RUSSIAN ATTACKS ON 2016 US ELECTION

Sources

- Assessing Russian Activities and Intentions in Recent US Elections, National Intelligence Council, January 6, 2017
- #Digital Deceit: The Technologies Behind Precision Propaganda on the Internet, Harvard Kennedy School on Media, Politics, and Public Policy, January, 2018
- Indictment – USA v. Internet Research Agency, February 16, 2018
Session Goals

- Summarize facts of Russian attack on the US 2016 presidential election
  - DNC
  - DCCC
  - Clinton campaign
  - Creation of conflict and chaos
- Explore underlying technology used in the attack
- Consider potential for future election attacks
- Consider options to reduce the threat in future elections
- Stimulate thinking on implications for US policy

Barr Report

- Released 3/24/19
- Summarized findings of the Mueller special investigation into Russian interference in the 2016 election
- Finding categories
  - Russian interference – Russian government actors hacked into computers and also conducted disinformation and social media operations aimed to interfere with election
  - Conspiracy – “investigation did not establish that members of the Trump Campaign conspired or coordinated with the Russian government in its election interference activities”
  - Obstruction of justice – no prosecutorial judgement
2016 Election Results

- Donald Trump wins US Presidential election, despite receiving 2.8M fewer overall votes than Hillary Clinton
- Margin of victory in US electoral College is approximately 77,000 votes in 3 states

US System of Elections

- Historical blend of direct and indirect elections
- Representatives
  - Elected once every 2 years
  - Direct election
- Senators
  - Elected once every 6 years
  - Direct election with the 17th Amendment (1913)
- President
  - Elected once every 4 years
  - Electoral college system
General Background

• Some concerns with the US voting systems following the 2000 Presidential election
• Limited coordinated attempt to modernize/update US voting systems
• Voter suppression efforts
• Partisan disputes of voter eligibility
• Questions of legitimacy of voter registration data
• Proposed voter ID laws

Relevant Laws

• Illegal for foreign nationals and foreign governments to make contributions or spend money to influence an election
• Bars agents of any foreign entity from engaging in political activities without registering with the US Attorney General
Intelligence Gathering & Assessment

- US Intelligence agencies have been gathering information on the 2016 election, but much of that material remains classified
- Leading agencies
  - Central Intelligence Agency (CIA)
  - Federal Bureau of Investigation (FBI)
  - National Security Agency (NSA)

Mueller report (not yet released) expected to contain results of intelligence gathering

2016 Election Results Assessment (1/6/17)

- US intelligence agencies made no assessment of the impact that Russian activities had on the election results
- Ordered by Russian President Vladimir Putin
- Russian efforts consistent with efforts to undermine US-led democratic order
- Russian goals
  - Undermine public faith in US democratic process
  - Denigrate Hillary Clinton, harming her electability and potential presidency
  - Preference for Donald Trump

Note: Russian aims were furthered by the attack, independent of which candidate won the 2016 election
DNC

- Democratic National Committee
- Coordinates strategy to support Democratic election candidates
- Early subject of attack
- Private political organization (not a government agency)
- Protected only by private IT staff (not subject to NSA/FBI cyber protection)
- Infosec Institute tests revealed massive security flaws

Scope of Attack

- Coordinated teams of attackers, reportedly numbering in the hundreds
- Multi-year attack, probably originating in 2014
- "activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations"

Trump: hackers could be Russia, China, or a "guy sitting on their bed who weighs 400 pounds."
**Timeline**

- Fall 2015 – NSA and FBI detect unusual DNC traffic
- Spring 2016 – Hack detected at DNC, showing massive loss of contributors, opposition research, chats, and e-mails
- Summer 2016 – DNC acknowledges a hack, claimed by Guccifer 2.0, who states he leaked DNC e-mails to WikiLeaks
- Summer 2016 – Spear-phishing attack on DCCC
- Summer-Fall 2016 – documents released at the start of the Democratic National Convention
- 2/16/18 – Indictment against Russian connected individuals

**Attack Participants**

- Bears - security term for various Russian intelligence affiliated organizations
- Internet Research Agency – Putin affiliated organization
- Guccifer 2.0 – persona of Russian hackers
- DC Leaks – Publishes leaked e-mail messages (linked to Fancy Bear)
- WikiLeaks – Publisher of leaked documents
- Democratic National Committee (DNC) – political arm of Democratic Party
- CrowdStrike – Internet security company
- Clinton Foundation – Charitable foundations set up by Bill & Hillary Clinton
Russian Attack Targets

1. Email and document servers
2. Voter rolls
3. Social media

Email and Document Attacks

Image: Macaws Infotech
Attack Components

- In July 2015, Russian Intelligence gained access to DNC networks and maintained access until at least June 2016
- GRU (General Staff Main Intelligence Directorate) began cyber operations on the US election by March 2016
- GRU operations resulted in the compromise of personal e-mail accounts of Democratic Party officials and political figures
- By May 2016, GRU exfiltrated large volumes of data from the DNC
- GRU used the Guccifer 2.0 persona, DCLeaks, and WikiLeaks to release US victim data (also used media outlets)
- Spring 2016 – Clinton campaign chairman, John Podesta, was victimized by a spear-phishing attack, and inadvertently disclosed his e-mail password

Actions and dates taken from 1/17 Intel Report

Cyber War Attackers

- Cyber Bears are Russian hack groups allied with Russian intelligence, but operating independently
- Advanced Persistent Threats (APTs) are usually
  - nation-state actors because of the size and scope of their operations
  - associated with malware
- Conducted attacks against other Russian adversaries (e.g., Estonia)
- Relatively easy to identify
- Cyber Bears were referred to by CrowdStrike as:
  - Cozy bear (APT29)
  - Fancy bear (APT28)
  - Venomous bear – 2008 cyber-attack on US CentCom

Cyber bears are described as aligned with Russian organized crime
Cozy Bear Techniques

- **Typosquatting**
  - buy a URL very similar to a well-known site
  - Used to lure victims into downloading malware
- **Malware (Malicious software)** – harmful or intrusive software
- **Spear-Phishing**
  - technique used to gain access to DNC servers
  - Linked attack victim to misdepartment.com - a site identical to the real MIS Department site
  - Fake site downloads a malware kit

Note the example of typosquatting

Nature of Stolen Material

- 1. Truly negative material, for example
  - Strategies that should be neutral, but favor one candidate
  - Disparaging remarks about some candidates
- 2. Material that suggests wrongdoings, but contains little actual damaging information
  - Example – Hillary e-mail references
- 3. Innocuous material that could be twisted to suggest wrongdoing
  - Example Cheese Pizza = Child Pornography

Items 2 and 3 require attackers to suggest negative views of otherwise neutral information
### Public Release of Stolen Documents

- Effective use of stolen material requires
  - Analysis of content for damaging material
  - Use of a **cutout** (third party, used to distance the release from the attackers)
- Timed release - aligned with events in 2016 election campaigns
- Timed for maximum election effect
- The degree of coordination with people inside the US is vaguely known, but no directly related indictments
  - Trump Tower meeting
  - Release of polling data
  - Meetings between Trump campaign officials and Russians

More details expected with the release of the Mueller Report

### Document Release Organizations

- Guccifer 2.0
- WikiLeaks
- DCLeaks
- RT
Guccifer 2.0

• Persona (i.e., façade) of group that hacked the DNC
• Assessed as being created by Russian intelligence services to cover for interference in 2016 election
• Self-reported as Romanian
• Name refers to Guccifer
  • Marcel Lazar Lehel
  • Romanian hacker responsible for some US attacks
  • Technique – learn victim info, then guess passwords
  • January 2014 - Jailed in Romania
  • Extradited to US, and jailed in September, 2016
  • Reportedly returned to Romania to complete jail term there before completing US jail term

“we assess with high confidence that Russian military intelligence used the Guccifer 2.0 persona and DCLeaks.com to release US victim data” – 1/17 intel report

WikiLeaks

• Founded in 2006 by Julian Assange – hacker who penetrated secure networks
• Outlet for leaked documents
• “Giant library of the world’s most persecuted documents”
• Published Iraq, Afghanistan, Guantanamo docs/videos
• Assange
  • Was in a London embassy, avoiding extradition on a rape charge
  • attitudes towards Russia changed around the time of the rape charge
  • Currently negotiating release/asylum

Have you seen The Post?
RT

- Formerly Russia Today
- Media arm of the Russian government
- Paid American contrarians (e.g., Michael Flynn)
- Themes
  - Criticism of western governments
  - Promotion of radical dissent
  - Promotion of alternate US parties
  - Change of US system through revolution
  - Anti-fracking

CrowdStrike

- American cyber security company located in Silicon Valley
- Worked counter-measures in several high-profile cyber-attacks
- Identified details of the attack on the DNC
- Valuation over $1B
Attack on Voter Rolls

Attacker Goals

- Cause voting disruptions
- Delegitimize the voting process
- Create concerns of voter fraud

“types of systems Russian actors targeted or compromised were not involved in vote tallying” - 1/17 Intelligence Report
Background

- Voting systems are highly distributed within the US
- No standardization of
  - Voting technology
  - Data collection
  - Voter registration
- Voting systems/technology largely controlled by states
- 2000 election raised issues of voting device security

Note: Result of the 2000 presidential election was essentially undecidable

Actions

- “Since early 2014, Russian intelligence accessed elements of multiple state or local electoral boards”
- “Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment”
- Successful attack on Illinois voter registration (personal data on 200,000 voters)
- Cyber-attack in August 2016 against a US company to obtain information on election HW/SW
  - Resulted in a voter registration themed spear-phishing campaign targeting local US government organizations
- October 2016, attackers offered election-related products and services
- Attackers sent test e-mails, testing attacks against absentee ballot system

Results of the 2016 attack unknown, but likely resulted in at least one compromised system
Potential Voter Registration Attacks

- Many state voter registration DBs are on-line
  - E.g., electronic poll books (used to check voters in)
  - NSA document refers to a company that makes electronic poll books
- Possible attack strategies
  - Disrupt the electoral process
  - Names could be deleted from the voter rolls
  - Changes to voter roll data are possible

Social Media Attacks
**Attack Goals**

- Weaponize stolen information by targeting it to selected groups and amplifying it
- Create chaos through the distribution of false information
- Target people within a society, influencing their beliefs and behaviors
- Reduce trust in US government
- Increase chaos
- Discredit public and private institutions

---

**Video**

- [https://nyti.ms/2z2TIHb](https://nyti.ms/2z2TIHb)

*Politics*

How Russian Bots Invade Our Elections

How do bots and trolls work to infiltrate social media platforms and influence U.S. elections? We take a closer look at these insidious online posts to explain how they work.
Bots and Trolls

- **Trolls** – Humans who generate fake news stories, e-mails, messages, etc.
- **Bots** (software robot or web robot) – software app that runs automated tasks over the internet

![Image: Valentina Kulagina, 1930](image)

Attack Strategies

1. **Access streams of online information to influence networked groups**
   - Inserted propaganda must fit the narrative of the networked group (e.g., Clinton Foundation or Benghazi)

2. **Use the trend mechanism in social media (mainly Twitter)**
   - Insert propaganda into a social media platform
   - Using bots, create a trend
   - Social media users will notice the trend and further increase the awareness of the trend

3. **Combination of 1 and 2**
   - If the topic is successfully trending, the propaganda is sometimes continued in mainstream media

Twitter estimates that 15% of its accounts are bots
Social Media Trending

- Social media sites use an algorithm to analyze text to create a list of popular topics
- Trend Attack Methods
  - Trend distribution – apply a message (propaganda) to every trending topic
  - Trend hijacking – taking over a trending topic through the use of bots
  - Trend creation – amplifying a propaganda topic with bots
- Bots are programmed to
  - Tweet at various intervals
  - Respond to certain words
  - Retweet when directed by a master account

Twitter launched a “bot purge” following the 2/16/18 indictment of IRA officials
Other purges since early 2018

Internet Research Agency (IRA)

- Troll farm with main location in St. Petersburg, Russia
- Reportedly employs 600 people across Russia
- Ex-employees and indictment reported tasks
  - Fake social media accounts (Facebook, Twitter, Instagram, YouTube)
  - Use stolen identities to post on social media
  - Circulate pro-Kremlin propaganda
  - Spread derogatory information about Russian opponents
- Likely financed by a close Putin ally (Yevgeny Prigozhin) with ties to Russian intelligence services
- Defendants travelled to US and procured US infrastructure to hide Russian origin of work
- Departments – graphics, data analysis, search engine optimization, IT, and finance
IRA Social Media Attacks

- Specialists impersonated US people in bogus accounts
- Sensitive to US work times and holidays
- Supported radical groups oppositional social movements
- Increased dissatisfaction with social and economic situation
- Many created groups had hundreds of thousands of followers:
  - Secured borders
  - Blacktivist – Organized Baltimore rally to mark death of Freddie Gray
  - South united
  - Heart of Texas – Promotes Texas secession
  - United Muslims of America
  - Tennessee GOP (@TEN_GOP) – 100,000 followers

Example – Creating Social Unrest

- Houston, May, 2016
  - One group protested the threat of radical Islam, while a larger group of counter-protestors gathered nearby
  - Both groups were organized by IRA attackers

"130 rallies were promoted by 13 Russian pages, which reached 126 million Americans with provocative content on race, guns, immigration and other volatile issues" – NYT, 2/18/18
Example - Twitter / WikiLeaks

- 7/23/16 – Trump tweeted “The WikiLeaks e-mail release today was so bad to Sanders that it will make it impossible for him to support her, unless he is a fraud”
- Assange immediately replied to the Trump tweet and linked to the DNC document cache, with the message “everyone can see for themselves”

Donald Trump probably has a about 25M Twitter followers.
But many more (30M+) Trump (and other politician) followers are fake

Disinformation Campaign

- 9/17 disclosure by Facebook that it sold $100K in ads to Russian troll farm (3,300 ads)
- Ads
  - Named Trump and Clinton
  - Focused on amplifying dissent (LGBT, race, immigration, gun rights) and directed at people interested in the subjects
  - Targeted geographically and to people susceptible to political messaging
- 2/18 indictment of IRA revealed details of campaign

Huge ethical conflict for Facebook (and other social media organizations)
IRA Activities

- IRA infrastructure
  - Purchased space on US servers
  - VPNs connect Russian servers to US servers to mask activities - opening accounts, communicating with US persons, and accessing social media accounts
  - Registered and controlled hundreds of Web-based email accounts to appear to be US-based
- IRA used stolen or forged identities
  - Opened accounts at PayPal
  - Created false identification (e.g., driver’s license)
  - Used fake identities for social media posts
  - Maintained accounts and purchased ads on social media

2/18 Indictment Charges

- Staged political rallies inside US
- IRA employees posed as US grassroots entities and US persons, and
  - Solicited and compensated US persons to promote or disparage candidates
  - “Communicated with unwitting individuals associated with the Trump Campaign and with other political activists to seek to coordinate political activity”
Social Media Response

- Gradual Realization of the impact of social media on news dissemination
- Some policy adjustments by Facebook and Twitter

![Image: Shutterstock]

Defense Measures

![Image: Shutterstock]
Future US Elections

- Potential for continued attack during 2020 election
- Issue: Cost/difficulty of cyber defense is much greater than cost/difficulty of cyber attack
- Approaches
  - Improved defense
  - Deterrence

Class Discussion

- Do you consider the Russian attack on the 2016 US election to be consistent with kinetic attacks? For example,
  - 9/11
  - Pearl Harbor
- To help prevent a future attack, do you think that we should use some announced response as a deterrent? If so, how severe?
  - Sanctions
  - Cyber attack
  - Limited kinetic attack
  - Covert actions
Class Discussion

- What is your view of WikiLeaks? (good or bad)
- Should Julian Assange be prosecuted?
- Was it be ethical for Trump campaign staff to use Democratic strategy information openly available in WikiLeaks?
- Has your social media usage changed because of prevalence of disinformation attacks?

Questions