PROTECTING THE INTEGRITY OF US FEDERAL ELECTIONS: USING BIOMETRICS FOR FREE, FAIR, TRANSPARENT AND SECURE ELECTIONS

by

Braxton Mark Lee More

A Capstone Project Submitted to the Faculty of

Utica College

April 2018

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Cybersecurity

المنارة للاستشارات

www.manaraa.com

ProQuest Number: 10808196

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 10808196

Published by ProQuest LLC (2018). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

المنارة للاستشارات

www.manaraa.com

© Copyright 2018 by Braxton Mark Lee More

All Rights Reserved

للاستشارات المنارة

www.manaraa.com

Abstract

Addressing the impact of state-sponsored interference in US elections and countering that interference using biometric voter registration systems. The information provided in this study is both important and relevant to the current threat of state-sponsored actors, like Russia, using technology to interfere with the US electoral process and undermine voter confidence. Looking at numerous case studies of nations worldwide using biometrics in their elections provide promising insight into the implementation of biometric voting systems. It also offers insight into any pitfalls that could be encountered while implanting these systems and then use those to provide for seamless integration into the US electoral process. The findings of this study conclude that while there are social and political challenges that would need to be overcome in the US, the use of biometric voting systems would ultimately ensure a free, fair, transparent and secure election process.

Keywords: cybersecurity, elections, biometrics, social media, russian interference, policy, Dr. Professor Stephen Maher J.D., Professor Jesus Lopez.

المنارة للاستشارات

www.manaraa.com

Table of Contents

المنارة للاستشارات
www.manaraa.com

المنارة للاستشارات
www.manaraa.com

List of Illustrative Materials

المنارة للاستشارات
www.manaraa.com

Statement of the Problem

Definition of the Problem

A year after the 2016 general election, the United States Department of Homeland Security (DHS) notified election officials in 21 states that they had been the target of state-sponsored hacking originating from the Russian Government (Horwitz, Nakashima & Gold, 2017). For a democratically founded country, the confirmation of Russian interference shook United States (US) ideals and confidence that democracy can ensure free and fair elections. Voting for public representatives is an essential foundation to democracies around the world. For a democracy, it is imperative that elections be free, fair and transparent. By ensuring these fundamentals, democratically elected governments instill confidence and faith in the process with the voting population. While initial reports indicate that the alleged state-sponsored hacking by the Russian Government on voting systems across the US may have amounted to nothing more than a probe[1], the inherent nature and extent of the hacking is a cause for concern. If outside actors can hack voting machines, voter databases or any other election systems, such actions could undermine the validity of elections and shake the foundations of a nation's democracy. Indeed, it already has. With technology expanding at an ever-increasing rate and cybercrime growing at an even faster rate, reformation of election processes is needed to protect the integrity of US elections from both foreign and domestic interference to ensure a free, fair, transparent and secure election process.

[1] In June 2017, acting Director of the Office of Intelligence and Analysis Cyber Division, Samuel Liles, testified that the 21 states affected in the Russian hacking attempt did not impact vote-tally machines and appeared to be looking only for vulnerabilities (Horwitz, Nakashima & Gold, 2017).

المنارة للاستشارات
www.manaraa.com

200 Years of US Elections

The US has been fine-tuning the election process for over 200 years. While eligibility of voters and many other facets of elections have changed significantly since the first US election in 1788, much has not. Reforming a process so interwoven into the fabric of the US will not be without challenges. However, protecting such a vital process is imperative to counter the rising cyber threats. Upholding the critical principle that an eligible voter can vote only once guarantees the integrity of elections. As Thad E. Hall of the University of Utah explains:

> "For citizens to exercise their democratic right to vote, there must be a comprehensive and inclusive electoral register, also called a voters list; and this must be carefully maintained to ensure that each eligible citizen is registered to vote once and only once" (Hall, 2013).

In the US the protection of voter databases is critical. Under the National Voter Registration Act of 1993, the US Election Assistance Commission (EAC) was given responsibility to develop a national voter registration form to increase voter registration across the country (Federal Register, 2010). This act provided a way for more eligible voters to register[2]. With laws like the National Voter Registration Act of 1993, the US government provided a way of making elections more free and fair, but also comes with more significant risks that must be accounted for. As threats of interference by state-sponsored hackers such as Russia have become more prevalent,

[2] Eligible voters can register to vote at their department of motor vehicles, armed service recruitment centers or state and county public assistance offices. Also, in 37 states plus the District of Columbia, eligible voters may register online. US citizens living overseas or serving in the military may register and vote using the Federal Voting Assistance Program (USA.GOV, 2018).

المنارة للاستشارات
www.manaraa.com

defense of these databases must adapt. By using existing laws and processes in combination with biometric technology, nations can improve the ability to mitigate threats of election interference.

Little has changed in the US when it comes to election day. Hard-copy lists are used by poll workers to cross-reference voter provided identification, and with limited to no additional authentication, the voter is given their ballot. Technology has rendered this method of verification unreliable, insecure and entirely obsolete. Though voter fraud by an individual is a concern, most studies have concluded that there is no apparent wide-spread occurrence of it in US elections. One such study by Justin Levitt of Loyola Law School, as reported by the Washington Post, suggests that "…while voter impersonation does indeed happen, it happens so rarely that the rate is approximately one instance out of ever[sic] 32 million ballots cast," (Ingraham, 2017). It is, therefore, not necessarily a threat that comes from the individual voter, but outside actors are attempting to disrupt voter confidence in the election process. By implementing and using biometric voter registration and authentication on a national scale, this would aid in ensuring free, fair, transparent and secure elections. Collecting and housing fingerprint, retinal scan and facial recognition biometric data in a centralized Federal database would be vital to this implementation. Doing this also grants the ability to authenticate voters and identify any potential voter fraud not only by individuals but also help to mitigate election interference by state and nonstate-sponsored hackers.

Current Research Gaps

As previously discussed, biometrics as a means of identity authentication is not by any means a new technology or process. Biometrics have been used in law enforcement for decades,

www.manaraa.com

precisely regarding fingerprints. It was not until the early 2000's that the use and implementation of biometric systems started to become more widespread. In fact, since 9/11, many countries around the world have looked for ways to improve airport security, while minimizing the impact on passengers. Heathrow International Airport, in London, is one example where facial recognition has been in use since 2008 (Atikins Global, 2013). The practical use of biometrics can be seen in airport security, corporate and government buildings, and even on an individual's mobile device. The explosive development of biometric systems was created out of the necessity for security against the global war on terrorism. With biometrics becoming more widely used for numerous identity verification functions, the use of biometrics is still in its infancy as being a streamlined and full-proof process. According to a case study conducted by Peter Wolf at the International Institute for Democracy and Electoral Assistance (IDEA),

> "The number of countries adopting biometrics in elections has steadily increased to over 50, with significant differences between regions: while there are virtually no users in Europe, about half of the countries in Africa and Latin America use this technology in elections." (Wolf, 2017).

Most nations using biometric information in their election process have been developing countries. As a result, there is little comparative research as to how a similar election process would function if implemented in the US.

With the significant gap in research existing primarily in the feasibility of implementing biometric voter registration and authentication in the US, considering several questions will help to make these gaps smaller. (1) What are the potential benefits and drawbacks of biometric

المنارة للاستشارات

www.manaraa.com

registration and authentication, (2) what challenges could be encountered trying to move eligible voters to a biometric voting system and (3) how can Federal elections be streamlined across state lines to ensure consistent and secure standards? By answering these questions as well as using the research from developing countries already using biometrics, lessening the gap in voter-based biometric research.

A National Concern

Protecting the integrity of US Federal elections from both foreign and domestic interference and ensuring a free, fair, transparent and secure election process is a pressing national concern. This research paper will focus on fundamental concepts to aid, improve and uphold the ideals of the democratic elections in the US and reinforce the confidence in US voters in the election process. The research provided in this paper will help provide a starting point and framework for local, state, and Federal officials to develop policy geared towards improving and defending the integrity of the US election process. With biometric technology being the focal point of this paper, this research will also help direct technology companies in building national biometric voting solutions. For individuals in academia, this research paper will aid in the continued exploration, development and research into biometrics. Additionally, the contents of this research paper will seek to address the concerns of the average US voter.

Literature Review

History of Biometrics

Coming from the Greek word “bio,” meaning life and “metrics,” meaning to measure, the concept of biometric identification is not a newly discovered idea or technology. Identifying an individual by the features that make one unique is something that has been present as long as

المنارة للاستشارات
www.manaraa.com

humanity has been in existence. For example, on the small Indonesian island of Borneo, archaeologists found handprints stenciled on the cave wall dating back almost 35,000 to 40,000 years old, which archaeologist believe are some of the first examples of unique signatures (Battersby, 2014). While this example is a very old and primitive, it shows an innate sense that individual identity, whether for recognition, remembrance, or simple identification, has been a part of humanities history for a long time. Jumping ahead in the story of humanity, a 14th-century Persian text “Jaamehol-Tawarikh,” discussed how an individual could be identified using their fingerprints. It was then in the 17th century that anatomy professor Marcello Malpighi found that an individual’s fingerprint consisted of ridges, spirals, and loops, which German anatomist J. C. A. Mayer would first declare to be unique to everyone in 1788 (Mayhew, 2018). This information would later pave the way for the 20th century for the modern fingerprint biometric technology that is used as an indispensable tool for both government and private sector functions.

While fingerprints are the oldest forms of biometric identification, it was not until the 20th-century that other forms of how an individual can be uniquely identified were discovered. In 1936 Ophthalmologist Frank Burch found that iris patterns could be measured and were unique. Later, in the 1960’s facial recognition systems were developed to measure eyes, ears, nose, and mouth on the photographs, as well as the first model for speech recognition (Mayhew, 2018). As computers began to be able to process more data at faster rates, the ability to automate the individual discovery process made biometrics more feasible at scale.

www.manaraa.com

Decentralization of Presidential Elections

In the US, elections for the Presidency is a process that has always been administered by the states. Under the Tenth Amendment of the US Constitution, "Each state shall appoint, in such a manner as the Legislature thereof may direct, a Number of Electors, equal to the whole Number of Senators and Representatives to which the state may be entitled in the Congress…" (US Constitution, 1791). Known as the Electoral College, states within the US are responsible for collecting and tallying votes. Dependent on specific laws of a given US state, the tallied votes are then passed along to a US state's electors, who are expected to vote based on the results of the tallied ballots. With nothing explicitly having been laid out in the US Constitution that would limit state's powers over the administering of Federal elections, the Tenth Amendment gives this very authority to US states.

The ever-increasing threat of election interference from state-sponsored actors, such as Russia, has generated a new challenge for states. Not only do nations now have to ensure that voter laws are followed but they also now must ensure that the integrity and security of voting systems are upheld. The first line of defense for US states in this regard is to in turn ensure that voter registration databases are maintained, secure, and always up to date. Many US states have varied methods of registration based on state-specific laws, but almost all of them require the minimum of one's full legal name, date of birth, and social security number to register. Technology has made registration even more accessible as many US states allow for online registration. With the decentralized nature of US Federal elections and the responsibility resting with the states that administer them, it is essential to look to the US Constitution, while also

المنارة للاستشارات
www.manaraa.com

adapting for a 21st-century solution that will unify and streamline the way American's choose the US President.

National Voter Registration Act (NVRA) of 1993

The US Constitution does not offer much regarding guidance on how US states should administer Federal elections. Since the ratification of the US Constitution, there have been Amendments that have solidified national rules and guidelines that US states must follow. One such guidance was signed into law in 1993. NVRA "provides that citizens can register to vote by mail using mail-in-forms developed by each US state and the Election Assistance Commission," and "also creates requirements for how states maintain voter registration lists for Federal elections," (NVRA, 1993). As the US has grown and matured, so too have the way in which the US has needed to adapt to how processes are run. The NVRA not only made voter registration more accessible but created a streamlined national mail registry and how US states were expected to maintain their voter lists.

Help America Vote Act (HAVA) of 2002 – Election Modernization

Under President George W. Bush, the Help America Vote Act (HAVA) was signed into law in late 2002. Under this law, new Federal standards were put into place that US states had to follow for all Federal elections. Those provisions included "creating a new Federal agency to serve as a clearinghouse for election administration information," "providing funds to states to improve election administration and replace outdated voting systems," and "creating minimum standards for states to follow in several key areas of election administration," (HAVA, 2002).

للاستشارات المنارة
www.manaraa.com

What triggered the need for this law to be passed in the first place was the chaos that ensued during the 2000 US presidential elections. As stated in Martha Kropf and David C. Kimball's book, "Helping America Vote: The Limits of Election Reform," multiple system failures across the US, including fraud with dogs and dead people having been registered to vote, voting system errors, and more specifically, the punch card ballots used in Florida (Kropf and Kimball, 2012). This act radically modernized the way US Federal elections were to be carried out as well as ensured that states were consistent nationally to at least a minimum level.

Protecting the American Process for Election Results Act – PAPER Act

As previously explored, the (HAVA) of 2002 helped to modernize the US election process and has helped to make Federal elections more streamlined across US state lines. With the election interference from Russia, which has been under investigation since the 2016 Presidential elections, there have been calls to amend HAVA. Introduced September 2017, Republican Representative from North Carolina, Mark Meadows, introduced an amendment known as "Protecting the American Process for Election Results Act" or the "PAPER Act." The bill states:

> "To amend the Help America Vote Act of 2002 to direct the Election Assistance Commission to develop best practices for States to use to protect the integrity of elections for Federal office, to make election technology improvement grants to States for adopting and applying such best practices in the administration of elections for Federal office, and for other purposes." (H.R.3751 - PAPER Act, 2017)

المنارة للاستشارات
www.manaraa.com

As of March 2018, this bill has only been introduced to the House of Representatives, but it outlines critical provisions that will ultimately lead to the helping states “develop best practices” for future elections. The bill also helps to modernize the US election process and help it to adapt to the growing threat from external state-sponsored hackers. Furthermore, the bill offers US states Federal grants to each state that meets the provisions outlined in the bill. By providing funding, US states will be able to build a more robust and streamlined election process in the future.

State-Sponsored Election Interference

Based on a leaked, top-secret National Security Agency (NSA) document[3], actors “executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on election-related software and hardware solutions, according to information that became available in Aril 2017,” (NSA, 2017). The threat from external state-sponsored actors has been growing more with every election year, which has politicians, election officials and industry experts looking for ways to counter future interference. While it has been widely assumed that no actual voting tabulation machine was breached and that no vote manipulation occurred, the threat that a state-sponsored hacker could manipulate votes, either by changing or deleting votes, for future elections.

National US Biometric Voter Registration

As of 2018, there are no US states that use biometrics to either register or verify voters. As previously described, biometric technology has been a part of the Federal Bureau of

[3] This document had top-secret information redacted and has been widely reported on from US and other media outlets.

المنارة للاستشارات
www.manaraa.com

Investigation's (FBI) Identification Division since 1903, so the technology itself is not a new advancement. For the average individual, however, this technology is new and becoming more widely used to the average individual user. In the 21st century, it is hard to go very far without seeing a smartphone, tablet, or laptop computer that has facial, fingerprint, or voice recognition technology built into the device. The use of biometric technology has recently begun to find its way into other nation's electoral processes to verify their voter's identities, with the goal of creating more fair and transparent elections. While foreign nations have started to adopt biometric voting processes, this technology has been slow to find its way into US elections. In fact, in late 2015 the Integrated Biometrics, an FBI-compliant fingerprint scanner developer, signed a deal with the Brazilian government to provide fingerprint scanners[4] to help register and enroll eligible voters (Elsevier, 2015). Numerous other nations around the world are taking similar steps as Brazil to curb rampant voter fraud with their countries, like in Nigeria wherein 1999, "subsequent elections suffered from voter fraud as people voted more than once and ballots we cast by dead and fictitious people," (Jaracz, 2011). While voter fraud is not a major problem that impacts the US, the use of this technology would help to solidify the integrity of Federal elections. In the US, over two-thirds of US states require some form of voter ID card on election day. There is substantial debate from both Republicans and Democrats about the legitimacy as to whether biometric identification (ID) cards could solve the issues with voter ID during elections. A stated in an article by Robert Pastor of the Los Angeles Times, "A biometric

[4] 13,000 of Integrated Biometric's Watson Minis fingerprint scanners were provided to Brazil.

المنارة للاستشارات
www.manaraa.com

card has a permanent and unique means of identifying each person and therefore cannot be hacked or forged," (Pastor, 2013).

Discussion of the Findings

Protecting US Elections

Protecting the integrity of US elections from both foreign and domestic interference to the end of ensuring a free, fair, transparent and secure election process is of paramount importance. While there have been many changes since the founding of the US regarding elections and how they are administered, the core foundation has not changed. The ideals of Democracy and a nation ruled by the people, for the people is something that is at the very tradition and lifeblood of the US. With that knowledge, it is essential to know where the US has been, what changes it has made along the way, where it is now, and what does the future hold.

Through history, humanity's desire to be able to associate deeds and actions to any given individual has been vital. Whether for attributing the work of an artist or the crimes of a suspect, it is innate in human nature to identify individuals. Biometric authentication technology is merely an evolution of that innate nature and is needed in the US election process. Since US elections are decentralized and are arbitrated by each US state's election officials, it has created a difficult situation to be able to streamline the process across the US. As discussed laws at the Federal level, there have been laws passed over the years to address some of these state-to-state inconsistencies. Beginning with NVRA of 1993, which streamlined the way states administer voter registration for Federal elections, to HAVA of 2002, which set minimum standards for Federal elections.

المنارة للاستشارات
www.manaraa.com

Election Interference

Russian Interference in US Elections.

Much of the discussion around election interference has mainly revolved around the 2016 US general election and Russian meddling. While the Russian government denies any involvement in the interference, based on a report put out by the Director of National Intelligence,

> "Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation indirectness, level of activity, and scope of effort compared to previous operations. We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin, and the Russian Government developed a clear preference for President-elect Trump," (Office of the Director of National Intelligence, 2017).

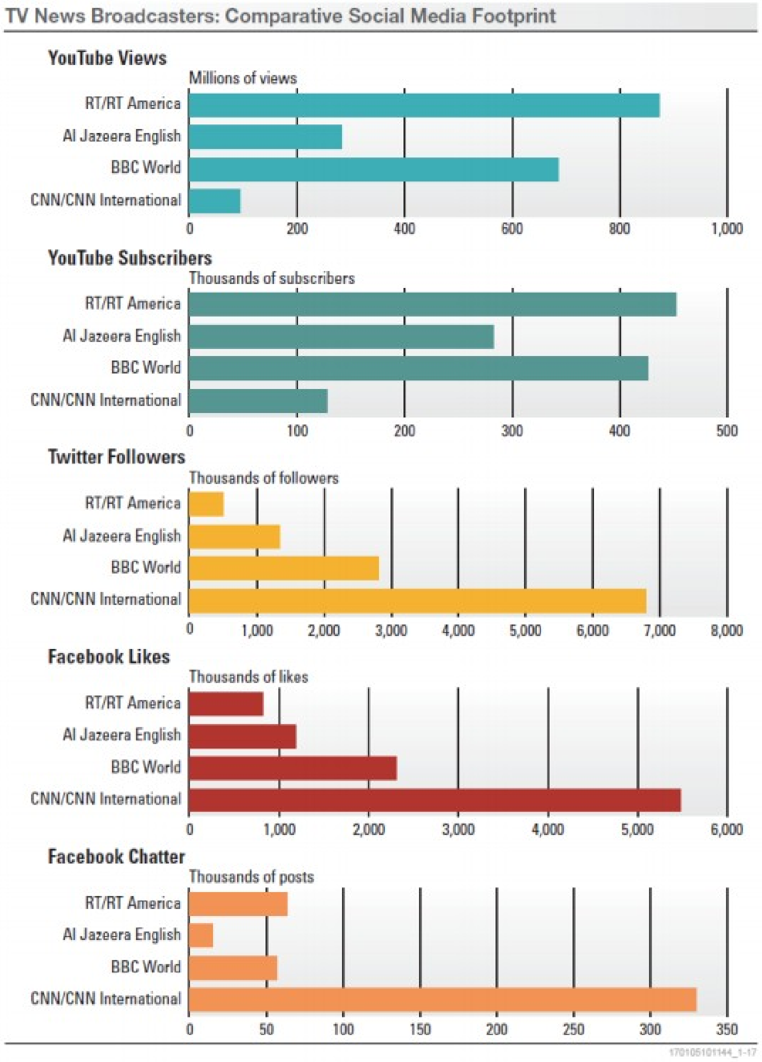
This information makes it clear that the Russians, especially Putin, understand how the US electoral system operates. The Electoral College makes the US very much a numbers game. A campaign that is specifically aimed at influencing voters in key battleground states could mean the difference for a Presidential candidate winning or losing. The fact that Russia understands this dynamic in the US, this makes their influence campaigns a significant risk to future elections.

المنارة للاستشارات

www.manaraa.com

Much of the activity that has been identified with this influence campaign was directed at social media websites primarily on Facebook, Twitter, and YouTube. The ability to sway and influence US voters is exceptionally high, especially with the potential virality of content that is posted to these social media mediums. It is no surprise to see then that there is a significant social media footprint from Russia’s state media outlet, RT, which is very active on many of the most popular social media websites.

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.



المنارة للاستشارات
www.manaraa.com

The information provided in Figure 1 shows that RT/RT America has a dominant presence on video social media platform YouTube. The information shows that RT/RT America has a significant presence on social media, but that is not evidence of interference as CNN, by and large, is dominant in all the other social media platforms. Also, evidence of large-scale campaigns of misinformation conducted by Internet Research Agency (IRA), a Russian troll farm, all through Facebook and Twitter leads to even more compelling parallels. With “70 accounts on Facebook, 65 accounts on Instagram and 138 Facebook pages” (Murdock, 2018) the Russian troll farm “attempted to organize 129 events. Some 338,300 unique Facebook accounts viewed the events, the company said. Facebook said about 62,500 marked they were attending one of the events and 25,800 accounts marked they were interested,” (Carbone, 2018). Facebook has since banned the IRA from its platform and has made repeated pledges that they will attempt to prevent this in the future. These startling findings show how easily foreign state-sponsored hackers were able to generate traffic and organize events and rallies in the US, to undermine the election process.

The US is Not Russia’s Only Target. European nations are also starting to uncover similar interference in their elections, even while the investigation continues to mount in the US to get the whole picture into Russia’s election interference. In a report by The Washington Post’s Rick Noack,

“In the past three years, Russian interference has expanded into such countries as the United States, Germany, France, and Britain, among others. These efforts have ranged widely. For instance, to prevent Montenegro from joining NATO, the Kremlin likely sponsored an

www.manaraa.com

October 2016 coup attempt. In several European countries, Russia helped fund far-right parties such as the National Front in the run-up to France’s 2017 election. Russia waged disinformation campaigns in other countries. And, in Norway and Germany, Russia launched phishing attacks against parties and campaigns,” (Noack, 2018).

Much like the days of the Cold War era, the Russian government, under President Vladimir Putin, has gradually been emerging from the ashes of the Soviet Union to be a significant global power again. The findings that Russia is becoming more engaged in these subversive activities increases the need to create cyber countermeasures to mitigate the interference in a sovereign nation’s election process.

US Adversary Challenges

The Bear Coming Out of Hibernation. The collapse of the Soviet Union in 1989 sent a shockwave across geopolitical landscape seemingly overnight. Many of the satellite nations that made up the USSR had declared independence, further fracturing the might of the Soviet Union. With the USSR having no means to counter the collapse militarily or economically, the US declared victory in the Cold War. With the first election of Boris Yeltsin in 1991, following the collapse, Russia was no longer the Soviet Union but was officially recognized as the Russian Federation. Over the course of nearly two decades, Russia has struggled with political, military, economic, and societal turmoil. The once dominant Soviet Union was now struggling for survival. The 2000 presidential election of Vladamir Putin, however, changed the course of Russia.

المنارة للاستشارات
www.manaraa.com

Under the leadership of Putin, Russia has seen something of a revival. Though Putin's methods over the years have been questionable at best, he has helped to lead Russia on a path of economic growth, which in turn has helped to improve the other challenges that have been facing Russia since the collapse of the Soviet Union. In fact, the changes and direction that Putin has led Russia to have led to a significant trust from the Russian people. A Pew Research poll conducted in 2017 shows that "A full 87% have some or much confidence in Vladimir Putin's handling of global issues…" (Vice, 2017). Though the validity of such a poll could be debated, regardless, it shows the Putin has a firm grasp on making Russia a leading superpower once again.

Not until recently has Russia been able to challenge the US on a global scale. The eruption of the Syrian Civil War changed that. Since Russia's military has not been in any significant full-scale military operations, except for the Georgian invasion in 2008 and Crimea, Syria has been the perfect place for Russia to gain practical military experience. In support of the Assad regime, Russia has aided the Syrian government by pushing back rebels across Syria. More and more every day, Putin's Russia is rising from the ashes of the Soviet Union and proving once again that they can and will be a significant world superpower again.

Russia Versus the West – A New Cold War. Russia's widespread interference in western nation's elections and military actions in Ukraine and Syria are creating an environment for a new cold war. In Syria, Russia has had a military presence with the aim of propping up the Assad regime. The US, in contrast, has aligned itself with moderate rebel groups who are

المنارة للاستشارات

www.manaraa.com

actively fighting against the Assad regime. This scenario has put the US and Russia in a precarious geopolitical position that has the potential to erupt into full-scale confrontation.

Following a suspected chemical gas attack in Douma, Syria on April 7, 2017, which resulted in the deaths of 40 Syrian civilians, Russia's declared that they have "…evidence that proves Britain was directly involved in organizing this provocation," (BBC, 2018). Over the course of a week, the US and European allies mulled over what the proper response to the attacks should be. Western powers declared that there was substantial evidence that the Assad regime directed the chemical attacks on Douma, in contradiction to Russia's claims. In a surprise aerial strike, the US and European allies launched targeted strikes on military targets suspected of the manufacturing and storage of Syrian chemical weapons.

The April 14th strikes marked a new level of escalation in Syria and prompted the UN Secretary General, Antonio Guterres, to declare that "the Cold War is back with a vengeance," (BBC, 2018). Russia and western nations are once again at opposing sides of diverse global interests. Russia's campaign to undermine elections internationally, asserting its power over nations like Ukraine, and even allegedly targeting former Soviet spy with a nerve agent in the UK, are just some examples of Russia posturing and aiming to be a dominant world power again. The dynamic of this new cold war is far more dangerous than the previous cold war, however.

During the Cold War, the constant fear of an all-out nuclear war was ever present on the everyone's minds. The genuine threat of nuclear annihilation created a tense and anxiety-ridden global society, which also acted as a deterrence. Just the fear of nuclear retaliation helped to

المنارة للاستشارات

www.manaraa.com

deter Russia and the US from using nuclear weapons. Instead, the US took on a policy of containing the spread of Communism, where ever the ideology attempted to spread. The result of this containment policy led to proxy wars, including Korean War, Vietnam War, the Soviet-Afghan War, and many more. The collapse of the Soviet Union in 1989 ended the Cold War as well as the constant fear of nuclear annihilation. During the Cold War, both the US and Russia, while adversaries, had a mutual respect and fear of the other's power. Today, however, that mutual respect is somewhat diminished if not absent. Going back to the statement of the UN Secretary-General, Guterres continued by saying, "The mechanisms and the safeguards to manage the risks of escalation that existed in the past no longer seem to be present," (BBC, 2018). Though the fear of imminent nuclear destruction may not be present, the election interference and Syrian conflict are creating the potential of a direct US, and Russian conflict is becoming increasingly more likely.

Threats from China. In 2015, the US and China signed a truce which promised that both sides would refrain from hacking private companies. The relationship between the US and China has at best been a love, hate relationship. In the US, it is nearly impossible for one to go anywhere without finding something that was made in China. Many of the parts that are used in phones and computers are made in China. While China is a significant trade partner with the US, China is always looking for ways to improve their technologies to continue their rapid economic growth. As a result, the need for the 2015 truce came in response to Chinese state-sponsored hackers targeting companies specifically for intellectual property. In fact, much of the political

المنارة للاستشارات
www.manaraa.com

rhetoric against China from President Donald Trump has been centered around the theft of intellectual property by China and according to the New York Times, the theft of intellectual property covers a wide array of areas such as “counterfeiting fashion designs, pirating movies and video games, patent infringement and stealing proprietary technology and software,” (Blair, Alexander, 2017).

Theft of intellectual property does not necessarily relate to a threat to US elections as much as it does to a company’s bottom-line, but the implication of such blatant theft could have further implications. While there have not been any clear indications that the Chinese have outright violated the 2015 truce, there have been indications that hackers at least from China have been engaging in cyber-attacks on US companies as well as espionage. To that point, in 2016, cybersecurity company FireEye saw Wekby, a suspected Chinese hacker group, target numerous US, Canadian, and European based targets in the petrochemical, tech, and insurance industries (Greenburg, 2017). While it appears that China is toeing the diplomatic line in these attacks, the Chinese have the skills and sophistication to be a severe cyber threat to the US.

Threats from Iran. Iran, much like Russia, is in an adversarial and even hostile relationship with the US. Going back as far as the 1978 Iranian Revolution, the Theocratic Islamic Republic has been at odds with the US ever since. The conflict in the Middle East is complicated, and many of the conflicts revolve around a power struggle between two countries, Iran and Saudi Arabia. These two Middle Eastern powers are continually engaging one another through proxy wars, much in the same fashion as Russia and the US engaged in proxy wars during the Cold War. Amid this conflict, the US has established strong economic and military

المنارة للاستشارات
www.manaraa.com

ties with Saudi Arabia. On top of that, the US's alliance with Israel has further deepened the adversarial relationship between the US and Iran.

Iran has kept its distance in a confrontation with the US and only really enabling insurgency and terrorism in Iraq, Afghanistan, and Syria against the US. Where Iran has been able to engage the US directly is in cyberspace. Over the years cyber security company, FireEye, has been tracking and researching cyber-attacks originating in the Middle East, with attention to Iranian based hackers. Having identified a group known as APT33 and were able to identify "…APT33 malware tied to an Iranian persona who may have been employed by the Iranian government…" (FireEye, 2017). Iran's cyber capabilities have proven to be quite sophisticated, and with Iran's close friendship with Russia, Iran is likely learning from Russia's capabilities. Given the hostile relationship that Iran has with the US, this presents an additional and potentially dangerous cybersecurity threat to the US and its allies internationally.

Threats from North Korea. The reclusive nation of North Korea has been a significant diplomatic stumbling block for US Presidents as far back as Richard Nixon. Many things are not fully understood about North Korea, but one thing that is known is that they have historically been very hostile to the US and its allies. The threat that North Korea's nuclear program overshadows another threat from this nation that, if not curtailed, could prove to be detrimental to US economic interests and even critical US infrastructure.

A group known as the Lazarus Group, which has been attributed as being of North Korean origin, unleashed a ransomware attack around the world. Using a vulnerability and a tool

المنارة للاستشارات
www.manaraa.com

that was secretly created by the NSA, known as EternalBlue, the Lazarus Group exploited computers running Microsoft's Windows 10 operating system (OS) and demanded bitcoin in exchange for the decryption key on the computer's files (Fruhlinger, 2017). This attack, referred to as WannaCry, was one of the worst incidents of global ransomware that had been seen. It highlighted the threat that a small group of hackers could cause. This attack was financially motivated, and it has been assumed that many of these cyber-attacks that have been perpetrated by North Korea are a means to funding the heavily sanctioned nation.

The financially motivated attacks put businesses on edge and can keep corporate security teams up at night, but the real danger is when these attacks are turned into weapons. The bellicose rhetoric that routinely comes out of North Korea could go from mere words to real action. Instead of the cyber-attacks being financially driven, they could be focused on pure sabotage and disruption. Attacks like WannaCry have shown that North Korea is a real cyber threat and could begin to take plays straight out of the Russian playbook. North Korea has the potential to become a significant interference in US elections and the economy. By using ransomware and denial of service (DDoS) attacks, the North Korean government could severely disrupt, if not cripple, multiple industries across the US.

Challenges of US Federal Elections

Electoral College. Since the ratification of the US Constitution until 2018, the US has had 44 Presidents[5]. In that time there have only been four instances where the President-Elect

[5] President Donald Trump is currently the 45th President, but there have only been 44 Presidents under the current US Constitution, with President Grover Cleveland having served two non-consecutive terms.

المنارة للاستشارات
www.manaraa.com

won the electoral vote but did not receive the popular vote. As was previously stated, the Tenth Amendment of the US Constitution mandates that "Each state shall appoint, in such a manner as the Legislature thereof may direct, a Number of Electors, equal to the whole Number of Senators and Representatives to which the state may be entitled in the Congress…" (US Constitution, 1791). This body of electors is known as the Electoral College. Based on the overall population of a given US state, this determines the number of electoral votes be assigned to a given state. The six states that command that largest populations and electoral votes are California, Texas, New York, Florida, Illinois, and Pennsylvania[6]. Based on the results of the 2016 Presidential Election, Donald Trump received 306 electoral votes and 46.6% of the popular vote, while Hilary Clinton received 232 electoral votes and 48.5% of the popular vote.

US elections are a game of numbers. A Presidential candidate can win or lose depending on whether they can win the votes of crucial battleground states, such as Florida, Ohio, Iowa, as well as other states. Rather than how many actual votes were cast in favor of a candidate a Presidential candidate can win the election based on the number of electoral votes, rendering the popular vote unimportant. This situation first occurred in 1824 with John Quincy Adams, followed by Andrew Jackson. More notably and in recent memory, the 2000 election of George W. Bush and again in 2016 with Donald Trump, both did not receive the popular vote, but did capture enough battleground states to win the Presidency ultimately. As a result, the Electoral

[6] Electoral Vote Counts: California (55), Texas (38), New York (29), Florida (29), Illinois (20), and Pennsylvania (20).

المنارة للاستشارات
www.manaraa.com

College process, among other factors, has generated an overall lack of public confidence in the electoral process and a weakness that state-sponsored actors can take advantage of.

Bi-Partisan Polarization. The lack of confidence in the electoral process is further fueled by the deeply entrenched bi-partisan polarization between Republicans and Democrats. Both parties tend to disagree on how policy should be carried out. As a result, there is a significant amount of gridlock in getting new, significant legislation passed at all levels of government. As shown in a poll conducted by Pew Research Center in 2016, "…Voters said little progress had been made over the last eight years across major areas…" (Pew Research Center, 2016). This perception-based attitude is in part a result of partisan politics at times trivializing issues.

Electoral Integrity Across US States. Due to the decentralized nature of the US election process, many local and state governments have different laws that likely differ from the laws in any other US state. Except for Federally mandated laws like NVRA, HAVA, or other similar constitutional laws or guidelines, states are free to run their elections how they see fit. For example, according to the National Conference of State Legislatures (NCSL), there 34 states that request or require voters to show some form of identification, while the other 16 states verify voters through other means at polling locations. (Underhill, 2018). Even if the states that require identification, there are even varying degrees of what kind of identification and how strictly the enforcement is of these laws. Based on research from the Brennan Center for Justice states that "There have been a handful of substantiated cases of individual ineligible voters attempting to defraud the election system. But, by any measure, voter fraud is extraordinarily rare," (Levitt,

المنارة للاستشارات

www.manaraa.com

2007). This finding shows that perhaps election fraud is not a primary concern, yet it remains a significant concern for many and continues to be a significant challenge in US elections.

Biometric Voter Registration and Authentication

National Voter Biometric Database. Voter identification, as mentioned previously, is an actively debated topic. For those who oppose it, they assert, as illustrated by the American Civil Liberties Union (ACLU) that about 11% of Americans do not have any form of government ID, that, to obtain a voter id, costs individuals money to obtain underlying documentation to get the identification, travel is a burden on individuals with disabilities or who live in rural areas, reduce voter turnout, as well as discriminatory in how states enforce their identification laws." (ACLU, 2017). In many regards, the points that the ACLU and others bring up are valid concerns and many of which have been addressed even in Federal legislation.

On the opposite side of the aisle are those who are in favor of strong voter identification laws. As put forth by the Bill of Right Institute, strong voter identification laws verify a voter's identity to ensure a one-vote-per-person system. They also assert that, "there are many cases in which people registered in multiple states vote multiple times, deceased registered voters cast a ballot—someone is fraudulently claiming to be the deceased voter, and non-citizens vote in large numbers, though they do not possess the legal right to do so," (Bill of Right Institute, 2018).

By creating a national voter biometric database, many of the concerns on both those for and against are addressed. As pointed out by the ACE Project, biometric voter cards are reliable; it acknowledges a voter is registered, and it can also be customized to have several forms of identification, like photograph, fingerprints, or signature. Other benefits highlighted are that they

المنارة للاستشارات
www.manaraa.com

can be digitally marked, eliminating any attempt to vote twice, it is excellent for voters who have no fixed address, a voter can vote anywhere and still be counted once, among many other advantages (ACE Project, 2013). As for the potential of state-sponsored interference, the use of biometric identification cards would help to at least mitigate any future potential of over inflating election results, as the digital signature that would be captured upon voting could raise red flags early.

While there would have to be significant reforms in place at the Federal level, US states could be aided with grants to be able to facilitate the collection and issuance of biometric voter identification cards. As an added point, given that many American's have at one time or another provided fingerprints, especially if they are a Federal employee, these fingerprints are already stored in the FBI's fingerprint database. This information could then be shared with local and state election officials to help facilitate a timelier process of issuing the biometric identification.

Comparison of the Findings to Other Nations

Nigeria – Requires Biometrics in National Elections. In 2011, then DigitalPersona Director of Product Marketing, Chris Trytten, stated that "In Africa, many countries are embracing democracy," and that "The foundation for democracy [necessitates] secure voting systems to provide results people trust," (Jaracz, 2011). In the same year, Nigeria began collecting biometric information that would then be used to create biometric identification cards. Starting in January 2011 and as little as three months before the national election, Nigeria was able to register 73 million of the population or roughly half of their population, and the election received bipartisan praise from both observers and citizens stated that the election was fair

www.manaraa.com

(Jaracz, 2011). The implications of this system, in a nation that has historically had a very turbulent political past and having broken away from its military-run junta government in 1999 is promising and shows future potential in the development of biometric voting systems in the US and globally.

Brazil – National Biometric Rollout in 2018. Brazil, like Nigeria, has had a turbulent political past. Brazil also was ruled by a military junta until the early to mid-1980's and has had a very rocky civilian-led government since then. Unlike most Democratic nations, Brazil is one of the few that also has compulsory election laws for its citizens. According to Chris Trytten, who is also helping Brazil with their biometric voting system, stated, "[The Brazilian government] went to great lengths to make this transparent. The process was completely audited, with a group of people who examined the software and hardware and digitally signed it to ensure its legitimacy," (Jaracz, 2011).

Yemen – Interrupted by Conflict. In the Middle East, democracy has been an elusive ideology that has encountered many challenges and even resistance. Yemen was one such Middle Eastern nation that was striving to legitimize their democratic republic up until late 2014. With help from the International Foundation for Electoral Systems (IFES), Yemen had plans to roll-out a nationwide biometric-based voter registry for fall of 2014, ahead of the 2015 constitutional referendum (IFES, 2014). However, the Houthi led coup d'état on the Yemenis capital in September of 2014 brought this entire process to a halt[7]. This case study does highlight

[7] As of March 26, 2018, at least 10,000 Yemenis had been killed by the fighting, with more than 40,000 casualties overall, with millions more displaced (Aljazeera.com, 2018).

المنارة للاستشارات
www.manaraa.com

a general failure to implement the biometric-based voter registration in Yemen but does offer valuable insights. The example in Yemen shows that even nations going through politically turbulent are looking to biometrics to improve and legitimize their governments, where confidence in such institutions is typically low.

Solomon Islands – Biometrics in the Pacific. Look at a map of the world, finding the Solomon Islands could be a challenge if one did not know where to look. This small Pacific island nation, off the east coast of Papua New Guinea, is currently in the process of implementing a biometric voter registration system. Supported by the EU and Australia, via the United Nations Development Program (UNDP), the Strengthening the Electoral Cycle Project in the Solomon Islands (SECSIP) aims to achieve voter awareness and engagement, electoral reform, and have a more accurate voter registry and better-administered elections (UNDP, 2017). The continued success of the implementation of the Solomon Island's biometric voter registration has shown the valuable benefits of using biometrics to tighten up voter registration records and ultimately ensure more reliable and transparent elections.

Afghanistan – Eliminating Widespread Voter Fraud. Since the 2001 invasion of Afghanistan by the US-led coalition, Afghanistan has understandably had some significant challenges throughout the nation. A nearly two-decades-old war with the Taliban, Al-Qaeda, and other insurgency elements have ravaged the nation and its people. Building a stable democracy in a nation that has been at the center of centuries of conflict makes Afghanistan one of the more ambitious attempts at implementing biometrics in their electoral process. However, this is a challenge that the nation's Independent Election Commission (IEC) is actively pursuing.

المنارة للاستشارات
www.manaraa.com

Collecting two sets of biometric data for each applicant, which will include a full set of digital fingerprints and a facial photograph the IEC will be able to overhaul their voter records, while also meeting the requirements for the new national ID card (Darnolf, 2017). By doing this, Afghanistan could be closer to eliminating the widespread voter fraud that has occurred in past elections and arguably has one of its first genuinely reliable elections.

Zimbabwe – Voter Registration and Verification. Zimbabwe is one of several African nations looking to have more free and fair elections using biometrics. Beginning in March 2017, Zimbabwe captured voters' biometric information using their fingerprints and facial imaging and stored in a central database (Gambanga, 2017). Political upheaval has been a common problem in Zimbabwe, even amid these electoral reforms. Under the rule of Robert Mugabe and the dominant ZANU-PF party since the 1980's, Zimbabwe has had a mix of significant national improvements as well as equally significant corruption and human rights violations. Though there will be no electronic voting in Zimbabwe for the 2018 election, with Robert Mugabe having stepped down under mounting pressure, Zimbabwe will be using the Biometric system for voter registration to ensure that voting records are accurate (Gambanga, 2017). Zimbabwe is expected to implement the biometric system in its entirety in the future with the further development of the system.

Somaliland – Legitimacy Through Biometrics. The self-declared nation of Somaliland is a nation that might be the best example of a successful implementation of a biometric voting system. On November 13, 2017, this small autonomous nation was the first nation in Africa and the world to use iris recognition-based voting systems (Awkei, 2017). Using iris biometrics for

المنارة للاستشارات
www.manaraa.com

voting illustrated the benefits of the technology by reducing, if not wholly, eliminating duplicate voting. The biometric voting systems, in turn, help to not only legitimize Somaliland's electoral process but also show the world that it is a stable and viable nation, worthy of international recognition. Somaliland does still face many challenges regarding foreign relations, but their use of biometric voting systems shows the viability of these systems and the benefits they can provide when implemented successfully.

Limitations of the Study

In 2018 there is currently no US state that uses biometric identification to facilitate voter authentication in elections. There are some use cases of other nations utilizing biometrics in elections, like in Brazil, Nigeria, Somaliland and several other nations; however, many of these countries have only begun to apply them at the national level. The goal of this study is to address the significant limitation that there have not been many comprehensive case studies conducted in the US that illustrate the viability and justification of the creation of a national voter biometric database. Due to the complexities of the US electoral system and a reduced prevalence of voter fraud, use cases from those other nations will only be helpful to a point. Further research and more case studies would be required to mitigate the level of limitations of this study and to apply it to US elections.

Also, the most significant limitation of this study resides less in the actual implementation of the technology, but in the voters themselves. Americans have a serious trust problem when it comes to the US federal government and implementing a technology that would require the collection of biometric information could be problematic. In fact, according to a

المنارة للاستشارات

www.manaraa.com

Gallup poll conducted in 2017 showed that only 28 percent of Americans have a favorable opinion of the US federal government (Jones, Newport, Saad, 2017). With this low level of trust and much of that trust issue being directed at Washington D.C., the chances of a political divide and overall resistance would be expected.

The other limitation that arises out of this trust issue is that there have been numerous high-profile data breaches that have left personal information vulnerable. The breach at Equifax, misuse of user's Facebook information by Cambridge Analytica, and many other violations of one's privacy has created a problem. Confidence in companies and the government's ability to protect digital information has been dramatically diminished. To ask Americans to provide their unique biometric information could prove to be a hard-political fight and a significant limitation of the study.

Recommendation

The US Legislative Branch

The US Legislative Branch is the primary governing body that would need to take the lead on passing a law that will offer robust federal support and guidance to US states regarding federal elections. On March 23rd, 2018, some progress was made to provide such aid to the states. With the passage of the omnibus appropriations bill for the fiscal year 2018 will "set aside nearly $400 million in funds across two election cybersecurity initiatives: the pre-existing Election Assistance Commission, as well as a new Election Infrastructure Security Initiative under the Department of Homeland Security," (Burr, 2018). Additionally, setting up a framework for the national biometric database, as well as ensuring proper security standards will

المنارة للاستشارات
www.manaraa.com

be put in place to protect all the information that will be stored. It is recommended that the law being passed will put the federal government in a support and oversight role to ensure that states are administering federal elections in a consistent and streamlined manner.

National Voter Biometric Database Framework. The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is a perfect example of a national database that can acquire, collect, classify, and preserve identification and can be disseminated to all authorized entities. Creating a new election database that is separate, but comparable to how the IAFIS operates. Adding the ability to be able to migrate fingerprint data from IAFIS over to the new federal election biometric database will provide an efficient way for individuals to register quickly and without the need to provide their biometric information again. The federal election database would also need to be able to communicate to US state biometric databases so that the national database will be able to deconflict duplicate or ineligible entries across all 50 states. By following the framework of IAFIS, this will ensure election integrity and prevent potential election fraud.

Protecting the National Election Biometric Database

Maintaining tight security on the national election biometric database is not only recommended but vital for the overall viability of this system. To provide the level of security that is needed will require a dedicated security team that monitors and maintains the database. Resources would need to be allocated either from already existing funding for the Executive Branch or the Legislative Branch will need to provide additional funding to support the defense of the election database.

المنارة للاستشارات

www.manaraa.com

Giving the database security role to (DHS) would be a reasonable step, as the DHS already runs the National Cybersecurity and Communications Integration Center (NCCIC) and the National Infrastructure Coordinating Center (NICC). These DHS centers already work to ensure that US critical infrastructure is secure. On January 6th, 2017, DHS also designated electoral systems as critical infrastructure. "Under the new designation, states that request cybersecurity assistance can receive swifter access to threat intelligence and be able to participate in joint defense exercises." (Starks, 2017). DHS is already heavily involved in protecting the electoral process and would require few resources to provide the necessary security.

Another option would be giving the database security role to US Cyber Command. Like DHS, US Cyber Command is already a well-structured entity that is dedicated to protecting the US from cyber-attacks from both foreign and domestic hackers. US Cyber Command operates under the Department of Defense (DoD) and according to their mission statement US Cyber Command, "plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified DoD information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." (U.S. Strategic Command, 2009). US Cyber Command is, however, primarily a military-operated entity. Giving this power to the military could present potential reservations among US voters and local, state, and federal politicians and would have to implemented in such a manner as to ensure full transparency to the public.

المنارة للاستشارات

www.manaraa.com

Protecting the national election biometric database is a vital step that must be done correctly. Ensuring that proper resources are allocated to set up and protect the database is an essential first step that the Legislative Branch would need to determine. After that, determining who would oversee securing the database would be the next step. DHS and US Cyber Command both have the resources and personnel to implement a proper security plan for the election database. Since DHS is already looking at electoral systems as critical infrastructure and providing states and companies with services and resources, DHS would likely be the recommended choice. US Cyber Command would be just as well equipped to take on this role; however, since it is a military entity under the DoD, it could potentially be more difficult to get US voter and politician buy-in.

Buy-In from the States. Creating a law that will allow for federal support and oversight in federal elections while not taking over the state's control will be imperative to gain buy-in from the states. Using the laws that already exist, like NAVA, HAVA, and the PAPER Act, and building upon that will help strengthen the law. Crucial provisions that should be included are that states will need to create a central state election biometric database that will be able to communicate with the national election biometric database. There will also need to be a provision that guides the states on how they should register new and existing voters into this new system. It is essential to provide for lateral movement to the states since many states are different and have their unique challenges when it comes to elections that the federal government will not be able to account for.

المنارة للاستشارات
www.manaraa.com

States will need help to implement the program, whether it be administrative or technological support. This is where the support from the leading federal entity, like DHS, will come into play. The federal entity will be able to act in a consultant capacity to help states bring the new federal election process in line and aid in the biometric collection process if necessary. As for the oversight aspect of the entity, it is not about the control over how states are administering their elections, but instead, it will ensure that minimum requirements are met. The focus of oversight would be to ensure each state is collecting biometric information, issuing national biometric voter identification cards, and providing a set standard of database security for state election biometric databases. It is imperative that states still maintain control over how they administer their elections, with the federal government acting only as an advisor to help implement the new law to guarantee state buy-in,

Election Interference Recommendations

Outside threats from state-sponsored hackers, such as Russia, are a significant concern that must be addressed. Creating a national biometric system is a good start, as that will prevent potential voter fraud in the event a voting machine was hacked into. Addressing social media websites like Facebook, Twitter, Instagram, and others is another area that must be looked at to prevent campaigns of misinformation. Additionally, creating a policy that results in a strong response from the US in the event of election interference will help to deter adversaries from engaging in these tactics.

Voting Machines – Biometric Defense. Implementing biometric voter ID not only prevents citizens from being able to commit fraud, but it also prevents it from external

المنارة للاستشارات
www.manaraa.com

adversaries as well. If a state-sponsored adversary was able to gain access to a voting machine, there is not much the hacker would be able to do, other than cause a denial of service. Using biometric identification prevents the use of voting number inflation because as the votes pass through the national database, these votes would be de-conflicted and rendered invalid. It is advised that the election system is constructed in a manner that the voter biometric identification card would be scanned upon arrival at the polling place to confirm voter eligibility, which would create a database entry log. The voter would then need to use the biometric card on the voting machine which would create another entry log. Upon completion of the ballot, removing the biometric card would then create another log, which would show when the ballot was completed. So, even if the hacker would be able to gain access to the voting machine, they would have to account for three separate event logs that the state and national biometric databases will utilize to deconflict any voting irregularities or anomalies.

The Problem with Social Media. The US and much of the world enjoys interacting with one another on social media websites. Social media has brought the world closer than ever before and has led to the proliferation of ideas. Like with all things, where it is good, there is also bad. These social media websites are giving state-sponsored hackers a platform in which to spread misinformation. Given the revelations of state-sponsored hackers and "Russian troll farms" in the 2016 election, the need to find a way to prevent future misinformation campaigns in the future is vital.

المنارة للاستشارات
www.manaraa.com

Further issues related to social media revolves around the overall privacy and security of user's information. One such example would be the recent revelations of the data-mining company, Cambridge Analytica, and their role in the misuse of over 50 million user's personal information on Facebook. Former Cambridge Analytica employee turned whistleblower, Christopher Wylie, revealed that Cambridge Analytica was active in over 200 political campaigns worldwide, from Brexit to the 2016 US Presidential Election, attempting to sway voters in those elections. (The LNP Editorial Board, 2018). This situation has not only put Facebook in the spotlight but shows a severe problem that social media presents regarding user information. The misuse of all this private user data is a severe breach of user trust and has serious implications that the information being gathered from users is harmful to democracies worldwide. Events like this could lead to government reactions that include but not limited to regulating social media providers to the way in which they handle and share user data with third-party groups.

Regulations on social media giants like Facebook, Twitter, and Google would more than likely prevent future occurrences, but slowing the innovation that is produced by these companies would likely suffer. These companies first need to be willing to admit that there is an inherent problem that they cannot fix on their own. Just like the support that would be provided to the states to implement the biometric systems and databases, the federal government could partner with these companies. By acting in a consultancy role, the federal government will be able to assist in creating stronger defenses against misinformation campaigns. This would also allow these companies to continue to innovate as they have been without regulatory burdens.

المنارة للاستشارات
www.manaraa.com

Digital Nuclear Deterrent. There is little deterrence in the digital realm and cybercrime is a low risk, high reward action that many are taking advantage of. The same goes for interfering with the elections of other nations. Lack of consequences or strong responses ultimately enables state-sponsored actors to engage in these activities. Much like the days of nuclear deterrence, the US must create a policy that will make adversaries think twice before engaging in hostile digital actions.

The digital nuclear deterrence policy would likely be carried out by US Cyber Command, as it is developing more and more into an offensive cyber force. When an adversary is identified it should be the policy that the US will retaliate in force, regardless of the perpetrator. This policy would inevitably define the scope of cyber warfare but is necessary. By having a strong response policy, this would help to mitigate future state-sponsored attacks.

Pros for Digital Nuclear Deterrence. By having a digital nuclear deterrence that would be arbitrated by US Cyber Command, several aspects to this would be beneficial. Presently, US Cyber Command is an organization that is already well-structured and conducting cyber operations daily. Being on the front lines of the US's cyber defense and offense would make US Cyber Command a logical choice to set up deterrence posture. Since this is a military organization, it also has the added benefit of getting high talent from many different backgrounds, which would help to create an agile and creative cyber force that would be able to counter and initiate cyber-attacks coming from adversarial

المنارة للاستشارات
www.manaraa.com

state-sponsored hackers. US Cyber Command would be the most well prepared and able organization to carry out and conduct such a policy.

Cons Against Digital Nuclear Deterrence. While a policy set up a digital nuclear deterrent through US Cyber Command could be a way to create a high risk, low reward situation for hackers, there are potential problems that could arise from a policy like this. By creating a very aggressive cyber response following a breach, some potential political ramifications would need to be considered. Much like wars must typically be justified, or risk international condemnation, a nation must show evidence and rationale for the action. Much of cyber warfare is done in the dark and rarely does any nation typically claim responsibility for the action. By creating a digital nuclear deterrent, the US would mostly be coming out of the shadows and would likely need to justify targets to at least their allies, if not the international community. Additionally, most targeted cyber-attacks have been benign regarding actual life impact. A digital nuclear deterrence could inadvertently create a scenario where instead of interfering with elections, state- sponsored hackers are turning off the cooling reactors in nuclear power plants. While the cons are something that needs to be considered carefully, in either case, the US must move to put safeguards in place to ensure that cyber-attacks do not go from benign to deadly.

Recommendation Feasibility

Voter Biometric Policy. The ability to implement new systems and process for elections may be daunting, but they are impossible. Some companies are already highly specialized in

المنارة للاستشارات
www.manaraa.com

implementing biometric voting systems, so it would not be hard to convert over to these systems in the US. Perhaps the most significant challenge will be getting individuals registered. Many individuals have at one time or another provided fingerprints. Utilizing the information that is already stored and migrating it over to the voting databases would make registering much more feasible. That would leave the remaining population that has never given fingerprints. With the support from the federal government, states would be able to determine the best way to collect this information, which would not be hard, but could take time to complete.

The most prominent challenge comes from the US Legislative Branch. This entire policy hinges on the ability of Congress to pass a bipartisan law that will allow for these changes to be implemented nationally. This would not be a law that would want to be passed quickly. Ensuring that both Republican and Democrat representatives come together to put together a bill that addresses the current problems with the US election process is essential and therefore should not be rushed or politicized. Once Congress can pass a law that can incorporate the recommendations in this study, the feasibility implementing a national election biometric database will be closer to reality.

Social Media Partnership. There is no shortage of skepticism when the federal government wants to get involved in something. It is hard for companies like Facebook, Twitter, and Google to ignore the fact that their platforms were used to create misinformation that could have potentially swayed the 2016 election. It is the recommendation of this study that the federal government does not act as a regulator or overseer, but more like a partner. By utilizing the resources of the federal government, these companies will be able to create stronger defenses on

المنارة للاستشارات

www.manaraa.com

their platforms, which will help to protect the integrity of US elections. This would also ensure the autonomy of these social media platforms and prevent any innovation crushing regulations from having to be implemented to achieve election integrity. The overall feasibility of the recommendation mostly with how the companies would receive such a recommendation and how open to a close partnership with the federal government they are. There would also likely need to be a guarantee from the federal government that upon conclusion of the partnership, that they will no longer have access to any systems the company may have provided them with.

Conclusion

The confirmation of Russian interference in the 2016 elections shook US ideals and confidence that democracy can ensure free and fair elections. Technology continues to grow at a rate that is outpacing the ability to defend against hostile adversaries and cybercrime is growing at an even faster rate. To ensure a free, fair, transparent and secure election process, reforming the election necessary. The US has been working to fine-tune the election process for over 200 years, so it is a natural process for the US to take the needed steps to take the necessary steps.

The way forward is not by only making sure that current voting systems are secure. The US must create look into new technologies that can be used to defend against adversaries at the source. As of 2018, hard-copy lists are still used by poll workers to cross-reference voter provided identification, and with limited to no additional authentication, the voter is given their ballot. Modern technology has rendered this method of verification unreliable, insecure and

المنارة للاستشارات

www.manaraa.com

entirely obsolete and needs to be changed. By having the US switch to biometric centric voter registration and authentication, the US will be able to preserve the integrity of future elections.

As discussed, the use of biometrics is not a new technology, so it has been extensively tested as a viable form of identity verification. As it relates to this study, the issue is that there are some gaps in knowledge as to what a biometric election system would look like here in the US. Many countries have successfully implemented biometrics in their elections, but the population and political climate of some of those nations still leave some questions as to how it would work in the US.

Throughout this study the primary theme has been how does the US protect the integrity of US Federal elections from both foreign and domestic interference and ensuring a free, fair, transparent and secure election process is a pressing national concern. This is a question of national concern and is a question that must be answered sooner rather than later. Focusing on biometrics to register, store, and authenticate US voter's information provides the one way that the US may achieve the ability confidently protect the integrity of elections.

By looking at the overall history of the use of biometrics helps to conceptualize the use in a modern context. Biometrics have been used to identify individuals as far back as 35,000 to 40,000 years ago, with just a simple hand impression on a cave wall in Indonesia. As time went on, humanity found that individuals fingerprint not only have specific patterns to them but that they are also unique to the individual. This discovery has been indispensable in the progression of law enforcement, as well as in the government and private sector.

المنارة للاستشارات
www.manaraa.com

In the US, it was discussed how elections for the US Presidency has always been administered by the states. This is the power that has been given to the states by the Tenth Amendment of the US Constitution. As a result, each state differs in how elections are administered and even how voters are verified. As situations have arisen, the federal government has had to curtail some of that power by providing laws that guide the states as to how they need to administer federal elections.

Under the National Registration Act of 1993, this provided US citizens the ability to register to vote by mail, which also led to the creation of the national mail registry. Several years later, the US would then pass the Help America Vote Act of 2002, in response to the 2000 elections. This law helped to address multiple election system failures, with the prime example resulting from Florida’s punch card ballots. This act helped to modernize US Federal elections and ensure states were administering elections more consistently. Later in 2016, another election law was passed, known as the Protecting the American Process for Election Results Act or PAPER Act. This bill amended provisions within HAVA and set guild lines to states on how they were to protect the integrity of US elections and provide grants to states who improved election technology. Through these bills, the US has been able to adapt and modernize as the need arose.

The use of biometrics is exceptionally prevalent in our society today. Nearly every hand-held device has the option to use fingerprint, facial, and voice recognition to unlock the device and apps. While biometrics are being used in other nations for elections, the currently are no

المنارة للاستشارات
www.manaraa.com

states that are utilizing this technology. The use of this technology could be used in elections to reduce what little voter fraud that occurs in the US as well as protect the integrity of elections from outside adversaries.

With the rise of Russian interference in US elections, as well as elections of European nations, steps must be taken to counter these actions. The presence of “Russian troll farms” on social media platforms is also a cause for concern and must be addressed not only by the federal government but the very companies that control these platforms. The Russian government, under Vladamir Putin, has been vying for a top position on the world stage again. With their presence in Syria in allegiance to the Assad regime, Russia is rechallenging western nations. Actions like the election interference and Syria must be met with stiff US action to face any challenges that the Russian government may pose.

Along with Russia, numerous other adversarial nations represent a real threat to the US. Among them is China, who seeks to undermine the US in the global economy which could, in turn, result in using cyber-attacks to not only steal intellectual property but to also contribute to election interference. The growth and rapid expansion of China have made them a significant force on the world stage and present a potentially high adversarial risk.

Threats from Iran and North Korea also pose a significant problem to the US. Those these two nations are smaller on the world stage, they both hold a great deal of power in the diplomatic arena. Both nations have also proven that they are adept at carrying out cyber-attacks that can wreak some serious havoc around the world.

المنارة للاستشارات
www.manaraa.com

This study has pointed out the complexities of US Federal elections. With the Electoral College, bi-partisan polarization, and electoral integrity across all 50 states, managing federal elections can be daunting. By establishing a biometric voter registration and authentication system, the use of a national voter biometric database would help to streamline these complex processes. In fact, looking at nations like Nigeria, Brazil, and other nations who have had turbulent political histories, have been able to implement biometrics into their elections and have thus proven highly successful. Using these nations as an example, the US should begin to make this change into a biometric voting system to further protect the integrity of US elections.

Since there are currently no states using biometrics in elections in 2018, there is a significant limitation as to how precisely the biometrics would work in the US. Many nations are in their infancy of using biometric technology, so while the information coming out about their elections under these systems are optimistic, there is still room for uncertainty. This study has set out to help address one of the very limitations to this study, which is that there is no real comprehensive case study conducted in the US that can be used to identify potential shortcomings. Biometrics is used in elections is a relatively new topic that would require further investigation and case studies to further address the validity of the use of biometrics in elections.

While challenging, the feasibility of creating an electoral system based on biometric authentication is doable. Many citizens have provided fingerprints at one time or another that could easily be migrated to the new systems. From there it would be a process of finding the best way to register other voters and move on from there. Again, the most prominent hurdle is not

المنارة للاستشارات
www.manaraa.com

necessarily the implementation of the system itself, but getting legislative support as well as state buy-in to the system. As for the feasibility of the government working in partnership with companies, this is also very doable. The government is already very much involved with many private companies. By coming together with these social media platforms, solutions to these election interference problems could be resolved more efficiently.

The world is continuously changing, and threats from adversaries are always changing and adapting. Looking at ways to change and adapt faster than the adversary is something that is vital for the US. Technology has so far proven to be a blessing and a curse. To ensure that the ideals of the US are maintained, it is crucial that the US look for ways to use technology, while also not restricting the rights of the individual. As this topic is further discussed and solutions are uncovered, the use of biometrics has a future in US elections.

المنارة للاستشارات
www.manaraa.com

References

ACLU. (n.d.). Oppose Voter ID Legislation - Fact Sheet. Retrieved March 11, 2018, from https://www.aclu.org/other/oppose-voter-id-legislation-fact-sheet

Akwei, I. (2017, November 14). Somaliland is first in the world to use iris biometric voting system [Hi-Tech]. Retrieved April 1, 2018, from http://www.africanews.com/2017/11/14/somaliland-is-first-in-the-world-to-use-iris-biometric-voting-system-hi-tech/

Al Jazeera. (2018, March 25). Key facts about the war in Yemen. Retrieved April 02, 2018, from https://www.aljazeera.com/news/2016/06/key-facts-war-yemen-160607112342462.html

Atkins Global. (n.d.). Passenger Management Case Studies | Biometrics in Airports. Retrieved February 04, 2018, from http://auroracs.co.uk/case-study-atkins-passenger-management/

Battersby, M. (2014, October 09). 40,000-year-old cave paintings include oldest hand stencil known to science. Retrieved March 11, 2018, from https://www.independent.co.uk/arts-entertainment/art/news/40000-year-old-cave-paintings-include-oldest-hand-stencil-known-to-science-9783840.html

Bill of Right Institute. (n.d.). Debating Voter ID. Retrieved March 11, 2018, from http://www.billofrightsinstitute.org/educate/educator-resources/lessons-plans/current-events/voter-id-debate/

Carbone, C. (2018, January 28). Facebook, Google, Twitter open up to Congress about Russian misinformation. Retrieved March 11, 2018, from http://www.foxnews.com/tech/2018/01/28/facebook-google-twitter-open-up-to-congress-about-russian-misinformation.html

Darnolf, S. (2017, November 02). Reducing Voter Fraud in Afghanistan. Retrieved April 1, 2018, from https://www.usip.org/publications/2017/11/reducing-voter-fraud-afghanistan

FBI. (2016, June 10). IAFIS. Retrieved March 25, 2018, from https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis

Fingerhut, H. (2016, November 10). A Divided and Pessimistic Electorate. Retrieved March 11, 2018, from http://www.people-press.org/2016/11/10/a-divided-and-pessimistic-electorate/

للاستشارات المنارة

www.manaraa.com

Fruhlinger, J. (2017, September 27). What is WannaCry ransomware, how does it infect, and who was responsible? Retrieved from https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Gambanga, N. (2017, January 25). Zimbabwe rules out biometric voting in 2018 elections, electronic system for registration only. Retrieved April 1, 2018, from https://www.techzim.co.zw/2017/01/zimbabwe-rules-biometric-voting-2018-elections-electronic-system-registration/

Hall, T. (2013). US voter registration reform. Electoral Studies, 32(4), 589-596. Doi:10.1016/j.electstud.2013.07.017

Horwitz, S., Nakashima, E., & Gold, M. (2017). Department of homeland security tells states about russian hacking during 2016 election. The Washington Post, (sept 22 2017): Na.

Ingraham, C. (2017, January 25). Here are nine investigations on voter fraud that found virtually nothing. Retrieved February 04, 2018, from https://www.washingtonpost.com/news/wonk/wp/2017/01/25/here-are-nine-major-investigations-on-voter-fraud-that-found-virtually-nothing/?utm_term=.49a1eda2e2f6

International Foundation for Electoral Systems. (2014, July 17). IFES Supports New Biometric Voter Registration System in Yemen. Retrieved April 1, 2018, from http://www.ifes.org/news/ifes-supports-new-biometric-voter-registration-system-yemen

Jaracz, J. (2011, December 07). Countries adopt biometrics for voter ID, fraud prevention. Retrieved March 11, 2018, from https://www.secureidnews.com/news-item/countries-adopt-biometrics-for-voter-id-fraud-prevention/

Jones, J. M., Newport, F., & Saad, L. (2017, November 01). How Americans Perceive Government in 2017. Retrieved from http://news.gallup.com/opinion/polling-matters/221171/americans-perceive-government-2017.aspx?g_source=link_NEWSV9&g_medium=&g_campaign=item_&g_content=How Americans Perceive Government in 2017

Levitt, J. (2011). The Truth About Voter Fraud. Retrieved March 11, 2018, from http://www.brennancenter.org/sites/default/files/legacy/The%20Truth%20About%20Voter%20Fraud.pdf

Mayhew, Stephen. (2018, March 08). History of Biometrics. Retrieved March 11, 2018, from https://www.biometricupdate.com/201802/history-of-biometrics-2

المنارة للاستشارات

www.manaraa.com

Meadows, M. (2017, September 12). Text - H.R.3751 - 115th Congress (2017-2018): PAPER Act. Retrieved March 11, 2018, from https://www.congress.gov/bill/115th-congress/house-bill/3751/text

Murdock, J. (2018, April 04). Facebook's "troll farm" problem haunts social network with over 270 new profiles found. Retrieved from http://www.newsweek.com/what-internet-research-agency-facebook-shuts-hundreds-accounts-linked-russia-870889

National Security Agency. (2016, November). NSA Report on Russian Spearfishing. Retrieved March 11, 2018, from https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf

National voter registration act. (2010). Federal Register, Na

Noack, R. (2018, January 10). Everything we know so far about Russian election meddling in Europe. Retrieved March 11, 2018, from https://www.washingtonpost.com/news/worldviews/wp/2018/01/10/everything-we-know-so-far-about-russian-election-meddling-in-europe/?utm_term=.689dcd4d82a2

Pastor, R. A. (2013, Jan 29). Identifying solutions; on voter fraud and illegal immigration, biometric ID cards could help. Los Angeles Times Retrieved from https://search.proquest.com/docview/1282197976?accountid=28902

Starks, T. (2017, January 06). DHS labels elections as 'critical infrastructure'. Retrieved March

The ACE Project. (2012). Voter Registration. Retrieved March 11, 2018, from http://aceproject.org/ace-en/topics/vr/vra/vra08/vra08a

The LNP Editorial Board. (2018, March 25). If you use Facebook, and care how your personal information is used, you ought to want to see Facebook regulated. Retrieved April 1, 2018, from http://lancasteronline.com/opinion/editorials/if-you-use-facebook-and-care-how-your-personal-information/article_e82387b2-2edd-11e8-8f30-03587d561f3d.html

The Office of the Director of National Intelligence. (2016, January 06). Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution. Retrieved March 11, 2018, from https://www.dni.gov/files/documents/ICA_2017_01.pdf

U.S. Strategic Command. (2010, May 25). U.S. Cyber Command Fact Sheet. Retrieved March 25, 2018, from

المنارة للاستشارات
www.manaraa.com

www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet UPDATED replaces May 21 Fact Sheet.pdf

Underhill, W. (n.d.). VOTER IDENTIFICATION REQUIREMENTS | VOTER ID LAWS. Retrieved March 11, 2018, from http://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx

UNDP Solomon Islands. (2017, July 10). Strengthening the Electoral Cycle Project in the Solomon Islands Final Evaluation.

Wolf, P. (2017). Introducing Biometric Technology in Elections. 1-77. Retrieved from https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections.pdf

المنارة للاستشارات

www.manaraa.com