GLOBAL CYBER POLICY WATCH

INTERFERENCE IN THE 2020 PRESIDENTIAL CAMPAIGNS

AUGUST 2020

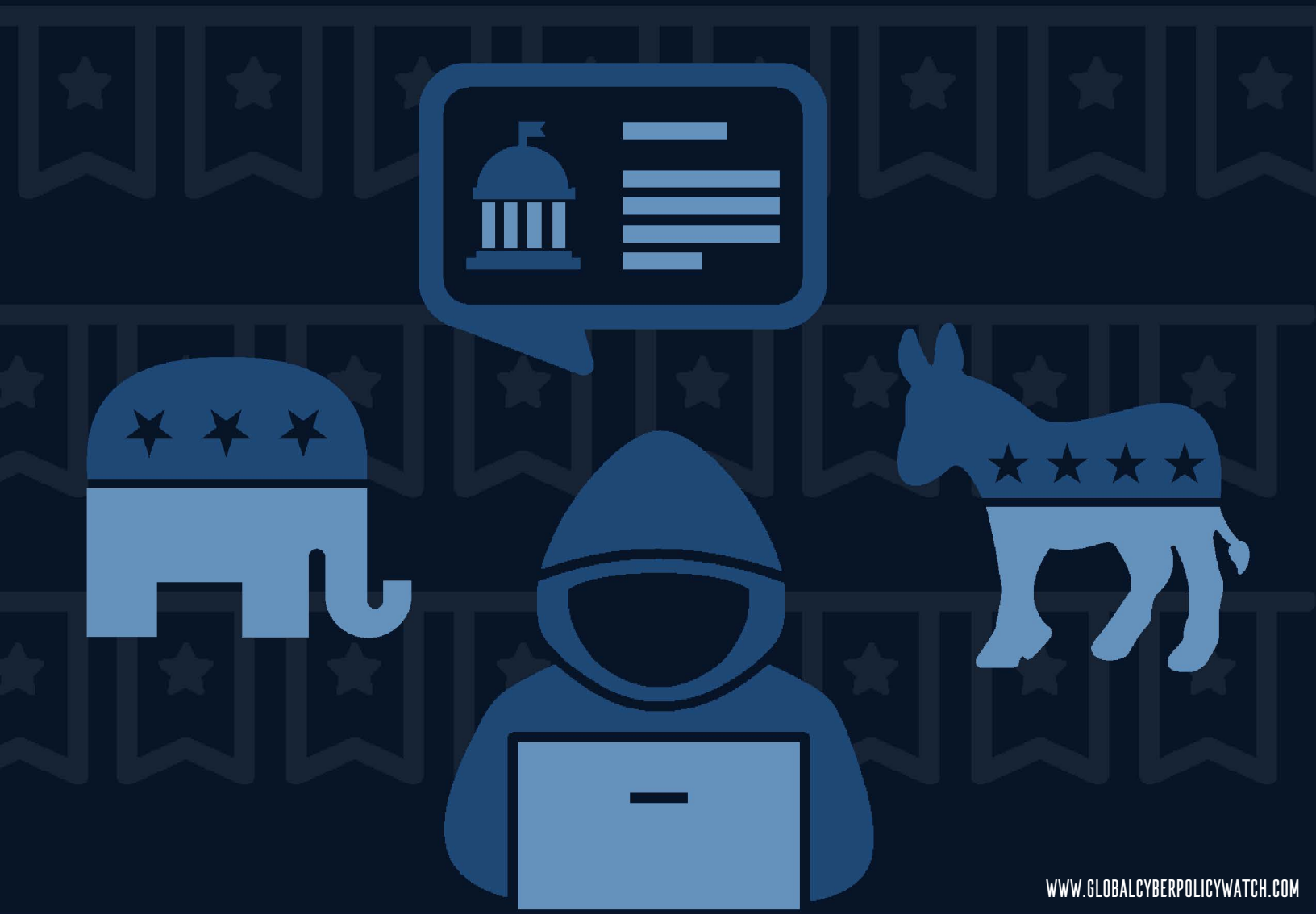

Table of Contents

INTERFERENCE IN THE 2020 PRESIDENTIAL CAMPAIGNS

INTRODUCTION

In the wake of the 2016 General Election, election security and the role of foreign influence over democratic processes has become one of the most discussed political topics in the United States. This stems from evidence demonstrating foreign actors did indeed interfere and exploit systems in place during the 2016 presidential election process. Most notable of these foreign actors was the Russian government which was able to carry out large-scale and varied efforts in the form of misinformation campaigning, political institution hacking, and "troll farming."

Widespread consensus on these interference efforts has Americans concerned about what that may mean for the 2020 cycle which has been underway for roughly 18 months now. Pew Research quantified the acceptance of foreign interference as an American political reality in a February 2020 survey where 72% of American respondents said it is very or somewhat likely that Russia or other foreign governments would try to influence the November 2020 election.[2]

Belief in the replication of 2016 practices isn't without its merits. Interference headlines have already surfaced in the 2020 cycle with both the Democratic and Republican candidates weathering attacks from global adversaries. Most recent reports include a Google disclosure in June 2020 citing a Chinese-based cyber-attack on Democratic candidate Joe Biden's top campaign staff as well as an Iranian-led effort on the Trump campaign.[3]

Since the lessons of 2016, campaigns across the spectrum have taken both unilateral and collaborative measures to protect against threats from Russia and the like. Additionally, federal agencies have coordinated with state officials to implement steps and processes that are intended to better secure elections at the often more vulnerable and under-resourced, local level.

1. Riley, Tonya. "The Cybersecurity 202: Virtual Campaigning Could Give Hackers New Ways to Attack the 2020 Election." The Washington Post. WP Company, April 7, 2020. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/07/the-cybersecurity-202-virtual-campaigning-could-give-hackers-new-ways-to-attack-the-2020-election/5e8b4f7488e0fa101a75bbc3/.
2. Doherty, Carroll. "Fast Facts about Americans' Views on Russia amid Allegations of 2020 Election Interference." Pew Research Center. Pew Research Center, February 21, 2020. https://www.pewresearch.org/fact-tank/2020/02/21/fast-facts-about-americans-views-on-russia-amid-allegations-of-2020-election-interference/.
3. Sanger, David E., and Nicole Perlroth. "Chinese Hackers Target Email Accounts of Biden Campaign Staff, Google Says." The New York Times. The New York Times, June 4, 2020. https://www.nytimes.com/2020/06/04/us/politics/china-joe-biden-hackers.html.

THREATS FACING THE CAMPAIGNS

In today's age of technology, accounts and passwords are some of the most important pieces of personal data on the market. During a presidential campaign, these items have increased importance because they are the keys to campaign communications, finance, and planning. The attack carried out against former Vice President Joe Biden's campaign is known as "spear-phishing attack" and aimed to compromise the personal emails of campaign staff.[4] In a typical spear-phishing attack, an antagonistic entity will send an electronic message posing as a reputable or trustworthy source and will try to coerce the victim into compromising his or her email by inputting or revealing personal information such as passwords or credit card numbers. The campaign has stated that to their knowledge all attempts were fortunately unsuccessful.

The attack against President Trump's campaign was similar to the one faced by the Biden camp. Iranian-based hackers tried to compromise the emails of the President's staff and campaign reporters, while also targeting campaign accounts on social media. This attack is not only similar to the attack on the Biden campaign, but it is also reportedly very similar to a cyber-attack Iran launched on the Trump campaign back in August of 2019 showing a pattern of targeted aggression and strategy. While the tactics of these foreign actors has remained largely familiar and unchanged in recent years, the overall implication of cyber incursions itself has developed since the last presidential election. First and foremost, the COVID-19 pandemic has forced operations around the world to go virtual, placing an increased importance on what happens in the cyber space. Additionally, the United States has not necessarily garnered any good will with some of these forces in the interim. For example, the U.S. withdrawal from the Joint Comprehensive Plan of Action (JCPOA) has burdened an already complex relationship between the U.S. and Iran, making cyber-attacks like these an attractive option for a nation wanting to display power and influence without the negative externalities of combative aggression. Despite some reiterative methods, the threat scenario for campaigns remains ever-changing. Therefore, it is imperative that these organizations both prepare and brace themselves for a wide range of threats in the days leading up to November 3rd.

> **"For the past five years, the European Commission has been one of Europe's main drivers of change in the digital world."**

The Biden Team, from all appearances, seems to be particularly attuned to the risks. The Democratic camp has reportedly implemented multiple preventative measures including Domain-based Message Authentication, Reporting, and Conformance (DMARC), an email security protocol to secure their system from being compromised. They were one of the earliest and most effective adopters of this strategy, being only one of eight Democratic campaigns to the strictest DMARC protocols back in February of this year. According to Agari, a leading email security firm, Biden has not only implemented more stringent email security measures than his opponent, President

4. Ibid

Trump, but he also has better systems in place to protect voters and donors interacting with his campaign from cyber threats as well.[5]

A NEW ELECTION LANDSCAPE

No other election cycle besides that of the 1918 Wilson-era mid-term has faced a global pandemic of this magnitude. The ongoing COVID-19 pandemic presents new hurdles to the election process, largely relating to technological advancements as campaigns have had to move to the remote world with virtual platforms replacing time-honored in-person strategies.[6] This has caused voter contact to take place predominantly digitally or over the phone, something that without a doubt increases overall exposure to cyber attackers. Thus far, the online videoing and web conference platform Zoom has been adopted as the commonplace for business meetings and interactions during quarantine and social distancing policies. Due to the rapid and large-scale increase in the use of Zoom, hackers have been targeting the platform, bringing to light an array of security threats such as the aptly termed "zoombombing". Zoombombing is when people not intended to be on a call join in and cause disruption in a host of ways, such as by sending or reading racist materials to the rest of the participants on the call.[7] Currently, Zoom has enabled measures to ensure the privacy of a call, including participant screening features and the ability to privately list the call number, to help catch or stop a potential actor with malicious intent from zoombombing others' calls This is a potential point of concern for the 2020 presidential campaigns because there is little that can be done to secure their virtual events meant for public consumption, other than using the options Zoom already offers. It is of note that this wave of cyber threats in this increasingly used digital space at Zoom mirrors a larger uptick in general cyber-crime that has coincided with expanded online use during the pandemic.

Prior to the Coronavirus outbreak, private companies were already stepping up to help 2020 political candidates protect themselves from outside actors. Defending Digital Campaigns (DDC) is a non-profit and non-partisan coalition of sorts and has brought together over 20 technology companies - ranging from industry giants Facebook or Amazon, to more specialized companies, such as the previously mentioned Agari - in order to provide free cyber and election inference protection to any campaign that will have them.[8]

> **"By improving the cybersecurity of Europe and building out its promise of a DSM, the Juncker Commission has given EU citizens confidence in the promise of an online world."**

While private companies working in elections is an alarming thought for some, there has been an overall growing call for private companies to offer their services to assist in election security.[9] These calls are in large part due to resource constraints. Comprehensive cyber security measures come at a high monetary cost that many campaigns can't afford. Additionally, most staffs do not carry the expertise to actually create and deploy an effective cybersecurity

5. "Presidential Campaign Security 2020: Election Email Security." Agari, 2020. https://www.agari.com/election-security-2020/.
6. Riley, Tonya. "The Cybersecurity 202: Virtual Campaigning Could Give Hackers New Ways to Attack the 2020 Election." The Washington Post. WP Company, April 7, 2020. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/07/the-cybersecurity-202-virtual-campaigning-could-give-hackers-new-ways-to-attack-the-2020-election/5e8b4f7488e0fa101a75bbc3/.
7. Lorenz, Taylor. "'Zoombombing': When Video Conferences Go Wrong." The New York Times. The New York Times, March 20, 2020. https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html.
8. "Partners." Defending Digital Campaigns. Accessed June 22, 2020. https://www.defendcampaigns.org/partners.
9. Dobrygowski, Daniel. "Why Companies Need to Help Ensure Election Integrity." Harvard Business Review, February 13, 2020. https://hbr.org/2020/02/why-companies-need-to-help-ensure-election-integrity.

strategy even if provided one by a third-party. These major barriers to cyber protection are what has prompted the work DDC is doing.[10] While their mission seems righteous, the DDC is aware that conflicts of interest could arise. As such, the organization has pledged to not share information from any campaign, will not endorse any campaign, and will address the needs of a campaign in a vacuum irrespective of any benefits a given company could derive from its decision-making.[11]

CYBERSECURITY OUTSIDE OF THE PRESIDENTIAL RACE

Cybersecurity is more than just a federal problem. At the state level, there is great cause for concern that foreign actors can, and will, play an integral role in 2020 elections. The 2016 cycle is proof the desire to interfere is there. In 2016, 21 states were targeted by hackers whose aim was to compromise voter registration systems and undermine American elections.[12] Fortunately, Illinois was the only state to have reportedly experienced a breach.[13] Now, going into this election, experts believe further attacks are all but guaranteed putting security at the forefront of my state and federal officials' concerns.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) director promised the upcoming election will be "the most secure, most protected election in the history of the United States of America."[14] To do so, CISA will work in partnership with the U.S. Election Assistance Commission (EAC), the body for election information and guidelines. Part of their strategy is to host regular communications between states and the EAC in the lead-up to the November election. Biweekly calls will facilitate multi-level information sharing between state and federal staff that is hoped to improve communication at large and ultimately offer a more secure electoral process. In addition to increased deliberations, CISA has introduced the "Tabletop in a Box," a 58-page scenario practice guide created by CISA to help states prepare for a wide range of events that could happen during the election, such as news and social media manipulation, spear-phishing campaigns, Denial of Service (DoS) attacks and the exploitation of state and county board election networks. Iowa,

> **"By December 31, 2019, the NIS Cooperation Group is expected to have agreed upon a diplomatic toolkit of measures to address and mitigate the risks identified at both the national and EU levels."**

which underwent attacks in 2016 , has publicly noted the new developments' usefulness. Iowa Secretary of State and President of the National Association of Secretaries of State, Paul Pate, has said that recent expansions of the federal government's role in cybersecurity efforts at the state-level have been helpful saying "they've played a big role in helping create the connection" and keeping states apprised of ongoing threats.

1. Riley, Tonya.

Conclusion

It is exceedingly important to garner a comprehensive understanding of the actions being taken by both allies and adversaries in the cyber environment. The European Union is an obvious strategic partner of the U.S., and its own position on cybersecurity has spillovers into our domestic network, ranging from economic to security concerns. The EU has established its leadership and commitment through the proposal and enforcement of a number of cyber-related policies introduced by the European Commission.

Cybersecurity has proven to be a bipartisan issue. There is much to anticipate in the upcoming years; beyond the excitement of technological advances such as a more accessible digital marketplace and 5G capabilities, there is a new Commission that is situated to pursue these innovations and protect its citizens in the process. The viability and longevity of the cybersecurity objectives initiated by the Juncker Commission are dependent on the incoming von der Leyen Commission's ability to recognize and adapt to the evolving threat landscape.

"The European Union is an obvious strategic partner of the U.S., and its own position on cybersecurity has spillovers into our domestic network, ranging from economic to security concerns."

1. Riley, Tonya. "The Cybersecurity 202: Virtual Campaigning Could Give Hackers New Ways to Attack the 2020 Election." The Washington Post. WP Company, April 7, 2020. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/07/the-cybersecurity-202-virtual-campaigning-could-give-hackers-new-ways-to-attack-the-2020-election/5e8b4f7488e0fa101a75bbc3/.
2. Doherty, Carroll. "Fast Facts about Americans' Views on Russia amid Allegations of 2020 Election Interference." Pew Research Center. Pew Research Center, February 21, 2020. https://www.pewresearch.org/fact-tank/2020/02/21/fast-facts-about-americans-views-on-russia-amid-allegations-of-2020-election-interference/.
3. Sanger, David E., and Nicole Perlroth. "Chinese Hackers Target Email Accounts of Biden Campaign Staff, Google Says." The New York Times. The New York Times, June 4, 2020. https://www.nytimes.com/2020/06/04/us/politics/china-joe-biden-hackers.html.