Russia’s Campaign
to
Influence U.S. Elections

Office of the West Virginia Secretary of State
Don’t fall for it!
Who Is Behind It?

To Putin, the End Justifies the Means

In 2016, Russia spent millions ($) distributing misleading & false info on social media to:

• **Disrupt** U.S. democratic election processes
• Cause U.S. citizens to **doubt election systems & results**
• Turn U.S. citizens against government
• Create distrust, **sow discord** & generate chaos
• Pit people against one another
What is the Goal?

• Divide, Discredit, and Distract the West
  • Have us not **trust** our own government
  • Degrade NATO cohesiveness
  • Turn us on **ourselves**

• Themes from Russian Attacks Overseas:
  • Western policy failures, setbacks, **incompetence**
  • Russia’s successes
  • **Unpredictability** of the U.S.
Why Are They Doing It?

Can’t compete with U.S. economically
Can’t stand toe to toe with U.S. militarily
Only hope to stay competitive is to bring U.S. down from the inside
How are they doing it?

Information Operations

Propaganda is as Old as War itself

- The **scale is new**, given the internet
- Russia has weaponized the internet
- Russia seeks “**Information Dominance**” vs US openness, security

Intensified by Artificial Intelligence (AI)

- Bad actors now run **mass influence campaigns** like never before
- AI—efficient targeting of people most vulnerable to manipulation
The “Great Game” Cyber Style

Today’s Clash of Civilizations Takes Place on Social Media

Khrushchev

“You Americans are so gullible. You won't accept Communism outright; but we'll feed you small doses of Socialism until you finally wake up & find you already have Communism. We shall conquer you without firing a shot!”

• China’s “Art of War” – **win without fighting**

• Russia’s great chess tradition – **win by out-smarting opponent**

• America’s “Spirit of ‘76” -- **win on ideas**, human freedom, liberal democracy

• North Korea, Iran/Terrorist Organizations also quite active

• Groundwork laid for **foreign & domestic** attacks
Transformative Commodities Throughout History

- **Stone Age:** Stones
- **Agricultural Revolution:** Land
- **Bronze Age:** Copper
- **Industrial Revolution:** Oil/Iron/Steel
- **Information Age:** Data
The New “Great Game”

“Data is the New Oil”

Clive Humby

• World powers now struggle for data superiority
  (5G, AI, machine learning, quantum computing)

• Data has economic, political, & military importance

• All data/information becomes strategic
IoT, Blockchain, AI

“...The Rising Philosophy of the Day, I’d Say it is Dataism.”
David Brooks, NY Times

- Internet of Things (IoT) – quantum leap in available data
- Blockchain - Unchangeable, permanent data storage
- AI - Unfathomable capacity to retrieve/process data

- Enhances “Dataism”
  - Big Data
    - “Universe consists of data flows”
    - Value is determined by contribution to data processing
AI, Algorithms, Bots

“AI is the New Electricity”
Andrew Ng

• AI turns data into actionable intelligence
• AI allows micro-targeting to influence decision-making
• Algorithms – set rules to get directed jobs done
• Bots – “Web Robots” run tasks on internet, social media
• Data-driven social media is key to public opinion
How Does This Apply to Us?

Russia doesn’t have to break into data systems; they achieve goals on softer targets using AI, algorithms, bots, & micro targeting.
Using Our Strengths Against Us

*Freedom is the American Spirit*

In 2016, Russia’s cost for meddling in U.S. Elections was less-than ½ the expense of a single fighter jet.

**US Strengths = Freedoms**
- Freedom of press
- Freedom of speech
- Freedom of religion
- Freedom of assembly

Russia has leveraged all of these via social media!
The Power of Social Media

*Using Social Media it Was Easy for Russia to:*

- Reach millions of voters with **minimal costs**
- Exploit divisive & heated issues within the U.S.
- Incite opposition, division & protests
- Focus was on whoever was in front, to sow discord
- **Publically diminish** front-runners, generating mistrust
Russian Social Media Efforts in 2016
Statistics of known false/misleading activity

Twitter: 10 Million Tweets
Instagram: 116,000 posts
Facebook: 61,000 posts
Additional Videos: 1,000+

That’s almost 28,000 social media actions per day!
2016: Russia Scanned All 50 States

Over 20 had “Extra Penetrating Measures”

States Targeted by Russian Hackers

- 21 States Targeted According to DHS
- Every State Surrounding WV Except Kentucky

Foreign Interference is everywhere
Why You?

• You are 1 of over 4 billion internet users.
• Your demographic is most likely to share posts
• Social media presence is highest among ages 18-24
• High school seniors are newest generation of voters
• First-time voters in 2020 Election – be educated & prepared!
Russia’s Target: the American Spirit

5 Real-World Examples
Disinformation

Altered Candidate’s Photo to Manipulate Public

Pro-Stacey Abrams

Anti-Stacey Abrams

Heads up Georgia. The Muslim Brotherhood is backing Abrams.

Communist

#MuslimBrotherhood
Competing Rallies

Creation & Promotion of Competing Protests

Pro-Trump Rally

Anti-Trump Rally

Nov. 12, 2016
4 days after the election.
Inciting Tensions

Advertised Competing Protests at Same Location & Date

Pro-Islam

Anti-Islam
Discouraging Voters

Targeting Race

All out assault on African American voters using social media!
Oppression

Social Media Ads that Divide American Society

Anti-Law Enforcement

Pro-Law Enforcement
Other Major Foreign Cyber Adversaries of U.S.
Misinformation vs Disinformation

• **Misinformation**: false/inaccurate info, *regardless of intent*

• **Disinformation**: *deliberately misleading*, incorrect, or biased info; manipulated narratives, facts, propaganda, *spread with intent* to deceive or mislead
  
  • *Examples*: deep fakes, altered or augmented videos, partial truths
Misinformation Is Everywhere: AI Failure

The Technology 202: Notre Dame cathedral fire reveals tech companies' struggle to combat misinformation

YouTube's defenses against misinformation just backfired in a big way -- and ended up contributing to baseless speculation online that the Notre Dame cathedral fire resulted from a terrorist attack.
Anyone Can Spread Disinformation

Ian Bremmer: American Political Scientist, founder of Eurasia Group consulting firm in NY, DC, London
“Half-Truths”

Covington High School Students Exploited by News & Social Media

There are always two sides to a story.

1st reports made student appear as aggressor; yet, full video shows, in fact, the man with drum purposely confronted the students.
Disinformation

Russia’s new “Operation Infektion”

• Disinformation is like a **virus**
  
  • Russia plants fake news reports in 4 corners of world
  • They plant **secondary reports that cite first fake report**
  • Then, they watch it spread
  • Once circulated, hard to trace origin / “**ground zero**”
  • Soon, fake stories get into Western news outlets
Scope of the Operation

Infiltrated far more than just Facebook & Twitter

Targeted internet platforms across the world, posting in at least 6 languages

<table>
<thead>
<tr>
<th></th>
<th>English</th>
<th>Russian</th>
<th>German</th>
<th>French</th>
<th>Spanish</th>
<th>Ukrainian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reddit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>indybay.org</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>homment.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>change.org</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>meinbezirk.at</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mein-suedhessen.de</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>globedia.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mediavida.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>beforeitsnews.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Livejournal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cont.ws</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>jeuxvideo.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Impersonation of Political Figures

• Prime example of disinformation trying to divide U.S & U.K.

• Bad actors want us to turn on ourselves

• High profile figures impersonated easily
Edited/Augmented/Altered Videos

Deep Fakes – now extremely hard to spot
- Super-imposing other peoples’ faces onto real videos
- Anybody can be impersonated on social media
- Completely falsified videos, can be made to say anything

Altered Videos
- Unlike deep fakes, subject matter is not changed
- Real video is slowed down, sped up, etc. to alter perception

Both are incredibly dangerous
Altered Videos

Facebook: “We don’t have a policy that stipulates the information you post on Facebook must be true.”
The Power of Fake News
Everybody Sees it, *Not Everybody Knows it*

- **PEW:** 23% of adults had shared a made-up news story
- Youth particularly targeted as vulnerable to misinformation
- Bots & AI micro-targeting intensify effectiveness
What Can You Do?
Protect  Detect  Correct
First: Protect

• Be proactive
  • Question validity of social media posts
  • Verify information using reputable sources to fact-check

• Protect yourself, your devices, and internet accounts:
  • **Always** use multi-factor authentication & complex passwords
  • Use a different password for every account
  • **Think before you link**, click or share anything questionable
Second: Detect

- Identify phishing attempts & website impersonation
- Read all unauthorized access notices or alerts (email, texts, etc.)
- Don’t ignore suspicious activity
- **Ransomware** – locks all data, pay $ to regain access
Detect: Some Fact-Checking Resources

- **Opensecrets.org** – shows who receives $ from Russia
- **Realorfake.org** – exposes fake news sites
- **Politifact.com** – fact checks US politics
- **Factcheck.org** – holds politicians accountable
- **Stopfake.org** – fact-check by Ukrainian profs & students
- **Polygraph.info** – fact check by Radio Free Europe, VOA
- **Sunlightfoundation.com** – nonprofit newsroom
- **Propublica.org** – nonprofit newsroom
- **Bellingcat.org** – distributed, collaborative investigating
- **WhatsApp** – new tip line for misinformation (India)
Detect: Suspicious Emails

Microsoft Office Email365

Your New Password Request

Your password reset is in process and your current password will expire shortly, the password reset link will be forwarded to the new alternate email submitted.

Ignore this email notification your request will take effect shortly.

If you did not request this password reset
Use Cancel Request button to cancel the password reset and keep your password unchanged.

Cancel Request

This action will take a brief period before this request takes effect.
This is a mandatory communication about the service. To set communication preferences for other cases.

This message was sent from the email address is not monitored. Do not reply to this message.
Privacy | Legal Notices

Microsoft Corporation
600 Pine Street, Suite 352,
Seattle,
WA 98101, USA.

Spear Phishing, Whaling
Specific Targets/Credential Harvesting

*Source: actual emails received by West Virginia officials
Detect: Anyone Can Be Hacked

U.S. Senator’s campaign, national news

WV resident’s personal social media compromised by Russia
Third: Correct

*If You Become a Victim of a Cyber Incident:*

- Turn-off devices & disconnect from internet
- Change passwords to *all* accounts on a different device
- Report to internet/social media providers
- If asked for ransom ($ or other value), report to police
American Voting Machines

IMPORTANT FACT:

NO EVIDENCE Any Votes Were Changed In a U.S. Election!

US voting machines are decentralized & maintained independently by each state.

In WV, voting machines:

1. Are never connected to internet
   • > 1,700 precincts managed independently by 55 counties
   • Very difficult to hack; requires physical security breach

2. Produce paper ballots verified by each voter

3. Pre- & post-election audits ensure security & accuracy
Media’s Vital Role: They’re a Target Too!

Today, it’s **Who Reports the Votes**

Food for thought

What if a news agency is hacked & reports wrong winner?

Can we trust reported outcomes today?

Would public cry out for a recount or new election?

Would public question legitimacy of results?

---

Former Soviet Dictator Joseph Stalin
“What’s Going On?”
Marvin Gaye

3 Dimensional Chess

1. **Body** = Equipment, Ballots, Poll Books *(no problems)* **TRUTH**

2. **Mind** = Process, Tabulation, Voter Registration, Reporting *(some problems)*

3. **Spirit** = American Psyche, Acceptance *(real problems)* **TRUST**
   This remains main **vector of Russian attack**

Need both **Truth AND Trust**

When we buy into
“America has never been so divided”
**Russia wins!**
Conclusion

1. Stay alert: be conscious, aware & protect against false info.

2. Anticipate Russia’s tactics; < effectiveness by exposing antics.

3. Minds, not machines: Russia attacks our minds/spirit; hasn’t succeeded in attacking our voting machines.

4. Race with no finish line: must always stay ahead of bad actors.

5. It starts with you: educating the public protects our democracy, & you are our first line of defense.
REMEMBER

Russians Attacked Our Mind & Spirit, Not Our Machines

Foreign Interference Summary (2 minutes)

Foreign Interference Video (6 minutes)
For more information, contact:

The Office of the Secretary of State
State Capitol
Charleston, WV 25305
(304) 558-6000
https://sos.wv.gov