Election Security in an Information Age

How the Events of 2016 May Shape the Future of Democratic Elections

Anomali Special Report

Travis Farral | Director, Security Solutions

Table of Contents

Introduction

Over the last two years, there have been an increasing number of information security attacks on political organizations, government institutions, and political operatives. The German Bundestag[1], the Turkish AKP political party[2], NATO[3], the Ukrainian government[4], and the German Christian Democratic Union[5] political party are examples of organizations targeted since 2014. Some of these attacks have led to the release of damning information as troves of stolen emails and other documents were released to the Internet. The effect of releasing such information is apparently to bend public opinion to benefit those behind the attacks.

Stealing and releasing private information hasn't been the only avenue to influence public opinion, however. Armies of social media "trolls" have been employed by countries like Russia[6] and Turkey[7] to shape public opinion on state interests. "Fake news" efforts in Ukraine prompted the European Union to create a task force aimed at countering this kind of propaganda.[8]

The attacks related to the U.S. presidential election in 2016 have so far garnered the greatest amount of attention due to fears that Russia may have influenced the outcome of the election. This has prompted concern ahead of upcoming elections in other western nations such as Germany, Sweden, and France.[9]

---

[1] http://www.bbc.com/news/technology-36284447
[2] https://www.wired.com/2016/07/wikileaks-dumps-erdogan-emails-turkeys-failed-coup/
[3] http://www.dailymail.co.uk/news/article-2582071/Several-NATO-websites-hacked-cyber-attack-linked-crisis-Crimea.html
[4] http://www.unian.info/politics/1739956-poroshenko-ukraine-able-to-unleash-cyber-counterattack-against-russia.html
[5] http://www.telegraph.co.uk/news/2016/09/21/russia-blamed-for-hacking-attack-on-german-mps/
[6] https://www.nytimes.com/2015/06/07/magazine/the-agency.html
[7] http://www.dailydot.com/layer8/redhack-turkey-albayrak-censorship/
[8] https://euvsdisinfo.eu/
[9] http://www.dw.com/en/how-to-influence-voters-and-tamper-with-the-german-election/a-37196187

The suspected involvement of nation states in these activities is a central concern. Attribution is sometimes difficult or called into question. The concern of foreign nation involvement is well-placed. Interference on this level in democratic elections can shake the public's trust which is the foundation of any democratic government. The availability of an increasing amount of information via online sources only exacerbates efforts to defend against such attacks. The effectiveness of stealing and releasing politically damaging information as a means of shaping public opinion serves as a magnet for nation states and politically motivated actors alike.

Addressing the challenges presented by these kinds of attacks requires:

- Understanding potential targets
- Understanding exposures
- Developing a comprehensive plan for response and mitigation

Governments, political organizations, political activists, and even political volunteers should seek awareness of the emerging threats surrounding elections. Understanding this threat landscape, the adversaries involved, and a keen situational awareness are central efforts in countering these threats.

Governments and Interfering with Foreign Politics

Nations and governments have a long history of attempting to influence power in other nations. The methods used to influence have varied over time and based on abilities available. Strategic marriages, donations of resources, misinformation, espionage, interfering in elections, sabotage, assassinations, military power, and diplomacy have all been used to influence power in other nations or governments.

Recent history is replete with examples of nations interfering with the political affairs of other nations as an attempt at influencing power to their advantage. This type of political meddling is a component of modern statecraft. It is far more widespread than the public may realize.

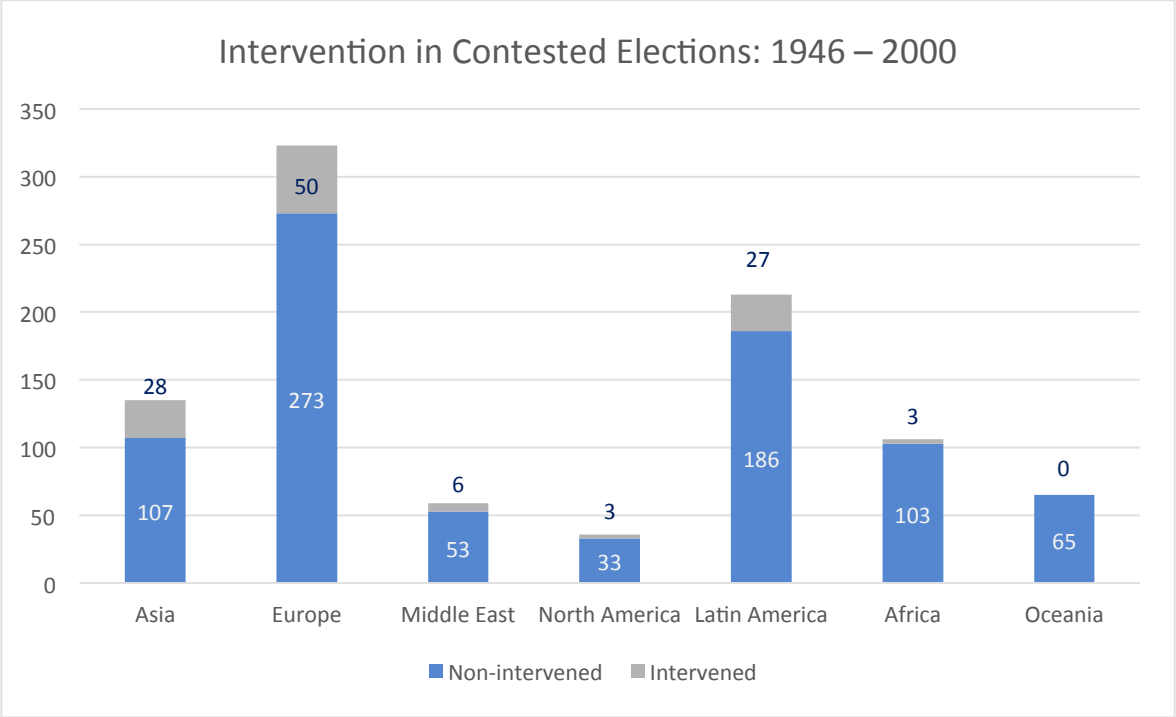
In the 1996 U.S. presidential election, for example, accusations arose that the People's Republic of China was funneling campaign contributions to the Democratic National Committee (DNC) in an apparent attempt to influence American policy in its favor.[10]

According to a database compiled by Dov Levin at Carnegie Mellon University, the United States and USSR (& Russia) interfered with foreign elections 117 times between 1946 and 2000[11]. That's just from what is known via open source information. There may be other examples still hidden in classified documents.

[10] http://www.washingtonpost.com/wp-srv/politics/special/campfin/stories/china1.htm
[11] http://journals.sagepub.com/doi/abs/10.1177/0738894216661190

"Accordingly, 11.3% of these elections, or about one of every nine competitive elections since the end of the Second World War, have been the targets of an electoral intervention."

Dov H. Levin, Partisan electoral interventions by the great powers: Introducing the PEIG Dataset



Source: Partisan electoral interventions by the great powers: Introducing the PEIG Dataset

A particularly poignant example is the CIA leaking of a 1956 secret speech by Nikita Khrushchev where he denounced Stalin. The intent was to broadly discredit Khrushchev and the Soviet system in general.[12]

In the 2004 Ukrainian presidential election, Russia was accused of using a variety of methods to influence the election in favor of pro-Russian candidate, Viktor

[12] http://arstechnica.com/tech-policy/2016/09/thanks-internet-messing-with-elections-not-just-for-the-cia-anymore/

Yanukovych, against his opponent Viktor Yushchenko.[13] The initial run-off election was reportedly won by Yanukovych. But Yushchenko, along with many of his supporters and international observers, immediately claimed the election had been rigged.[14] Many thousands of protesters took to the streets in what has been called the "Orange Revolution", in response to the widespread belief that the election had been rigged in favor of Yanukovych. The Ukrainian supreme court eventually annulled the results of the run-off based on evidence of fraud and ordered a second run-off. Yushchenko won after a highly scrutinized and monitored second run-off election.

In 2008, China was eventually blamed for hacking into the campaigns of U.S. presidential candidates McCain and Obama.[15] In that case, theft occurred but there was no apparent publication of any of any of the stolen information.

Other Recent Suspected Election Interference

Andrés Sepúlveda, a Columbian hacker, claims to have used a variety of means to influence elections in Nicaragua, Panama, Honduras, El Salvador, Colombia, Mexico, Costa Rica, Guatemala, and Venezuela over the last ten years.[16] He and his team allegedly engaged in a number of activities to support campaigns he was working for. Methods included compromising smart phones, websites, and other digital interception techniques. "My job was to do actions of dirty war and psychological operations, black propaganda, rumors—the whole dark side of politics that nobody knows exists but everyone can see," the hacker is quoted as saying. He is currently serving a ten-year sentence for charges related to these activities.

---

13 https://www2.gwu.edu/~ieresgwu/assets/docs/demokratizatsiya%20archive/GWASHU_DEMO_13_4/D761010XT7H55W67/D761010XT7H55W67.pdf

14 https://www.sussex.ac.uk/webteam/gateway/file.php?name=epern-election-briefing-no-16.pdf&site=266

15 http://www.newsweek.com/highlights-newsweeks-special-election-project-84883

16 https://www.bloomberg.com/features/2016-how-to-hack-an-election/

Cambodia's national voter list was published online by the Cambodian National Election Committee on the 3rd of January, 2017.[17] Soon thereafter, attackers from "overseas" successfully hacked the site and prevented access to the list but reportedly did not alter the list. The attack was discovered and access restored. Currently, no attribution has been made related to this incident. It is unknown what the motivation or intention was of the suspected attackers.

A report published by the Swedish Institute of Public Affairs in January of 2017 accuses Russia of spreading fake news and disinformation in Sweden.[18] While not directly related to elections, this kind of suspected interference could have ramifications on the upcoming Swedish general election in 2018. The report claims that Russia, through Russian state-owned media operating in Sweden coupled with social media campaigns, has been actively spreading disinformation, propaganda, and false documents to support Russian state interests.[19]

During the United States presidential election in 2016, Paul Manafort, campaign aide to then candidate Donald Trump, was forced to step down in the wake of a controversy that arose around alleged off-books cash payments received from a pro-Russian political party in Ukraine. At least one source suggests the allegations were an attempt to interfere with the political campaign of Donald Trump by elements of the Ukrainian government who viewed Trump as hostile to Ukrainian national interests.[20]

[17] http://www.voacambodia.com/a/election-officials-alleged-hacking-of-voter-list/3668846.html
[18] http://www.tandfonline.com/doi/full/10.1080/01402390.2016.1273830
[19] https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6604516
[20] http://www.politico.com/story/2017/01/ukraine-sabotage-trump-backfire-233446

The 2016 U.S. Presidential Election

The most profound example of supposed interference in a nation's electoral process by another nation is the hacking activities surrounding the 2016 U.S. presidential election. Russia has been repeatedly accused of hacking into email accounts and computer networks of political organizations, state election entities, and political operatives during the months prior to the November 2016 U.S. election. The subsequent release of thousands of stolen emails and documents has been portrayed as a deliberate attempt by Russia to influence the American electorate in the U.S. presidential election. While not an attempt to directly manipulate the voting process itself, influencing the election by releasing unsavory private details can achieve the same result as if the election apparatus itself had been hacked.

Releasing potentially negative information about a candidate is nothing new in politics. The "October surprise" is a common component of U.S. presidential elections: Negative details about a candidate are released one to three weeks before the election in early November. While Hillary Clinton's campaign was dealing with the release of stolen emails and documents, Donald Trump's campaign had had to deal with a more traditional October surprise of its own. In early October, an audio recording surfaced in which Mr. Trump could be heard making potentially offensive remarks about women.[21]

Yet the reason the release of negative information related to Hillary Clinton's campaign and the DNC is profoundly unique, because of the suspected source of the negative information and the volume of information released. Had certain emails been leaked by someone who might normally have access to them, this

[21] https://www.washingtonpost.com/politics/trump-recorded-having-extremely-lewd-conversation-about-women-in-2005/2016/10/07/3b9ce776-8cb4-11e6-bf8a-3d26847eeed4_story.html

situation would likely be considered typical politics. Because the source of the leaked information came as a result of theft (hacking) and was suspected to have come from a foreign nation, the U.S. government has become heavily involved in responding to the situation. The ramifications stretch beyond this single election.

Here is a summary of the events surrounding the attempt to influence the 2016 U.S. presidential election.

The world learned of the DNC hacks on June 14, 2016 as news hit the press that the DNC had been hacked. A post by Crowdstrike[22], who was retained to investigate the attacks at the DNC, revealed some key details of the investigation. The DNC gave Crowdstrike permission to release this information to the public. It is unknown if additional details are still kept secret or if Crowdstrike shared the entirety of their investigation. In their analysis, Crowdstrike noted similarities in the DNC attack and other attacks they had seen from not one but two separate Russian agencies. They even noted that while they had evidence that both groups had compromised the DNC, one of the groups had been inside the DNC network since the summer of 2015.

The following day, a free Wordpress blog was created and details were shared that seemed to refute the Crowdstrike findings[23]. The blog's author, "Guccifer 2.0", claimed that instead of the Russians, it was he who had hacked the DNC. To prove his authenticity, he shared several documents purported to have come from the DNC hack. He claimed to have given the "main part" of what was stolen from the DNC to Wikileaks who would be publishing them soon.

Crowdstrike responded by updating their previous blog post and standing by their attribution to entities tied to the Russian government.
In the following week, several other information security companies added bits of additional analysis and sided with Crowdstrike's overall assessment that the

[22] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
[23] https://guccifer2.wordpress.com

attacks most likely came from Russia albeit with varying degrees of certainty that was the case.[24][25][26]

Guccifer 2.0 released several more documents in a few additional blog posts and then did an interview with Motherboard where he claimed to be Romanian and disliked Russia.[27] He also created a Twitter account and invited members of the press to ask him questions via direct message.[28]

As more details about Guccifer 2.0 came out, analysts suspected that he was not who he claimed to be.[29] [30] Most striking was his apparent lack of fluency in Romanian which should be his mother tongue if he is truly from Romania. It was suspected that this persona was created by Russian hackers to deflect blame after Crowdstrike's accusation.

A website called "DC Leaks" began publishing some of the emails supposedly purloined by Guccifer 2.0.[31] The Guccifer 2.0 persona offered to share early access to some of the emails that would be hosted on DC Leaks to The Smoking Gun website.[32] This suggested that Guccifer 2.0 either had direct access to the DC Leaks website backend or was a trusted contact of the site's ownership. DC Leaks went on to publish details about several politicians from both the Republican and Democratic parties.

---

[24] https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
[25] http://www.threatgeek.com/2016/06/dnc_update.html
[26] https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html
[27] https://motherboard.vice.com/read/dnc-hacker-guccifer-20-interview
[28] https://twitter.com/GUCCIFER_2
[29] http://arstechnica.com/security/2016/06/guccifer-leak-of-dnc-trump-research-has-a-russians-fingerprints-on-it/
[30] http://thehill.com/policy/cybersecurity/287558-guccifer-20-drops-new-dnc-docs
[31] http://dcleaks.com
[32] http://thesmokinggun.com/documents/investigation/tracking-russian-hackers-638295

As promised, on July 22, 2016, Wikileaks published a trove of 19,252 emails and 8,034 attachments supposedly from the DNC hack.[33] One of the major revelations from these documents was the apparent coordination between the DNC and the Clinton campaign to work against Bernie Sanders and secure the democratic nomination for Hillary Clinton.[34] Several prominent members of the Democratic National Committee resigned in the resulting fallout including DNC chairperson Debbie Wasserman Schultz.[35]

Hillary Clinton's campaign didn't refute the contents of the released emails. Instead, they accused Russia not only of the hack itself but of deliberately trying to help Trump win the election. This accusation was echoed by some media outlets, some security industry experts, and some members of the US intelligence community (IC).[36]

Julian Assange, the enigmatic proprietor of Wikileaks, strongly denied the Russian allegations. He claimed that the leaks came from a Democratic insider. This claim was eventually backed by another figure closely associated with Wikileaks.[37]

In August 2016, news broke that voter databases in Arizona, Illinois, and potentially two other states may have been attacked by hackers. The voter database in Illinois had been accessed but not altered while the Arizona voter database had not been successfully accessed by attackers according to investigators. The FBI suspected Russians of the breaches but did not point the finger at the Russian government.[38] Details have not been released publicly that support this attribution.

---

[33] https://wikileaks.org/dnc-emails/
[34] http://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html?_r=0
[35] http://www.npr.org/2016/07/24/487264278/debbie-wasserman-schultz-announces-resignation-with-convention-set-to-begin
[36] http://www.chicagotribune.com/news/nationworld/politics/ct-clinton-russia-dnc-email-hack-20160724-story.html
[37] http://www.washingtontimes.com/news/2016/dec/14/craig-murray-says-source-of-hillary-clinton-campai/
[38] https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html

Guccifer 2.0 continued posting documents and other details, eventually claiming that he also hacked the DCCC (the Democratic Congressional Campaign Committee).[39] This revelation came two weeks after news that the FBI was investigating a possible breach at the DCCC.[40] On October 4, 2016, Guccifer 2.0 also claimed to have hacked the Clinton Foundation. This claim was disputed by officials from the Clinton Foundation.[41]

On October 7, 2016, Wikileaks released a batch of 2050 emails from Hillary Clinton's campaign chairman, John Podesta.[42] Wikileaks continued to release emails from Podesta's account over the following weeks, until two days before the election. In total, over 50,000 emails were released from Podesta's email account.[43]

Also on October 7, 2016, the Obama administration officially blamed Russia for hacking political elements in the United States. The administration accused the Russian government of releasing sensitive information in an effort "to interfere with the U.S. election process."[44]

Guccifer 2.0 posted on November 4th, just days before the election, that he had hacked the Federal Election Commission and that Democrats had active plans to rig the election for Hillary Clinton.[45]

The Election and Beyond

In the end, Donald Trump won the election despite many reliable polls showing Clinton with a favorable lead. Trump's surprise victory, coupled with all the

[39] http://www.nbcnews.com/news/us-news/guccifer-2-0-releases-documents-dccc-hack-n629631
[40] http://www.politico.com/story/2016/07/dccc-hack-fbi-226398
[41] http://fortune.com/2016/10/04/clinton-foundation-guccifer-hack-claim/
[42] http://www.foxnews.com/politics/2016/10/11/7-biggest-revelations-from-wikileaks-release-podesta-emails.html
[43] http://www.cnn.com/2016/11/06/politics/wikileaks-dnc-emails-surprise/
[44] http://www.nbcnews.com/news/us-news/u-s-publicly-blames-russian-government-hacking-n662066
[45] https://guccifer2.wordpress.com/2016/11/04/info-from-inside-the-fec-the-democrats-may-rig-the-elections/

hacking activity and release of private information, has led to the belief that Russia actively worked to influence the election for Trump who ended up winning.

It is not possible to tell from available data what impact the release of the hacked emails and other documents ultimately had on Election Day. Assessing how that one issue weighed on voters is considerably challenging, due to several other factors: Other negative news that plagued Hillary Clinton's campaign, the populist message of Donald Trump, and an announcement that the FBI was going to re-open a case involving Hillary Clinton just days before the election. Were there some significantly negative news directly related to Clinton amongst the released emails, the effect on voters may have been easier to gauge. The true impact of hacking on the election may never be known.

President Obama's Actions Against Russia

On December 29, 2016, President Obama issued an executive order coupled with a statement[46] that certain actions would be taken by the United States in response to the Russian hacking activities related to the 2016 election. These actions reflect the assertion by U.S. spy agencies that they do indeed have direct evidence of the involvement of those entities named. At the very least there exists enough confidence for the Obama administration to proceed with retaliatory measures against Russia.

Specific actions taken:

- **Sanctions**
  - Russian GRU
  - Russian FSB
  - Two Russian intelligence services
  - Four officers of the GRU
  - Three companies accused of providing material support to the GRU

[46] https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

- **Designation by the Treasury**
  - Two Russian individuals accused of using "cyber-enabled means to cause misappropriation of funds and personally identifiable information"
- **Shut downs**
  - Two compounds long known to be used by Russians for intelligence-related purposes
- **Expulsions from the U.S.**
  - 35 Russian intelligence operatives

In addition, President Obama promised that further actions could be taken at a "time and place" of the administration's choosing. These, he said may include unpublicized activities. Reference to activities that would not be publicized could be interpreted as "covert" activities but the President's true meaning of this threat is unknown.

Information Released by the U.S. Government

Also timed with President Obama's response on December 29, 2016, the Department of Homeland Security and the Federal Bureau of Investigation released a Joint Analysis Report (JAR-16-20296 "GRIZZLY STEPPE") on Russian Malicious Cyber Activity.[47] The release included a list of indicators associated with the hacking activities suspected of coming from entities associated with Russian government. The list contained many indicators that were also used by other malware families not associated with the Russian government, The Onion Router (TOR)[48] exit nodes which could be used by anyone who uses the service, and IP addresses of legitimate companies (such as Yahoo, Microsoft, and Twitter) or legitimate Content Delivery Networks (CDNs) including some that are used by popular services like Skype and Microsoft Azure. Several of the file hashes included in the release were well known by antivirus vendors and associated with commonly seen malware families. The report also includes a diagram of the tradecraft used by the suspected adversaries. However, the diagram explains

[47] https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity
[48] https://www.torproject.org/

common tactics used throughout the hacking community – not specific tradecraft that can be attributed only to the Russians.

Wordfence, who provides security for the popular Wordpress blogging platform, said the following about the indicators and samples released in the Joint Analysis Report from the U.S. government:

> *"The IP addresses that DHS provided may have been used for an attack by a state actor like Russia. But they don't appear to provide any association with Russia. They are probably used by a wide range of other malicious actors, especially the 15% of IP addresses that are Tor exit nodes.*
>
> *The malware sample is old, widely used and appears to be Ukrainian. It has no apparent relationship with Russian intelligence and it would be an indicator of compromise for any website."*[49]

In a critique of the JAR-16-20296 GRIZZLY STEPPE report, security researcher Robert M. Lee summarizes the report by saying, "the DHS/FBI GRIZZLY STEPPE report does not meet its stated intent of helping network defenders and instead choose to focus on a confusing assortment of attribution, non-descriptive indicators, and re-hashed tradecraft".[50]

These criticisms, while accurate, don't necessarily reflect incompetence on the part of the U.S. government, but more likely reflect the trouble in what they are allowed to reveal. The government appears to be sharing what it can to support their conclusions to the public. They may be unwilling or unable to reveal a "smoking gun" that might solidly implicate those behind the attacks. It may have been better for them to have left out the bits of evidence that don't have any real value from the report.

Declassified Report Released

On January 6, 2017, the U.S. Office of the Director of National Intelligence released a declassified report aimed at bolstering its case that the Russian

[49] https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack/
[50] http://www.robertmlee.org/critiques-of-the-dhsfbis-grizzly-steppe-report/

government was behind the election-related attacks of 2016.[51] The report was devoid of clear evidence pointing to Russian government involvement, but did offer more substantial details than the GRIZZLY STEPPE report. In a public hearing prior to the report's release, Director of National Intelligence James Clapper, alluded to the presence of additional classified evidence supporting their conclusions. But, he said this evidence would not be released publicly as it would reveal secret sources and methods too "sensitive and fragile" to compromise.[52]

The report wasn't without critics. U.S. House Intelligence Committee Chairman Pete Hoekstra pointed out that while the report supposedly reflected the views of all 17 U.S. intelligence agencies, only three agencies appeared to be involved in the creation of the report. Particularly curious was the absence of agencies with direct interests in the matter such as the Department of Homeland Security and the Defense Intelligence Agency. He also pointed out that the report lacked usual verbiage indicating it was jointly coordinated amongst the U.S. intelligence community and lacked the presence of dissenting views from the report's conclusions.[53]

More detailed criticism about the report came from journalist and anti-Putin activist Masha Gessen.[54] In an article, she points out holes in the report's conclusions based on her own analysis and knowledge of Russian events.

Timed with the release of the declassified report was a classification by the Department of Homeland Security that U.S. elections systems are critical infrastructure.[55] The designation could provide various government resources to U.S. election authorities including improved communication and information sharing. These resources are voluntary. The designation does not apply to

---

[51] https://icontherecord.tumblr.com/post/155494946443/odni-statement-on-declassified-intelligence
[52] http://bigstory.ap.org/article/2760ab8835494a7190df91fe718a644a/top-us-intelligence-officials-testify-russian-hacking
[53] http://www.foxnews.com/opinion/2017/01/07/was-fridays-declassified-report-claiming-russian-hacking-2016-election-rigged.html
[54] http://www.nybooks.com/daily/2017/01/09/russia-trump-election-flawed-intelligence/
[55] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

campaigns or political parties so this would not have had an impact on the hacking events of the 2016 election.

Reactions from Other Nations

Just days after the release of the declassified U.S. report, the Joint Committee on the National Security Strategy in the U.K. launched an inquiry into cybersecurity.[56] They mention that the government would treat an information security attack on the U.K. as seriously as a conventional attack.

The head of Germany's domestic security agency, Hans-Georg Maaβen said, "We must also be in a position to attack an enemy and stop them from carrying out further attacks on us."[57]

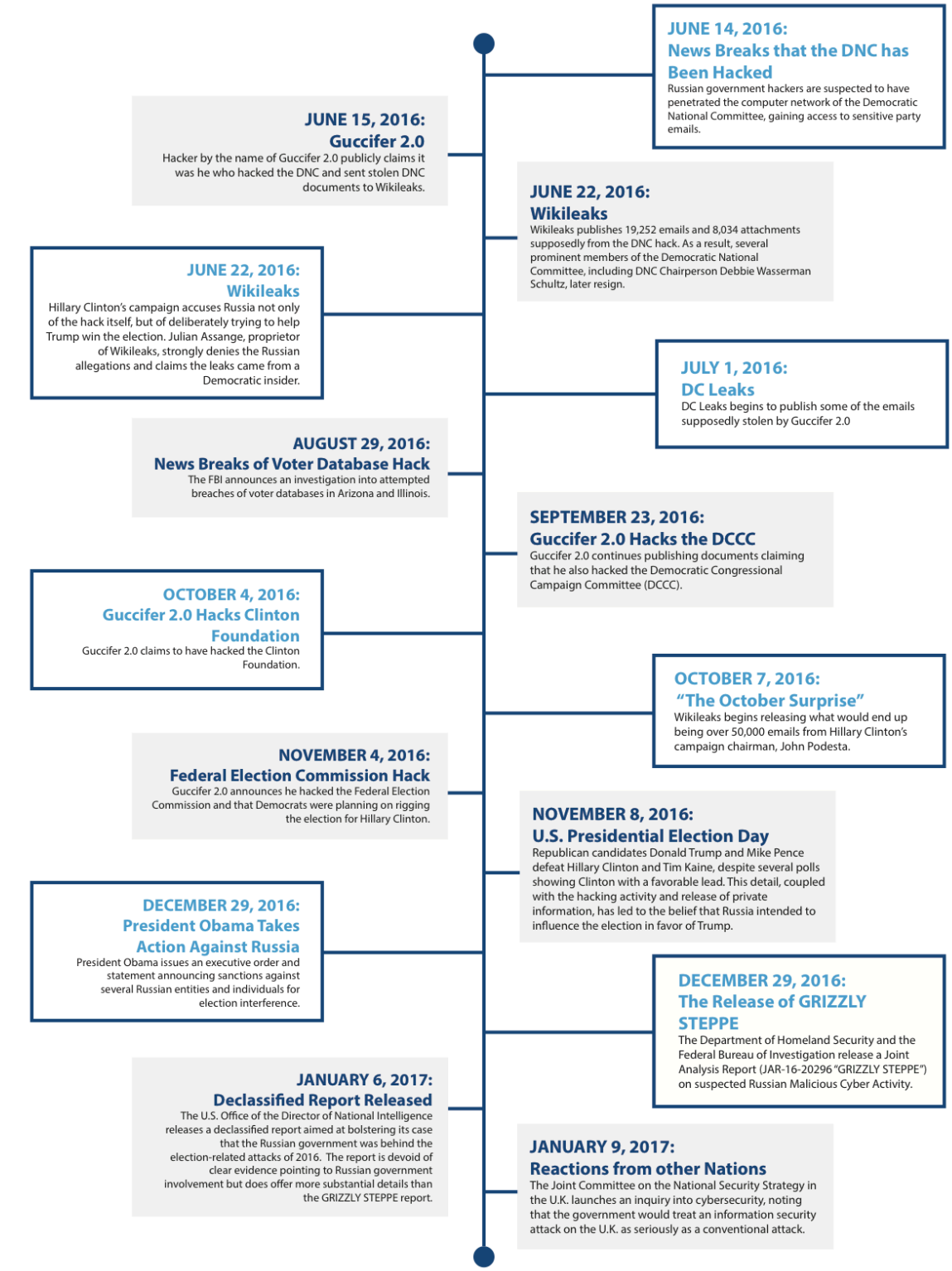
Montenegro has also vowed to enhance its security measures after dealing with election-related attacks of its own in 2016.[58] The country claimed to have seen a huge increase in the quantity and sophistication of attacks on government-related sites throughout 2016. They accuse Russia of attempting to meddle in its elections. Russia has denied any involvement.

Ukraine, who has been engaged in a military conflict with Russia since 2014, has beefed up its own information security capabilities. "We have a very strong cyber division, so Ukraine is able to unleash a counterattack," said Ukrainian President, Petro Poroshenko.[59]

---

[56] https://www.parliament.uk/business/committees/committees-a-z/joint-select/national-security-strategy/news-parliament-2015/cyber-security-inquiry-2016-17/
[57] http://www.politico.eu/article/security-chief-germany-must-go-on-cybersecurity-offensive/
[58] http://www.balkaninsight.com/en/article/montenegro-on-alert-over-cyber-attacks-01-09-2017
[59] http://www.unian.info/politics/1739956-poroshenko-ukraine-able-to-unleash-cyber-counterattack-against-russia.html

2016 U.S. Presidential Election Timeline



ANOMALI

The Difficulty of Attribution

Central to discussions about the hacking activities related to the U.S. presidential election is the issue of attribution to Russia, and particularly to the Russian government. Attribution is an oft-debated topic within information security circles that isn't confined to the events of 2016. It would be too easy for different actors to reproduce many types of evidence often cited for attribution.

The 2014 attack on Sony Pictures has been attributed to the North Korean by the U.S. government.[60] Yet a number of security researchers and journalists have called this attribution into question.[61]

To bring this issue some perspective, here are some example bits of evidence that could be associated with an attack that wouldn't be hard for any modestly skilled attacker to do:

- Create an account on Yandex, Mail.ru, QQ mail, or other foreign language webmail provider to use for domain registrations or other communication
- Use similar infrastructure used in other attacks such as certain discount domain registrars, hosting companies, Virtual Private Network (VPN) providers, or Virutal Private Server providers
- Use The Onion Router (TOR)[62] network to anonymize traffic during the attacks
- Change computer keyboard settings to a foreign language (such as Russian or Mandarin)

[60] https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
[61] https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/
[62] https://www.torproject.org

- Perform activities during typical workday hours in the region of choice (Beijing or Moscow for instance)
- Use PowerShell frameworks like Empire[63] during the compromise or even use exact PowerShell commands used in other attacks if known
- Include foreign language comments in scripts or malware used
- Use techniques like phishing emails to deliver malware or attempt to steal credentials through fake login pages
- Use URL shortening services to obfuscate links to malicious infrastructure or links to malware (for example, Bit.ly)
- Use widely available hacking tools like Mimikatz[64] in attacks
- Using proxies or compromised systems to perform attacks from IP addresses in other countries

Using these types of evidence as the basis for attribution draws skepticism because of how easily they could be done by a wide range of attackers.

Investigating Information Security Attacks

Information security attack investigations aren't terribly different from conventional criminal investigations. In both examples, evidence is collected and used to build a case. Certain types of evidence are more valuable than others. In a conventional criminal case, DNA may be considered far more valuable than say a partial footprint lifted from the crime scene. DNA could be used to identify a specific individual as having been involved whereas the footprint may apply to thousands of individuals who wore that type and size of shoe.

Similarly, certain evidence such as a cryptographic key could carry the same level of confidence in an information security investigation as DNA would in a conventional crime. Other hard to mimic details also make for better attribution. However, as with a conventional crime, this kind of evidence isn't always available. Or if it is, it may not match any known suspects.

---

[63] https://www.powershellempire.com/
[64] https://github.com/gentilkiwi/mimikatz

Barring the presence of DNA that might match a particular suspect in a conventional crime, investigators may be left with trying to piece together various bits of evidence to narrow the list of possible suspects. Perhaps in addition to a partial footprint, other pieces of evidence are added such as time of day the crime occurred, evidence of tools used at the crime scene, motivations of who would be interested in committing the crime, relation to similar cases and other clues that might be added to the case. Eventually, a motive can be deduced and a profile of the actor who committed the crime begins to take shape.

Information security attack investigations are no different in that it most often isn't the individual pieces of evidence standing on their own which leads to attribution but the body of evidence taken as a whole. The confidence level in the resulting attribution is derived from the value of the evidence collected and the likelihood the attack could have been done by someone other than the attributed actor or group.

For example, look at the following evidence collection from a handful of potentially related attacks (simplified for demonstration purposes – not based on real data):

Date	Target	Method	Tools	Infrastructure	Command & Control	Domain Reg Co	Domain Reg Date	Domain Reg Email
3-Jan-17	Cell phone manufact	Phishing	Fake login page	172.17.13.243		ABC123 Domains	12-Dec-17	John0A394@aol.com
3-Jan-17	Cell phone manufact.	Phishing	Fake login page	172.17.13.249		ABC123 Domains	16-Dec-17	Private
5-Jan-17	Electronic components manufact	Phishing	Remote access tool - CuteRAT	172.17.13.243	192.168.207.13	ABC123 Domains	30-Nov-17	John09394@aol.com
9-Jan-17	Marketing company	Phishing	Fake login page	192.168.207.6		ABC123 Domains	5-Jan-17	Private
11-Jan-17	Electronic components manufact	Phishing	Remote access tool - CuteRAT	10.127.99.11	192.168.207.32	ABC123 Domains	1-Aug-16	Jane3A767@aol.com

The evidence suggests these attacks might be related based on the following details:

- Similar infrastructure is used as indicated by the IP addresses associated across multiple attacks
- There is correlation in the types of targets in the attacks
- The delivery mechanism was the same in all the attacks
- The same domain registrar was used to register the domains in all the attacks
- There are "connector" pieces of evidence tying some of the attacks together in a more substantial way
  - The same email address was used to register two of the domains suggesting the same actor was involved in both of the attacks.
  - The same IP address was used to host fake login pages for two of the attacks

Tying all this evidence together starts to paint a picture that suggests the same actor or group may be behind all of these attacks. It may not be possible, based solely on these details, to associate the attacks with a specific individual or group at this point. However, taking the profile created from this evidence and correlating with past attacks might fill out the picture of this actor or group even further. Similar tools, techniques, apparent goals, and potentially even more substantive connectors like specific email addresses can all be used to link to additional attacks. As the body of evidence grows, the picture of who may have been behind the attacks continues to solidify.

Ultimately, there may not be a smoking gun that points to a specific individual or group. The evidence for linking certain attacks to the same actor may be mostly circumstantial. The prevailing narrative will stand unless contrary evidence is discovered to refute its assumptions or a smoking gun is discovered that removes doubt in it. In the end, confidence levels in any attribution made must reflect the strength of the evidence presented to support it.

Going back to the presented example of collected evidence, imagine if some very specific evidence was collected from one of the observed attacks. This new evidence may not yield much based on what is known so far. But due to its value

as a very specific identifier, it is not shared publicly. We will use a secure shell key fingerprint (SSH key fingerprint) collected from a packet capture of one of the attacks.[65] Collection of the same type of evidence from another attack yields an exact match. This is a much more solid connection between the attacks because, like DNA, the odds of an accidental match with SSH keys are mathematically extremely high. This allows the new evidence collected in this case to be substantively connected to at least one previous attack.

Date	Target	Client SSH Key Observed
3-Jan-17	Cell phone mfg	
3-Jan-17	Cell phone mfg	
5-Jan-17	Supplier of cell phone components	a2fad2fdbb964e4b81f3a57d1eaca499
9-Jan-17	Marketing co	
11-Jan-17	Supplier of cell phone components	a2fad2fdbb964e4b81f3a57d1eaca499

Finding a computer with the private SSH key that matches this fingerprint would be a major breakthrough in potentially identifying the exact individual behind these two attacks at least (barring finding this private key on other systems as well). Without this there may not be the ability to identify a specific actor or group behind the attack with the evidence collected so far. However, the profile of who was behind these attacks continues to get more clear and now there is a very specific way to connect these two attacks to potentially others.

As the list of evidence grows, the attacker's profile gets more specific. The list of known actors with the means, motive, and opportunity to perform the associated attacks may shrink to only a handful or even to a specific actor or group. It could also be a new actor who doesn't exactly match any previously known actors or

[65] https://passionateaboutis.blogspot.co.uk/2015/07/ssh-fingerprint-from-pcap.html

groups. The confidence level of this attribution may also grow as more is learned through the collection of new evidence.

Like any other type of investigation, it's those bits that get overlooked by attackers and left behind that can be their undoing. Computer forensics can turn up a lot of evidence that is hard to forge or erase. Many details that surface about what was done and how it was done can serve both the response to the incident but also provide clues towards attribution.

The difficulty that arises around attribution, especially with public statements on attribution, is that the attributed evidence is often too weak, incomplete, or mostly circumstantial. This leads information security professionals, journalists, and others to call the attribution into question. Certain pieces of evidence may exist but aren't shared publicly such as the SSH key fingerprint used in the example above. Releasing these types of details can hurt the investigation and subsequent others. For example, if an SSH key is publicly reported as an indicator, the actor may realize their mistake and may change their SSH key every time they do a new attack, making correlation with other attacks much harder.

Intelligence Vs. Criminal Evidence

There is a significant difference between providing intelligence about an attacker and gathering enough evidence from a past attack to deliver a criminal conviction. First, the focus of intelligence isn't just post-incident forensics but analysis around the situation as a whole, its relation to other events, and estimates on potential future activities. There is strategic and tactical value in this type of information when done well. There is always the potential for intelligence to be wrong or miss the mark but it is provided as a best judgement based on available details. This is very different than law enforcement collecting facts about a specific incident or series of incidents to build a criminal case. The result of a criminal investigation must prove the case presented beyond a shadow of a doubt. The educated speculation so valuable in threat intelligence is often useless in court. Taking criminal investigations to this level protects against wrongful convictions and helps ensure only the guilty are punished.

Intelligence companies or government intelligence agencies may include attribution as part of a broader analysis around a particular event or series of

events. The confidence level associated with their assessment is meant to reflect the quality of the information obtained and how solid the resulting judgment is. It's up to the consumers of this information to decide any actions to take based on those details.

Criminal Convictions

Attribution to a specific individual has been successfully done well enough to obtain criminal convictions in quite a few well-known cases involving information security attacks or other computer crimes. Forensic evidence left on computers touched during attacks or used in computer-related crimes can reveal many clues. This evidence coupled with evidence available to law enforcement from additional sources through subpoenas and warrants, government-specific sources, and government databases can be enough to indict specific individuals and ultimately obtain convictions.

In a Virginia courtroom in May of 2016, a Romanian hacker named Marcel Lahel Lazar pled guilty to charges related to breaking into email and Facebook accounts of several prominent world figures.[66] He even claimed to have hacked into the famed private email server of Hillary Clinton although this was never substantiated. The hacker, who went by the name Guccifer (the inspiration for the name of the unrelated Guccifer 2.0 persona related to the 2016 U.S. presidential election), was arrested by Romanian authorities in 2014 and eventually extradited to the United States. He was sentenced to fifty-two months in prison, which he will serve before returning to Romania to serve out the remains of his seven-year sentence there.[67]

Ross Ulbricht was arrested in 2013 and subsequently convicted on narcotics trafficking and other charges related to running the famed underground marketplace, the Silk Road. The marketplace, which peddled drugs, fake

[66] http://www.nbcnews.com/news/us-news/guccifer-hacker-who-says-he-breached-clinton-server-pleads-guilty-n580186

[67] https://www.washingtonpost.com/local/public-safety/guccifer-hacker-who-revealed-clintons-use-of-a-private-email-address-sentenced-to-52-months/2016/09/01/4f42dc62-6f91-11e6-8365-b19e428a975e_story.html

passports, and even hit men for hire, had been running since 2011 and racked up an estimated $1.2 billion in sales. It was hidden in the TOR (The Onion Router) network and was therefore hidden from the typical tracking techniques that could be used for addresses directly on the Internet. In the process of advertising the presence of the marketplace when it first launched in 2011, Ulbricht had posted in some forums under the pseudonym "altoid." Later that year, he posted in another forum under the same pseudonym, looking for bitcoin experts to help him with a start-up company. He instructed those interested to respond to his personal email address, rossulbricht@gmail.com.[68] While this evidence helped aid the FBI in the investigation, it was additional evidence taken from subpoenaed records from Google, along with Silk Road's servers themselves, that helped seal the case against Ulbricht. It is currently unknown how the FBI was able to track down these servers hidden inside the TOR network. Yet Ulbricht was arrested while he was signed in as Dread Pirate Roberts on the Silk Road's website taking away any doubt he was involved in running the site.[69]

Public Attribution

Intelligence analysts and criminal investigators don't always have the chance to catch their guy actually sitting at the keyboard committing a crime. But they can use all the sources and methods at their disposure to get as close to that level of confidence as possible. Forensic investigations of affected systems, thoughtful collection of additional data, and previous experience all play a role in making a solid judgement on attribution. Law enforcement has additional tools such as warrants, subpoenas, and government databases to aid in their investigations. Government agencies have access to collection sources and methods not available commercially and unable to be disclosed publicly.

In criminal investigations involving secretive sources and methods for collecting evidence, the agency must consider what can be used in court and what they would be willing to divulge. The agency may already know who committed the crime but because this knowledge came as a result of sources and methods they

[68] http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/
[69] http://time.com/3673321/silk-road-dread-pirate-roberts/

are unable or unwilling to disclose, they may have to go backwards and find additional evidence through more traditional methods that they can disclose in court.

This may have been the case in the Ross Ulbricht investigation. It's possible the FBI knew it was likely Ulbricht before investigating him due to information captured through secret methods of compromising the anonymity of the TOR network. They may have then performed a more traditional collection of evidence including catching him in the act in order to build a court-worthy case. This way they wouldn't have to disclose their methods of piercing the TOR network's veil of anonymity. That method's usefulness in other criminal cases where TOR is used would be too valuable to "burn" by sharing that evidence in court. While it's not currently public knowledge exactly what twists and turns the FBI's investigation of the Silk Road took, there is a growing body of evidence that the FBI uses exploits in TOR software to gather evidence.

In a 2013 case in Ireland, the FBI was allowed to share that it had taken control of TOR servers belonging to Freedom Hosting to gather evidence in a child pornography case.[70] A recent vulnerability in the Firefox browser software, used as the core of the TOR Browser used for surfing the web anonymously, was also blamed on the FBI.[71] The FBI has not officially accepted blame for this exploit, however. Other cases have been dropped in the past rather than reveal the sources and methods used to collect crucial evidence in court.[72][73]

This is the dilemma when it comes to attribution in a public setting. Intelligence agencies and law enforcement have access to sources and methods unavailable outside of government. The cost of revealing their methods or tools is often much higher than the cost of letting a single criminal go or taking a public relations hit for not explaining why they believe something to be true. Even for private companies who have incident response services for computer breaches,

---

[70] https://www.wired.com/2013/09/freedom-hosting-fbi/
[71] http://arstechnica.com/security/2016/11/firefox-0day-used-against-tor-users-almost-identical-to-one-fbi-used-in-2013/
[72] http://www.theregister.co.uk/2017/01/06/fbi_lets_people_off_to_keep_methods_secret/
[73] http://www.theregister.co.uk/2015/04/21/st_louis_stingray/

it's not in their best interest to reveal everything that they know about a specific breach. The full details are part of their proprietary intellectual property that they can use to provide protection to their customers against those adversaries. Giving away too much information only empowers their adversaries to change their tactics. It also enables their competitors to leverage the details they've worked hard to obtain. These factors may then result in public documentation that contains some of the evidence to support the conclusions made but isn't reflective of everything known to support the attribution.

Attribution in the Attacks During the 2016 U.S. Election

In the case of the 2016 U.S. presidential election, the evidence that has come out that supports involvement by elements of the Russian government is compelling. But it is not strong enough on its own to refute all other possibilities. This is the source of the criticism of this attribution. In the end, it is a matter of faith in the institutions making the accusation as to whether one believes the attribution to be accurate.

The United States government may indeed have direct evidence that elements of the Russian government sought to influence the 2016 U.S. presidential election. The Russians would know that the U.S. would not be willing to let the public in on how they know it was Russia. Thus far, the Russians have simply denied the allegations. It becomes a battle in the court of public opinion with neither side providing firm proof that it was or wasn't the Russian government behind the attacks.

Security companies like Crowdstrike, FireEye, TrendMicro and others highly suspect the Russian government was behind the attacks on the U.S. election. They may have strong, privately held evidence that Russia was behind these and several other high-profile attacks in other nations. There is a growing amount of evidence in the public domain that suggests the Russian government is involved, at least in an ancillary way, in a great number of information security attacks that conveniently align with Russian state interests.[74][75]

[74] https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html

Conclusion

"The best defense is for our public to know what's going on so they can take it with a grain of salt."

U.S. Senator Angus King referring to Baltic states dealing with Russian interference in their elections - Jan. 5, 2017[76]

Secure elections are a cornerstone of Western democracies. Protecting the integrity of elections then, is paramount to protecting the foundations of Western society. The threat of hacking, not only of systems connected to elections themselves but also the political entities connected to elections, is now an important element of protecting elections.

Something that is important to capture in these events is the element of asymmetric warfare involved. Elections can be influenced by hacking a political operative's phone or email, releasing compromised details to the public, and thereby potentially influencing the results of the entire election. Any actor or group capable of creating and deploying successful phishing attacks designed to steal credentials or deploy malware could conceivably perform similar attacks to what was seen in the 2016 U.S. presidential election. With all the attention these attacks have received, attacks from new actors should be expected in future elections. Consider the results achieved: an election in question and now a foreign policy response from the White House. These are significant considering the relatively low cost of performing the attacks.

The result is that lone wolf actors like Marcel Lahel Lazar who target political figures will continue to be threats to elections in addition to nation states. Considering the potential benefits in outcome, hackers-for-hire like Andrés

---

[75] http://blog.trendmicro.com/trendlabs-security-intelligence/cyber-propaganda-influenced-politics-2016/

[76] https://www.c-span.org/video/?420936-1/senior-intelligence-officials-resolute-russian-role-electionyear-hacking

Sepúlveda may also become more common threats to elections. Even young, aspiring hackers looking to make a name for themselves can be a threat to elections. In February of 2016, a 16-year old was arrested in the U.K. after allegedly hacking into the personal email account of then CIA director, John Brennan.[77]

It is not just the business email accounts of political operatives which can be used to influence an election. Personal email accounts, social media accounts, and other online services can all be targeted to obtain sensitive and potentially politically damaging information. Targets now include not only the politicians themselves but anyone connected with them. Any of these targets could provide salacious details that could prove valuable in swaying public opinion.

It may not be possible to provide enough evidence to fully convict Russia of attempting to influence the 2016 U.S. presidential election in the court of public opinion. It should be noted, however, that the actions taken by those responsible for the attacks certainly do align with Russian state interests. If Russia is willing to take these sorts of actions, it can be expected that further activities involving Russian state interests are likely.

Another point widely known amongst information security companies is which types of malware are associated with Russian state-sponsored actors. Why these Russian actors, who are often touted as sophisticated and stealthy, continue to use the same malware families that have only been attributed to their use is a curiosity. It may be that they aren't concerned enough about potentially being known to expend the effort to develop new malware or leverage other available options. Lack of additional evidence still provides them some level of plausible deniability to the public.

As long as politicians, political organizations, and other political operatives continue to engage in behaviors considered to reflect corruption by members of the electorate, the draw for hacking and releasing their private information will

[77] http://www.telegraph.co.uk/news/uknews/crime/12154592/British-teenager-suspected-of-being-a-mystery-hacker-who-stole-CIA-boss-emails.html

be strong. The more connected our society becomes, the more avenues for obtaining and releasing sensitive details becomes. The challenges of protecting all these potential attack avenues is broad and will get broader as more options become available. The need for heavy collaboration during campaigns and behind the scenes coordination of large numbers of resources only exposes these entities further.

Democratic governments will only be able to do so much to protect political organizations against these attacks. Since primary targets include private organizations and private individuals, offering guidance for keeping secure may be one of the few options available for protection. Diplomacy, prosecution, and retaliation against those responsible would also be on the table, however. That is to assume the culprit(s) behind any attacks can be found.

What can be done

For nations, a full arsenal of responses is available including sanctions, diplomacy, regulations aimed at improving defenses, legislation, retaliation, or even conventional warfare. As mentioned, some nations are even considering becoming more offensive in their response to attacks against critical infrastructure including elections.

For private organizations, these options aren't on the table. Trend Micro shared some recommendations for political organizations to help resist security attacks.[59] It includes some good advice including reducing attack surface, patching regularly, and performing regular penetration testing. In addition to these, leveraging two-factor authentication for at least remote email access and remote network access is a good thing to include. Even free accounts like Gmail include the ability to apply this protection.

Education is another valuable tool in preventing attack vectors like phishing. Ensuring that those who might be privy to sensitive information are educated on how to protect social media accounts, email, and smart phones against typical attacks can help them resist attempts at compromising them.

Intelligence sharing not only amongst organizations involved in elections but also amongst political organizations and industries who may have already experienced

attacks from nation states can help develop proactive defenses against attacks. Attackers see major benefits from siloed intelligence sharing. When one industry is targeted for a period of time by a particular nation state, certain details are learned. When another industry is subsequently targeted, these same lessons are now learned afresh by new organizations. Sharing intelligence between these industries can help not only proactively respond to attacks but can also lead to deeper details learned and better attribution across subsequent attacks. This can lead to developing a broad, collective profile of common attackers including those suspected to be associated with nation states.

Helping the electorate understand the potential goals and methods of influence nation states might use in their elections is another way to defend election integrity. Developing a general sensitivity to media bias, false reporting, and other factors of influence in elections will help them discern truth from fiction and focus on facts instead of bias.

Elections are complex events. Hacking is only one threat to election integrity that must be taken into consideration. Governments using all the resources at their disposal to protect elections along with thoughtful protections employed by political organizations and a well-educated electorate can all help ensure that elections are as safe as possible from outside influence.