investment that you have made in funding for CISA's election security is a huge step in the right direction.

I think they have done an excellent job of getting the confidence of the Secretaries of State. I think, over time, that will filter down. But it is a long, tedious process. But as we set the standards and best practices, I am confident it will roll to the—to every level of our election infrastructure.

Mr. KATKO. OK. Anybody like to offer——

Mr. STENGEL. I would only say I am the disinformation guy, not the campaign security guy.

[Laughter.]

Mr. STENGEL. While you can harden election voting systems, it is very hard to harden anything to prevent disinformation, in part because people welcome it. It is part of confirmation bias.

Mr. KATKO. Right. That is part of the problem here. People have to understand that there is election interference, but that—which we know is going on right now, and that is what you are trying to stop.

But then we also have what we are all concerned with, is them actually hacking into the tabulations. We haven't seen that yet, and that is what we are trying to guard against. They are certainly trying to do it, and that is why we need to have these risk-auditing procedures, to make sure that those numbers have integrity.

But I thank you all and yield back the balance of my time.

Mr. RICHMOND. The gentleman from New York yields back. I will now recognize the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for your testimony today.

There is certainly no greater responsibility we have than to protect our elections, if we are going to protect our democracy. I appreciate the work you are doing in helping us to get to a better place.

Mr. Stengel, I will start with you, if I could. In your testimony you mentioned that—the rise of domestic disinformation is becoming an even greater threat than external disinformation campaigns, as we approach 2020.

So I wanted to ask you, and you can please elaborate, on why you are saying domestic disinformation is becoming a threat now, and why you assess it a greater threat and scope than the external campaigns like the Russian interference that much of the focus has been on.

Mr. STENGEL. So one of the organizations that I am affiliated with is the Digital Forensics Lab at the Atlantic Council, and they evaluate that there has been a very large increase in domestic disinformation.

When you think about it, even if you talk about the 100,000 items that the Internet Research Agency placed on Facebook, or the more than 10 million tweets, it—they—it gets leverage, and it gets virality from Americans, not from other Russians. Yes, the Russians have a bunch of bots, but all of this is picked up by American users, and then it is amplified, and that creates the volume, domestically, which is actually larger than the disinformation that is created by the Russians and other actors.

Mr. LANGEVIN. But was it started externally and just—are you saying amplified it internally, or are you talking about it is——

Mr. STENGEL. Yes, so——

Mr. LANGEVIN. Generated by some organized internal effort?

Mr. STENGEL. It is—the foreign stuff is started externally, and then it is amplified internally. But there is plenty of domestic disinformation from all kinds of fringe groups on the right and the left, and a lot of experts believe that the domestic space—domestic disinformationists will actually ultimately dwarf the foreign disinformationists.

Mr. LANGEVIN. So in your testimony—continuing on with you, Mr. Stengel—you testified that democracies just aren't very good at combating disinformation. I certainly—I agree. One of the things that I focused on, along with one of our new Members of the subcommittee, Ms. Slotkin, is building resilience to disinformation, much as we have built resilience to cyber attacks or acts of terror.

So can you please elaborate on how you believe we can build resilience? What does digital literacy education look like? How can we teach digital literacy to Americans of all ages, including older Americans who are already out of school?

You know, I understand the idea of, you know, debate and discourse, but this is something different than we are talking about. How do we build in this resilience to disinformation?

Mr. STENGEL. Yes, I mean, the—I agree with the thrust of your question.

One of the things I found in Government, as a person who used to create content, is that countering content by us is often counterproductive. People are not receptive to it, and we are the enemy that they are already attacking.

I do think digital literacy and information literacy is something that should be taught in the schools. I suggest that, actually, the platform companies should be financing those kinds of lesson plans. There are a number of organizations, non-profits, that teach digital

literacy and media literacy. I think, in the future, we will look at the fact that we didn't teach this in schools as silly as not teaching computer programming.

So part of it is this—the resilience is to make people a little bit more skeptical. I think the fact that we are talking about it, about disinformation in general, is the first line of defense because it makes people a little bit wary of the information that they do get. That is, in fact, a good thing.

Mr. LANGEVIN. Critical thinking is the—I think the key here. But thank you for that perspective.

Dr. Blaze, Professor Blaze, good to see you again. You mentioned in your testimony that hostile state actors can be particularly formidable, because their goal may simply be to disrupt an election or call into question its legitimacy, instead of electing a particular candidate. I agree with that concern.

Unfortunately, we know that Russia succeeded in causing voters to lose confidence in the election system in 2016. What steps can we take to maintain voters' confidence in our elections, even in the case of disruption? How can we restore lost confidence in our system? Are these solutions largely technical, or are there policy or strategic communications avenues that we should be pursuing?

Mr. BLAZE. Well, certainly there are, you know, policy components to all of this. My expertise is on the technological things we need to do.

What I would strongly advocate is that we harden the systems as best we can so that, by the use of things like hand-marked paper ballots and risk-limiting audits conducted routinely, election officials have a good answer when people question the legitimacy of the outcome. We can say we are doing rigorous techniques that give us high assurance and high confidence in the outcome of the election, in spite of the inevitable weaknesses and inevitable attacks against them.

Similarly, we need to harden things like voter registration databases, procedures for handling provisional ballots and so forth, so that when disruptions occur, we can recover from them quickly enough so that there is no question about whether people were able to vote in the first place. Those are, you know, critical technical safeguards that serve as a foundation for the policy initiatives that you discussed.

Mr. LANGEVIN. Thank you. I know my time has expired, but thank you all for your testimony here today. Your perspective is very helpful.

Thank you, Mr. Chairman. I yield back.

Mr. RICHMOND. The gentleman from Rhode Island has yielded back. The gentleman from Texas, Mr. Taylor, is now recognized for 5 minutes.

Mr. TAYLOR. Thank you, Mr. Chairman. I appreciate the witnesses being here.

Professor Blaze, I really appreciated your testimony. I just wanted to ask one question. So you are recommending that we go to a paperless—recommend we get rid of paperless DRE voting machines and go to precinct-counted optical scan ballots. So that is your recommendation, right?

Mr. BLAZE. That is correct. I should point out that is not merely my recommendation.

Mr. TAYLOR. Oh, sure.

Mr. BLAZE. A National Academies report represents the consensus of experts on this, the foundation of that——

Mr. TAYLOR. If—what is a realistic projection to try to implement that at the Federal level? I mean, is that something we could do for the next—for the primaries in March? Is that something we could do for the general election next fall? Is that something that we could do over a 4-year period, 6-year period? Do you have any projection for kind-of what would be a reasonable time frame to get that done?

Mr. BLAZE. Some States are already using the technology that is needed, so that is great. Other States are not. There is certainly some lead time in—for purchasing, for training, and for ultimate deployment.

You know, I think, certainly, the primaries—for any State not using that equipment right now, the primaries are a pretty aggressive goal to have.

The general election is also an aggressive goal, but it is not one that is out of the question to achieve, if we have a—if we have, as we should, a strong interest in doing so.

Mr. TAYLOR. But—OK. Maybe—if you haven't put pen to paper, I am not trying to put you in a box. Have you put pen to paper on this, or is this just kind of a recommendation?

Mr. BLAZE. Well, it is—you know, it is highly variable from jurisdiction to jurisdiction. So it is hard to generalize about how to deploy it——

Mr. TAYLOR. You are fine. Again, I am not trying to put you in a box. Just—different people have different ideas on how long it takes to do these—some of these things, and some of them are really—it is a big ask, right, to do every voting machine in America and change it over?

I appreciate that you haven't—I think it is probably fair you don't know, which is fine. I don't know, either. But I think I would certainly want to give it a few years to try to do something of this magnitude.

Your comments on voter registration on page 3 of your written testimony, there is an implicit supposition within a voter registration—that you are saying that voter registration is important. Is that a fair statement?

Mr. BLAZE. Certainly the integrity of the voter registration databases is absolutely critical to conducting——

Mr. TAYLOR. OK.

Mr. BLAZE [continuing]. High-integrity elections.

Mr. TAYLOR. So, you know, in my home State of Texas, we require—people can mail in voter registration, but they actually have to vote in person and be verified that it really is a human being, and not, you know, someone trying to steal an election by mailing in 100 voter registrations and get 100 mail-in ballots, and then fill those back in.

So a system of voter—so we have voter registrars in Texas. We—so we have a series of checks to try to make sure there isn't fraud,

which I assume you would believe would—fraud undermines a belief in the election system. Is that a fair statement?

Mr. BLAZE. Absolutely. I think we are fortunate that studies have shown that fraud at the individual voter level is, fortunately, quite rare.

Mr. TAYLOR. Well, that may be your experience, but certainly not mine.

So what I—but just going back to trying to stop fraud, so again, in Texas we have a very—a system for trying to stop fraud on a voter registration basis. Do you think we should throw out that system? Should we throw out the voter registration systems in all the States, and sort-of let people register however they would choose?

Mr. BLAZE. Well, you know, I certainly think that making it easy for people who are authorized to vote to become part of the voter rolls is a critical function of any election system.

Mr. TAYLOR. Does it make sense to have——

Mr. BLAZE. And——

Mr. TAYLOR [continuing]. Some mechanism——

Mr. BLAZE. And——

Mr. TAYLOR. Does it make sense to have a mechanism to make sure that voters are really voters, and not people trying to steal elections?

Mr. BLAZE. That is certainly one of the roles of each State, to——

Mr. TAYLOR. So that is a yes?

Mr. BLAZE [continuing]. To perform.

Mr. TAYLOR. It makes sense to stop people from stealing elections, or we should just throw open—get rid of the registrar system in this country and let anybody who wants—let anybody register anybody?

Mr. BLAZE. Well, it ultimately is a risk management question. So I think, in order to properly answer that—and it is, you know, a bit outside of my own expertise—we would have to, you know, weigh the expected amount of fraud, which, as I understand it, is relatively small, but that is, again, not my area, against the benefit of making it easier for people to vote.

Mr. TAYLOR. So should we get rid of States' provisions for protecting the voter registration system or not?

Mr. BLAZE. Well, the—you know, I think——

Mr. TAYLOR. That is a yes-or-no question.

Mr. BLAZE. I will defer to the National Academies study on the precise recommendation——

Mr. TAYLOR. So you don't know?

Mr. BLAZE. [continuing]. Managing voter registration databases.

Mr. TAYLOR. What do you——

Mr. BLAZE. I am here to discuss—and my expertise is on—the technical protections——

Mr. TAYLOR. But your—you are testifying in writing that you think that voter registration is important to protect, right?

Mr. BLAZE. Absolutely.

Mr. TAYLOR. OK. Should we have laws to protect that, or not?

Mr. BLAZE. Well, of course, we should have laws to protect that.

Mr. TAYLOR. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. RICHMOND. The gentleman's time has expired. I now recognize the gentlewoman from Illinois, Ms. Underwood.

Ms. UNDERWOOD. Thank you, Mr. Chairman. I am really excited to take part in this committee's third hearing this Congress centered on election security. I greatly appreciate the commitment and leadership shown by both Chairman Thompson and Chairman Richmond, who recognize the present and growing threat foreign adversaries pose to our most sacred democratic institutions.

On-line disinformation is one of those growing threats as we approach the 2020 election. Last year, for the first time ever, more Americans got their news from social media than they did from print newspapers.

So to Mr. Stengel, what should social media companies be doing to prevent attempts to sow disinformation on their platforms, and are they doing it?

Mr. STENGEL. Yes, I would just note that you can get news from the *New York Times* and the *Washington Post* on your phone, as well.

But I do recommend—and I wasn't explicit about it in my testimony, but I think amending the Communications Decency Act, particularly section 230, to give the platform companies liability for the content that they publish.

Right now they are not considered publishers. They have complete immunity from everything that they have. As I say, they can't have the same liability that a newspaper has, or a magazine, just in part because of the volume. But they need to make a good-faith effort, a reasonable effort, to take off different types of content that violate their terms of service. I would argue hate speech, demonstrably false speech, deep fakes don't have a role in our elections.

Ms. UNDERWOOD. And——

Mr. STENGEL. They need to have liability for taking that stuff down.

Ms. UNDERWOOD. OK. So my constituents, like many others in the country, want to learn more about how they can increase their social media literacy. So could you answer this question that was submitted by one of my constituents?

Can you clearly describe the difference between misinformation and disinformation?

Mr. STENGEL. Yes. I would define the difference as follows: Disinformation is deliberately false information meant to deceive; misinformation can be just a mistake. It is not necessarily deliberate, although it can be. Disinformation is the much more dangerous and damaging version of that.

Ms. UNDERWOOD. From your point of view, it is the disinformation that is being used by the foreign adversaries on the social media platforms.

Mr. STENGEL. Yes, the Russian disinformation, which we are very familiar with, was false information designed to deceive. Part of the reason disinformation is effective is it often has a kernel of truth in it. It is not completely made up out of whole cloth, it is a combination of fact and fiction.

Ms. UNDERWOOD. Mr. Blaze, thank you and DEFCON Voting Village for organizing the informational briefing last month for Members of Congress. I appreciate your efforts to call attention to the

security gaps present in way too many of our voting machines used across the country.

What more do you believe voting equipment vendors need to be doing to reduce vulnerabilities?

Mr. BLAZE. Well, first of all, thank you so much for having us.

The—you know, ultimately, vendors have 2 roles here. First is it is critically important that they be responsive, and welcome reports of vulnerabilities and reports of bugs and problems in their system, and rapidly turn that around into defenses against those well-known vulnerabilities. We have seen the—since 2007, the same vulnerabilities present in deployed systems used for live elections, and there is really no reason that those cannot have been fixed by now.

But second, vendors—I would urge vendors to produce systems in accordance with the recommendations of the National Academies study, which very firmly reject DRE technology that is still being produced, still being sold by the major voting vendors, even though we understand that it cannot be adequately secured, and we cannot perform risk-limiting audits on it.

Ms. UNDERWOOD. Thank you.

Mr. Stengel, as a former senior State Department official, you have been on the front lines of dissecting and analyzing how foreign governments and other non-state actors are weaponizing information. We also just heard the Ranking Member inquire about the appropriations, and how much money the Federal Government is appropriating.

In a field hearing in my district last month we had an expert sitting on a panel like this testify that the United States would need to spend $2.2 billion in order to properly secure Federal elections ahead of 2020, and we have seen news reports of Senator McConnell being willing to appropriate 10 percent of that, $250 million.

Based on your expertise, do you feel this administration's response and preparations for the upcoming 2020 election are sufficient? If not, what improvements would need to be made?

Mr. STENGEL. Again, I am not an expert in election security, but from—even from the premise of your question, I think we don't spend nearly enough on election security. In fact, we don't make elections easy for people to vote in, whether that is changing the date to a weekend, whether that is opening several days.

I do think it is quite extraordinary, when you think of the—you know, the marketing budget of a company like Proctor and Gamble, it is probably $25 billion, and we spend less than $1 billion on our own election, it shows what we value and what we don't value.

Ms. UNDERWOOD. Sure. The 2020 election is now less than a year away, and we must not be caught off guard. I appreciate all the witnesses for being here today to offer your recommendations and work to ensure elections are secure.

I yield back.

Mr. RICHMOND. The gentlelady from Illinois has now yielded back. I will now recognize the gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you, Mr. Chairman, and thank you to the full committee Chair, Ranking Member, subcommittee Ranking Member. This is a very important hearing.

It is good to see you again, Mr. Stengel, and thank all of you for your work here in the—here at the—in the Government, Federal Government, that some of you have worked in in the past.

Let me say how serious this hearing is. Probably to ensure that democracy thrives, we probably need to have these meetings almost every other day.

Let me frame my questions from the perspective of 2 points that I want to make. It is general knowledge, and in the recent impeachment investigations even stated, that Russia intends to investigate—excuse me, to interfere with the 2020 elections.

Mr. Stengel, I just want to go to you, having experience in the State Department, and being an avid expert on international issues. Do you have any knowledge of Ukraine's involvement in the 2016 election?

Mr. STENGEL. I do not.

Ms. JACKSON LEE. Do you have knowledge of the—in the general arena of information—that the intelligence community documented that Russia interfered in the 2016 election?

Mr. STENGEL. Yes. I mean that is absolutely indisputable, and we saw that both from Classified sources and non-Classified sources.

Ms. JACKSON LEE. So let me go to General Taylor. Thank you very much. Let me go to General Taylor.

Thank you, welcome. It is good to see you again. I have been on this committee since the heinous act of 9/11. I have seen superior [sic] and consistent Secretaries of Homeland Security. We may have had a policy difference here and there, but I have seen the Department take its rightful role in securing the Nation.

Certainly we know that we can improve from 2016, but tell me what the state of DHS is as we go into the 2020 elections, in terms of its capability, staffing, leadership on this very vital issue of election security, in your opinion.

General TAYLOR. In my opinion, Congresswoman, the most heartening thing I see in DHS around this issue of election security is CISA, and the investment that this committee has made in making CISA more capable of addressing this issue, and the work that CISA has done to build confidence in the secretaries of state, and down to the State and local election officials. So——

Ms. JACKSON LEE. Do we have the staffing and the orderliness that we need, going into 2020, in this Department now?

General TAYLOR. I think we have a huge start. But as you have mentioned, this is—to me, this is the same issue we face as we left 9/11. This is not going to happen overnight. It is going to happen with consistent investment over time, and confidence-building in our State and local officials that the Federal Government is here to help, not necessarily to get in the way.

We have done that on counterterrorism. It has taken 15 years. We can do it on election security. I think CISA is well on its way to getting that——

Ms. JACKSON LEE. You feel the staffing presently—I don't know if you have access to——

General TAYLOR. I do not.

Ms. JACKSON LEE. So you cannot comment on the staffing that we presently have in DHS——

General TAYLOR. I can only comment on the investment this committee——

Ms. JACKSON LEE. Right.

General TAYLOR [continuing]. Has made——

Ms. JACKSON LEE. But not on the implementation.

General TAYLOR. Correct.

Ms. JACKSON LEE. Thank you. Let me—thank you very much.

Let me—Dr. Blaze, your expertise in what could happen, let me ask you whether you feel comfortable as to whether or not we are actually prepared for a disruption that we might not expect.

I am introducing something called the failsafe elections bill that deals with paper ballots and other issues. But, in particular, it is to secure the technology, the attentiveness to the question of what could happen that were not expected. If you would—if I could yield to you on that question.

Mr. BLAZE. Well, I will say that, of course, we don't know what we don't know.

But I will say that one thing we do know is that if there has not been a large-scale disruption or attack against our election infrastructure that has been successful, it is not because our systems are robust, but rather because nobody has seriously tried to do it.

I think it is only a matter of time before our national adversaries turn their resources in earnest on us, and——

Ms. JACKSON LEE. Give us one thing—and so 2020 might be the year. We don't know. Give us your 1 or 2 that we really need to deal with in this short period of time, as we move to 2020.

Mr. BLAZE. Vastly increased resources to protect State and local election infrastructure, rapid deployment of paper ballot voting machines, and risk-limiting audits.

Ms. JACKSON LEE. Mr. Stengel, my last point on the disinformation, I just want to be clear on what you said, because, as you well know, in past elections African Americans have been told that the election day is on Saturday, and in actuality it was on Tuesday. Absolutely disinformation to oppress, suppress the vote.

Did you say that disinformation, the provider's obligation to take it down, they should be liable for it? Was that what you were saying, or——

Mr. STENGEL. I think disinformation——

Mr. RICHMOND. The gentlelady is out of time. I will permit you to answer the question.

Mr. STENGEL. I think disinformation, which is deliberately false information that is meant to deceive, if it is proven false, if it is indisputably false and meant to deceive, yes, the platform company should take that down.

Ms. JACKSON LEE. Thank you so very much. I yield back.

Mr. RICHMOND. The gentlelady yields back. We will do a second round of questioning, and I will yield 5 minutes to myself.

General Taylor, Congresswoman Underwood asked the question of if we are doing enough, or if the administration and the Federal Government is doing enough on election security. Would you like to weigh in on that?

General TAYLOR. As I said in answering Ms. Jackson Lee's question, I think we have begun a process that is going to take time

to build the confidence in State and local election officials that we can benchmark each other and improve the cybersecurity status of our election systems.

I have a great deal of confidence in Mr. Masterson over at CISA, and the work that he has done since he has been leading the election security effort there. I think it is developing good fruit. It is not—nowhere near where it needs to be over time.

I don't think this is one—again, I think of it from a war on terrorism point of view, and it took us almost 15 years to develop the capacity to do what we have done here since 9/11. So I see it in that vein.

Mr. RICHMOND. Ms. Badanes, let me ask you. In October Microsoft reported significant cyber activity by a threat group you called Phosphorous, which targeted a U.S. Presidential campaign. Can you tell us more about that cyber activity? No. 1, how Microsoft found out about it, and No. 2, what did you do with that information?

Ms. BADANES. Sure. There is a group at Microsoft called Microsoft Threat Intelligence Center. We call them MSTIC. For the last 10 years they have been, essentially, hunting nation-state adversaries. They track a lot of their behavior and identify if they are attempting to target any of our customers.

So recently they noticed that a group that we call Phosphorous, as you noted, who operates out of Iran, was targeting the individual personal consumer accounts of a lot of very interesting targets. They were current and former Government officials, members of the media, and, as you mentioned, a staffer for a Presidential campaign.

Once they were able to confirm that information, and make sure that what they were seeing checked out with a few other sources, they then started notifying. So we notified the individuals who had been attacked, provided them with actionable information—in many cases, things that they could do to check their own logs themselves. Then we notified our friends and colleagues in Government to let them know the activity we were seeing.

Then, the final step we took was actually talk about it publicly. We put out a blog post, where we described the action we were seeing, because we thought it was very important to be transparent when we see that kind of activity, especially the kinds of customers they were targeting.

Mr. RICHMOND. Thank you. Let me ask the panel just some general questions. If you could just say yes or no, it would be very helpful.

No. 1, it is universally agreed without much contradiction that Russia did, in fact, meddle in the 2016 Presidential election. Would you agree?

General TAYLOR. Yes, sir.

Ms. BADANES. Yes.

Mr. BLAZE. Yes.

Mr. STENGEL. They didn't meddle; they attacked our infrastructure and the core of our democracy.

Mr. RICHMOND. Agreed. Second, and there are nation-state actors, and there are a lot of people out there that are trying to affect

the 2020 election, from infrastructure to disinformation to our very voting machines. Would you agree with that?

General TAYLOR. Yes.

Mr. BLAZE. Undoubtedly.

Ms. BADANES. Yes.

Mr. STENGEL. Yes, and the Senate Intelligence Committee report said the Russians have done more since 2016 than they did leading up to 2016.

Mr. RICHMOND. Would you also universally agree that the Federal Government has not put the resources there to combat and protect our very democracy that depends on fair, free elections, where every vote matters?

Mr. STENGEL. Yes.

General TAYLOR. Yes.

Mr. BLAZE. Yes.

Ms. BADANES. More could certainly be done.

Mr. RICHMOND. Then let me ask you another question, because it always comes up from people about this rampant action by individual citizens to go vote who are not voters, and that there is some alleged rampant election fraud perpetrated by individuals.

Has anyone seen or aware of a rampant effort by U.S. citizens to vote who may not be qualified to vote, or election fraud?

Mr. STENGEL. No.

General TAYLOR. Not that I have seen.

Mr. BLAZE. Not that I am aware of.

Ms. BADANES. It is not my area of expertise, but no.

Mr. RICHMOND. I will just close with this. It is very important for the people in this country to believe in the elections that we have, and that the person who wins is the person who was supposed to win, and received the most votes in the regular election, or, in the case of a President, did in fact win the State so that they could win the electoral college.

I want to thank you all for what you all are doing, the effort that you are putting forward, to make sure that you offer your subject-matter expertise to how we protect our elections, how to make sure they are fair, how to make sure the winner is the winner. So I just want to thank you all for coming.

With that I will yield back and yield to the Ranking Member of the full committee, Mr. Katko.

Mr. KATKO. Thank you, Mr. Richmond. Those are great questions, I think, and they establish how serious the predicament we are in right now.

A couple of quick questions for Mr. Blaze. If you can keep your answers really short, then I got a question for everybody. Mr. Blaze, just a point of clarification. About what percentage of voters in the United States have a paper ballot to—back-up system?

Mr. BLAZE. That number has, fortunately, been increasing. I don't have the precise number at my fingertips. I believe there are something like 19 States, currently, that don't use any form of paper.

Mr. KATKO. OK, all right. I wanted to just have you briefly explain what a risk-limiting audit is, and what the costs are involved in a risk-limiting audit.

Mr. BLAZE. All right. I will be as brief as I can. Essentially, a risk-limiting audit is a statistical technique for sampling ballots and comparing, by a human observation——

Mr. KATKO. After the election——

Mr. BLAZE. After the election, comparing by human observation what is printed on the ballot with what was recorded.

To the—as you see more ballots that match, you gain more confidence that the machine tally showed you the correct election outcome. If you see mismatches you have to look at more ballots and compare them.

Mr. KATKO. The risk, of course—the problem is a lot of the local election districts simply don't have the manpower or the funds to do that. Correct?

Mr. BLAZE. That is right. Manpower, funds, experience, and mandate.

Mr. KATKO. OK. Now I want to ask a question for all of you, and I think I will start with Mr. Stengel, because you kind-of alluded to this a little bit, that Russia is, in particular, is refining their efforts in this regard.

How has Russia's strategies evolved with respect to election interference in 2016, and what should we be most concerned with with what they are doing now that they didn't do in 2016?

Mr. STENGEL. Yes, I don't know the answer to the question of how—of what—of how the Russian strategy has evolved. What I do know is that the platform companies have taken down extraordinary amounts of content.

There was an extraordinary story this past week that Facebook had eliminated 5.4 billion—that is B, with a B—fake accounts. I don't know how many of those were Russians, but certainly a significant number.

The reporting that I have read about this—and I don't have access to the same intelligence I used to have—is that they are doing more microtargeting this time. They are looking at voters where there is already existing divisions, and trying to widen them and, again, sowing doubt about the integrity of the election. That is their ultimate goal.

Mr. KATKO. OK. Anybody else want to add to that?

General.

General TAYLOR. I agree. I think the one thing I learned in 40 years of intelligence, if something works well, keep at it and get better at it. I think that is what the Russians learned in 2016, and they have—their efforts have continued to evolve to get more sophisticated and more effective.

Mr. KATKO. OK. Ms. Badanes, anything you want to add to that, or——

Ms. BADANES. All I would add is it is important to note that they are likely not the only player in the game this time around. So, while the strategies of one adversary are important, from the protection standpoint the tactics are a lot of what we look at, how campaigns and election officials protect themselves regardless of who is coming after them.

Mr. KATKO. OK. So what have we done better that we didn't do in 2016? What have we done—we, being the election officials in the

Federal Government—to help with the election officials? What have we done better?

What—and then, last, what else can we do? So you can add that——

General TAYLOR. I will start. When Secretary Johnson indicated that the election infrastructure would be part of our—critical infrastructure was the first step. I think the investment that Congress has made in CISA and CISA's activities, and the confidence that they built among state—secretaries of state has been a huge step forward from where we started.

I think you will recall when Secretary Johnson first designated elections as critical infrastructure, the pushback from the States was pretty significant. I think we have built a lot more confidence that the Federal Government is truly here to help, not to dictate how elections are run.

Mr. KATKO. Anybody else want to add to that?

Ms. BADANES. I would just add that the communication amongst all the stakeholders has vastly improved. We recognize that in 2016, a lot of time, if something happened in a municipality, they didn't know who to call. They didn't know who to call at the FBI, DHS. If it was a platform company or a tech company, they weren't sure who to reach out to.

Those communication lines are much stronger. There have been many tabletop exercises and other activities to ensure that people know how to respond if and when something does occur.

Mr. BLAZE. I will add to that that there is now consensus from technical experts on precisely what to do that didn't exist at the time the Help America Vote Act was passed. We are—have the benefit of pretty clear guidance from the National Academies report, for example, on precisely how to introduce new resources to better protect our elections.

Mr. STENGEL. I would only say that, in combating disinformation, which is different than what we are talking about here, I am not aware of anything that Congress or the Federal Government has done to combat disinformation.

Mr. KATKO. OK. I would yield back the balance of my time. Thank you.

Mr. RICHMOND. The gentleman from New York yields back. I now recognize the gentlewoman from Illinois, Ms. Underwood, for 5 minutes.

Ms. UNDERWOOD. Thank you, Mr. Chairman.

In Dr. Blaze's written testimony, you outlined a series of technical observations about the election infrastructure that we have in our country. I just wanted to just drill down on this point.

Which do you think is the most vulnerable, ahead of 2020?

Mr. BLAZE. Well——

Ms. UNDERWOOD. For a cyber attack.

Mr. BLAZE. Right. So I think the—aside from the voting machines, which have been discussed quite a bit, the protection of back-end infrastructure, particularly the voter registration databases that are used to produce the poll books that voters check in with on Election Day, are utterly critical to protect, and we have, literally, thousands of different election administrators all protecting them in slightly different ways.

Ms. UNDERWOOD. That is so alarming to me. I am from Illinois. I represent a community in northern Illinois. That was exactly what got hacked for us in 2016. It was the on-line voter registration systems and some 76,000 Illinois voters, whose information was compromised.

OK. So in General Taylor's written testimony, you went into some minimum standards for campaign cybersecurity. In your written testimony you said that there should be an incentive to spend certain dollars across the board amongst campaigns to incentivize each campaign to make those investments.

I am just wondering if you wanted to expand for the committee about what you think that type of incentive should look like, or what those campaigns should be investing in, more specifically.

General TAYLOR. Well, specifically, what I am referring to there is the fact that campaigns, by and large, are start-ups, and don't have the expertise or—to do sophisticated cybersecurity against the adversaries that they face.

Ms. UNDERWOOD. Right.

General TAYLOR. So the encouragement would be for them to work with a company or an organization like U.S. CyberDome to provide that expertise in a systematic way with funding from donors to our 401—501(c)(4) organization.

So it is the investment in organizations like Microsoft or CyberDome that will provide those services free of charge to the campaigns that will raise the level of security that they will have, moving forward.

Ms. UNDERWOOD. OK. Then also in your testimony, sir, your written testimony, you described how there is a bit of a shortage in qualified workers that have the experience required to do this type of sophisticated cyber defense on behalf of the United States electoral process. Just wondering if you wanted to comment on that.

General TAYLOR. Certainly. It takes years of expertise to build the understanding of how the adversary works, and how to apply the tools of cybersecurity. A college graduate in cybersecurity is not going to have that expertise, and that is why we have tried to bring together folks with that kind of expertise to apply it to individual campaigns in a systematic way, as opposed to a haphazard way.

Ms. UNDERWOOD. With experience, then, in playing cyber defense——

General TAYLOR. And——

Ms. UNDERWOOD [continuing]. Against the Russians, the Chinese, the Iranians——

General TAYLOR. Exactly.

Ms. UNDERWOOD [continuing]. And the other foreign actors that threaten our elections.

General TAYLOR. Who have very significant experience in the defense area of cybersecurity and have applied those tools very successfully over the years.

Ms. UNDERWOOD. So, with that in mind—thank you, General Taylor—Ms. Badanes—OK, yes, Badanes—could you comment, then, on Microsoft's ability to source that talent, given the relative lack of availability around the country?

Do you feel that your company was able to recruit the individuals that do have the ability to play that type of cyber defense that the general was describing?

Ms. BADANES. Sure. Microsoft is, actually, one of the most attacked companies in the world. So, when it comes to cybersecurity, it is something that we have had to take seriously for our own protection.

We have been able to take our learnings from protecting ourselves, and also apply those to protecting our customers. That includes recruiting the talent that we need to both protect ourselves and also go into that front-line role of protecting our customers.

Ms. UNDERWOOD. So those individuals, your cybersecurity professionals, then would have had previous experience?

Ms. BADANES. In many cases. We have a lot of—real quick, previous experience?

Ms. UNDERWOOD. Against these foreign adversaries that General Taylor was outlining, right?

Ms. BADANES. Sure——

Ms. UNDERWOOD. The Chinese, the Iranians, the Russians that have—are the known foreign actors that threaten——

Ms. BADANES. Yes——

Ms. UNDERWOOD [continuing]. Our election system.

Ms. BADANES. In particular, the MSTIC team that we work with very closely recruits a lot of individuals from previous Government experience, where they faced similar threats.

Ms. UNDERWOOD. Thank you. So, I mean, it is clear to me that if large technology companies like Microsoft have to go out and recruit these types of very experienced, talented individuals, that campaigns are not going to be able to do that. Certainly, States that barely have an IT person to manage the whole system dedicated to their board of elections or whatever, a secretary of state, they are not going to be able to recruit those people, too.

So it sounds to me like we have a real work force issue, in addition to a lack of some standards and requirements.

General TAYLOR. I think there is a work force issue across the board, in terms of cybersecurity, for the country. But more specifically, from our perspective, we believe that we can harness the expertise of the cybersecurity community, focus on campaigns——

Ms. UNDERWOOD. Right.

General TAYLOR [continuing]. And do so in a systematic way, which will provide better protection than hiring a—you know, a college graduate to be your cybersecurity person trying to take on the Russians.

Ms. UNDERWOOD. Thank you for your testimony. I yield back.

Mr. RICHMOND. The gentlelady from Illinois yields back. The gentlewoman from Texas, Ms. Jackson Lee, is recognized for 5 minutes.

Ms. JACKSON LEE. Let me—again, let me thank the witnesses, and let me share with you these points if you can listen to this fact—points, and then I will raise some questions.

The Russian General Staff Main Intelligence Director, GRU, is suspected by our intelligence agencies of having begun cyber operations targeting United States elections as early as March 2016. They took on the persona of Guccifer 2.0, DCLeaks.com, and

Wikileaks as the identities that would be reported as having involvement in the work that they had undertaken to undermine our Nation's Presidential election.

Russia is blamed for breaching 21 local and State election systems, which they have studied extensively. In February 2018 Special Counsel Robert Mueller released indictments of 13 Russians, at least one of whom has direct ties to Russian President Vladimir Putin. The 37-page indictment details the actions taken to interfere with the U.S. political system, including the 2016 U.S. Presidential election.

Among the charges, which include charges for obstruction of justice, are several especially notable details. The indictment states that 13 defendants posed as U.S. persons and created false U.S. personas and operated social media pages and groups designed to attract U.S. audiences.

Dr. Blaze, are we better off now than we were pre-2016 and into 2016, as it relates to the operatives that we might expect—Iran, Russia, China?

Mr. BLAZE. Well, I think, in some sense, we are better off because we are discussing it, the fact that we are having these hearings. But on the other hand, 2016 could be seen as a demonstration of how successful this approach can be with very limited resources.

So I think, in particular, this is—the experience of 2016 provides great encouragement to even smaller National adversaries than the—those with the GRU at their disposal.

Ms. JACKSON LEE. Do you believe, when information counters documented intelligence reports that Russia was the entity that interfered in 2016, and representations from government officials keep utilizing Ukraine as having a server, or having been involved, does that give a sign of victory to our adversaries, when that kind of dialog is still going on?

Mr. BLAZE. If you are asking me, I think it is, you know, very important that our intelligence services be fully utilized, and their expertise listened to in building our defenses. So to the extent that we are distracted about these things, that only weakens us.

Ms. JACKSON LEE. Do you still maintain that we need to ramp up the monetary investment quickly to be able to be prepared for what we may not suspect might happen in 2020?

Mr. BLAZE. I think this is an urgent priority.

Ms. JACKSON LEE. Your comment, I think, 19 or 20 States don't have paper ballots?

Mr. BLAZE. That is right. I don't have the precise numbers at my disposal, but there are voters in a large number of States who still don't use paper——

Ms. JACKSON LEE. I count that as a crisis. That is about one-third of the 50 States that don't have paper ballots, that something disruptive could occur and they have no record.

Mr. BLAZE. I think we are—we have been very fortunate if something hasn't occurred yet.

Ms. JACKSON LEE. Secretary Stengel, again, we have, I think, operatives that think they are successful because, in the public sphere, there is a comment that Ukraine may have had a server, may have had something to do with 2016. Do you count that as

disinformation at its paramount level? What else could be said, going into 2020?

Mr. STENGEL. Yes, Congresswoman, I think that is an example of disinformation. To go to your previous question, I think our adversaries regard it as a victory when they can get that kind of information in the digital bloodstream of the United States, and you have people in the Government not believing what our intelligence sources say is absolutely indisputable, and going—having recourse to some of this disinformation and strange theories that is—are not proven at all. I think our adversaries see that as a victory.

Ms. JACKSON LEE. With that in mind, let me just say—and let me thank the witness from Microsoft. Let me just quickly ask.

You continue to shore up your system to protect against those who want to attack Microsoft, right? It is a daily, everyday basis.

Ms. BADANES. Absolutely. It is a race without a finish line.

Ms. JACKSON LEE. So let me just say I think CISA is a very important new entity. But listening to all of the witnesses, I am almost saying that we should declare a war room. We are a couple of months out from the major Presidential primaries, with one party having any number of candidates. That is the crux of our democracy for the highest office in the land.

I appreciate Dr. Krebs and his work, but I really believe that we need an effective war room working on behalf of the Federal Government and working with all the States. This is—stakes are high, and this is going to be serious in 2020.

I thank you all for the contribution you have made today.

I yield back.

Mr. RICHMOND. The gentlelady from Texas yields back. I will now recognize the gentleman from Ohio, Mr. Roy—Joyce.

Mr. JOYCE. I love Ohio, but I am from Pennsylvania.

Mr. RICHMOND. Oh, I am sorry.

Mr. JOYCE. That is all right.

Ms. Badanes, I think it is important that you, representing Microsoft, are here today. You discuss the work on protecting campaigns. But in your written testimony you mentioned that you work on election integrity. Can you elaborate on that work, please?

Ms. BADANES. Yes, sure. Thank you for the question. So, as I mentioned in the testimony, our program is focused on 3 pillars, which are actually quite similar to the hearing today. We focus on campaign security, disinformation defense, and election security.

So when we approach that space, as I said earlier, one of the things we were looking for was identifying ways that our company uniquely could fit in and make a contribution. One thing that we have done is to encourage the work of Dr. Josh Benaloh, who actually contributed to the National Academies report, and is well-known in the election security community. He is a senior cryptographer in Microsoft Research, and he has created a concept called end-to-end verifiability in elections.

So we have built out the code for that. It is now available, open-source, on what is called GitHub, which is a site where open source code lives, and we have invited vendors new and old to take that code and use it to make their system stronger. We are working with them actively to identify pilots where we can test that kind of application.

Mr. JOYCE. You also mentioned Account Guard and Microsoft 365 for campaigns. Can you tell us about Election Guard, please?

Ms. BADANES. Sure. So I actually didn't reference that the open-source software development kit is called Election Guard.

Mr. JOYCE. It is called Election Guard.

Ms. BADANES. Yes, yes.

Mr. JOYCE. Can you go into some more details of how you can see that impacting the 2020 elections?

Ms. BADANES. It will be difficult for it to be rolled out in time for the 2020 election in any notable way, other than a few pilots. However, the way that it impacts voters—and that is what we are really focused on—it comes down to that question of was my vote counted, can I trust that my vote made it all the way through?

What end-to-end verifiability enables is a voter to cast their vote, take a tracking number back with them. That vote is now encrypted. Whether it is through a ballot marking device, or whether it is through hand-marked paper ballots into a scanner, it can be applied in lots of different ways.

But the voter, at the end of the election, can check and make sure that their vote actually made it into the final tally. So it really is, ultimately, about voter confidence.

Mr. JOYCE. Can you elaborate on research and development at Microsoft? Do you consider this to be a field of development that Microsoft is committed to?

Ms. BADANES. So, interestingly, where Dr. Benaloh sits within the company is within Microsoft Research. So, as a team, the Defending Democracy Program, we are actually quite small. But what we are able to do is work across the company, in particular, with our researchers, identify projects they are working on that could be applicable in the election and campaign space, and where there is a good fit we can then work with them to make that research real and be part of the commercial offerings.

Mr. JOYCE. Thank you. My next questions are for Dr. Blaze.

Pennsylvania recently launched a risk-limiting audit pilot project. Can you speak of how that project has been perceived, and how that was rolled out in 2 different communities in Pennsylvania?

Mr. BLAZE. Right. If I understand, Philadelphia, my former home town, was one of those cities. You know, it is vitally important that States and local jurisdictions get experience with risk-limiting audits.

You know, I think the—Pennsylvania needs to be applauded for doing this. The experience from Pennsylvania is going to be extremely valuable to both Pennsylvania and other jurisdictions, looking forward. So this is, you know, a very positive thing, in my view.

Mr. JOYCE. Conversely, Dr. Blaze, do you see any potential disadvantages utilizing risk-limiting audits?

Mr. BLAZE. No. We simply have to do them. I think the biggest disadvantage we face is that if there isn't a National standard for doing them, they are being rolled out very slowly and, you know, this needs to be accelerated with things like the Pennsylvania pilot project.

Mr. JOYCE. Thank you, and I thank all of the witnesses for being here today. I yield my time.

Mr. RICHMOND. The gentleman yields back. I just want to echo the sentiment of my colleague from Pennsylvania and thank you all for being here and covering such an important topic. I believe that it is bipartisan, that we want to protect our elections and protect our democracy, and make sure that every vote matters.

So, with that, the Members of the committee may have additional questions for the witnesses. We ask that you respond expeditiously in writing to those questions.

Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 4:24 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN CEDRIC L. RICHMOND FOR FRANCIS X. TAYLOR

Question 1. Political campaigns, with their limited resources and staff, are a rich target for adversaries. Are political campaigns doing enough to defend themselves from cyber attack? What more is needed?

Answer. Generally, campaigns are not doing enough to defend themselves from cyber attack. Campaigns are not adequately resourced to defend against many expert, persistent, and well-funded threat actors such as nation-states. Most campaigns do not have enough technical expertise or historical experience against the myriad threats they face. Simply put, if they have not previously detected and responded to sophisticated threat actors, they will not be able to. Even campaigns with a very knowledgeable cybersecurity professional on-staff are hindered. One person alone cannot repel the Korean People's Army or the Armed Forces of the Islamic Republic of Iran.

Congress should consider specifying minimum cybersecurity standards for Federal candidate committees. Campaigns may have greater incentive to spend effort and funds on cyber protections if they know their competitors are obligated to the same expenditures. Today, a campaign's singular focus is to get elected. Any effort not directly in support of getting elected, is not funded or underfunded. For election campaigns, every dollar spent on services like cybersecurity is a dollar that is not being spent on their core mission. Even proactive candidates may think twice about spending effort and money on cybersecurity, for fear this diversion of resources will result in less votes than their competitors. This results in a lack of incentive for campaigns to address cybersecurity more fully, despite the imminent threat.

A minimum standard would "level the playing field" and also ensure foundational cybersecurity safeguards are implemented across committees. The specific cybersecurity standards need not be authored from scratch. A large catalog of U.S. Federal cybersecurity publications exists now and might be adapted specifically for political campaigns. Finally, given the relationship between Federal candidate committees and National party committees, Congress should also consider specifying minimum cybersecurity standards for National party committees.

Congress should consider mandating that all U.S. Government cyber threat intelligence be disseminated in computer-readable formats, in addition to prose. This simple requirement would go along way to ensuring that action can be taken swiftly once cyber threat intelligence information is received. Today, cyber threat information is mainly conveyed in formats that cannot be automatically processed by computers. In cyber space, the pace of engagement is extremely fast. It far outpaces the rate of re-formatting threat intelligence. We are fighting an asymmetrical war on the cyber front, and we must adjust. I do not espouse a specific format. I would leave that up to the experts. Expressing all threat information in computer-readable formats will be a big step forward.

Congress should consider funding efforts to automate de-classification. De-classification processes also cost cyber defenders critical time. However, these challenges are more complex to solve. Over-classification is something that intelligence organizations should evaluate for themselves. In other words, is it possible that certain aspects of the threat information never needed to be classified to begin with? Accelerating de-classification should also be considered. We are living in an age where machine learning is broadly applied, and artificial intelligence is starting to be well-understood. These technologies hold significant promise to automate large portions of the de-classification process.

It's noteworthy that computer-readable formats and de-classification of cyber threat intelligence are also big challenges to the U.S. Federal Government sharing information with private sector, whether in the interest of protecting critical infrastructure or for other reasons. I urge careful consideration of these topics, given their importance at-large.

Question 2. Recent reports suggest that foreign governments like Russia are ramping up influence operations in places with fledgling democracies or more fragile economies, such as Africa, and using increasingly aggressive tactics.

What is the next frontier of foreign influence operations, and how might it matter for U.S. National security?

Answer. A RAND blog from June 2019 does a very good job in summarizing what I believe to be the next frontier in foreign influence operations. The author states what many of us have been seeing for some time, "nation-state cyber wars are already well under way." The lack of international norms means that cyber attacks fall into gray areas below total war. Nation-state actors (e.g. Russia, Iran, and China) exploit that uncertainty and pose serious risks to U.S. National security. Their exploits threaten critical infrastructure, including transportation, food delivery, utilities, and commerce in general.

The Department of Homeland Security (DHS) has provided solid guidance (published May 15, 2018) toward developing a more robust cybersecurity strategy for the homeland that focuses on better defenses. DHS proposed that the United States seek to build deeper partnerships with industry to foster an aligned cybersecurity ecosystem to enable more effective collaboration and information sharing.

DHS has encouraged the accelerated use of innovative and emerging technologies such as artificial intelligence and machine learning, with an eye toward protecting critical infrastructure. DHS has determined that the effects of cyber attacks against critical infrastructure could be better mitigated through the creation of comprehensive playbooks to unify Government actions across defense, homeland security, law enforcement, intelligence, and State agencies. This could drive uniformity in action across the National security enterprise for defensive measures.

Question 3. The Obama administration filled the position of National Security Council's cybersecurity coordinator, who coordinated Federal efforts related to cybersecurity. Do you believe such a role is necessary in the coordination of the various agencies' responses to election security?

Answer. The increasing reliance of our Nation on technology means the cybersecurity coordinator role has never been more important. Not only is the cybersecurity coordinator critical for coordination of Federal efforts related to cybersecurity, but this role must also oversee alignment of Federal efforts with those of private sector and other levels of government. This alignment is vital for areas such as critical infrastructure, to include election security, where the majority of our critical infrastructure exists outside of the Federal Government.

QUESTIONS FROM CHAIRMAN CEDRIC L. RICHMOND FOR RICHARD STENGEL

Question 1. Political campaigns, with their limited resources and staff, are a rich target for adversaries. Are political campaigns doing enough to defend themselves from cyber attack? What more is needed?

Answer. While I am not an expert on cybersecurity and I do not have any data on what the political campaigns are doing, I would suspect that they are not doing nearly enough. They are ripe targets. We saw that in 2016; it will be even more true in 2020. Moreover, there are new methods that have been developed since 2016 that make campaigns more vulnerable. Deep fakes and the manipulation of data, in addition to cyber hacking and disinformation are now among the many things campaigns need to be concerned about. In information war, offensive weapons are more sophisticated than defensive weapons. Campaigns should have full-time teams dedicated to defending themselves in the cyber realm.

Question 2. Recent reports suggest that foreign governments like Russia are ramping up influence operations in places with fledgling democracies or more fragile economies, such as Africa, and using increasingly aggressive tactics.

What is the next frontier of foreign influence operations, and how might it matter for U.S. National security?

Answer. The recent *New York Times* story about Russian influence operations in Madagascar (Nov. 11, 2019) illustrates the concerns contained in the question. In that story, the Russians were trying to sway a political campaign to help Russian business. Their interests are always unscrupulous: To help Russian interests and to undermine democracy. The Russians, especially outside the United States, combine political influence operations with commercial ones. The Chinese tend to concentrate only on commercial ones. In the case of the Chinese, they believe commercial ties will lead to political ones. In both cases, they seek to erode the strength of American alliances abroad—and that is a long-term threat to U.S. National security.

Question 3. What do you mean when you say that the primary weapons in the global information war are "weaponized information and grievance?" How were these weapons used in the 2016 Presidential election?

Answer. The weaponization of information and the weaponization of grievance are two different things. The former is a description of global information war, in which bad actors both steal information and distort it to influence and deceive their targets. The weaponization of grievance is a fancy way of saying that some politicians and leaders magnify and exploit voters' frustrations and unhappiness instead of proposing solutions and policy. In the case of weaponizing information, the Internet Research Agency in St. Petersburg created false narratives about U.S. Presidential candidates. The Russians also stoked resentment among both white conservative voters and African-American voters with false claims and deceptive advice.

QUESTIONS FROM CHAIRMAN CEDRIC L. RICHMOND FOR MATT BLAZE

Question 1. Political campaigns, with their limited resources and staff, are a rich target for adversaries. Are political campaigns doing enough to defend themselves from cyber attack? What more is needed?

Answer. Response was not received at the time of publication.

Question 2. Recent reports suggest that foreign governments like Russia are ramping up influence operations in places with fledgling democracies or more fragile economies, such as Africa, and using increasingly aggressive tactics.

What is the next frontier of foreign influence operations, and how might it matter for U.S. National security?

Answer. Response was not received at the time of publication.

Question 3. As one of the organizers of the DEFCON voting village, you have been able to hack voting machines, vote scanners, and ballot marking devices. What do you see as the greatest strength and weakness in our election infrastructure?

What technical threats to election infrastructure are most concerning to you in 2020?

Answer. Response was not received at the time of publication.

Question 4. This month, The Brennan Center for Justice issued a report calling on Congress to establish a framework for Federal certification of election vendors, the private companies that manufacture voting equipment and maintain voter registration databases, which would include the establishment of Federal standards and the ability for Federal officials to monitor compliance and address violations.

Are vendors doing enough to defend voting systems? What more is needed?

Answer. Response was not received at the time of publication.

Question 5. Although you have disclosed these vulnerabilities to vendors, many of these devices will still be in use for the 2020 National election. How have vendors responded to your disclosures?

And do jurisdictions that use these machines face a high risk of being compromised?

Do you believe that election vendors are well-situated to withstand attacks from nation-state actors?

Are there supply chain security certifications that must met for vendors to be able to participate in National elections?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN CEDRIC L. RICHMOND FOR GINNY BADANES

Question 1. Political campaigns, with their limited resources and staff, are a rich target for adversaries. Are political campaigns doing enough to defend themselves from cyber attack? What more is needed?

Answer. Political campaigns in the United States range from a small thousand-dollar budget operation with a single staff member to a large multi-million-dollar budget organization with hundreds of staff. No matter their size or resources, all face the potential threat of attack from well-funded adversaries. Many campaigns are taking fundamental steps to protect themselves, but more can always be done.

The most impactful thing a political campaign can do to protect itself is to train members of the team on the importance of basic cyber hygiene. These trainings should promote practices such as using a password management tool, turning two-factor authentication on all their accounts, and using a secure communications platform for sensitive messages.

Such trainings will not alter the behavior of staff unless campaign leadership first creates a culture of cybersecurity awareness within the organization. When the candidate, campaign manager, and other prominent officials demonstrate a commitment to cybersecurity with their own devices and accounts, prioritize trainings, and

provide secure software for the team to use, they demonstrate that cybersecurity is something everyone on the team is expected to care about.

However, campaigns can only do so much to protect themselves. There is a role for the private sector to play in supporting these efforts as well. For example, at Microsoft we have made top-tier communications and productivity tools (M365 for Campaigns) available at non-profit pricing so that campaigns can access the security features they need at a price that is reflective of their budget reality. Similar initiatives being spear-headed by organizations such as Defending Digital Campaigns and CyberDome will continue to provide campaigns with the kind of support they need to defend themselves against sophisticated adversaries.

Question 2. Recent reports suggest that foreign governments like Russia are ramping up influence operations in places with fledgling democracies or more fragile economies, such as Africa, and using increasingly aggressive tactics.

What is the next frontier of foreign influence operations, and how might it matter for U.S. National security?

Answer. Identifying the kind of influence operations our adversaries will try next is a challenge that many in both the private and public sector are aggressively investigating. There has emerged consensus on a few things, specifically: (1) Adversaries have already begun and will continue influence operations targeting the 2020 U.S. elections, and (2) adversaries will not follow the same playbook they ran in 2016.

While a multi-stakeholder approach is under way to identify and combat these operations, it should be noted that key participants in that process are the voters themselves. An informed public is one of the best defenses that can be used against such operations. A good example of arming citizens with information that is helpful to this effort is the recent infographic created by the Cyber & Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS). This infographic clearly demonstrates how disinformation is constructed and spread by adversaries, using the clever topic of whether pineapple belongs on pizza.[1] Additional engagement with the public using tools like this is a helpful step toward preparing the public for these on-going influence operations.

As researchers look into what other tactics might be used in future influence operations, one emerging threat that is gaining attention is the increased potential for bad actors to use artificial intelligence to create malicious synthetic media, better known as "Deepfakes". While advances in synthetic media have clear benefits (such as synthetic voice used to improve accessibility technology), the increased access to synthetic media technology also leads to the risk of exploitation.

Stakeholders from academia, civil society, and industry are currently working together to advance best practices for the ethical use of AI. One such effort includes a recent "Deepfakes Detection Challenge" Microsoft helped launch together with Facebook and the Partnership on AI, a technology industry consortium focused on best practices for AI systems, which invites researchers to build new technologies that can help detect deepfakes and manipulated media.

The emergence of deepfakes is just one possible avenue our adversaries will pursue in their efforts to disrupt the 2020 U.S. elections, and there is more to be done to combat this possible threat as well as others. Microsoft remains committed to working with other stakeholders to contribute to solutions as these and other threats emerge.

○

[1] CISA Disinformation Infographic—*https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf.*