Chapter 4

Gaming Communication on the Global Stage:

Social Media Disinformation in Crisis Situations

Mark Kumleben and Samuel C. Woolley

In December 2016, then Pakistani defense minister Khawaja Asif tweeted a none-too-subtle threat: "Israeli def min threatens nuclear retaliation presuming pak role in Syria against Daesh. Israel forgets Pakistan is a Nuclear state too."[1] In this tweet, Asif was reacting to a completely fictitious threat allegedly made by Israel's defense minister, published by fake news website AWD News, related to a purported Pakistani role in supporting the Islamic State (also known as Daesh or ISIS). The Israeli Defense Ministry denied the statement, also through Twitter, and the diplomatic issue was settled with nothing worse than embarrassment for Asif. Future such incidents of nuclear misinformation, however, may end with more than bruised egos.

In a geopolitical environment where military action is often taken to advance a strategic narrative rather than to seize physical resources, social media can become a critical source of narrative change and a unique type of open-source intelligence.[2] Strategic narratives are purposeful communications employed to persuade or influence target audiences to undertake action. Targets can include allies and partners and, in conflict situations, adversaries when deployed alongside other forms of power.[3] Computational propaganda, which involves the deliberate and frequently automated manipulation and distribution of misleading information over social media, threatens the integrity of that information space, both compromising leaders' ability to use social media for legitimate purposes and contaminating any intelligence gleaned from these platforms.[4] In a crisis scenario, speed and accuracy of information flow are key to mitigating damage. Generally, this includes the ability of decision makers to communicate with the public and to be aware of large-scale patterns of civilian activity. Currently, social media are an effective and inexpensive way to do this, but computational propaganda may turn these websites from assets into liabilities.

In this chapter we address the ways in which various tools and tactics, from automated bots imitating real people to state-sponsored trolling targeting activists and journalists, are being used to interrupt and confuse information flows during crises.[5] These mechanisms for manipulating political communication, and the cybertroops often behind them, have played a role in major elections and security crises in more than thirty countries to date.[6] In particular, we focus on how digital propaganda affects leaders' perceptions of current events and unpack the role of social media platforms as crucial communication devices in these cases. First we define computational propaganda and political bots and explain the ways in which they are generally leveraged for control and coercion in political communication. Then we discuss the role of social media in crisis communication. Finally we explore two case studies—a false alarm in Hawaii and advertisements targeted at political figures in the United Kingdom—in which computational propaganda and social media have played a role in pivotal crises.

Computational Propaganda, Political Bots, and Crisis Communication

Computational propaganda is a phenomenon unique to political communication in the digital age. It is best defined as the use of automation, algorithms, and big data over social media in attempts to manipulate public opinion.[7] Propaganda, what author Philip Taylor calls "munitions of the mind," is an effort to use psychology to affect human perception and behavior in a conflict.[8] What separates the emergent form of computational propaganda from former iterations is that it is most usually automated and anonymous. Examples include Russian-backed online campaigns to influence elections in France and Germany in 2017 via misinformation and disinformation. Whereas efforts to propagate biased or misleading information prior to widespread use of the internet were dependent upon traditional one-to-many media (television, newspapers, pamphlets, radio, etc.), computational propaganda relies upon social media platforms such as Facebook and Twitter. These sites host content from billions of users, a many-to-many communication model that can be as useful for sowing confusion and misleading information as for promoting democratic conversation. Computational propaganda makes use of ever-increasing computational power and advancements in artificial intelligence to massively amplify certain ideas, people, or institutions while suppressing information on others.[9] In addition to influencing public opinion through social media, computational propaganda manipulates perceptions of public opinion, misleading media outlets and decision makers alike. In the complex ecosystem of social media, this manipulation not only affects public opinion directly—it also distorts opinion formers' and decision makers' understanding of public sentiment.

Political bots are a crucial tool for computational propaganda. These automated computer programs are built to look like real social media users and can communicate with human users in "AstroTurf" (fake grassroots) efforts to spread disinformation, boost interaction, or defame opposition.[10] They use automation to achieve what Woolley has termed "manufacturing consensus" to give the illusion of popularity or dissent over social media in order to create bandwagon support or derision for a politician or political idea.[11] Tens of thousands of political bots and botnets (groups of bots) imitate human users in order to spread political messages on websites such as Twitter and Facebook.[12] Currently, Twitter boasts 335 million users, of which as many as 15 percent are estimated to be bots.[13] Bots can post material much faster than humans can and require comparatively little investment for even the most sophisticated programs. Because social media bot networks are available for hire, even technologically unsophisticated actors can use them. Social media attacks are force multipliers for any attempt to create confusion and disorder, particularly in crisis situations. As social media become increasingly important in surveying public opinion and predicting public reactions to events, computational propaganda becomes a potential complication.

Political bots can be divided into several categories: sockpuppet bots, amplifier bots (which are linked to approval bots), spam bots, troll bots, and sleeper bots.[14]

Sockpuppet bots, also known as cyborgs, are accounts that are part human and part bot.[15] To create such an account, a human will register an account on Twitter and then will set up automated programs to post tweets, intermittently tweeting nonautomated tweets and interacting with friends, resulting in account behavior that mixes both manual and automated operations.[16] These bots are often used to start conversations online that are subsequently spread and legitimized by amplifier and approval bots.

Amplifier bots are fully automated accounts that are employed to spread information by “liking,” sharing, retweeting, and republishing content.[17] This activity is often performed in conjunction with approval bots, which like, retweet, and comment on specific posts and profiles to validate their credibility.[18] Both amplifier and approval bots are implemented to manufacture consensus for fringe politicians and false normalcy for extremist ideas.[19]

Spam bots are used to disrupt streams of communication, often through the flooding of hashtags with irrelevant noise in order to redirect trending topics.[20]

Troll bots are deployed to harass and silence specific individuals and groups, such as female journalists and activists.[21] They often overwhelm profiles with threats or spread jeopardizing private information about their targets, among other intimidation tactics.

Sleeper bots are bots that can engage in all of the aforementioned behaviors but are distinguished in that they can lie dormant for long stretches of time. Consequently, if mobilized, thousands of sleeper bot accounts can emerge and spread massive amounts of disinformation at once. These bots are also harder to detect due to the fact that their profiles have established internet histories, making it easier for them to masquerade as authentic accounts.

Computational propaganda has been used by political actors across the world and in many different ways. It has been a major factor in interrupting the normal flow of information and political communications during elections and major events in democratic countries including France, Germany, the United States, and the United Kingdom.[22] In countries including Azerbaijan, Bahrain, Mexico, Russia, Turkey, and Ukraine, government-sanctioned actors have used massive networks of bots to deluge journalists and democratic activists with libel and threats.[23] The Islamic State and other terrorist groups have consistently used social media bots in order to exaggerate their online presence and promote radicalization.[24]

So far, computational propaganda has been particularly noticeable on Twitter. This is in part because of that company's historic openness to automation as well as its policies allowing public developers to deploy their own communication software on the platform. As a platform designed for spreading messages to the public, and one where journalists congregate in efforts to both spread and gather news, it is a natural target for political bots.[25] Furthermore, many politicians use the platform for self-promotion and public information sharing.[26] However, politicians do not control the discussion, even on political issues. Rather, research suggests that "non-elite actors, such as individual bloggers and concerned citizens" produce the majority of the most widely read tweets.[27] Twitter sorts posts on issues based on the tagged words they contain, such as #Syria or #NATOSummit. This is particularly tempting to bots, which can take over a popular hashtag's search results with their coordinated messaging. The Assad regime has made use of bot networks to take over hashtags that had been used to spread information about the Syrian conflict, posting irrelevant content to crowd out real news.[28]

The manipulation of public opinion online using bots and disinformation is not, however, solely relegated to Twitter—though its use there has been more widely studied because the company, unlike its competitors, has a more open policy for sharing data with academic researchers. Facebook, YouTube, WhatsApp, Instagram, Reddit, and a variety of other social media platforms around the globe have facilitated the flow of computational propaganda during major political events.[29] In this chapter, we focus on case studies that involve Twitter because—in these cases—political leaders, news entities, and propagandists used the site in efforts to control information flows during crisis situations. We argue, however, that the cases outlined here are representative of similar occurrences on Facebook, YouTube, and other social media platforms. These cases are meant to be not exhaustive but rather illustrative of a broader trend.

Social Media and Crisis Communication

In a crisis situation, governments must avoid public disorder if they are to properly coordinate a response. In the context of a nuclear attack where limited information is available, public panic would amplify the chaos, causing trillions of dollars in indirect damage.[30] Social media, including Twitter, are considered useful tools for informing and organizing the public in disaster scenarios, though they are far from perfect.[31] Although great numbers of affected people used Twitter during Hurricane Sandy, tweets became less and less informative as the crisis worsened and citizens were in greater need of information.[32] After the 2013 Boston Marathon bombings, Americans took to social media to discuss the hunt for the bombers, but misinformation spread far more quickly than attempts to correct it.[33] Such online rumor mills can result in a compounding cycle of disinformation, where prominent figures repeat or discuss disinformation that is then reported on by media outlets, sowing confusion even in the attempt to provide clarity.[34] Journalists often find information on social media and news articles from traditional media outlets are commonly shared by social media users.

It is hopeless to try to stop citizens from using social media to find information, since it is many people's primary mode of access to news and communication, particularly in situations like natural disasters where phone networks may be jammed.[35] Social media are thus as essential a part of civil defense as any other warning system. In a nuclear context, civil defense is not simply damage mitigation, but also part of credible deterrence.[36] If adversaries know that they will be able to use computational propaganda to sow panic, they may be more willing to act, believing that the leaders of a panic-stricken country will be more vulnerable in high-stakes negotiations.

Different countries have different cultural perceptions of the escalatory nature of cyberattacks and information warfare. Russian cyberwarfare institutions are quite aware of divergences in NATO and Russian approaches to information warfare—where NATO defines information warfare as tactical and limited, Russia sees it as a continuation of peacetime politics by other means.[37] Government communications, information operations, computational propaganda, and cyberattacks all exist on a spectrum of political internet activity. Varying understandings of that spectrum may cause unintended or unexpected escalation—although propaganda attacks will not take us over the brink of open hostilities, they may bring us unnecessarily closer to it. Propaganda itself may not be an act of war, but it can often be seen as a way to "prepare the ground" for direct or indirect action, to make the population in a target country more vulnerable to other forms of power deployed to attempt to persuade the government to change its policies.[38] Furthermore, public disorder may act as an escalatory force in itself, as civilian officeholders will feel pressure to react to foreign propaganda campaigns, particularly when these campaigns are conducted through means which are seen as illegitimate or deceitful.

Case Studies

Social media disinformation affects the flow of information in a crisis situation in two major, symmetric, ways. It attacks the transmission of information from the government to the public and from the public to decision makers. As such, we will present one case study of each type, highlighting how disinformation may interfere with timely and accurate communication.

Hawaii and North Korea: Government-to-Public Communication

On January 13, 2018, the Hawaii Emergency Management Agency sent out a cell phone alert warning residents of a ballistic missile threat heading for the state. In the half hour before an official notification of the false alarm was issued, public figures in Hawaii took to Twitter to inform the public that the warning was sent in error. Although Representative Tulsi Gabbard responded quickly, it took Governor David Ige fifteen minutes to access his Twitter account.[39] The alert was not fully countermanded for thirty-eight minutes. The United States has not prioritized civil defense against nuclear threats since the Cold War, although civil defense could reduce the casualties from a terrorist or rogue state attack.[40] This lack of public awareness means that nuclear false alarms may result in confusion and disorder rather than orderly safety preparations. This provides an opportunity for hostile actors to use information networks to replicate incidents like the Hawaii panic.

Information warfare may be a secondary consideration for targeted governments in many crisis scenarios where other, more direct forms of the use of force—particularly military—are at play, but it retains relevance in any case where decision makers must communicate with the public. Deployed as part of a hybrid cyberattack strategy, including attacks on infrastructure and penetration of government networks, computational propaganda could seriously damage the political will required to maintain standoffs with foreign powers. For instance, North Korean hackers could trigger a similar false alarm to the Hawaii scenario, but follow that up with a deluge of alarmist misinformation to extend the panic and compound the damage from other cyberattacks. According to cybersecurity experts, many American public alert and emergency management systems—even 911 calls—are highly vulnerable to hacking which could either jam these systems or falsely activate them.[41] The public response to such an event would be difficult to predict, but the political fallout could easily affect the decision making of civilian leadership.

Perhaps worse than merely causing alarm, such events undermine existing civil defense preparedness. In 2005, a false alarm was erroneously issued mandating the evacuation of Connecticut. Because the alarm did not seem credible, almost nobody followed its instructions.[42] A disinformation campaign which sought to undermine public confidence in such alerts could reduce preparedness in vulnerable populations. This would be a powerful tool for states seeking asymmetric advantages against a more powerful adversary. US forces in Korea have reportedly received false messages via SMS and Facebook ordering evacuations.[43] This is a seriously worrying sign that North Korea understands the potential of social media to wage information warfare. Although the US military is a comparatively hard target, North Korea could amplify the effect of its limited nuclear capacity by desensitizing civilians (including military families or contractors) to nuclear alerts, issuing false evacuation orders from shelters, or countermanding real warnings. This tactic would be available to most actors—state or non-state—whose strategies would benefit from mass confusion.

Jeremy Corbyn: Public-to-Government Influence

Jeremy Corbyn, the far-left leader of Britain's Labour Party, is unlikely ever to engage in nuclear brinkmanship. In fact, Corbyn has refused to say whether or not he would ever fire nuclear weapons, even in retaliation.[44] However, as part of a tide of antiestablishment politics, Corbyn provides a worrying example of how outsider politicians may be dangerously vulnerable to misinformation.

During the 2017 election campaign, Labour campaign chiefs who disagreed with Corbyn's strategy devised targeted ads to be seen by Corbyn and his close aides, deceiving Corbyn into thinking that the campaign staff were following his instructions.[45] These ads would have contained left-wing messages favored by Corbyn, but which campaign

HQ considered ineffective. Tom Baldwin, a former Labour director of communications, claims that party officials spent around £5,000 on these targeted ads in order to save money for other initiatives. This is a worryingly small cost for the ear of a powerful figure, and it has only come to light because of the peculiar internal circumstances of the Labour Party. We have no idea who else is targeting ads at Corbyn, or at decision makers in other countries who use their own social media accounts rather than delegating them to staff. Advertisements on social media can be displayed to extremely narrow demographic groups and lists of targets, in practice ensuring that they are seen by a single person.[46] TV ads run during *Fox and Friends* have been both explicitly and implicitly targeted at President Trump.[47] But the UK campaign is the first solid evidence we have that social media ads are being targeted to influence decision makers.

Corbyn's supporters in the Labour Party are known for their use of social media, both as a campaign tool and as a means of information gathering. Corbyn follows thousands of journalists, campaigners, and Labour Party members and may see information or arguments posted by any of these people. Corbyn is also seriously distrusted by the military and intelligence services in the United Kingdom and would likely reciprocate that suspicion in turn.[48] If a leader such as Corbyn—with antiestablishment tendencies and easily influenced by social media—were to come to power in a nuclear-armed country, targeted social media misinformation could be a powerful method of influence.

Though Corbyn himself is clearly a pacifist, such a scenario could easily arise in a more dangerous situation. In Pakistan, for instance, Prime Minister Imran Khan's successful campaign made heavy use of social media to encourage voting.[49] These trends will only increase in countries without reliable election infrastructure. As the case of disinformation at the beginning of this chapter shows, Pakistan's former defense minister evidently uses Twitter on his own, without checks on what he may be reading or repeating.[50] If such deception attacks can be carried out by campaign staffers, they would be trivial for a state actor to implement—convincing a foreign leader that he is hearing the real concerns of the people, not the intelligence briefings he mistrusts. When public opinion on dangerous issues is running high, as it often does over questions like Kashmir or the South China Sea, a populist leader could potentially be manipulated by his social media exposure. Online nationalism runs so high in China over territorial disputes that the government has had to censor social media users calling for war with the Philippines, a US ally.[51] While China has extensive control of its social media ecosystem, countries which use US-based social media platforms like Facebook would have great difficulty tamping down warlike popular sentiment, whether from real users or propaganda campaigns. A leader who sees social media as the voice of the people may follow that voice regardless of its true origin.

Conclusion

Social media have become near-ubiquitous tools for spreading information, and their use will only continue to expand in this capacity. Moreover, social media use is increasing in many developing countries, some of which, such as India and Pakistan, are longtime adversaries and offer potential for generating nuclear crises. In future crisis scenarios, governments will need to use social media to supplement traditional alert systems, but as we have seen in this chapter, they may be vulnerable to being attacked through disinformation campaigns or direct cyberwarfare. Decision makers will also use social media more as information-gathering tools, both through open-source intelligence and via their own personal accounts. This creates a vulnerability that cuts two ways: antiestablishment candidates who distrust their intelligence services may be misled by social media disinformation while decision makers with insufficient institutional support (such as Khawaja Asif) may be tricked by fake news.

In short, social media are an ever-growing part of the information environment that underlies decision making. Computational propaganda contaminates that environment, bringing information warfare straight into our pockets. The danger is that computational propaganda interferes with information flow between leaders and civilians—both the transmission of decisions to the public and decision makers' understanding of public sentiment.

Notes

1. Emma Graham-Harrison, "Fake News Story Prompts Pakistan to Issue Nuclear Warning to Israel," *The Guardian*, December 25, 2016, https://www.theguardian.com/world/2016/dec/26/fake-news-story-prompts-pakistan-to-issue-nuclear-warning-to-israel.

2. Karsten Friis and Jens Ringsmose, eds., *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (New York: Routledge, 2016).

3. Laura Roselle, Alister Miskimmon, and Ben O'Loughlin, "Strategic Narrative: A New Means to Understand Soft Power," *Media, War & Conflict* 7, no. 1 (April 2014): 70–84, https://doi.org/10.1177/1750635213516696.

4. Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents—Introduction," *International Journal of Communication* 10 (2016): 4482–90.

5. Nick Monaco and Carly Nyss, "State-Sponsored Trolling: How Governments Are Deploying Fake News as Part of Broader Harassment Campaigns," Institute for the Future working research papers, February 2018.

6. Samantha Bradshaw and Philip Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," Computational Propaganda Project Working Paper Series (Oxford, UK: Oxford University, June 2017), http://comprop.oii.ox.ac.uk/2017/07/17/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation.

7. Woolley and Howard, "Political Communication, Computational Propaganda, and Autonomous Agents—Introduction."

8. Philip M. Taylor, "Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day" (Manchester, UK: Manchester University Press, 2003).

9. Bradshaw and Howard, "Troops, Trolls and Troublemakers."

10. Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," Working Paper 2017.11, Project on Computational Propaganda, Oxford University, June 2017.

11. Samuel C. Woolley and Douglas Guilbeault, "Computational Propaganda in the United States of America: Manufacturing Consensus Online," Work-

ing Paper 2017.5, Project on Computational Propaganda, Oxford University, June 2017.

12. Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini, "The Rise of Social Bots," *Communications of the ACM* 59, no. 7 (July 2016): 96–104, https://doi.org/10.1145/2818717.

13. Alessandro Bessi and Emilio Ferrara, "Social Bots Distort the 2016 U.S. Presidential Election Online Discussion," *First Monday* 21, no. 11 (November 7, 2016), https://doi.org/10.5210/fm.v21i11.7090.

14. Woolley and Howard, "Computational Propaganda Worldwide: Executive Summary."

15. Renee DiResta, John Little, Jonathon Morgan, Lisa-Maria Neudert, and Ben Nimmo, "The Bots That Are Changing Politics," Vice, *Motherboard* (blog), November 2, 2017, https://motherboard.vice.com/en_us/article/mb37k4/twitter-facebook-google-bots-misinformation-changing-politics.

16. Zi Chu, Steven Gianvecchio, Haining Wang, and Sushil Jajodia, "Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?" *IEEE Transactions on Dependable and Secure Computing* 9, no. 6 (November/December 2012): 811–24, https://doi.org/10.1109/TDSC.2012.75.

17. DiResta et al., "The Bots That Are Changing Politics."

18. Ibid.

19. Woolley and Guilbeault, "Computational Propaganda in the United States."

20. Katina Michael, "Bots Trending Now: Disinformation and Calculated Manipulation of the Masses," *IEEE Technology and Society* 36, no. 2 (June 2017): 6–11, https://doi.org/10.1109/MTS.2017.2697067.

21. Andalusia Knoll Soloff, "Mexico's Troll Bots Are Threatening the Lives of Activists," Vice, *Motherboard* (blog), March 9, 2017, https://motherboard.vice.com/en_us/article/mg4b38/mexicos-troll-bots-are-threatening-the-lives-of-activists.

22. Clementine Desiguad, Philip N. Howard, Samantha Bradshaw, Bence Kollanyi, and Gillian Bolsover, "Junk News and Bots during the French Presidential Election: What Are French Voters Sharing over Twitter in Round Two?" Comprop Data Memo 2017.4, May 4, 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/05/What-Are-French-Voters-Sharing-Over-Twitter-Between-the-Two-Rounds-v7.pdf; Douglas Guilbeault and Samuel Woolley, "How Twitter Bots Are Shaping the Election," *The Atlantic*, November 1, 2016, https://www.theatlantic.com/technology/archive/2016/11/election-bots/506072; Philip N. Howard and Bence Kollanyi, "Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum," ArXiv:1606.06356, June 20, 2016, http://arxiv.org/abs/1606.06356; Lisa-Maria Neudert, "Computational Propaganda in Germany: A Cautionary

Tale," Working Paper 2017.7, Project on Computational Propaganda, Oxford University, June 2017.

23. Monaco and Nyss, "State-Sponsored Trolling."

24. Leanna Garfield, "ISIS Has Created Thousands of Political Bots—and Hacktivists Want You to Destroy Them," *Business Insider*, December 14, 2015, http://uk.businessinsider.com/anonymous-battles-isis-political-bots-2015-12.

25. Paul Farhi, "The Twitter Explosion," *American Journalism Review* 31, no. 3 (June 1, 2009): 26–32; Anders Olof Larsson and Moe Hallvard, "Bots or Journalists? News Sharing on Twitter," *Communications: The European Journal of Communication Research* 40, no. 3 (2015): 361–370, https://doi.org/10.1515/commun-2015-0014.

26. Jennifer Golbeck, Justin M. Grimes, and Anthony Rogers, "Twitter Use by the U.S. Congress," *Journal of the American Society for Information Science and Technology* 61, no. 8 (August 2010): 1612–21, https://doi.org/10.1002/asi.21344.

27. Todd P. Newman, "Tracking the Release of IPCC AR5 on Twitter: Users, Comments, and Sources Following the Release of the Working Group I Summary for Policymakers," *Public Understanding of Science* 26, no. 7 (October 1, 2017): 815–25, https://doi.org/10.1177/0963662516628477.

28. Norah Abokhodair, Daisy Yoo, and David W. McDonald, "Dissecting a Social Botnet: Growth, Content and Influence in Twitter," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, New York, March 14–18, 2015: 839–851, https://doi.org/10.1145/2675133.2675208.

29. Samuel C. Woolley, "Automating Power: Social Bot Interference in Global Politics," *First Monday* 21, no. 4 (April 4, 2016), http://firstmonday.org/ojs/index.php/fm/article/view/6161.

30. Jonathan Medalia, "Nuclear Terrorism: A Brief Review of Threats and Responses," Congressional Research Service, February 10, 2005, http://www.dtic.mil/docs/citations/ADA437865.

31. Alexander Mills, Rui Chen, JinKyu Lee, and H. Raghav Rao, "Web 2.0 Emergency Applications: How Useful Can Twitter Be for Emergency Response?" *Journal of Information Privacy and Security* 5, no. 3 (July 1, 2009): 3–26, https://doi.org/10.1080/15536548.2009.10855867.

32. Patric R. Spence, Kenneth A. Lachlan, Xialing Lin, and Maria del Greco, "Variability in Twitter Content Across the Stages of a Natural Disaster: Implications for Crisis Communication," *Communication Quarterly* 63, no. 2 (March 15, 2015): 171–86.

33. Kate Starbird, Jim Maddock, Mania Orand, Peg Achterman, and Robert M. Mason, "Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing," Illinois Digital Environment for Access to Learning and Scholarship, March 1, 2014, https://doi.org/10.9776/14308.

34. Woolley and Guilbeault, "Computational Propaganda in the United States."

35. Huiji Gao, Geoffrey Barbier, and Rebecca Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief," *IEEE Intelligent Systems* 26, no. 3 (May/June 2011): 10–14, https://doi.org/10.1109/MIS.2011.52.

36. Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (Cambridge, UK: Cambridge University Press, 2017).

37. Keir Giles, "The Next Phase of Russian Information Warfare," NATO Strategic Communications Centre for Excellence, November 2017, 16.

38. Keir Giles, "Working Paper: Russia‘s Hybrid Warfare: A Success in Propaganda,“ Bundesakademie Für Sicherheitspolitik," February 18, 2015, https://www.baks.bund.de/de/aktuelles/working-paper-russias-hybrid-warfare-a-success-in-propaganda.

39. Michael Sheetz, "Hawaii's Governor Knew the Missile Alert Was Fake in Two Minutes—But He Didn't Know His Twitter Password," CNBC, January 23, 2018, https://www.cnbc.com/2018/01/23/hawaii-gov-ige-knew-missile-alert-fake-didnt-know-twitter-password.html.

40. Gordon Sander, "Americans Are Unprepared for a Nuclear Attack," *Politico*, June 11, 2018, https://politi.co/2touIgW.

41. Tim Starks, "Hawaii Missile Alert Highlights Hacking Threat to Emergency Systems," *Politico*, January 16, 2018, http://politi.co/2Dl5ktv.

42. Mark Pazniokas, "Connecticut Evacuation: False Alarm," *Hartford Courant*, February 2, 2005, http://articles.courant.com/2005-02-02/news/0502020861_1_evacuation-order-false-alarm-emergency-alert-system.

43. Kim Gamel, "US Forces Korea Warns of Fake Evacuation Messages," *Stars and Stripes*, September 21, 2017, https://www.stripes.com/news/pacific/us-forces-korea-warns-of-fake-evacuation-messages-1.488792#.WcUkpsZulLO.

44. Jim Pickard and Henry Mance, "Jeremy Corbyn Backs Away from Nuclear Question," *Financial Times*, May 12, 2017, https://www.ft.com/content/d2ca7f4c-36ef-11e7-99bd-13beb0903fa3.

45. Tim Shipman, "Labour HQ Used Facebook Ads to Deceive Jeremy Corbyn during Election Campaign," *The Times*, July 14, 2018, https://www.thetimes.co.uk/article/labour-hq-used-facebook-ads-to-deceive-jeremy-corbyn-during-election-campaign-grlx75c27.

46. Michael Harf, "Sniper Targeting on Facebook: How to Target ONE Specific Person with Super Targeted Ads," *Medium* (blog), December 5, 2017, https://medium.com/@MichaelH_3009/sniper-targeting-on-facebook-how-to-target-one-specific-person-with-super-targeted-ads-515ba6e068f6.

47. Simon Dumenco, "John Oliver Is Running Ads on Cable News to Educate Just One Viewer: Donald Trump," *Ad Age*, February 13, 2017, http://adage.com/article/the-media-guy/john-oliver-running-ads-cable-news-educate-trump/307963.

48. Claire Newell, Hayley Dixon, Luke Heighton, and Harry Yorke, "MI5 Opened File on Jeremy Corbyn amid Concerns over His IRA Links," *The Telegraph*, May 19, 2017, https://www.telegraph.co.uk/news/2017/05/19/exclusive-mi5-opened-file-jeremy-corbyn-amid-concerns-ira-links.

49. Falah Gulzar, "Imran Khan: Social Media's Prime Minister?" *Gulf News*, June 26, 2018, https://gulfnews.com/news/asia/pakistan/imran-khan-social-media-s-prime-minister-1.2242467.

50. Graham-Harrison, "Fake News Story."

51. Kenneth Tan, "Chinese Censors Harmonize Online Posts Calling for War Following South China Sea Ruling," *Shanghaiist* (blog), July 13, 2016, http://shanghaiist.com/2016/07/13/hague_ruling_censored.