

## Election Interference Cards

### SOCIAL MEDIA

#### Card 1

Concern about Russian meddling in U.S. elections has prompted U.S. officials to investigate how Russia used social media to interfere in U.S. politics. Internet security experts claim Russian companies used internet robots, or “bots,” to act like humans when posting to social media platforms like Twitter and Facebook. Former FBI agent Clint Watts explains that bots “can create accounts that look like you and talk like you, which makes you more likely to believe it. The other thing is it can replicate a message so many times, the more times you see it the more likely you are to believe it. So it can actually create false worlds in the social media space.”

This card is based on information from:

Westervelt, Eric. “How Russia Weaponized Social Media With ‘Social Bots.’” National Public Radio, November 5, 2017.

### SOCIAL MEDIA

#### Card 2

In October 2017, the Senate Judiciary Committee on Crime and Terrorism called on executives from Twitter, Facebook, and Google to testify as part of an investigation into Russia’s actions in the 2016 U.S. election. Senator Lindsey Graham, Republican from South Carolina, noted, “Technologies can be used to undermine our democracy and put our nation at risk.... We’ve seen an example of this in 2016 to create chaos within our democracy. Information is power. Ideas are the essence of democracy. The exchange of ideas...is one of the things that we cherish the most. We have to be on guard as a nation [against] people who want to undermine our way of life using these platforms against us. And I think this is the national security challenge of the 21st century.”

This card is based on information from:

“Russia and Social Media Hearing.” C-SPAN, October 31, 2017.

### SOCIAL MEDIA

#### Card 3

Before Facebook executives testified before the Senate Judiciary Committee, the company acknowledged that between 2015 and 2017 Russia’s Internet Research Agency created posts on Facebook. NBC reported that “by Facebook’s estimation, [these posts] reached potentially half of the 250 million Americans who are eligible to vote.... The shared content that Facebook estimates reached 126 million Americans was likely hard, if not impossible, for users of the social media platform to identify as originating from Russia.”

This card is based on information from:

Lee, Carol E., and Jo Ling Kent. “Facebook: Russian-backed Election Content Reached 126 Million Americans.” NBC News, October 30, 2017.

O’Reilly, Andrew. “Russian Trolls and Bots Disrupting US Democracy via Facebook and Twitter.” Fox News, October 31, 2017.

### SOCIAL MEDIA

#### Card 4

Russian content posted to social media sites often included fake news stories, such as a story about an ISIS attack on a chemical plant in Louisiana (which never happened). Posted content sometimes supported both conservative and liberal views. So what did the Russians hope to accomplish? Some analysts argue that the Russians’ goal may have been to sow divisions among people in the United States and cast doubt about the United States’ democratic system of government.

This card is based on information from:

Lapowsky, Issie. “Eight Revealing Moments From the Second Day of Russia Hearings.” *Wired*, November 2, 2017.

“Dark Web: How Russian Trolls Spread Fake News.” *The Week*, November 6, 2017.

Name: \_\_\_\_\_

### **SOCIAL MEDIA Card 5**

A February 2018 U.S. Justice Department press release announced that a grand jury in the District of Columbia charged “thirteen Russian nationals and three Russian companies for committing federal crimes while seeking to interfere in the United States political system, including the 2016 Presidential election. The defendants allegedly conducted what they [the grand jury] called ‘information warfare against the United States,’ with the stated goal of ‘spread[ing] distrust towards the candidates and the political system in general.’” In referring to the criminal charges, Deputy Attorney General Rod J. Rosenstein said, “The indictment alleges that the Russian conspirators want to promote discord in the United States and undermine public confidence in democracy. We must not allow them to succeed.”

This card is based on information from:

The United States Department of Justice Office of Public Affairs. “Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System.” February 16, 2018.

### **SOCIAL MEDIA Card 6**

A portion of a February 2018 U.S. Justice Department press release: “To hide the Russian origin of their activities, the defendants allegedly purchased space on computer servers located within the United States to set up a virtual private network. The defendants used that infrastructure to establish hundreds of accounts on social media networks such as Facebook, Instagram, and Twitter, making it appear that the accounts were controlled by persons within the United States. They used stolen or fictitious American identities, fraudulent bank accounts, and false identification documents. The defendants posed as politically and socially active Americans, advocating for and against particular political candidates. They established social media pages and groups to communicate with unwitting Americans. They also purchased political advertisements on social media.”

This card is based on information from:

The United States Department of Justice Office of Public Affairs. “Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System.” February 16, 2018.

Name: \_\_\_\_\_

## INTERNATIONAL EVENTS Card 1

According to a Reuters news report on a statement by Germany's domestic intelligence agency, "Russian intelligence agencies were probably responsible for a massive cyber attack on Germany's lower house of parliament [in 2015] which forced its computer systems to be shut down for days." In a related story, the BBC reported that "Germany's domestic intelligence agency has accused Russia of being behind a series of cyber attacks on German state computer systems.... The attack on the German parliament sought to install software that would have given the attackers permanent access to computers used by staff and MPs [members of Parliament]. Other attacks involved gathering data about critical infrastructure such as power plants and other utilities, Mr. Maassen [head of Germany's intelligence agency] said."

This card is based on information from:

Barkin, Noah, and Sabine Siebold. "Germany Says Russia Probably behind Cyber Attack on Bundestag." Reuters, May 13, 2016.

"Russia 'was behind German Parliament Hack.'" BBC, May 13, 2016.

## INTERNATIONAL EVENTS

### Card 2

In the months leading up to Britain's 2016 referendum vote on leaving or remaining in the European Union (Brexit), reports suggest that Russians may have attempted to influence the vote. A Guardian newspaper report indicated that joint research by the University of California, Berkeley and Swansea University "reportedly identified 150,000 Twitter accounts with various Russian ties that disseminated messages about Brexit."

This card is based on information from:

Kirkpatrick, David. "Signs of Russian Meddling in Brexit Referendum." *The New York Times*, November 15, 2017.

Wintour, Patrick. "Russian Bid to Influence Brexit Vote Detailed in New US Senate Report." *The Guardian*, January 10, 2018.

## INTERNATIONAL EVENTS

### Card 3

In the Netherlands, the Dutch intelligence service indicated in its annual report that Russia tried to influence the March 2017 Dutch election by spreading fake news. The director of the Dutch agency told the media, "In its efforts to position itself as a superpower, Russia is not afraid of using Cold War methods to obtain political influence. Russia is using the freedom of open and democratic societies of the West [to do this]."

The Dutch use paper ballots to vote, but in 2017 they decided to count votes manually instead of electronically because of warnings from cybersecurity experts.

This card is based on information from:

Kroet, Cynthia. "Russia Spread Fake News during Dutch Election: Report." POLITICO, January 28, 2018.

Kroet, Cynthia. "Dutch Votes to Be Counted Manually over Hacking Fears." POLITICO, January 28, 2018

## INTERNATIONAL EVENTS

### Card 4

Only a few weeks before France's May 2017 presidential election, hackers leaked documents from candidate Emmanuel Macron's campaign online. Reuters news reported that some experts said the campaign was "targeted by a cyber espionage group linked...to the Russian military intelligence agency GRU."

In a hearing before the U.S. Senate's Armed Services Committee in May 2017, National Security Agency (NSA) Director Michael Rogers testified that he had warned French officials about Russian attempts to interfere in their elections, saying, "We're watching the Russians. We are seeing them penetrate some of your infrastructure."

This card is based on information from:

Auchard, Eric. "Macron Campaign Was Target of Cyber Attacks by Spy-linked Group." Reuters, April 24, 2017.

Groll, Elias. "NSA Director: Russia Hacked French 'Infrastructure' Ahead of Vote." Foreign Policy, May 9, 2017.

**U.S. ELECTIONS****Card 1**

When U.S. citizens vote in a federal election (such as for a member of Congress or the President), the election is administered by state governments as authorized by Article 1 of the Constitution. Voting procedures vary from state to state. In most states, each county or local jurisdiction makes its own decisions about which election equipment to use. While some states use paper ballots, others use touch-screen technology. Any attempt to interfere with an election would require targeting an individual county or state's election system.

This card is based on information from:

"Voting and Election History." USA.gov. January 2, 2018.

"Voting and Election Laws." USA.gov. January 19, 2018.

**U.S. ELECTIONS****Card 2**

In 2017, the U.S. Department of Homeland Security confirmed that it had evidence of attempts to interfere in election systems in twenty-one states during the 2016 elections. These included the states of Alabama, Alaska, Arizona, California, Colorado, Connecticut, Delaware, Florida, Illinois, Iowa, Maryland, Minnesota, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Texas, Virginia, Washington, and Wisconsin.

Federal authorities did not indicate which country might be attempting to hack into election infrastructure, but state elections officials have. According to the Associated Press, Wisconsin Election Commission reported that "the state's systems were targeted by 'Russian government cyber actors.'"

This card is based on information from:

Mulvihill, Geoff, and Jake Pearson. "Federal Government Notifies 21 States of Election Hacking." AP News, September 23, 2017.

**U.S. ELECTIONS****Card 3**

The Associated Press reported that federal officials said "the targets included voter registration systems but not vote tallying software.... Only Illinois reported that hackers had succeeded in breaching its voter systems. Other states said their cybersecurity efforts turned back efforts to get crucial information." There is no evidence that the attempted hacking affected the actual voting in any of the states or the outcome of the 2016 elections.

This card is based on information from:

Mulvihill, Geoff, and Jake Pearson. "Federal Government Notifies 21 States of Election Hacking." AP News, September 23, 2017.

**U.S. ELECTIONS****Card 4**

There can be an uneasy relationship between state officials and the federal government over election security. State officials want to preserve their constitutional right to administer elections. But the 2016 elections also made clear that states depend on intelligence from the federal government (through agencies like the FBI, CIA, and NSA) to know if their states are vulnerable to election interference from foreign countries.

This card is based on information from:

Parks, Miles. "Election Chiefs 'Straddle The Line Between Sounding The Alarm And Being Alarmist.'" National Public Radio, February 19, 2018.

Name: \_\_\_\_\_

## U.S. ELECTIONS

### Card 5

Looking ahead to the 2018 elections, federal and state elections officials are sharing information and coordinating efforts to ensure that the elections are free from election interference. In testimony before the Senate Intelligence Committee in February 2018, Director of National Intelligence Dan Coats said, “There should be no doubt that Russia perceived its past efforts as successful and views the 2018 midterm elections as a potential target for Russian influence operations.” He also warned that the Russian government would “use elections as opportunities to undermine democracy, sow discord and undermine our values.”

This card is based on information from:

Chalfant, Morgan. “Trump Intel Chief: ‘No Doubt’ Russia Sees 2018 Midterms as Potential Target.” *The Hill*, February 13, 2018.

## U.S. ELECTIONS

### Card 6

Many experts have weighed in on how we might improve election security. Lawrence Norden at the Democracy Program at New York University School of Law, believes “we need to replace outdated systems and upgrade security practices. That includes replacing paperless electronic voting machines so there is a voter-marked paper record of every vote, and conducting post-election audits to compare the paper records to software generated results. There are two bills in Congress...that have significant bipartisan support and would get states and localities money to help ensure this happens nationally. Unfortunately, neither has received a committee hearing or vote yet.”

This card is based on information from:

Stewart, Emily. “Russian Election Interference Is Far from Over. I Asked 9 Experts How to Stop It.” *Vox*, February 19, 2018.