Information Operations

Information Operations

- Attack someone using information—bits
- Sometimes, it's propaganda—but Propaganda 2.0, geared to the Internet era
- Other times, it's hacking
- During the 2016 election campaign, Russia did both of these and more

Caution

- This is a moving target
- There are new assertions every day about what actually happened
  - (And, of course, new denials)
- IMPORTANT: Some assertions are in dispute; some are even credibly disputed
- NOTE WELL: This is *not* a lecture about the (alleged) evils of the Trump campaign—such details are included *only* to provide context
  - Collusion, real or imagined, is out of scope!

Hacking

The DNC

- "Someone"—the US intelligence community says, with high confidence, that it was Russia—hacked a Democratic National Committee email server.
- They also hacked John Podesta's email
  - Podesta was the chair of Clinton's 2016 campaign committee
- These were strategically leaked by "Guccifer 2.0"
  - Some "leaked" documents purporting to be from the Clinton Foundation were from elsewhere or were forgeries

The DNC's Response

- In late 2015, the FBI warned a DNC sysadmin about Russian attacks
  - He thought the phone call was bogus, did a cursory scan of a computer, but basically ignored it
- The DNC did very little more in response, until it was too late
- The Russians didn't vanish…

The DNC Emails

- Wikileaks released tens of thousands of emails taken from the DNC
- (Some claim that this was done in coordination with the Trump campaign)
- (Roger Stone, a Trump friend and advisor, has stated he communicated with Julian Assange)

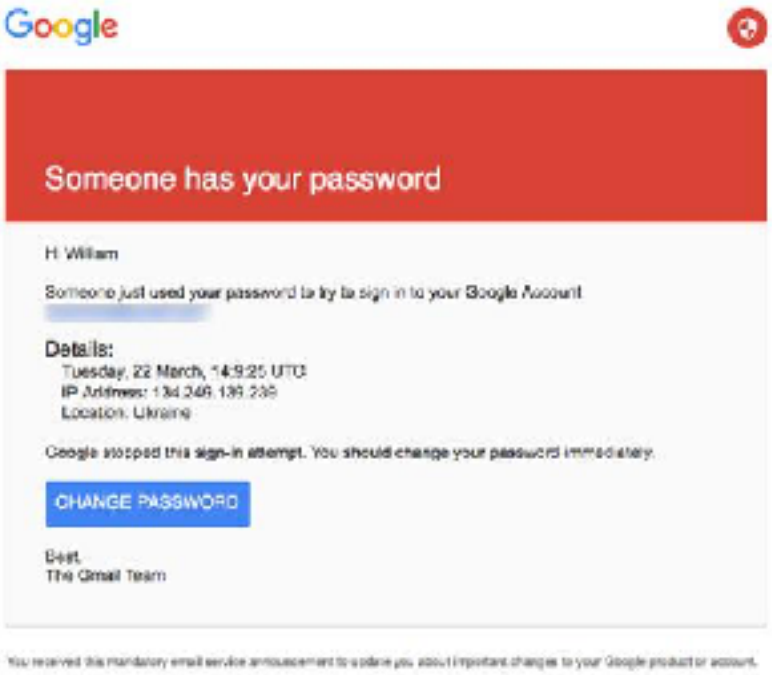
Wikileaks

- On October 7 at 4:00pm, the Washington Post broke the story about the Access Hollywood tape
- Two hours later, Wikileaks published 2,000 of John Podesta's stolen emails
- Clinton: "And I've no doubt in my mind that there was some communication if not coordination to drop those the first time in response to the Hollywood Access tape."

http://www.abc.net.au/news/2017-10-16/hillary-clinton-says-julian-assange-helped-donald-trump-win/9047944

Podesta's Email

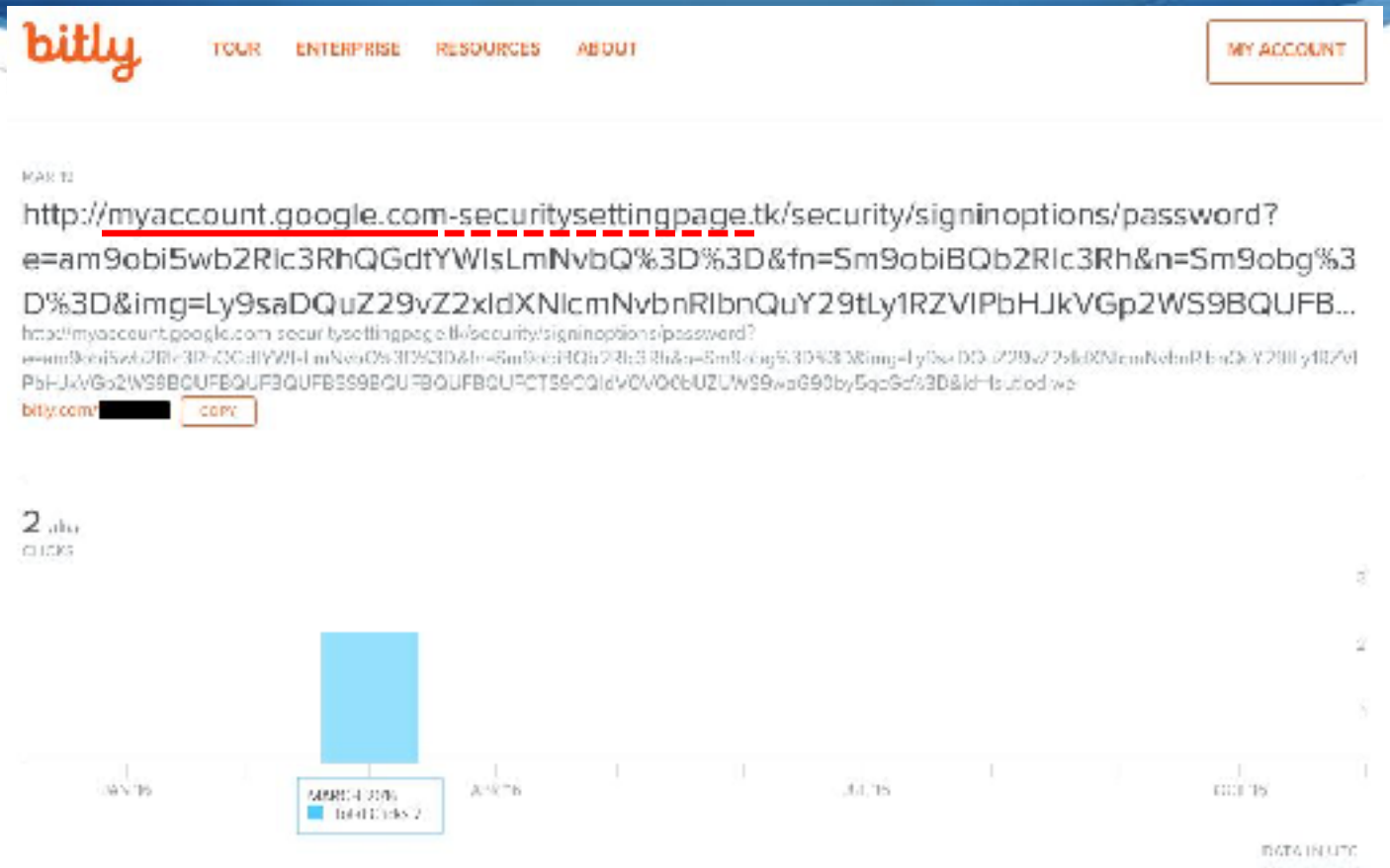
- Podesta received an email like this
- Podesta was suspicious and checked; his sysadmin said it was legit
  - Apparently, he meant to say "not legit"
- The link goes to a bit.ly address
- The attackers didn't secure their bitly acount…



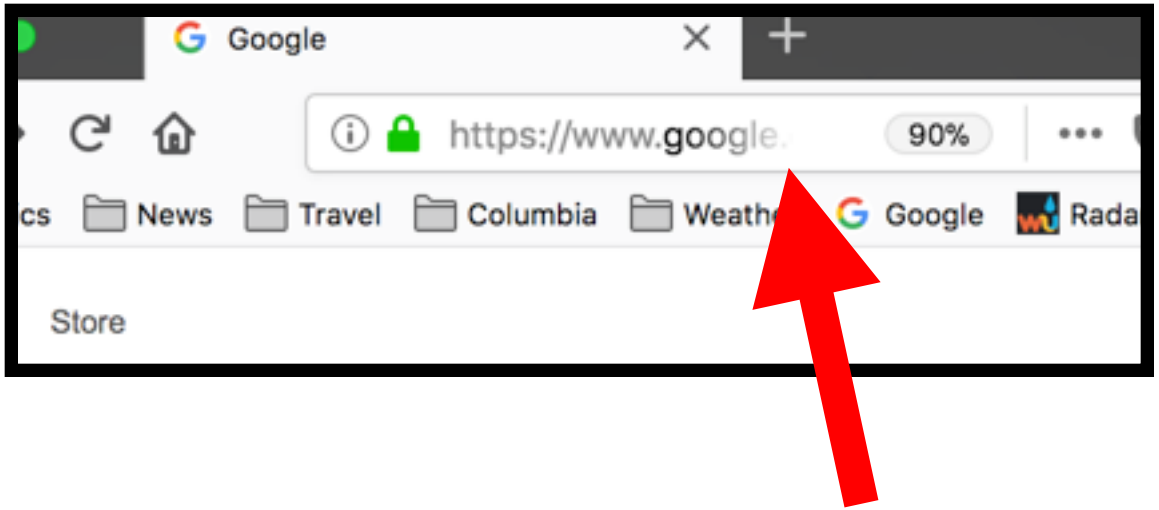
(What's bit.ly?)

- bit.ly is a URL-shortener—it maps a long URL to something that takes up less space and is easier to type
- Why does it exist as a commercial enterprise?
- All such requests go to their web site, which sets and receives cookies, receives `Referer:` lines, and generally tracks users around the web

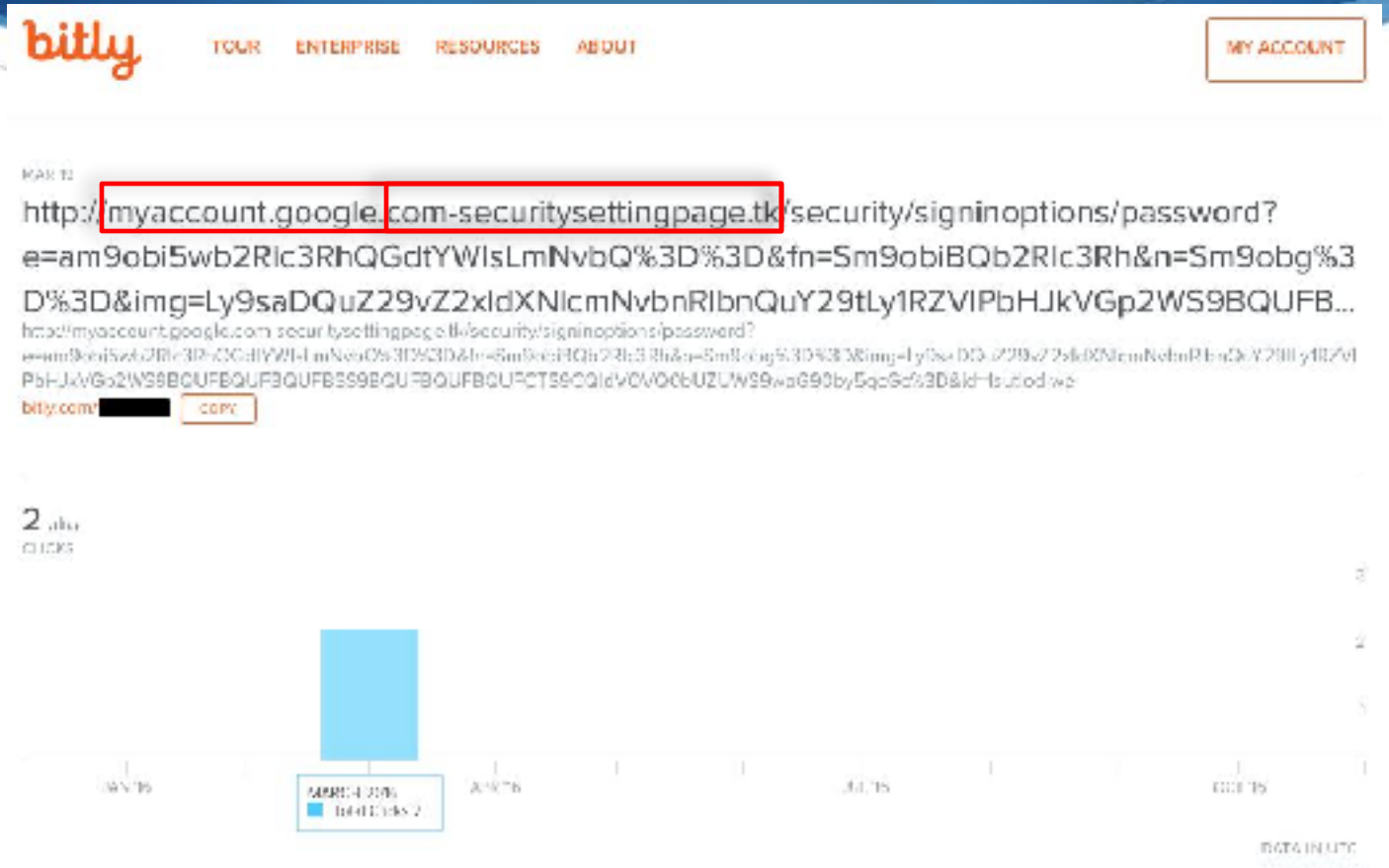
Looks Legit at First Glance



Displaying the URL



The Actual Hostname



Spear-Phishing

- This was a spear-phishing attack—email intended for Podesta and only for Podesta, to steal his gmail password
- A defense: some form of "two-factor authentication", such as the Yubikey

(Photo by Yubico, via Wikipedia)

Two-Factor Authentication

- Passwords are "something you know"
  - They can be guessed; more seriously, they can be replayed
- Tokens (including phones) are "something you have"
  - The output of most tokens is not replayable
  - Some use public key cryptography; others output some function of the time of day
- (Also: biometrics, e.g., fingerprints: "something you are")

Who Did It?

- Both the US intelligence community (the "IC") and many private security firms attributed the attack to Russia
- Two different hacking groups involved
  - "Cozy Bear" (AKA APT29): the FSB and/or SVR (the two parts of what was once the KGB)
  - "Fancy Bear" (APT28): the GRU (Russian—and once Soviet—military intelligence)

More Russian Hacking

- The Russians also went after the election systems
- Voting machines are hackable—but they're not good targets
  - There are more than 3,000 counties in the US; most run their own voting systems
  - There are many different types of voting machines, and most (usually) aren't on the Internet
- But—what about the registration database? What about the poll books?

Enter the Russians

- DHS says that Russia probed the election systems of many different states
  - The exact number is in dispute
- Were they adding voters? Deleting voters? Stealing information?
  - Durham County, NC had electronic poll book problems—some suspect hacking, though this is hotly disputed

NBC's Report

"The U.S. intelligence community developed substantial evidence that state websites or voter registration systems in seven states were compromised by Russian-backed covert operatives prior to the 2016 election — but never told the states involved, according to multiple U.S. officials.

"Top-secret intelligence requested by President Barack Obama in his last weeks in office identified seven states where analysts — synthesizing months of work — had reason to believe Russian operatives had compromised state websites or databases."

https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296

DHS Response

- "Recent NBC reporting has misrepresented facts and confused the public with regard to Department of Homeland Security and state and local government efforts to combat election hacking. First off, let me be clear: we have no evidence—old or new—that any votes in the 2016 elections were manipulated by Russian hackers." (https://www.dhs.gov/news/2018/02/12/dhs-statement-nbc-news-coverage-election-hacking)
- But—NBC didn't claim that *votes* were manipulated…

What Did Hacking Accomplish?

- The release of the stolen emails seems to have had some effect, though the extent isn't clear
  - They certainly were a distraction
- The timing is very suspicious
- No credible evidence of actual attacks on voting machines
- It remains unclear what the purpose or effect was of registration database probes

Propaganda 2.0

Social Media

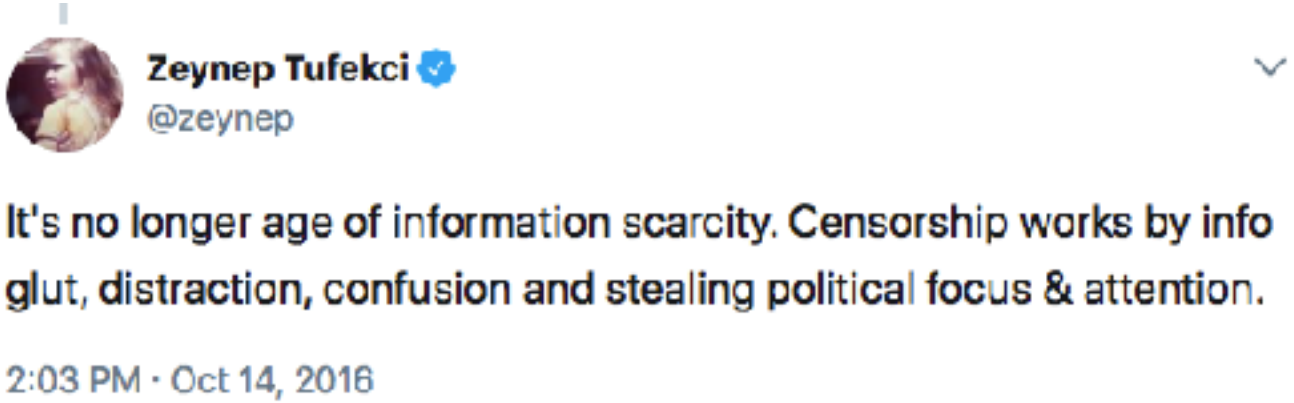
- The Russians clearly used social media in an attempt to meddle with the election
- The stories are often vague and contradictory, and sometimes downright weird
- This is a moving target; there's more news every day
- Did they really use Pokémon Go to fan racial unrest?
- Did they really tell their operatives to watch "House of Cards" to understand American politics?
- (Mueller claims that some Russian operatives visited the US)

Tactics

- Use of Facebook, Twitter, and Google
  - Others?
- Bots, to post things, drive up follower counts, repost
  - The exact number is subject to dispute
- Ads
- Bloggers; fake news
- Perhaps offering the Trump campaign damaging information about Clinton
- ("Kompromat" on Trump?)

Distraction?

- Create enough fake news and/or dubious news and/or targeted news to drown out the real stuff
- Goal: leave people uncertain where to go for reliable information



Russian Goals

- Defeat Clinton
  - Some stories claim that Putin hates her for her actions while Secretary of State
  - Mueller indictment dates the earliest activities to 2014
- Weaken the US
  - Create or fan dissension
    - Backed: Black Lives Matter; far right groups; Sanders; Stein
    - Or so some stories claim
  - Create doubts about the legitimacy of the election
- Weaken US allies, especially NATO

Targeting

- Stealing voter rolls from state election sites?
- Cambridge Analytica? (per vox.com)
- Internet Research Agency, in St. Petersburg?
  - Indicted by Mueller's grand jury!
- Machine learning from Twitter feeds?
- Geographical targeting, e.g., swing states

Are They Going Elsewhere?

- Some reports allege links to the Brexit campaign
- Fake news in France, just before the election
- Germany?
- Elsewhere?
- The US intelligence community says that Russia is already working on this year's mid-term elections

Amplification

Limited Direct Actions

- Russia ran some social media bots, especially on Twitter and Facebook
- They bought some ads
- Assorted people knowingly created fake stories as clickbait
- They retweeted/reposted stuff

But it seemed to have disproportionately large impact!

The Ads

- Yes, there were some direct ad purchases
- The Russians also paid to have some Facebook posts promoted
- But: they were reposted *a lot*. Why?

Facebook is Great at Targeting

"With 210 million U.S. users logging in monthly, Facebook offers candidates and their allies the ability to zero in on potential voters who are likely to embrace their messages and make them go viral — identifying them by geography, gender, interests and their behavior across the Internet, including their 'likes' for music, food and travel. The company owes its rich trove of data to its users, who turn over details about their personal lives every time they engage with the platform."

(https://www.washingtonpost.com/politics/trump-campaigns-embrace-of-facebook-shows-companys-growing-reach-in-elections/2017/10/08/e5e5f156-a93b-11e7-b3aa-c0e2e1d41e38_story.html)

The Russians and Facebook

- The Russians used Facebook's targeting to reach people who would be likely to repost their stories
- "The news that Russians used Facebook to try to influence voters showed that people with 'no interest in adhering to facts or the truth are able to message to select pockets of the population to elicit an emotional response, and no one knows that it is happening,' said Keegan Goudiss, who served as director of digital advertising for Sen. Bernie Sanders's presidential campaign, which relied heavily on Facebook."

Twitter

- Twitter's targeting probably isn't as precise, but it can be easier for bots to make something go viral
- Create a hashtag; have other bots retweet it
  - Hope your followers do, too
- It doesn't take that many retweets, on an absolute basis, to make your hashtag show up as "trending"
- At that point, lots of other people will see it—and some will retweet

Fake News

- A variety of people around the world created fake “click bait” stories
  - "FBI Agent Suspected In Hillary Email Leaks Found Dead In Apparent Murder-Suicide”
  - “Hillary’s Illegal Email Just Killed Its First American Spy”
  - “Clinton Foundation ship caught smuggling refugees!"
- Why?

Some Stories on Fake News Sites

- https://www.npr.org/sections/alltechconsidered/2016/11/23/503146770/npr-finds-the-head-of-a-covert-fake-news-operation-in-the-suburbs
- https://www.wired.com/2017/02/veles-macedonia-fake-news/
- http://www.politifact.com/punditfact/article/2017/may/31/If-youre-fooled-by-fake-news-this-man-probably-wro/
- https://www.theguardian.com/technology/2016/aug/24/facebook-clickbait-political-news-sites-us-election-trump

Profit? Ideology?

- Some fake news purveyors were liberals trying to troll the right
  - "The website does make clear its true purpose, saying it 'is a satirical publication that uses the imagination of liberals to expose the extreme bigotry and hate and subsequent blind gullibility that festers in right-wing nutjobs.'" (Politifact)
- Others wanted money: "Coler fits into a pattern of other faux news sites that make good money, especially by targeting Trump supporters." (NPR)
- But why did it work?

"We Have Met the Enemy and He is Us"

"A New York Times examination of hundreds of those posts shows that one of the most powerful weapons that Russian agents used to reshape American politics was the anger, passion and misinformation that real Americans were broadcasting across social media platforms."

…

"'This is cultural hacking,' said Jonathan Albright, research director at Columbia University's Tow Center for Digital Journalism. 'They are using systems that were already set up by these platforms to increase engagement. They're feeding outrage — and it's easy to do, because outrage and emotion is how people share.'"

(New York Times)

Social Networks Are Amplifiers

- The Russians did not introduce new concepts into American political discourse
- Instead, they used American technology and American companies to exacerbate existing tensions
  - "'The Heart of Texas group had more success with a Houston rally to "Stop the Islamization of Texas,' which provoked an angry confrontation in May 2016. United Muslims of America, another Russian creation, called its own rally to 'Save Islamic Knowledge' for the same time and place, outside the Islamic Da'wah Center." (NYT)

Propaganda 2.0

- The Russian bots took advantage of the common features of the modern Internet
  - Speed of communication of communication
  - Disintermediation
  - Big data
- Their messages spread rapidly, without filtering by gatekeepers, and reached a susceptible audience

And What Do We Do About It?

Two Approaches

- Change one or more of these attributes
  - Speed of communication of communication
  - Disintermediation
  - Big data
- Or try to reduce susceptibility

Is either approach feasible?

What We Can't Do

- We probably cannot slow down the spread of information
  - There are too many commercial reasons to improve transmission speeds
- We can't make big data go away
  - This is a technique that's been tried since 1960
  - Again, there is a powerful commercial push behind it
  - (And you can't put toothpaste back into the tube…)

Solving Disintermediation?

- There once were intermediaries in mass communication systems: editors. Can we bring them back?
- Can human editors cope with the volume of news?
- (Can web sites afford enough humans?)
- Will algorithmic filtering work?
  - What about adversarial machine learning?
- It seems likely that Facebook et al. will try to build suitable algorithms
  - But—they profit from viral content

Susceptibility

- Americans' susceptibility to this sort of propaganda is equal parts political division and and lack of awareness
- A Russian attempt to influence the French election failed:
  - The Macron campaign planted fake emails, which were included in the Russian "leaks"
  - The Russians were careless and left metadata traces
  - The media and the public were aware of the possibility; they weren't in denial (and there's no Fox News equivalent in France)

American Political Division

- Solving that is a question for the sociologists and political scientists
- The Russian bots keep trying to stir up trouble, e.g., around the Parkland shootings
- Again, though—the underlying division is homegrown
- *But our technology is making it worse*

Scaring Them Away

- Can we deter future attacks?
- Is there some form of retaliation or potential retaliation that will induce the Russians to stop?
- Or will such retaliation spiral out of control?

We've Created New Technology Without Understanding its Effects, and We Can't Control It