Testimony of

Brigadier General (USAF, ret.) Francis X. Taylor

Executive Director, pro tempore
US CyberDome

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

The Road to 2020: Defending Against Election Interference

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 cyber security and dis-information 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.

U.S. 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 cyber security 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 dis-information can be used to manipulate the US 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 two 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 U.S. 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 on-line 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% 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 cyber security and dis-information. 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 cyber security 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 U.S. where campaigns can find someone with past experience defending against a wide-variety of nation-state cyber attacks or dis-information. 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 cyber security 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 cyber security 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 cyber security 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 cyber security, 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 cyber security. In addition to the above campaign observations, I offer a technical one. We still struggle with the "last mile" of cyber security 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 cyberspace, 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 brand 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.

Francis X. Taylor, Brigadier General (USAF, retired)

Mr. Taylor is the Executive Director (pro tempore) of US CyberDome. In this role, he orchestrates and oversees relations with donors, eligible committees, and qualified vendors.

Mr. Taylor is the President and CEO of FXTaylor Associates, LLC, specializing in Security, Crisis Management and Risk Management Consulting. He retired from the US Government on January 20, 2017. His last assignment was Under Secretary, Office of Intelligence and Analysis, US Department of Homeland Security.

From March 2005 to November 2013, Mr. Taylor served as Vice President and Chief Security Officer for the General Electric Company, Fairfield CT. Prior to joining GE, Mr. Taylor had a distinguished 35-year career in government service, where he held several senior positions managing investigations, security and counterterrorism issues.

He served as the Assistant Secretary of State for Diplomatic Security and Director of the Office of Foreign Missions, with the rank of Ambassador. He also served as the US Ambassador at Large and Coordinator for Counterterrorism for the Department of State from July 2001 to November 2002. After the September 11, 2001, attacks, he was a key advisor in assisting the President Bush and Secretary of State Powell in forming the international coalition against terrorism and developing aggressive international policy implementation to defeat terrorism.

During his 31 years of military service, Mr. Taylor served with distinction in numerous command and staff positions, rising to the rank of Brigadier General in September 1996. As the head of the Air Force Office of Special Investigations, he was responsible for providing commanders of all Air Force activities independent professional investigative services in fraud, counterintelligence, and major criminal matters.

Mr. Taylor is a member of Boards of the American Academy of Diplomacy and the Washington Institute for Foreign Affairs (WIFA). He is also a member of the International Security Management Association (ISMA), the International Association of Chiefs of Police (IACP) and the American College of National Security Leaders. He was recently elected to the Board of Directors of the Council on International Education Exchange (CIEE) He is also a Principal at Cambridge Global Advisors (CGA), Arlington VA.