

ISSUE BRIEF

Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents

SEPTEMBER 2018 LAURA GALANTE & SHAUN EE

FOREWORD

Of all the political ideas to defend themselves before the court of human history, few have proven as potent and as compelling as that of electoral democracy. Through the twentieth century, democracy has faced off many times against fascism, communism, and other ideologies, and proven itself time and again to have the stronger case. The central tenet of democracy—that people should be able to select for themselves the leaders who can best govern and meet their political needs—has ascended around the world, so much so that in many places it is difficult to remember that it was ever in doubt. Indeed, today’s authoritarians often go to great lengths to mimic the trappings of democracy, ceding the point that elections are the best means to deliver political legitimacy.

But in recent years, electoral democracy has once more come under challenge, threatening to undermine these hard-won social and political freedoms. Around the globe, tensions over the distribution of globalization’s boons have led to widespread discontent and a resurgence

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft’s legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

in populism, while revisionist governments—such as in the Kremlin—have demonstrated clear intent to manipulate these seismic political forces to discredit democracy in other countries. Among the foremost drivers of this challenge, however, has been the rise of new media and digital technologies, and their intersection with traditional political and social life. These technologies have at times demonstrated exhilarating promise, giving citizens new tools to organize and governments new tools to lead. But they have also created new vulnerabilities, both technological and societal, that malicious actors have proven able and willing to exploit, damaging public trust in democratic institutions, exploiting societal tensions, and eroding the foundation of our ruled based international system.

The magnitude and cross-cutting nature of this challenge means that no single actor can solve this problem alone. Any effective solution must draw together expertise from across all sectors, uniting technologists, policymakers, civil society, and corporate leaders alike. Coming from the Cyber Statecraft Initiative of the Atlantic Council's Scowcroft Center for Strategy and Security, this Issue Brief is one such attempt to do just that. In the spirit of our mission to build bridges between the technology and policy communities, the Council brought together a high-level group of experts and policymakers on the sidelines of the Munich Security Conference in February 2018.

Out of the many strands of that discussion, the Scowcroft Center's senior fellow Laura Galante then expertly wove together this Issue Brief. In January 2017, all seventeen United States intelligence agencies published a nearly unprecedented and unclassified assessment of Russian interference in the 2016 US presidential elections, which stated:

Moscow's influence campaign followed a messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by the Russian Government agencies, state-owned media, third party intermediaries, and paid social media users or “trolls.”

Cyber enabled influence operations encompass a range of activity that is separate, but mutually reinforcing, for instance hacking into an email account then releasing embarrassing or false information via social media content. This Issue Brief provides a lexicon and

tangible examples of cyber activity within a broader universe of election interference.

By providing a taxonomy of different forms and levels of state involvement in election interference, it gives a guide to the recent history of election influence and interference. From there, it posits what norms and tactics have emerged as commonalities in the behavior of nation-states, asking: How will the toolsets and norms we currently see in play shape nation-state use of technology in the future?

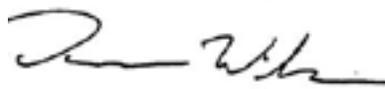
These may be titanic problems, but fortunately the Cyber Statecraft Initiative has not been alone in taking them on, and is working alongside a number of other centers throughout the Atlantic Council and beyond. Established in 1961 as part of a transatlantic effort to reinvigorate democracy and democratic values, the Council is uniquely positioned to tackle yet another set of challenges to democracy more than a half century later. Its Eurasia Center has called attention to Moscow's influence operations throughout Europe with its *Kremlin's Trojan Horses* reports, with two editions released in November 2016 and November 2017, and a forthcoming edition launching in November 2018. The Eurasia Center convened the Global Forum on Strategic Communications (StratCom) in September 2017 and October 2018, and launched DisinfoPortal.org, a one-stop interactive guide to the Kremlin's information war, bringing together thirty organizations and more than one hundred experts working to counter disinformation.

However, Russia is far from the only actor in this space, and the Digital Forensics Research Lab (DFRLab) has built a leading center of open source and digital forensic analysts, as well a global network of “digital sherlocks,” tracking events in governance, technology, security, and where each intersect as they occur. Over the past two years, the DFRLab has built capabilities to identify, expose, and explain disinformation where and when it occurs; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space. The DFRLab has focused on election integrity through a series of #ElectionWatch campaigns monitoring the spread of disinformation tactics and narratives around prominent global elections, partnering both with local actors and tech companies in countries as far-ranging

as Brazil, Colombia, France, Germany, Italy, Malaysia, and Mexico.

Ultimately, all these efforts—and more—will be needed to ensure that electoral democracy can stand up to the challenges of the twenty-first century. This Issue Brief is a part of that, aiming to continue the conversation around cyber enabled influence operations, not to be the final word on it. As technological progress continues apace, new developments that have little precedent in democracy's long history will continue to emerge. Whether those developments bolster democ-

racy—or whether they undermine it—will be decided by how well today's policymakers, technologists, and civil society cooperate to produce principles and standards that withstand the test of time.



Damon Wilson
Executive Vice President, Atlantic Council

INTRODUCTION

The past five years have demonstrated at least one thing about election interference: though it keeps happening, nobody can agree on just what it is. The 2016 US elections served as a flashpoint in recognizing modern election interference, but there have been numerous instances of interference in other European elections that can provide valuable lessons, and this report aims to connect them into a coherent and singular framework. While not meant to be exhaustive, this report assesses four elections and a referendum that have been characterized by attempted foreign interference.

The five case studies were selected because they illustrate a variety of actions associated with modern cyber and information operations from both a technical and psychological perspective. Each case study summarizes the openly available information about these incidents and identifies the state sponsorship and actions involved per the definitions developed for this report. The main objective in releasing this work is to classify the reported interference actions that took place and propose the norms of state behavior and response that have emerged in this realm.

These cases focus on suspected Russian government efforts, as the Russian government is widely acknowledged as the most active state in this domain. Numerous governments and independent security researchers have provided ample forensic, doctrinal, and circumstantial evidence that links interference actions to the Russian government, most prominently the Russian military's Main Intelligence Directorate (the *Glavnoje Razvedyvatel'noje Upravlenije*, or GRU). Nonetheless, this report makes an effort to identify specific sources and their basis for making claims of attribution to the Russian government.

Interference Terminology*

The following list of terms captures several of the actions commonly observed in modern cyber and information operations aimed at election interference as well as commonly documented levels of state involvement in those actions. Providing definitional clarity must be the key to wider public understanding and

* The definitions proposed in this publication reflect the views of the author for the purpose of this publication.

agreement on interference activities. A lack of specificity and consistency in terminology has contributed greatly to the confusion surrounding a number of the interference cases discussed in this report. If there is a single lesson from cyber activity over the last decade, it is that states must have a common lexicon in order to respond to cyber threats. It is not enough to simply speak of “hacking the vote.” Hopefully, by providing these initial terms, this report can spur a wider discussion on defining actions and sponsorship in this domain.

Interference Actions:

- **Infrastructure Exploitation:** An action—including reconnaissance and collection efforts—that gathers or distorts data or functionality of information technology (IT) systems or networks.
- **Vote Manipulation:** An action that alters vote tallies, vote input, vote transmission, or other modes of counting and transmitting the voters' true choices. This does not include actions intended simply to communicate a false result or otherwise cast doubt on the reliability of the vote.
- **Strategic Publication:** The public release of data that is obtained illicitly, typically through Infrastructure Exploitation, with the intent to embarrass, expose, or otherwise cast the subject in a negative light.
- **False-Front Engagement:** The fabrication of a false public identity by a person or group that subsequently takes actions to communicate, provoke, organize, or otherwise interact with others using the false identity.
- **Sentiment Amplification:** An action that increases the dissemination and prominence of a specific viewpoint. Sentiment Amplification can be conducted overtly, in which case the actor is clearly identifiable and there is no question of proper attribution. Covert Sentiment Amplification intentionally obscures the actor either by taking the form of False-Front Engagement or appearing to minimize the role of any actor behind the action.
- **Fabricated Content:** The propagation of written or broadcasted information that is false in nature or embellishes the truth. This may include actions that intentionally miscommunicate the number of votes

for a candidate or an election result, or other false and misleading statements.

State Involvement:

- **State-Directed:** An action that state officials, acting in their capacity as representatives of the government or government's leadership, have sanctioned and signaled their desire to achieve in some expressed manner.
- **State-Encouraged:** An action that state officials have not directly ordered or signaled, but one in which an individual or entity with good knowledge (usually ascertained from close contact with current or former state officials) of the state's objectives can partake with reasonable assurance that these efforts will be viewed favorably.
- **State-Aligned:** An action that individuals or entities conduct with the intention to support specific or general state objectives.

Key Actors:

- **Advanced Persistent Threat (APT) 28:** Also known as "Fancy Bear" or "Sofacy," APT28 is a Russian government-sponsored hacking group that has been implicated in multiple high-profile cyberattacks and intrusions since 2014—including the 2015 hack of the German *Bundestag* and the 2016 hack of US political organizations. Numerous government agencies including the US intelligence community and Department of Justice have stated that the group APT28 is part of the Russian military's main intelligence directorate, the GRU.¹

- **APT29:** Also known as "Cozy Bear" or "CozyDuke," APT29 is another Russian government-sponsored hacking group that, like APT28, has been implicated in several high-profile cyberattacks, including the 2016 intrusion into the networks of the US Democratic National Committee (DNC), the US Department of State, and the White House, and has been attributed to Russia's Federal Security Service (the *Federal'naya sluzhba bezopasnosti*, or FSB).²
- **Internet Research Agency (IRA):** Based in St. Petersburg, Russia, the IRA is an organization, often referred to as a "troll farm," that uses social media accounts to propagate frequently pro-Kremlin disinformation and amplify divisive political content. The IRA has been implicated in disinformation spread around the 2016 United Kingdom "Brexit" referendum as well as the 2016 US presidential election; notably, twelve of the thirteen Russians indicted during the Mueller investigation were employees of the IRA.³
- **CyberBerkut:** A "hacktivist" group with a pro-Russian government sentiment, active primarily in Ukraine, with the name "Berkut" referring to a professional police unit that was involved in the repression of protests during the 2014 Ukrainian Revolution. Though CyberBerkut postures as a domestic opposition group with roots in the local Ukrainian political environment, claiming to fight "neo-fascism" in Ukraine, multiple agencies including the US Defense Intelligence Agency have labeled it as a "false persona" and a "front organization for Russian state-sponsored cyber activity."⁴ Numerous security researchers, including Citizen Lab, have linked "CyberBerkut" to APT28 based on evidence such as similarities in shortcode and domain name formats.⁵

1 Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," Crowdstrike, June 15, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

2 Morgan Chalfant, "Russian hacker claims he can prove he hacked DNC," *Hill*, December 28, 2017, <http://thehill.com/policy/cybersecurity/366696-russian-hacker-claims-he-can-prove-he-hacked-dnc>.

3 Adrian Chen, "The Agency," *New York Times Magazine*, June 2, 2015, <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>; "Inside the Internet Research Agency's lie machine," *The Economist*, February 22, 2018, <https://www.economist.com/briefing/2018/02/22/inside-the-internet-research-agencys-lie-machine>; Brian Barrett, "For Russia, Unraveling US Democracy Was Just Another Day Job," *WIRED*, February 17, 2018, <https://www.wired.com/story/mueller-indictment-internet-research-agency/>.

4 John R. Haines, "Russia's Use of Disinformation in the Ukraine Conflict," Foreign Policy Research Institute, February 17, 2015, <https://www.fpri.org/article/2015/02/russias-use-of-disinformation-in-the-ukraine-conflict/>; *2017 Russia Military Power Report: Building a Military to Support Great Power Aspirations*, US Defense Intelligence Agency, <http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf>; "Hacktivist Group CyberBerkut Behind Attacks on German Official Websites," *Trend Micro*, January 20, 2015, <https://blog.trendmicro.com/trendlabs-security-intelligence/hacktivist-group-cyberberkut-behind-attacks-on-german-official-websites/>; Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution* (2017): 0022002717737138.

5 Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, *Tainted Leaks: Disinformation and Phishing with a Russian Nexus*, The Citizen Lab, May 25, 2017, <https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/>.

	Ukraine, 2014	United Kingdom (UK), 2016	United States, 2016	France, 2017	Germany, 2017
Level of State Involvement	State-Directed	State-Encouraged	State-Directed	State-Aligned	State-Directed
Infrastructure Exploitation	X	*	X	X	X
Vote Manipulation	X				
Strategic Publication			X	X	
False Front Engagement		X	X		
Sentiment Amplification		X	X	X	X
Fabricated Content	X	X	X		X

* General reporting suggests that there was infrastructure exploitation in this case, but there is not enough evidence to be certain at this point of time.

UKRAINIAN PRESIDENTIAL ELECTION: MAY 25, 2014

Type: State-Directed

Incident

In 2014, months after ousting President Viktor Yanukovich, Ukrainians headed to the polls to elect a new president. But days before the vote, the pro-Russian hacking group CyberBerkut destroyed key vote tallying system files and leaked private emails and administrator documentation from Ukraine's Central Election Commission (CEC). CEC restored the system from backups but faced another wave of attacks

around the election, which delayed the release of results and nearly led to an incorrect announcement that the ultra-nationalist Dmytro Yarosh—who had less than 1 percent of the vote—was the winner.⁶

Analysis

- **Vote Manipulation:** Four days before the election, CEC programs to monitor voter turnout and tally votes were shut down for twenty hours by the deletion of key files.⁷
- **Infrastructure Exploitation:** CyberBerkut penetrated CEC systems two months prior to the election and

6 Nikolay Koval, "Revolution Hacking," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO CCD COE Publications, 2015), accessed August 22, 2018, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf. Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *Christian Science Monitor*, June 17, 2014, <https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers>.

7 Nolan Peterson, "How Russia's Cyberattacks Have Affected Ukraine," *Daily Signal*, December 16, 2016, <https://www.dailysignal.com/2016/12/16/how-russias-cyberattacks-have-affected-ukraine/>. Katya Gorchinskaya, Olga Rudenko, and William Schreiber, "Authorities: Hackers Foiled in Bid to Rig Ukraine Presidential Election Results," *KyivPost*, May 25, 2014, <https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html>.

posted internal emails and administrator documentation from the CEC four days before the election.⁸

- **Fabricated Content:** The CEC website was compromised so that it would display far-right Dmytro Tarosh as the winner; experts identified and corrected this, but Russian media continued to report the incorrect winner.⁹

Outcome: Unambiguous victory for Petro Poroshenko, who avoided a run-off election by winning an absolute majority (54.70 percent), and announced that the maintenance of Ukrainian territorial integrity—under threat from Russia’s annexation of Crimea and separatism in Donbass—would be a key part of his presidential agenda. It is unclear whether the interference actions successfully cast doubt on the legitimacy of the election.

Response

Government: As the incidents occurred, Nikolay Koval, the head of Ukraine’s Computer Emergency Response Team, reported that the malware used to collect the CEC’s emails and administrator data had been used previously by APT28.¹⁰

Media: Widely reported in Ukrainian media at the time, very limited global media attention and no coverage in OSCE election report. The insistence of Russian media outlets such as Russian Channel One on reporting the false winner and the simultaneous military con-

flict further the case for viewing this as state-directed interference.¹¹

UK “BREXIT” REFERENDUM: JUNE 23, 2016

Type: State-Encouraged

Incident

In the run-up to the 2016 Brexit Referendum, Russian-language bots executed an extensive social media campaign on social media platforms like Twitter, posting and amplifying pro-Brexit rhetoric.¹² These Twitter accounts were later shown to be operated by the Russia-based IRA in an attempt to sway the referendum’s vote toward the Leave.EU camp.¹³ In addition to the IRA, other Russian actors, including Russia Today, spent over one thousand dollars on referendum advertisements.¹⁴ On June 23, 2016, as tens of millions of UK citizens turned out to vote in the Brexit Referendum, the British power supply was targeted by hackers.

Analysis

- **Infrastructure Exploitation:** Russia targeted the UK energy network on the day of the referendum.¹⁵ In addition, in 2017, the UK Parliament’s Public Administration and Constitutional Affairs Committee

8 Max Smolaks, “Pro-Russian Hackers Attack Central Election Commission of Ukraine,” *Silicon UK*, May 23, 2014, https://www.silicon.co.uk/workspace/cyberberkut-hackers-attack-central-election-commission-of-ukraine-146180?inf_by=5ada0bf0671db808238b4c3b.

9 “Russian TV Announces Right Sector Leader Led Ukraine Polls,” Radio Free Europe, May 26, 2014, <https://www.rferl.org/a/russian-tv-announces-right-sector-leader-yarosh-led-ukraine-polls/25398882.html>

10 Koval, “Revolution Hacking.”

11 NATO CCD COE, “*Cyber War in Perspective: Russian Aggression Against Ukraine*,” 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf.

12 David Kirkpatrick, “Signs of Russian Meddling in Brexit Referendum,” *New York Times*, November 15, 2017, <https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html>.

13 Karla Adam and William Booth, “Rising alarm in Britain over Russian meddling in Brexit vote,” *Washington Post*, November 17, 2017, https://www.washingtonpost.com/world/europe/rising-alarm-in-britain-over-russian-meddling-in-brexit-vote/2017/11/17/2e987a30-cb34-11e7-b506-8a10ed11ecf5_story.html?utm_term=.05540c3f9028; Robert Booth, Matthew Weaver, Alex Hern, Stacey Smith and Shaun Walker, “Russia used hundreds of fake accounts to tweet about Brexit, data shows,” *Guardian*, November 14, 2017, <https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets>.

14 Matt Burgess, “Where the UK’s investigations into Russia’s Brexit meddling stand,” *WIRED*, January 30, 2018, <https://www.wired.co.uk/article/russia-brexit-influence-uk-twitter-facebook-google>; Booth, et al., “Russia used hundreds.”

15 “UK cyber-defence chief accuses Russia of hack attacks,” BBC, November 15, 2017, <https://www.bbc.com/news/technology-41997262>.”

(PACAC) reported that the British referendum website where citizens registered to vote may have been hacked.¹⁶

- **False Front Engagement:** Russian-managed Twitter bots were mobilized around the Brexit vote, although their impact appears to have been limited.¹⁷
- **Sentiment Amplification:** In the months preceding the Brexit referendum, hundreds of thousands of Russian-language Twitter accounts posted and amplified pro-Brexit messages.¹⁸
- **Fabricated Content:** Over four hundred accounts, run by the Russia-based IRA, were used to circulate disinformation during the run-up to the referendum.¹⁹

Outcome: The Leave campaign narrowly beat the Remain campaign with 51.89 percent of the referendum vote.²⁰

Response

Government: The head of the UK Government Communications Headquarters' (GCHQ) National Cyber Security Centre has publicly stated that Russian hackers targeted the UK's power supply on the day of the referendum.²¹ Conversely, there remains insufficient publicly available evidence to confirm whether the British referendum website was hacked and, if so, whether a nation-state was behind the operation.²² UK governmental agency investigations continue to probe

into the extent of Russia's role in fake news, misinformation, social media manipulation, and the Leave.EU campaign ties to Russia.²³ In 2017, UK Prime Minister Theresa May issued a stern public warning on Russian attempts to sow discord by using fake news stories published by Russian government media.²⁴

Media: British and American media have both covered Russian efforts to influence the Brexit vote more widely as new evidence of Russian social media manipulation and potential coordination between Leave.EU officials and Russian government officials have emerged. Global media coverage continues after details have emerged of Cambridge Analytica and Facebook's involvement in targeting UK voters and local media exposure of potential UK and Russian officials' ties.²⁵

US PRESIDENTIAL ELECTIONS: NOVEMBER 8, 2016

Type: State-Directed

Incident

In the run-up to the 2016 US presidential elections, Russian agents engaged in a multipronged influence campaign intended to "undermine public faith in the US democratic process, denigrate [Democratic candidate

16 "Brexit referendum website might have been hacked: UK lawmakers," *Reuters*, April 12, 2017, <https://uk.reuters.com/article/us-britain-eu-website/brexit-referendum-website-might-have-been-hacked-uk-lawmakers-idUKKBN17E0NS>; Ellie Burns, "Did hackers fix the Brexit vote with DDoS?" *Computer Business Review*, April 12, 2017, <https://www.cbronline.com/breaches/hackers-fix-brexit-vote-ddos/>.

17 Matt Burgess, "Twitter has admitted Russian trolls targeted the Brexit vote (a little bit)," *WIRED*, February 8, 2018, <https://www.wired.co.uk/article/twitter-russia-brexit-fake-news-facebook-russia>; Phillip N. Howard and Bence Kollyani, "Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum," Working Paper 2016.1, Oxford, UK: Project on Computational Propaganda.

18 David Kirkpatrick, "Signs of Russian Meddling in Brexit Referendum," *New York Times*, November 15, 2017, <https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html>.

19 Booth, et al., "Russia used hundreds."

20 "EU Referendum Results," The Electoral Commission, accessed August 13, 2018, <https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information>.

21 "UK cyber-defence chief accuses Russia of hack attacks."

22 "Brexit referendum website."

23 Nina dos Santos, "UK investigates alleged Russian links to Brexit campaign," *CNN*, July 4, 2018, <https://www.cnn.com/2018/07/04/uk/uk-brexit-russia-links-arron-banks-intl/index.html>.

24 Adam and Booth, "Rising alarm in Britain over Russian meddling in Brexit vote."

25 Adam Satariano and Sheera Frenkel, "Facebook Fined in UK Over Cambridge Analytica Leak," *New York Times*, July 10, 2018, <https://www.nytimes.com/2018/07/10/technology/facebook-fined-cambridge-analytica-britain.html>; Carole Cadwalladr, "Reporter Shows The Links Between The Men Behind Brexit And The Trump Campaign," Interview by Terry Gross, *Fresh Air*, NPR, July 19, 2018, audio, 37:04, <https://www.npr.org/templates/transcript/transcript.php?storyId=630443485>.

Hillary Clinton], and harm her electability and potential presidency.”²⁶ One aspect of this campaign began as early as 2014, and aimed to delegitimize the US political process by amplifying politically polarized views through social media accounts—often under false personas—managed by the Russia-based IRA.²⁷ Another aspect involved the compromise of US political organizations, most notably the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC), and subsequent leaking of emails and documents to damage Hillary Clinton’s candidacy.

Analysis

- **Infrastructure Exploitation:** Russian hacker groups APT29 (Cozy Bear) and APT28 (Fancy Bear) penetrated the DNC’s networks, apparently separately.²⁸ APT28 also gained access to the DCCC’s networks.²⁹ In addition, Russian actors targeted twenty-one US state or local electoral boards.³⁰
- **Strategic Publication:** Under the persona of “Guccifer 2.0” and using the platforms of DCLeaks.com and WikiLeaks, the GRU leaked documents obtained through their Infrastructure Exploitation campaigns.³¹ This was done serially at strategic points in

time during the campaign in order to damage Hillary Clinton’s candidacy.³²

- **False-Front Engagement:** The IRA created hundreds of social media accounts to impersonate Americans and propagate political beliefs on opposing ends of the political spectrum, going as far as to organize rallies and protests through these accounts.³³
- **Sentiment Amplification:** The advertisements and social media posts made by the IRA were used to exploit divisive political issues, such as racial tensions, that would undermine the Clinton campaign and increase political polarization.³⁴
- **Fabricated Content:** Posts made by IRA-managed social media accounts made factually incorrect claims, such as Hillary Clinton’s adviser blaming her for the loss of US lives in Benghazi and Google having a bias in its search engine favoring Hillary Clinton.³⁵

Outcome: Victory for Donald Trump over Hillary Clinton, although there currently remains no evidence that there was direct Vote Manipulation. However, Russian activities further exacerbated social and politi-

26 *Background to “Assessing Russian Activities and Intentions in Recent US Elections”:* The Analytic Process and Cyber Incident Attribution, Office of the Director of National Intelligence, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

27 Scott Shane and Mark Mazzetti, “Inside a 3-Year Russian Campaign to Influence US Voters,” *New York Times*, February 16, 2018, <https://www.nytimes.com/2018/02/16/us/politics/russia-mueller-election.html>.

28 Alperovitch, “Bears in the Midst.”

29 Eric Lichtblau, “Computer Systems Used by Clinton Campaign Are Said to Be Hacked, Apparently by Russians,” *New York Times*, July 29, 2016, <https://www.nytimes.com/2016/07/30/us/politics/clinton-campaign-hacked-russians.html?mabReward=A6>.

30 Callum Borchers, “What we know about the 21 states targeted by Russian hackers,” *Washington Post*, September 23, 2017, https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.2ba17a84ea61.

31 Eric Lipton, David E. Sanger, Scott Shane, “The Perfect Weapon: How Russian Cyberpower Invaded the US,” *New York Times*, December 13, 2016, <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html>.

32 Sean Gallagher, “DNC ‘lone hacker’ Guccifer 2.0 pegged as Russian spy after opsec fail,” *Ars Technica*, March 23, 2018, <https://arstechnica.com/tech-policy/2018/03/dnc-lone-hacker-guccifer-2-0-pegged-as-russian-spy-after-opsec-fail/>; Lily Hay Newman, “Yes, Even Elite Hackers Make Dumb Mistakes,” *WIRED*, March 25, 2018, <https://www.wired.com/story/guccifer-elite-hackers-mistakes/>.

33 Alicia Parlapano and Jasmine C. Lee, “The Propaganda Tools Used by Russians to Influence the 2016 Election,” *New York Times*, February 16, 2018, <https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html>. United States v. Viktor Borisovich Netyksho, et al., Case # 1:18-cr-00215-ABJ-1 (US District Court for the District of Columbia, July 13, 2018), <https://www.justice.gov/file/1080281/download>; “Complimentary Intel Report: Russia’s APT28 Strategically Evolves its Cyber Operations,” *FireEye*, accessed August 17, 2018, https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html?utm_source=google&utm_medium=cpc&utm_content=paid-search&gclid=EAlaIqobChM1xMuZ9aD03A1VA2x-Ch2_Rg_8EAYASAAEgIlyfD_BwE&gclid=aw.ds; “Who is Fancy Bear,” *CrowdStrike*, September 12, 2016, <https://www.crowdstrike.com/blog/who-is-fancy-bear/>.

34 Nick Penzenstadler, Brad Heath, and Jessica Guynn, “We read every one of the 3,517 Facebook ads bought by Russians. Here’s what we found,” *USA Today*, May 11, 2018, <https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/>.

35 Ben Nimmo, “#ElectionWatch: Beyond Russian Impact,” *Digital Forensics Research Lab*, February 27, 2018, <https://medium.com/dfrlab/electionwatch-beyond-russian-impact-2f5777677cc0>.

cal divisions within the country and undermined public faith in the US democratic process as a whole.

Response

Government: Prior to the election, US security firms, like CrowdStrike, were able to attribute the DNC hack to Russia.³⁶ US government and intelligence agencies, including the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the US Department of Homeland Security (DHS), followed this with an October 2016 joint statement assessing with high confidence that the Russian government-directed GRU was behind the DNC hack.³⁷ In January 2017, the US intelligence community issued a joint report, attributing Russian efforts to undermine the 2016 presidential elections, although the report “did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election.”³⁸ In the summer of 2018, special counsel Robert Mueller indicted 12 GRU officers for hacking the networks of DCCC and DNC, as well as releasing documents and emails in an effort to interfere with the presidential election.³⁹

Media: Initial media coverage focused predominantly on the content and sentiment of emails leaked following the DNC hack, particularly on the DNC’s preference for Hillary Clinton over her rival in the Democratic primary, Bernie Sanders.⁴⁰ As the election neared, the conversation was increasingly framed as a national security issue, but media responses varied depending on political leaning. Right-leaning media tended to deny or question the effects of the hack, while left-leaning media asserted it was an attack on democracy and US institutions.

FRENCH PRESIDENTIAL ELECTION: MAY 7, 2017

Type: State-Aligned

Incident

On May 5, two days before the French presidential election, nine gigabytes of data from Emmanuel Macron’s campaign, including documents and emails, was posted online on a document sharing website called Pastebin, and was further disseminated on 4Chan. The data was reportedly obtained by with spear-phishing methods and there are conflicting reports as to whether the documents contained fake information or not.⁴¹

Analysis

- **Infrastructure Exploitation:** Actors gained access to documents and emails of the Macron campaign through a spear-phishing operation.
- **Strategic Publication:** Documents obtained through the spear-phishing operation were released during the no-campaigning period immediately before the French presidential election, making it difficult for the Macron campaign to counter information released during the leak.
- **Sentiment Amplification:** Use of bots to amplify the messaging and rhetoric around the Macron leak, with just 5 percent of accounts promoting the hashtag #MacronGate accounting for nearly half of all the posts.⁴²

Outcome: Despite the leaking of campaign emails and the use of bots to promote anti-Macron rhetoric on so-

36 Alperovitch, “Bears in the Midst.”

37 “Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity,” Office of the Director of National Intelligence, accessed August 13, 2018, <https://www.dni.gov/index.php/nctc-who-we-are/organization/308-about/organization/information-sharing-environment/news/2108-joint-dhs-odni-fbi-statement-on-russian-malicious-cyber-activity>.

38 Background to “Assessing Russian Activities and Intentions in Recent US Elections,” Office of the Director of National Intelligence.

39 “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,” Department of Justice, July 13, 2018, <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>.

40 Ella Nilson, “The Mueller indictments reveal the timing of the DNC leak was intentional,” Vox, July 13, 2018, <https://www.vox.com/2018/7/13/17569030/mueller-indictments-russia-hackers-bernie-sanders-hillary-clinton-democratic-national-convention>.

41 April Glasser, “Macron’s French presidential campaign has been hacked less than 48 hours before the election,” Recode, May 6, 2017, <https://www.recode.net/2017/5/6/15567868/macron-hack-french-presidential-campaign>.

42 Mark Scott, “US Far-Right Activists Promote Hacking Attack Against Macron,” *New York Times*, May 6, 2017, <https://www.nytimes.com/2017/05/06/world/europe/emmanuel-macron-hack-french-election-marine-le-pen.html>.

cial media, Emmanuel Macron won over Marine Le Pen with 66.1 percent of the vote.

Response

Government: Initially, the hack was attributed to Russian actors and APT28 by various sources, including US CYBERCOM Commander Mike Rogers and two other US cybersecurity firms.⁴³ However, one month following the election, Guillaume Poupard, head of the French National Agency for the Security of Information Systems (the *Agence Nationale de la Sécurité des Systèmes d'Information*, or ANSSI), declared no conclusive evidence pointed to Russian groups had been found, and that simplicity of attacks pointed toward an actor with lower capabilities.⁴⁴

Media: Coverage of the hack in the run-up to the election was limited by several factors. The French Electoral Commission published an official statement one day before the election that the dissemination of fraudulently obtained data is liable to be classified as a criminal offense.⁴⁵ According to French law, a national ban on electioneering enters into effect forty-eight hours before an election, prohibiting media and the candidates from carrying or publishing election-related activities.⁴⁶ While it is challenging to gauge the exact impact, this clearly affected coverage of the Macron campaign leaks in traditional media outlets. Finally, the

lesson learned as a result of the Russian interference in the US election plausibly played a role in the mental preparation for destabilizing interventions as well as the balanced French response to the hack.⁴⁷

GERMAN FEDERAL ELECTIONS: SEPTEMBER 24, 2017

Type: State-Directed

Incident

In 2015, data was stolen (primarily emails) from multiple German political sources, including the Bundestag (the lower house of parliament) and the state offices of Chancellor Angela Merkel's Christian Democratic Union of Germany (the *Christlich Demokratische Union Deutschlands*, or CDU) party during a prolonged weeks-long cyberattack.⁴⁸ However, this data was ultimately not released. In addition to the data theft, German-language Russian media also produced fake stories and magnified issues, such as immigration, to stoke domestic tension as early as in 2016.⁴⁹ This was a social media campaign similar to that used in the US 2016 elections,

-
- 43 Andy Greenberg, "The NSA Confirms it: Russia Hacked French Election 'Infrastructure,'" *WIRED*, May 9, 2017, <https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/>; Alex Hern, "Macron hackers linked to Russian-affiliated group behind US attack," *The Guardian*, May 8, 2017, <https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack>.
- 44 "The Latest: France says no trace of Russian hacking Macron," Associated Press, June 1, 2017, <https://www.apnews.com/fc570e4b400f4c7db3b0d739e9dc5d4d>.
- 45 Jon Rogers, "French election: Publishing Macron emails could be a crime, says electoral commission," *Express*, May 6, 2017, <https://www.express.co.uk/news/world/801242/French-election-Macron-emails-crime-electoral-commission-Le-Pen>; Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle (@cnccep), "Communiqué : Suites de l'attaque informatique qu'a subie l'équipe de campagne de M. Macron," Twitter, May 6, 2017, <https://twitter.com/cnccep/status/860777820737470464>.
- 46 Marie-Laure Denis, "La régulation audiovisuelle et l'élection présidentielle," *Les Nouveaux Cahiers du Conseil constitutionnel* n°34 (January 2012), <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-regulation-audiovisuelle-et-l-election-presidentielle>.
- 47 Rachel Donadio, "Why the Macron Hacking Attack Landed With a Thud in France," *New York Times*, May 8, 2017, <https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html>; also, evidence of preparation for such an event – Laura Daniels, "How Russia hacked the French election," Politico, April 23, 2017, <https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/>.
- 48 Scott Neuman, "Russia's 'Fancy Bear' Reportedly Hacks German Government Network," NPR, March 1, 2018, <https://www.npr.org/sections/thetwo-way/2018/03/01/589787931/russias-fancy-bear-reportedly-hacks-german-government-networks>; Fabian Reinbold, "Is Moscow Planning Something? Germany Prepares for Possible Russian Election Meddling," *Der Spiegel*, September 7, 2017, <http://www.spiegel.de/international/germany/how-germany-is-preparing-for-russian-election-meddling-a-1166461.html>.
- 49 Rick Noack, "Everything we know so far about Russian election meddling in Europe," *Washington Post*, January 10, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/01/10/everything-we-know-so-far-about-russian-election-meddling-in-europe/?utm_term=.b931b16e2a63; Mark Scott, "Ahead of election, Germany seeks fake news antidote," Politico, August 31, 2017, <https://www.politico.eu/article/germany-election-campaign-fake-news-angela-merkel-trump-digital-misinformation/>; Constanze Stelzenmüller, "The impact of Russian interference on Germany's elections," Brookings Institution, June 28, 2017, <https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/>.

with bots, divisive rhetoric, warnings of electoral fraud, and “vote-rigging” claims toward the end of the vote.⁵⁰

Analysis

- **Infrastructure Exploitation:** In 2015, a group of hackers—likely APT28—gained administrator access to the Bundestag network and copied sixteen gigabytes of emails from lawmakers and their staff, although these were never released.⁵¹
- **Sentiment Amplification:** German-language Russian media focused on issues such as immigration that were politically polarizing. One group of university researchers noted social media accounts amplifying right-wing rhetoric and Russian media stories, but attributed this to the US “alt-right” rather than Russia.⁵²
- **Fabricated Content:** Both German-language Russian media and the right-wing Alternative for Germany (the *Alternative für Deutschland*, or AfD) party shared fabricated information, most famously the “Our Lisa” story which claimed that a young Russian-German woman had been raped by “Arab” migrants.⁵³

Outcome: Merkel’s party alliance between the CDU and Christian Social Union in Bavaria (the *Christlich-Soziale Union in Bayern*, or CSU) won 30 percent of the vote but achieved the worst result since 1940; the far-right, anti-immigration party, AfD, made gains and came in third place with 13.5 percent of the vote. Five months after the election, an agreement was reached with the Social Democratic Party of Germany (the *Sozialdemokratische Partei Deutschlands*, or SPD) for a governing coalition.

Response

Government: German officials blamed APT28 (Fancy Bear) for the 2015 hack of the Bundestag and other cyberattacks aimed at Chancellor Angela Merkel.⁵⁴ In May of 2016, Germany’s domestic intelligence agency, the Federal Office for the Protection of the Constitution (the *Bundesamt für Verfassungsschutz*, or BfV), stated that Russia was behind the 2015 hack of Bundestag and Merkel’s CDU.⁵⁵ The vice chairman of Merkel’s political party publicly announced that prior to the election debate, her website had been targeted by thousands of cyberattacks, many from Russian IP addresses.⁵⁶

Media: Lessons learned from both US and French presidential elections, combined with robust German institutions and less political polarization than in other countries, may have reduced the impact of misinformation. The major campaigns entered into a “gentlemen’s agreement” to avoid using data stolen during the 2015 cyberattacks should it emerge (which it ultimately did not).⁵⁷ However, both government and media extensively focused on the possibility of Russian interference during the election, sensitizing both politicians and citizens to that possibility.⁵⁸

NEW NORMS

As with any new weapon set or domain, establishing norms of state behavior has been the focus of diplo-

50 Maks Czuperski and Ben Nimmo, “#ElectionWatch: Final Hours Fake News Hype in Germany,” Digital Forensic Research Lab, September 23, 2017, <https://medium.com/dfrlab/electionwatch-final-hours-fake-news-hype-in-germany-cc9b8157cfb8>. “#ElectionWatch: Disinformation in Deutschland,” Digital Forensic Research Lab, September 27, 2017, <https://medium.com/dfrlab/electionwatch-disinformation-in-deutschland-a97b61d7b025>.

51 Patrick Beauth, Kai Biermann, Martin Klingst, and Holger Stark, “Merkel and the Fancy Bear,” *Die Zeit*, May 12, 2017, <https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/komplettansicht>.

52 Kim Hjelmggaard, “There is meddling in Germany’s election - not by Russia, but by the US right wing,” USA Today, September 20, 2017, <https://www.usatoday.com/story/news/world/2017/09/20/meddling-germany-election-not-russia-but-u-s-right-wing/676142001/>.

53 Czuperski and Nimmo, “#ElectionWatch: Germany’s AfD Utilizes Fake Imagery Ahead of Election.”

54 Neuman, “Russia’s ‘Fancy Bear’ Reportedly Hacks German Government Network.”

55 “Russia ‘was behind German parliament hack,’” BBC News, May 13, 2016, <https://www.bbc.com/news/technology-36284447>; Reinbold, “Is Moscow Planning Something?”

56 “Merkel ally cites thousands of cyber attacks from Russian IP addresses,” Reuters, September 4, 2017, <https://www.reuters.com/article/us-germany-election-cyber/merkel-ally-cites-thousands-of-cyber-attacks-from-russian-ip-addresses-idUSKCN1BF1FA>.

57 Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, May 23, 2018, <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435>.

58 Scott, “Germany seeks fake news antidote.”

mats and military strategists. Cyberspace and the actions taken within it have been particularly challenging to define, let alone develop a semblance of standards and acceptable actions.

Early on, the issue of attribution—or rather, the difficulty of attributing actions in cyberspace—was the preeminent obstacle for devising credible response frameworks. Over time, the public and private sectors' ability to identify, analyze, and present findings attributing cyber activity to specific actors improved dramatically. While attributing activity in cyberspace will always be a challenge, governments have become increasingly public in attributing malicious cyber activity. These public attribution statements and their counteractions serve as strong indicators of the norms that have been emerging in this area over the last several years.

Thus far, perhaps the norm most clearly established and most widely recognized is a prohibition on hacking intellectual property theft from private-sector networks. This norm has been established through: exposing the most active state actor, in this case China's People's Liberation Army (PLA); judicial actions like the 2014 US Department of Justice indictment of five PLA officers; consistent denunciation of this specific cyber-enabled activity by multiple heads of state, and eventually tariffs on goods benefiting from hacked intellectual property. From this, it has now become clear to a range of state and non-state actors that hacking intellectual property from private (nongovernment) targets will result in widespread condemnation and leads to the imposition of significant political and economic costs.

In contrast, election interference and information operations more broadly have presented a complicated set of political and definitional dimensions for effective norm-setting. In part, this difficulty arises from the two major differing perspectives states have taken as they define cyberspace. This philosophical divide hinges on whether a nation-state includes (in action and in word) information, and the effect that information can have via its disbursement through the Internet, in that nation-state's own sovereign purview and field of action.

Historically, states that take this expansive view of the domain, like Russia and China, have been more in-

clined to classify a wider set of actions as interference rather than milder attempts at influence. For example, the Kremlin has frequently interpreted US government statements as interference actions. One of the most notable examples was Secretary Clinton's speech regarding the large anti-government demonstrations, which had been set off by the 2011 Russian parliamentary elections. Secretary Clinton stated that "The Russian people, like people everywhere, deserve the right to have their voices heard and their votes counted... and that means they deserve free, fair, transparent elections and leaders who are accountable to them."

While the statement was uncontroversial to US and other democratically inclined audiences, then-Prime Minister Putin viewed the statement as a trigger to hostile action, saying: "She set the tone for certain actors inside the country; she gave the signal. They heard this signal and, with the support of the US State Department, started actively doing their work."⁵⁹ The norms below take this informational threat calculus into account simply because states like Russia are formulating their actions and responses in this way.

The following norm statements are an attempt to capture how the case studies presented here have shaped interpretations of permissible state action, response thresholds, and the calculus that actors are now considering before taking action in this realm:

1. If the state's representatives direct or encourage Infrastructure Exploitation or Vote Manipulation against a foreign state, the targeted state will consider this a breach of sovereignty and a hostile act.
2. If the state's representatives engage in overt Sentiment Amplification, Strategic Publication, or Content Fabrication, the targeted state or faction will not take meaningful retaliatory action unless they consider these actions as a direct call to Infrastructure Exploitation or Vote Manipulation—a consideration more likely to occur if the state views the informational domain as sovereign.
3. If a state defines their sovereignty to include the informational domain (e.g., a psychological domain beyond the physically defined boundaries of the

59 Simon Shuster, "All the Wrong Moves: Putin Plots His Strategy Against the Protesters," *TIME*, December 9, 2011, <http://content.time.com/time/world/article/0,8599,2101924,00.html>.

land, sea, air, or physical technological infrastructure of the internet), it is more likely to consider overt Sentiment Amplification and Strategic Publication as a hostile act and respond accordingly.

4. If the state's representatives direct or encourage False Front Engagement, covert Sentiment Amplification, or covert Strategic Publication, the targeted state will view these actions as hostile. Whether the targeted state views these acts as a breach of sovereignty or simply as an attempt at influence will dictate the severity of the state's response.

CONCLUSION

While policymakers and national security officials formulate responses to election interference, Russian state-directed efforts have continued—particularly against US targets. In August 2018, Microsoft announced that its Digital Crimes Unit had found evidence of APT28's planning efforts to engage in Infrastructure Manipulation against several conservative think tanks and the US Senate.⁶⁰ Later that same week, security researchers at several technology and social media companies detailed a long-running covert Sentiment Amplification effort involving multiple False Fronts and sponsored by the Iranian state, that was intended to promote narratives favorable to the current Iranian

government.⁶¹ These efforts demonstrate states' continued interest in exploiting networks and influencing opinions far beyond their borders.

The Russian government's investment in influence and network exploitation operations, built on the back of a new and fragmented media environment, created a space for new forms and techniques in electoral interference. But states are not the only entities that have been watching this phase of election interference, and the techniques demonstrated by the Russian government are readily replicable with a high return on investment. The dividends from such interference are too great to ignore, posing a question: what will the next phase of election interference look like, and who will be involved?

The Italian elections of March 2018 may present an initial answer to that question. During the run-up to the elections, fabricated news spread from social media accounts of supporters of anti-establishment parties like the Five Star Movement (5SM) and Lega, with disinformation being propagated and amplified by partisan journalistic sources.⁶² Yet though the narratives perpetuated indirectly helped Russian strategic objectives, asserting a connection between 5SM/Lega and Russia is difficult, and has been a source of confusion.⁶³

This difficulty in attribution should underscore an underlying point: actors with little to no state direction can still wield formidable influence and execute network exploitation operations. It is not only the impact of these techniques that is the most troubling—it is also their ease of replication. The 2018 Italian elections could be a

60 Elizabeth Dwoskin and Craig Timberg, "Microsoft says it has found a Russian operation targeting US political institutions," *Washington Post*, August 21, 2018, https://www.washingtonpost.com/business/economy/microsoft-says-it-has-found-a-russian-operation-targeting-us-political-institutions/2018/08/20/52273e14-a4d2-11e8-97ce-cc9042272f07_story.html?utm_term=.9df9add0b378.

61 Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian influence operation globalizes tech's war on disinformation," *Washington Post*, August 21, 2018, https://www.washingtonpost.com/technology/2018/08/21/russian-iran-created-facebook-pages-groups-accounts-mislead-users-around-world-company-says/?utm_term=.ad95203e1982.

62 Paul Harrison, "Italy's vote: Fake claims attempt to influence election," BBC, March 3, 2018, <https://www.bbc.com/news/world-europe-43214136>. Alberto Nardelli and Craig Silverman, "One Of The Biggest Alternative Media Networks In Italy Is Spreading Anti-Immigrant News And Misinformation On Facebook," BuzzFeed, November 21, 2017, https://www.buzzfeed.com/albertonardelli/one-of-the-biggest-alternative-media-networks-in-italy-is?utm_term=.skw02RWI6L#.dc6Rw0kz3e.

63 Alberto Nardelli and Craig Silverman, "Italy's Most Popular Political Party Is Leading Europe In Fake News And Kremlin Propaganda," BuzzFeed, November 29, 2016, https://www.buzzfeed.com/albertonardelli/italys-most-popular-political-party-is-leading-europe-in-fak?utm_term=.osyY2y8DpM#.ioOmZBGxr3; Ben Nimmo and Anna Pellegatta, "#ElectionWatch: Italy's Self-Made Bots: How the Lega's followers automate themselves," Digital Forensic Research Lab, January 25, 2018, <https://medium.com/dfrlab/electionwatch-italys-self-made-bots-200e2e268d0e>; Alina Polyakova, Markos Kounalakis, Antonis Klapsis, Luigi Sergio Germani, Jacopo Iacoboni, Francisco de Borja Lasheras, and Nicolás de Pedro, "The Kremlin's Trojan Horses 2.0," Atlantic Council, November 15, 2017, <http://www.atlanticcouncil.org/publications/reports/the-kremlin-s-trojan-horses-2-0>.

harbinger for non-state-directed interference with major political consequences, achieved with limited technical difficulty, replicable tools, and low barriers of entry.

Recommendations

1. Governments, security researchers, and others privy to the evolving tactics and evidence of Interference Actions taken by states and non-state actors should continue to expose these actions. Exposure in this domain has shown to be the necessary predicate for understanding and countering malicious activity.
2. Journalists, analysts, and other parties responsible for characterizing Interference Actions and influence operations should take all reasonable efforts to accurately describe the particular action at hand.

Vague terminology, and in particular the muddling of Infrastructure Exploitation, Vote Manipulation, and Sentiment Amplification, has led to critical misunderstandings in the public sphere.

3. The United States, along with other nation-states that traditionally value freedom of speech, expression, and a critical media environment, should be wary of classifying influence operations and Sentiment Amplification efforts as breaches of state sovereignty. While the dark side of global interconnectivity is increasingly becoming clear outside of security circles, the temptation to deem all foreign influence and interference operations as existential threats and breaches of state sovereignty undermines the varied information environment that allows democracies to thrive.



Laura Galante: Recognized as a leading authority on cyber threats, information operations, and intelligence analysis, Laura Galante founded Galante Strategies in 2017 to equip governments and corporations to respond effectively to cyber and information threats. Her recent work has included developing a cybersecurity framework for the Ukrainian government; briefing advanced cyber threats to the Italian government and financial sector; and raising national awareness of cybersecurity in Kosovo and Serbia. Currently a senior fellow at the Atlantic Council's Cyber Statecraft Initiative, Laura previously served as the director of global intelligence at the cybersecurity company, FireEye Inc. (formerly Mandiant). She frequently serves as a keynote speaker, having testified before the UN Security Council and given a TED talk at TED2017. Laura holds a BA in foreign affairs and Italian from the University of Virginia and a JD from the Catholic University of America.

Shaun Ee is a program assistant with the Asia Security Initiative and Cyber Statecraft Initiative of the Atlantic Council. Before joining the Council, he graduated from Washington University in St. Louis with a BA in philosophy-neuroscience-psychology and international and area studies.

Acknowledgments:

Thank you to the Howard Baker Forum for providing generous support for this project, allowing the Cyber Statecraft Initiative to address an issue of vital importance. The Atlantic Council team, particularly Klara Jordan and Safa Shahwan, provided support and oversight to this project and Anca Agachi, Timothy McGiff, and Heather Regnault provided invaluable research support.

Atlantic Council Board of Directors

INTERIM CHAIRMAN

*James L. Jones

CHAIRMAN EMERITUS

Brent Scowcroft

PRESIDENT AND CEO

*Frederick Kempe

EXECUTIVE VICE CHAIRS

*Adrienne Arsht

*Stephen J. Hadley

VICE CHAIRS

*Robert J. Abernethy

*Richard W. Edelman

*C. Boyden Gray

*George Lund

*Virginia A. Mulberger

*W. DeVier Pierson

*John J. Studzinski

TREASURER

*Brian C. McK. Henderson

SECRETARY

*Walter B. Slocombe

DIRECTORS

Stéphane Abrial

Odeh Aburdene

*Peter Ackerman

Timothy D. Adams

Bertrand-Marc Allen

*Michael Andersson

David D. Aufhauser

Matthew C. Bernstein

*Rafic A. Bizri

Dennis C. Blair

Thomas L. Blair

Philip M. Breedlove

Reuben E. Brigety II

Myron Brilliant

*Esther Brimmer

Reza Bundy

R. Nicholas Burns

Richard R. Burt

Michael Calvey

James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

George Chopivsky

Wesley K. Clark

David W. Craig

Helima Croft

*Ralph D. Crosby, Jr.

Nelson W. Cunningham

Ivo H. Daalder

*Ankit N. Desai

*Paula J. Dobriansky

Christopher J. Dodd

Thomas J. Egan, Jr.

*Stuart E. Eizenstat

Thomas R. Eldridge

Julie Finley

*Alan H. Fleischmann

Jendayi E. Frazer

Ronald M. Freeman

Courtney Geduldig

*Robert S. Gelbard

Gianni Di Giovanni

Thomas H. Glocer

Murathan Günal

John B. Goodman

*Sherri W. Goodman

Amir A. Handjani

John D. Harris, II

Frank Haun

Michael V. Hayden

Annette Heuser

Amos Hochstein

Ed Holland

*Karl V. Hopkins

Robert D. Hormats

Mary L. Howell

Wolfgang F. Ischinger

Deborah Lee James

Reuben Jeffery, III

Joia M. Johnson

Stephen R. Kappes

*Maria Pica Karp

Andre Kelleners

Sean Kevelighan

*Zalmay M. Khalilzad

Henry A. Kissinger

C. Jeffrey Knittel

Franklin D. Kramer

Laura Lane

Richard L. Lawson

*Jan M. Lodal

Douglas Lute

*Jane Holl Lute

William J. Lynn

Wendy W. Makins

Zaza Mamulaishvili

Mian M. Mansha

Gerardo Mato

William E. Mayer

Timothy McBride

John M. McHugh

Eric D.K. Melby

Franklin C. Miller

Judith A. Miller

*Alexander V. Mirtchev

Susan Molinari

Michael J. Morell

Richard Morningstar

Edward J. Newberry

Thomas R. Nides

Franco Nuschese

Joseph S. Nye

Hilda Ochoa-Brillembourg

Ahmet M. Oren

Sally A. Painter

*Ana I. Palacio

Carlos Pascual

Alan Pellegrini

David H. Petraeus

Thomas R. Pickering

Daniel B. Poneman

Dina H. Powell

Arnold L. Punaro

Robert Rangel

Thomas J. Ridge

Michael J. Rogers

Charles O. Rossotti

Robert O. Rowland

Harry Sachinis

Rajiv Shah

Stephen Shapiro

Wendy Sherman

Kris Singh

James G. Stavridis

Richard J.A. Steele

Paula Stern

Robert J. Stevens

Robert L. Stout, Jr.

*Ellen O. Tauscher

Nathan D. Tibbits

Frances M. Townsend

Clyde C. Tuggle

Melanne Vermeer

Charles F. Wald

Michael F. Walsh

Maciej Witucki

Neal S. Wolin

Guang Yang

Mary C. Yates

Dov S. Zakheim

HONORARY DIRECTORS

David C. Acheson

James A. Baker, III

Harold Brown

Frank C. Carlucci, III

Ashton B. Carter

Robert M. Gates

Michael G. Mullen

Leon E. Panetta

William J. Perry

Colin L. Powell

Condoleezza Rice

George P. Shultz

Horst Teltschik

John W. Warner

William H. Webster

**Executive Committee
Members*

List as of August 27, 2018



The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2018 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org