SECURING DEMOCRACY

IN THE DIGITAL AGE

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

ABOUT THE AUTHOR

Zoe Hawkins
Zoe is an Analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber policy issues.

WHAT IS ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI INTERNATIONAL CYBER POLICY CENTRE

The ASPI International Cyber Policy Centre (ICPC) brings together the various Australian Government departments with responsibilities for cyber issues, along with a range of private-sector partners and creative thinkers to assist Australia in creating constructive cyber policies both at home and abroad. The centre aims to facilitate conversations between government, the private sector and academia across the Asia–Pacific region to increase constructive dialogue on cyber issues and do its part to create a common understanding of the issues and possible solutions in cyberspace.

The ICPC has four key aims:

- Lift the level of Australian and Asia–Pacific public understanding and debate on cybersecurity.
- Provide a focus for developing innovative and high-quality public policy on cyber issues.
- Provide a means to hold Track 1.5 and Track 2 dialogue on cyber issues in the Asia–Pacific region.
- Link different levels of government, business and the public in a sustained dialogue on cybersecurity.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various funders.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

CommonwealthBank
THALES
.auDA .au DOMAIN ADMINISTRATION LTD

SECURING DEMOCRACY

IN THE DIGITAL AGE

ZOE HAWKINS

CONTENTS

INTRODUCTION

The proliferation of cyberspace and rise of social media have enriched and strengthened the application of democratic governance. Technological developments have expedited the international flow of information, improved freedom of speech in many areas of the world, and increased the quality of interaction, accountability and service delivery from democratic governments to their citizens. But these benefits must be balanced against a longstanding vulnerability of democracy to manipulation that cyberspace has enhanced in both scope and scale.

Cybersecurity isn't a new problem; however, for many years the focus of the threat of cyberspace to state sovereignty has been on cyberattacks causing damage to physical infrastructure, with effects analogous to kinetic attacks. The securitised image is usually that of cyberspace being leveraged to take out an electricity grid, open a dam or disable air traffic control systems. The potential chaos that this anticipated type of cyber-physical interference would cause has led to a growing focus on cyber defences for critical national infrastructure in networked countries.

This physical security concern and its associated policy responses are useful and important. However, to limit our understanding of the cyber threat to physical damage would be to overlook the integral role that cyber technologies play in less tangible elements of national security: democratic elections and supporting public information flows. Public trust in the reliability and integrity of the electoral process is the foundation of the social contract between the governing and the governed in liberal democracies, so citizens must be able to trust that the computer systems responsible for handling the execution of an election will deliver an accurate result.

Beyond that, the information ecosystem within which citizens deliberate on their voting choices is also subject to manipulation. Information operations designed to shape public sentiment by introducing new facts into the mix, whether false or accurate, can sway votes in advance of election day.

The 2016 US presidential election demonstrated the increasingly complex cyber and information environment in which democracies are operating. Using US case study illustrations, this report offers a conceptual framework by which to understand how cybersecurity and information security techniques can be used to compromise a modern-day election. The report places this case study in its historical context and outlines emerging approaches to this new normal of election interference before identifying associated policy considerations for democracies.

Case study: 2016 US presidential election infrastructure

In August 2016, the Cyber Division of the Federal Bureau of Investigation (FBI) released a 'flash alert' to states, which reported that hackers had successfully breached the voter registration databases of Arizona and Illinois.[1] By the end of September, reports that foreign hackers had targeted almost half of the US's state voter registration systems were circulating. Four were successfully breached, and FBI Director James Comey admitted that 'there's no doubt some bad actors have been poking around.'[2]

This hacking activity also sparked broader panic about cyber vulnerabilities in voting infrastructure being exploited to manipulate the election results. There was particular concern over the cybersecurity of digital voting booths, which are referred to as direct recording electronic (DRE) systems. In the wake of the troubled 2000 presidential election count, there was a move to modernise the US voting process from paper punching to digital machines. Unfortunately, the change took place without much consideration of security, and systems haven't been diligently upgraded since installation. The Institute for Critical Infrastructure states that, as a result, most voting machines in the US are 'less secure than a modern children's toy'.[3]

In the months leading up to the 2016 election, US media flurried around practical demonstrations of these cyber vulnerabilities. Princeton professor Andrew Appel demonstrated that a common DRE machine, used in Louisiana, New Jersey, Virginia and Pennsylvania, could be physically reconfigured within minutes to log votes incorrectly.[4] At the Black Hat hacking conference held in Las Vegas during August, Symantec revealed how voter access cards used by citizens to cast their votes at an e-voting machine could be reprogrammed to allow an individual to fraudulently submit hundreds of votes at a time.[5] The fact that an estimated 22% of voters would vote on versions of these vulnerable machines, which leave no auditable paper trail, became an acute point of public concern.[6] Media headlines such as 'America's electronic voting machines are scarily easy targets' and 'American elections will be hacked' indicate that public confidence in the integrity of the electoral process was being tested.[7]

Fortunately, no evidence has emerged in the wake of Donald Trump's victory that there was any cyber interference in the execution of the US election, and the Department of Homeland Security has asserted that 'the types of systems Russian actors targeted or compromised were not involved in vote tallying.'[8]

1 Michael Isikoff, 'FBI says foreign hackers penetrated state election systems', *Yahoo! News*, 29 August 2016, online.

2 Mike Levine, Pierre Thomas, 'Russian hackers targeted nearly half of states' voter registration systems, successfully infiltrated 4', *ABC News*, 29 September 2016, online.

3 James Scott, Drew Spaniel, *ICIT analysis: hacking elections is easy! Part one: tactics, techniques and procedures*, Institute for Critical Infrastructure Technology, August 2016, online.

4 Ben Wofford, 'Hot to hack an election in 7 minutes', *Politico*, 5 August 2016, online.

5 Laurie Segall, 'Just how secure are electronic voting machines?', *CNN Tech*, 9 August 2016, online.

6 Haley Sweetland Edwards, Chris Wilson, 'See how likely it is that your voting booth gets hacked', *Time*, 20 September 2016, online.

7 Brian Barrett, 'America's electronic voting machines are scarily easy targets', *Wired*, 2 August 2016, online; Bruce Schneier, 'American elections will be hacked', *New York Times*, 9 November 2016, online.

8 Office of the Director of National Intelligence, *Assessing Russian activities and intentions in recent US elections*, 6 January 2017, online.

Case study: 2016 US presidential election campaigns

In June 2016, five months before the US presidential election, the Democratic National Committee (DNC) was hacked and confidential email communications were accessed. Crowdstrike asserted that the network compromise was the work of two sophisticated Russian hacking groups, referred to as 'Cozy Bear' and 'Fancy Bear', while Guccifer 2.0, a lone Romanian hacker, publicly claimed responsibility.[9] On 22 July, just days before the Democratic National Convention, more than 20,000 emails stolen from the DNC server were published on Wikileaks.[10] The communications, allegedly sent by seven central DNC officials between January 2015 and May 2016, revealed evidence that DNC Chair Debbie Wasserman Schultz had failed to remain impartial and was in fact biased towards Hillary Clinton as the Democratic nominee over Bernie Sanders. The revelations prompted Wasserman's resignation.

A second Wikileaks data dump of stolen emails hit the public domain on 7 October, and this time it was the personal emails of Clinton's campaign chairman, John Podesta.[11] The gradual release of more than 58,000 emails over a period of a month offered further unflattering insights into Clinton, such as her engagement with Wall Street and the operation of the Clinton Foundation, further damaging her presidential hopes.[12] The Podesta emails were released right up until election day on 8 November, when the final tranche of 1,793 emails was published.

The Trump campaign and Wikileaks dismissed rumours that the leaks were evidence of the Russian Government trying to sabotage Clinton in favour of a Trump win, and Russian President Vladimir Putin denied any involvement in the hacks.[13] However, in December 2016, the Office of the Director of National Intelligence released an intelligence community assessment that explicitly stated, 'We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election.'[14] FBI Director James Comey confirmed to the House Intelligence Committee on 20 March 2017 that there's an ongoing investigation into 'the nature of any links between individuals associated with the Trump campaign and the Russian government and whether there was any coordination between the campaign and Russia's efforts.'[15] House and Senate intelligence committee probes into the nature and extent of Russia's election interference are underway. The Justice Department has also appointed a Special Counsel to oversee the FBI investigation into the incident.[16]

9 Dimitri Alperovitch, 'Bears in the midst: intrusion into the Democratic National Committee', *Crowdstrike Blog*, 15 June 2016, online; Guccifer2, 'Guccifer 2.0 DNC's servers hacked by a lone hacker', *Guccifer 2.0*, 15 June 2016, online.

10 'DNC email archive', *Wikileaks*, 22 July 2016, online.

11 'The Podesta emails', *Wikileaks*, 7 October 2016, online.

12 '18 revelations from Wikileaks' hacked Clinton emails', *BBC News*, 27 Octboer 2016, online.

13 'Debate fact check: reviewing what Donald Trump and Hillary Clinton said during the debate', *ABC News*, 10 October 2016, online; Julian Assange, 'Assange statement on the US election', *Wikileaks*, 8 November 2016, online; Shaun Walker, 'Vladimir Putin dismisses claims of meddling in US election', *The Guardian*, 27 October 2016, online.

14 Office of the Director of National Intelligence, *Assessing Russian activities and intentions in recent US election.*

15 ' James Comey confirms FBI is investigating Russian interference in election and links to Trump campaign', *Sydney Morning Herald*, 21 March 2017, online.

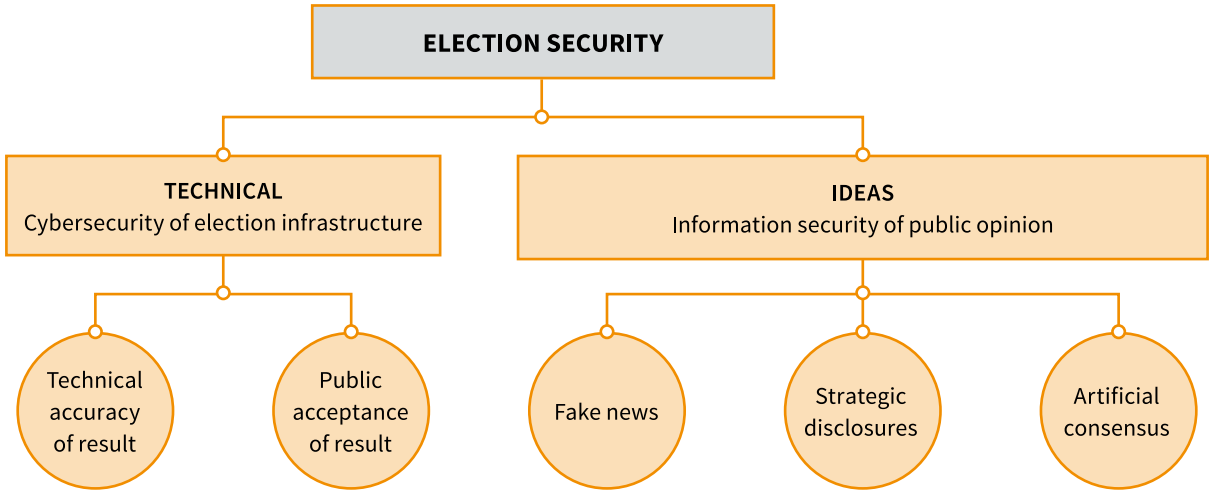
16 The United States Department of Justice, 'Appointment of Special Counsel', 17 May 2017, online.

FRAMEWORK FOR CONTEMPORARY ELECTION SECURITY

The 2016 US presidential election shed light on how technology can be leveraged to influence the democratic process. The way in which the complex issues that arose during the campaign were portrayed in US media also revealed how easily the various methods of achieving that influence can be misunderstood and conflated under the generalised and ambiguous umbrella of 'election hacking'.

Protecting the integrity of democracy is an important and difficult task. A nuanced appreciation of the different factors in play is vital to understand the cyber threat landscape and then tailor appropriate mitigation solutions and policy responses for each challenge. The framework below describes two distinct techniques that can conceivably be used to undermine the modern democratic process: compromising vote results by targeting election infrastructure, or preemptively shaping public voting opinion through fake news, strategic disclosures of compromising material and the creation of an artificial consensus (Figure 1).

FIGURE 1: A FRAMEWORK FOR ELECTORAL SECURITY



CYBERSECURITY OF ELECTION INFRASTRUCTURE

Public trust in the integrity of the electoral process is essential to peacefully resolving political competition and facilitating the smooth transition of power between democratic governments. Article 21 of the Universal Declaration of Human Rights emphasises that 'the will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections.'[17] Elections identify the new leadership of a country from a selection of competing candidates and therefore serve not only to select the winner but also to convince the unsuccessful candidates and their supporters that they lost. Therefore, the process must not only *be* fair and accurate, but must be *believed to be* fair and accurate. Producing convincing results is no small task, and doing so successfully is reliant on an intangible foundation of social trust in the establishment's operation of the democratic system. As Kofi Annan states, 'legitimacy is the crucial currency of government in our democratic age … victory without legitimacy is no victory at all.'[18]

17 United Nations, *Universal Declaration of Human Rights*, 10 December 1948, online.

18 Global Commission on Elections, Democracy and Security, *Deepening democracy: a strategy for improving the integrity of elections worldwide*, September 2012, online.

Developments in information technology have made the execution of this vital democratic process easier in many ways. Online voter registration databases, electronic voting machines and digital vote counting have arguably boosted the efficiency of elections. However, they have also introduced new risks to the security and stability of the process.

The cyber threat environment is constantly evolving, and technology is never foolproof. Even the most advanced countries are still struggling to achieve security by design in their e-governance systems, and election technology is yet to receive a high level of national security priority across the board, so almost every step of a digitised election becomes vulnerable to cyber compromise.

Compromising votes

In theory, cyber operations could be used to undermine the integrity of the vote counting process and covertly manipulate election results. While the average digital voting machine isn't connected to the internet, they're susceptible to physical tampering that can compromise the way they record votes. With some quick reprogramming, pushing the button for candidate A will submit a vote for candidate B instead.[19] Similarly, voter ID cards can be manipulated to allow for the intentional submission of multiple votes by one individual.[20] Vote tallies could also be changed in the collation process. When results from different areas of the country are being communicated across networks they are again vulnerable to manipulation, often travelling across insecure channels. Theoretically, targeting these weak spots offers a way to influence election results while leaving constituents none the wiser.

Compromising trust

While it's possible to commit electronic vote manipulation as described above, it would take significant resources to do it at the scale necessary to generate real change in an election result. Instead of being covertly changed, the reliability of an election result could simply be publicly called into question. Cyber operations that give the impression that a vote may not accurately reflect the will of the people could be sufficient to undermine public trust in the whole process. A selection of incidents that demonstrate the fragility of the electoral system to cyber compromise, such as manipulating voter databases to achieve targeted disenfranchisement on election day, could easily create fear of further undiscovered, large-scale tampering. This paranoia would be exacerbated by the fact that in many cases digital voting machines don't leave an audit trail by which to verify the accuracy of results. Additional ways to corroborate voting outcomes increase the difficulty of altering election results and help build trust and public acceptance of a victory.

Compromising election infrastructure in the US election

The US experience offered a small insight into the destabilisation of public confidence that can come from an isolated election infrastructure incident. The reported breach of voter registration databases in Arizona, Illinois and Florida, plus efforts against many more, showcased cybersecurity weakness and sparked a protracted public dialogue about the reliability of the election.[21] The significant proportion of votes that were to be submitted on digital voting machines that leave no verifiable paper trail intensified those concerns, prompting all but four states to seek cybersecurity support from the Department of Homeland Security before the end of October 2016.[22]

It's hard to measure the direct impact that these cybersecurity fears had on public trust in election infrastructure, especially in the light of Trump's unrelated allegations of 'large scale voter fraud' and warnings of a rigged election.[23] A combination of these factors is likely to have contributed to widespread nervousness over the reliability of the election.

Fortunately, with more than 2,000 different jurisdictions, US election voting infrastructure is highly decentralised. This means it would be extremely difficult to hack the system and change the outcome in a meaningful way unless the election were already an extremely close call.[24] The US intelligence community assessment released in January 2017 concluded that no tampering with vote-tallying systems took place.

Nevertheless, the vulnerabilities revealed and the resulting public dialogue highlighted that the protection currently afforded to these systems isn't commensurate with the significance of the function they serve.

19 Wofford, 'Hot to hack an election in 7 minutes'.

20 Segall, 'Just how secure are electronic voting machines?'.

21 Levine & Thomas, 'Russian hackers targeted nearly half of states' voter registration systems, successfully infiltrated 4'.

22 Tal Kopan, Jim Sciutto, 'Election 2016: cyber help requests now up to 46 states', *CNN*, 31 October 2016, online.

23 Donald Trump, Tweet, 17 October 2016, online.

24 Dina Gusovsky, 'A big threat facing the presidential election no one is talking about', *CNBC*, 2 September 2016, online.

SHAPING PUBLIC OPINION

The power of cyberspace to influence the democratic process lies in much more than just the nuts and bolts of the election infrastructure. Every vote cast on election day is the product of the information ecosystem of the preceding months. Shaping the nature and volume of information available to the public in the lead-up to an election is a sophisticated way of influencing voter decision-making and election outcomes.

In this method of tampering with elections, a culprit's digital fingerprints can never be directly linked to the election *per se*. Election decision-making can be influenced through the dissemination of 'fake news' or 'strategic disclosures', and the impact of this false or previously unavailable information can be increased through the creation of an 'artificial consensus' online.

Fake news

False information can be disseminated online to influence citizens' decision-making before election day. The democratisation of media means that this type of mass misinformation operation is easier than ever before.

DEMOCRATISATION OF MEDIA

The increasingly prominent role of social media in the international dissemination of news and information has changed the modern media landscape. This democratisation of media has been a positive development in many ways. It's changed the meaning and impact of freedom of speech, empowering previously overlooked minority groups and making governments accountable to an independent mass media movement. However, it's also provided a platform for the distribution of highly subjective, factually incorrect and sometimes purposeful misinformation. Distinguishing real information from fake news is becoming more challenging as falsehoods are passed off as 'alternative facts'.[25]

For traditional news services, such as newspapers and news channels, factual accuracy is usually seen as a reputational currency, and their brands are dependent on releasing information of a certain quality. The professionalism of news companies necessarily limits their number and allows for some measure of accountability.

The rise of the blogger, vlogger and tweeter has made everyone a journalist and sparked a boom in content creation by the general public. The transition from traditional media to lower threshold information sharing means there's been a proliferation of opinions published online—a great thing for freedom of expression. Unfortunately, this has created significant noise around important issues, diluted the credibility of news on many newsfeeds and enabled people to intentionally surround themselves with reinforcing ideas.

DISINFORMATION

This online landscape is ripe for use by malicious actors who wish to sway public opinion. The content creation free-for-all that has emerged can easily be used as a platform for information operations that inject false information to support strategic outcomes. Targeted disinformation can shape public sentiment towards a particular candidate or, at the very least, can cause confusion and sow doubt about the credibility of all news and narratives.

FAKE NEWS IN THE US ELECTION

The proliferation of fake news stories was a defining theme of the 2016 US presidential election. False stories and half-truths were created frequently, and their take-up by the general public was high. Worryingly, in the final months before the election, trending fake news headlines received higher Facebook engagement rates than the top headlines from traditional media outlets, such as the *New York Times* and *Washington Post* (Figure 2).[26] Stanford University research based on web browsing data, news article databases and post-election surveys reveals that the vast majority of popular fake news stories were pro-Trump.[27] Notable examples include the claims that he had been endorsed by Pope Francis and that Clinton was selling arms to Islamic State.[28]

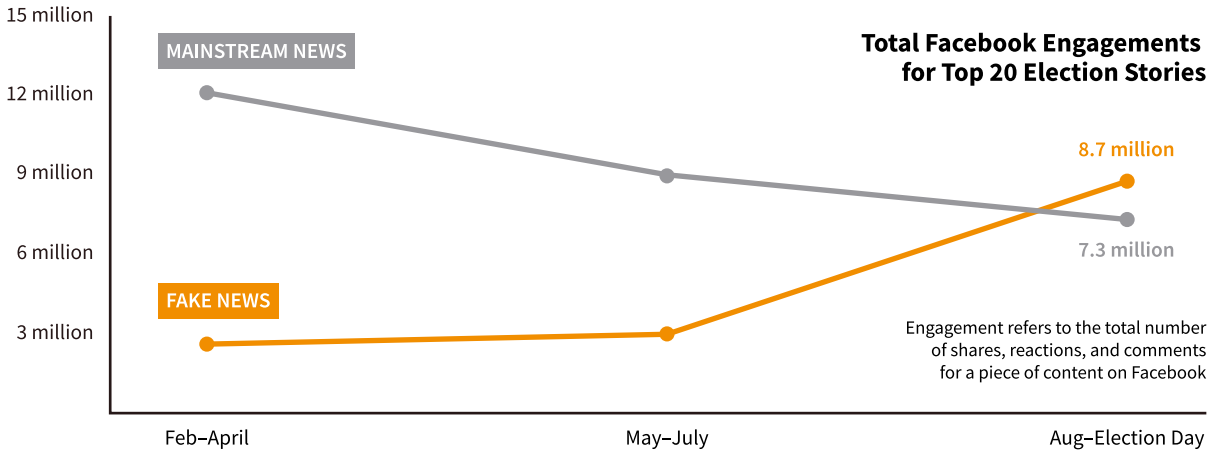
25 Mahita Gajanan, 'Kellyanne Conway defends White House's falsehoods as "alternative facts"', *Time*, 22 January 2017, online.

26 Craig Silverman, 'This analysis shows how viral fake election news stories outperformed real news on facebook', *BuzzFeed News*, 17 November 2016, online.

27 Hunt Allcott, Matthew Gentzkow, 'Social media and fake news in the 2016 election', *Journal of Economic Perspectives*, Spring 2017, 31(2):211–236, online.

28 Hannah Ritchie, 'Read all about it: the biggest fake news stories of 2016', *CNBC*, 30 December 2016, online.

FIGURE 2: ENGAGEMENT WITH MAINSTREAM AND FAKE NEWS

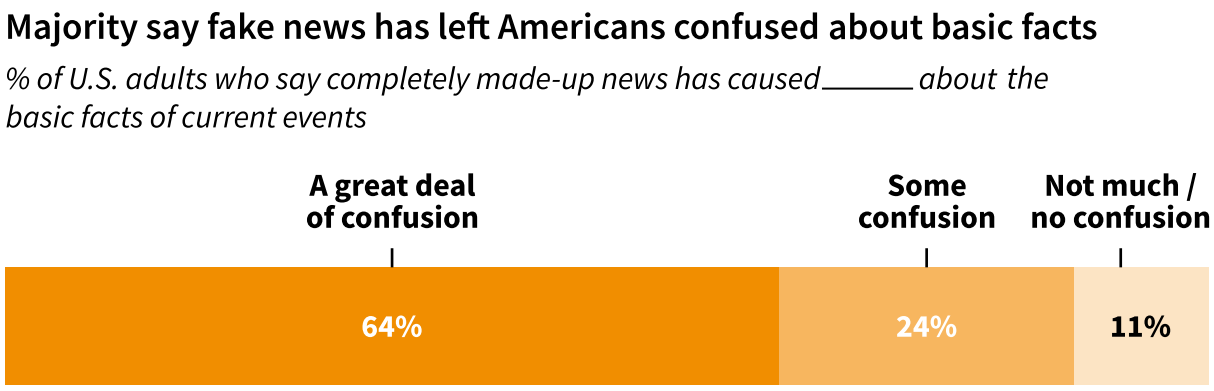


Source: Craig Silverman, 'This analysis shows how viral fake election news stories outperformed real news on Facebook', *BuzzFeed News*, 17 November 2016, online

To informed readers, such claims may seem unbelievable, but the made-up stories did shape some people's perception of reality. Famously, a North Carolina man was arrested for turning up armed with a gun at a pizzeria that had been wrongly identified by a fake news story as a front for a Clinton child-trafficking ring.[29] The incident, referred to as #pizzagate, illustrated the power of disinformation to activate individual beliefs and behaviours. Unsurprisingly, Clinton denounced the proliferation of fake news stories as an 'epidemic', and one that was having 'real world consequences'.[30]

Importantly, fake news stories don't have to convince everyone to be considered effective. Simply creating sufficient confusion can be enough to undermine confidence in official narratives. The Pew Research Center discovered in December 2016 that roughly two-thirds of Americans see fake news as having 'caused a great deal of confusion' (Figure 3).[31]

FIGURE 3: PEW RESEARCH CENTER POLL ON IMPACT OF FAKE NEWS



Survey conducted Dec 1-4, 2016

Source: Michael Barthel, Amy Mitchel and Jesse Holcomb, *Many Americans believe fake news is sowing confusion*, Pew Research Center, 15 December 2016, online.

Many of these fake news stories can be traced back to Russian sources, and the FBI is apparently investigating the role of news sites such as RT and Breitbart in creating and propagating disinformation during the election.[32]

29 Rebecca Morin, 'Armed man arrested near DC pizzeria targeted by fake news', *Politico*, 4 December 2016, online.

30 'Hillary Clinton warns of "fake news epidemic"', *BBC News*, 9 December 2016, online.

31 Michael Barthel, Amy Mitchel, Jesse Holcomb, *Many Americans believe fake news is sowing confusion*, Pew Research Center, 15 December 2016, online.

32 Peter Stone, Greg Gordon, 'FBI's Russian-influence probe includes a look at Breitbart, InfoWars news sites', *McClatchy Washington Bureau*, 20 March 2017, online.

Strategic disclosures

Information doesn't have to be false to influence voters' decision-making. Acquiring and distributing true but previously unavailable facts can change the way people make choices during an election. Sometimes referred to as 'doxxing', this approach involves 'maliciously disclosing information in a calculated fashion to inflict setbacks in political momentum and unity'.[33] Today, cyberspace can be used to both obtain and distribute this kind of damaging evidence.

OBTAINING COMPROMISING INFORMATION

Our digital footprints are growing, creating ever larger bodies of information in cyberspace that tell stories about our history, habits, weaknesses and communications. Election candidates will invariably have some elements of their lives, whether contemporary or historical, which could discredit them in the eyes of the public. For this reason, drawing boundaries between public and private life is a goal for most politicians.

However, drawing that line is increasingly difficult in the digital age. Those who would wish to undermine a political candidate can now gain a lot of compromising information via cyberspace. For example, the use of spear phishing email scams can give a malicious actor access to an individual's confidential communications, which can then be used to selectively release information that portrays them negatively to voters.

DISTRIBUTING COMPROMISING INFORMATION

Cyberspace is an excellent medium through which to distribute compromising information. Selectively curating and strategically disclosing the stolen information on a public online forum is a low-cost way to change public sentiment in the lead-up to an election. Social media or dedicated websites such as Wikileaks mean that it's never been easier to get an audience for your strategic narrative shaping.

Questions of authenticity will inevitably be raised about such disclosures, given the possibility that the released information has been doctored in part or whole. However, the frailty of public confidence means that the possibility of a scandal can be enough to rock the boat and change votes.

STRATEGIC DISCLOSURES IN THE US ELECTION

In 2016, Democratic presidential candidate Hillary Clinton was the target of a campaign of strategic disclosures designed to discredit her candidacy. Phishing email attacks were used to gain unauthorised access to the confidential communications of the DNC and Clinton's campaign manager, John Podesta. More than 20,000 DNC emails were published by Wikileaks in July 2016, revealing the committee's bias against Clinton's Democratic competitor, Bernie Sanders. The website then carried out an incremental dump of over 58,000 Podesta emails during October 2016, right up to the day of the election, shedding unfavourable light on the operation of the Clinton Foundation, among other things.

The number of factors in play during the final months of the US presidential election campaign, including the candidates' public debates, the FBI investigation into Clinton's email conduct as Secretary of State, and the Access Hollywood video of Trump, make it all but impossible to draw anything more than circumstantial conclusions on the impact of the email leaks on the election outcome.

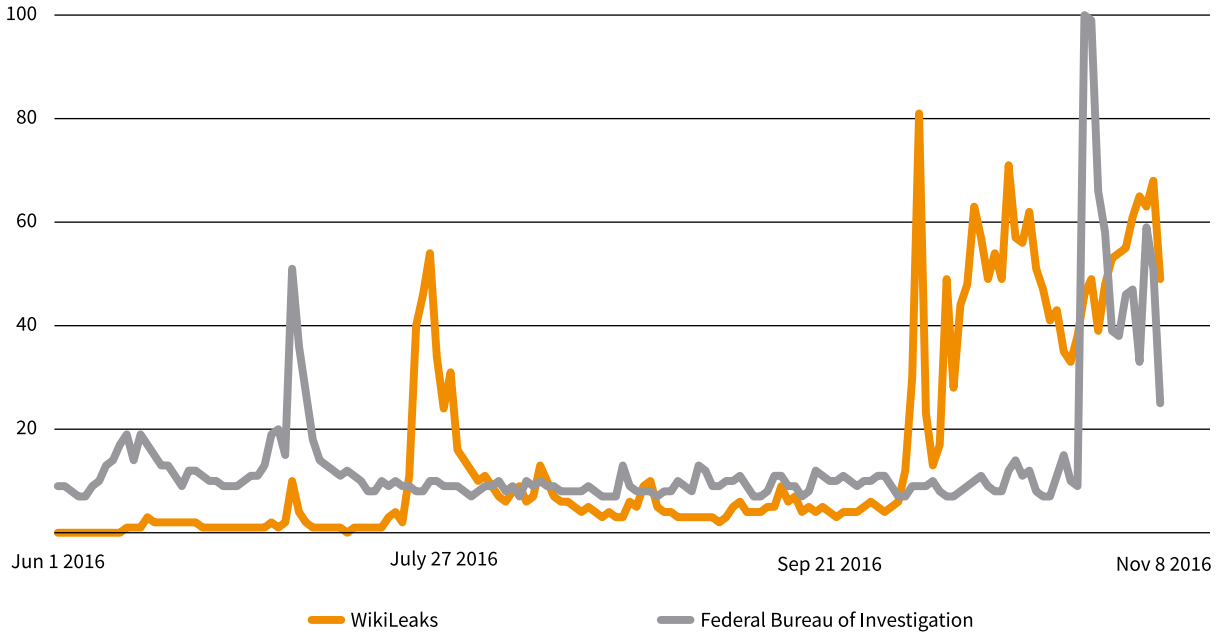
That said, Google Trend analytics reveal a sustained high level of public interest in searches for 'Wikileaks' in the six weeks before the election, which was only briefly overtaken by searches for 'Federal Bureau of Investigation' at the time of Comey's letter to Congress on 28 October (Figure 4).[34] Clinton asserts that she was 'on the way to winning' but that both the letter and Wikileaks emails were an 'intervening event' that 'raised doubts' among people who were originally going to vote for her.[35]

33 Simon Crosby, 'What the election can teach us about cybersecurity', *Forbes*, 31 January 2017, online.

34 Google Trend, online.

35 Nolan D McCaskill, Gabriel Debenedetti, 'Clinton: "I was on the way to winning" until Comey, Russia intervened', *Politico*, 2 May 2017, online.

FIGURE 4: GOOGLE SEARCHES FOR 'FEDERAL BUREAU OF INVESTIGATION' AND 'WIKILEAKS' FROM JUNE 2016 TO 8 NOVEMBER 2016



Note: The vertical axis represents search interest relative to the highest point on the chart for the US between 1 June and 8 November 2016. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. Likewise, a score of 0 means the term was less than 1% as popular as at the peak.

Source: Google Trends, online.

Artificial consensus

Both the above methods are ways to change or shape the information that's available to voters before they fill out their ballots. The prominence and impact of the information being injected, whether fake or disclosed, can also be manipulated using unique characteristics of social media technology.

ECHO CHAMBERS

The nature of modern social media technology entrenches partisan points of view. Newsfeed algorithms are designed to offer people what they want to read, based on their demonstrated preferences. Companies such as Facebook and Twitter design it that way to produce a positive customer experience and facilitate targeted advertising. However, the result is the creation of online silos, or 'echo chambers', that reduce the likelihood that an individual will be exposed to views contrary to their own.[36] Instead, they'll be provided with more and more content that supports their original position. This, paired with natural confirmation bias, can entrench a person's perspective and make it more extreme. So, while we have more information at our fingertips than ever before, an unsuspecting social media consumer may also be seeing fewer sides of a story than before.

BOTS

Not only do newsfeed algorithms often exclude opposing views, but 'bot' technology can give the false impression that a certain viewpoint is ascribed to by many people, maybe even the majority. Social media bots (short for 'robots') are accounts that automate the mass publishing of online content. They're usually highly active and operate as part of broader networks, or 'botnets', some of which have been found to number up to 350,000 accounts.[37] Bots of different kinds constituted more than half of all global internet traffic in 2016. Of those, 28.9% were 'bad bots', including 'impersonators', 'scrapers', 'spammers' and 'hacker tools'.[38]

36 Darrell M West, Jack Karsten, 'Inside the social media echo chamber', *Brookings*, 9 December 2016, online.

37 Juan Echeverria, Shi Zhou, *The 'Star Wars' botnet with >350k bots*, University College London, 10 January 2017, online

38 Imperva Incapsula, *Bot traffic report 2016*, online.

Bots aren't an inherently negative technology; some, such as @GoogleFacts, can be used to propagate innocuous information.[39] However, if left unchecked, their powers for immense volume creation can warp important public debates online. The coordination of botnets' automated traffic can dupe the algorithms of Facebook, Google and Twitter that quantitatively determine trending topics or hashtags in a way that 'can help steer the larger conversation in media'.[40] This contaminates the public dialogue and misrepresents public opinion on a particular issue.

TROLLS

Techniques to give the online impression of consensus aren't limited to automated bots. Dedicated 'troll armies' of individuals employed to create masses of content are also used to shape the appearance of public opinion on social media. Since as early as 2013, there have been organised teams of trolls, or 'troll farms', working around the clock in Russia to 'flood forums and social networks at home and abroad with anti-Western and pro-Kremlin comments'.[41]

SOCIAL (MEDIA) DECISION-MAKING

Human beings are inherently social creatures: factors such as community consensus are strong influences on our decision-making based on our desire to conform. Neuroscientist Matthew Lieberman's studies have shown that the interaction between the social and decision-making elements of the human brain influences individuals' behaviour on social media, and that individuals are more likely to accept messages that promote social inclusiveness and reject those that would isolate them from their peers.[42] RAND has also demonstrated the link between the 'volume' of an idea and its persuasiveness, explaining the effectiveness of 'Russia's "firehose of falsehood" propaganda model'.[43] A targeted use of bots can create the illusion of popularity for controversial ideas or candidates. Combined with the echo chamber phenomenon, this can foster an increasingly extreme and convinced viewpoint among social media users, whether the information is true or not. In this way, the collective allure of social media's artificial consensus can push uncertain individuals off the fence, posing a threat to the integrity of objective electoral decision-making.

ARTIFICIAL CONSENSUS IN THE US ELECTION

The role of social media automation in the 2016 US presidential election was 'unprecedented'.[44] Both candidates were supported at least in part by the voices of bot accounts. Trump relied most heavily on this technology: more than one-third of pro-Trump tweets were automated, while Clinton's tweets were bots almost a fifth of the time.[45]

For this reason, the reliability of online polling was compromised. An automated pro-Trump bombardment was used to sway polling done by institutions such as *Time*, *Fortune* and *CNBC* to give the result that Trump won the first presidential debate in September.[46]

During the campaign, Russian botmasters worked to amplify the profile of pro-Trump information and narratives through automation, while other individuals were employed as 'trolls' to post and comment on content that undermined Clinton online.[47]

39 GoogleFacts, *Twitter*, online.

40 Chris Zapone, 'Fake news: why the West is blind to Russia's propaganda today', *Sydney Morning Herald*, 31 January 2017, online.

41 Shaun Walker, 'Salutin' Putin: inside a Russian troll house', *The Guardian*, 2 April 2015, online.

42 Patrick Tucker, 'Why fake news spreads: a neurological explanation', *Defense One*, 23 March 2017, online.

43 Christopher Paul, Miriam Matthews, *The Russian 'firehose of falsehood' propaganda model: why it might work and options to counter it*, RAND Corporation, 2016, online.

44 Douglas Guilbeault, Samuel Woolley, 'How Twitter bots are shaping the election', *The Atlantic*, 1 November 2016, online.

45 Guilbeault & Woolley, 'How Twitter bots are shaping the election'.

46 Andrew Couts, Austin Powell, '4chan and Reddit bombarded debate polls to declare Trump the winner', *The Daily Dot*, 27 September 2016, online; Donald Trump, Tweet, 26 September 2016, online.

47 Stone & Gordon, 'FBI's Russian-influence probe includes a look at Breitbart, InfoWars news sites'.

ELECTION SECURITY: HISTORY AND FUTURE

NOT A NEW PROBLEM

Russia's influence operation in the US election has been seen as a watershed moment. Former acting head of the Central Intelligence Agency (CIA), Michael Morell, described the scenario as 'the political equivalent of 9/11'.[48] However, this was neither the first time a government has made efforts to sway elections in another country, nor the first time propaganda or strategically disclosed information has been used to achieve a particular outcome.

Interference in the domestic affairs of other states is an age-old pastime of great powers. Ironically, US history provides a rich precedent for election influencing. The CIA was notoriously active in shaping the outcome of democratic processes and undermining governments around the world during the second half of the 20th century, predominantly in Europe and Latin America. Key examples include the Italian general election in 1948, the installation of the Shah in Iran in 1953 and the 1954 Guatemalan coup.[49] In fact, new research indicates that, between the two of them, the US and USSR/Russia meddled in a staggering 117 elections between 1946 and 2000.[50]

The strategic value of compromising information isn't a new revelation, either. The use of information to harm the reputation of a specific target is an age-old tactic. There's a dedicated Russian word for information that can be leveraged to damage reputations and influence events: *kompromat*.[51] Similarly, the Chinese concept of 'internet terror' denotes the new level of accountability that local officials face now that information revealed online can be used to damage their reputations.[52]

In this sense, Russia's influence operations in the US election don't represent a whole new strategy, but old tricks achieved by different means. However, the differentiating factor is how cyber operations have made such interference much more effective. Modern technology has enabled the execution of this sort of campaign at a scale and scope previously unseen. It could be argued that the nature of social media also means that the information, whether disinformation or *kompromat*, can become self-propagating and self-sustaining in ways that traditional propaganda never was.

Russia's pursuit of this approach reflects what's been referred to as the 'Gerasimov doctrine', named after General Valery V Gerasimov, who stated that 'the role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.'[53]

In no way does this precedent mean that the strategy is acceptable. However, understanding the phenomenon of election security in its historical context and distinguishing between unacceptable and exceptional events *are* helpful in formulating policy responses.

48 Michael Morell, Suzanne Kelly, 'Fmr CIA Acting Dir. Michael Morell: "This is the political equivalent of 9/11"', *The Cipher Brief*, 11 December 2016, online.

49 Kaetan Mistry, 'Re-thinking American intervention in the 1948 Italian election: beyond a success-failure dichotomy', *Modern Italy*, 2011, 16(2): 179-194, online; Saeed Kamali Dehghan, Richard Norton Taylor, 'CIA admits role in 1953 Iranian coup', *The Guardian*, 19 August 2013, online; Kate Doyle, Peter Kornbluh, 'CIA and assassinations : the Guatemala 1954 documents', *The National Security Archive*, online.

50 Ishaan Tharoor, 'The long history of US interfering with elections elsewhere', *Washington Post*, 13 October 2016, online.

51 Amanda Taub, 'DNC hack raises a frightened question: what's next?', *New York Times*, 29 July 2016, online.

52 'China's internet: a giant cage', *The Economist*, 6 April 2013, online.

53 Neil MacFarquhar, 'A powerful Russian weapon: the spread of false stories', *New York Times*, 28 August 2016, online.

THE NEW NORMAL

Regrettably, evidence suggests that the targeting of the US presidential election by malicious cyber actors wasn't an isolated blip on the radar of international affairs. Russia's election influence operation was deemed by National Security Agency and Cyber Command head Admiral Michael Rogers to have been 'wildly successful', and looks likely to be a significant milestone on the road to a confronting new normal in contemporary election security.[54]

This concern has spread across Europe, before a wave of upcoming general elections on the continent in 2017. The UK is undertaking an inquiry into 'National Security in a Digital World' before its election on 8 June 2017.[55] The head of Germany's domestic intelligence agency, Hans-Georg Maassen, warned in December 2016 of an increase in disinformation and cyber operations targeting 'German government officials, members of parliament and employees of democratic parties' in the run-up to the country's federal elections.[56] The threat didn't dissipate, and Maassen announced that 'large amounts of data' had been stolen in a breach of the Bundestag during May 2017.[57]

France's May 2017 election was clearly in the firing line. Cybersecurity firm TrendMicro revealed evidence that a malicious hacking group known as 'Fancy Bear' (or Pawn Storm), which targeted the DNC in the US, had been going after the emails of moderate candidate Emmanuel Macron.[58] Shortly before the election, emails from Macron's campaign were leaked online in a last-ditch attempt to undermine the centrist candidate—an action that Macron's campaign said 'put the vital interests of democracy in jeopardy'.[59]

Some private-sector companies are stepping up to support governments to deal with this challenge. Google and its sister company, Jigsaw, have released a suite of cybersecurity tools called Protect Your Election.[60] The technology behind the announcement isn't new, but what's groundbreaking is that these tools are being offered for free on an application basis to news organisations, human rights groups and election monitoring sites to protect the integrity of democratic processes. It's hoped that tools such as Project Shield, Password Alert and 2-Step Verification will help ensure information access and accuracy in the lead-up to elections this year.[61] Facebook also took it upon itself to educate British citizens on how to spot fake news in the lead-up to the June 2017 UK general election by taking out full-page adverts in a variety of British newspapers.[62]

However, there are also areas of growing friction between government and industry on this issue. Germany is considering legislation that makes social media companies responsible for monitoring and removing hate speech and fake news from their platforms, threatening fines of up to €50 million for failure to comply.[63] The debate over how to simultaneously defend freedom of speech and prevent the spread of fake news is likely to intensify in liberal democracies in the near term.

54 Scott Malone, 'Russian election hacking "wildly successful" in creating discord: former US lawmaker', *Reuters*, 3 May 2017, online.

55 Joint Committee on the National Security Strategy, 'Cyber security: UK National Security in a Digital World inquiry', online.

56 'Germany sees rise in Russian propaganda, cyber attacks', *Reuters*, 9 December 2016, online.

57 Andrea Shalal, 'Germany challenges Russia over alleged cyberattacks', *Reuters*, 4 May 2017, online.

58 Feike Hacquebord, 'Two years of Pawn Storm: examining an increasingly relevant threat', *Trend Micro,* April 2017, online.

59 Nick Miller, '"Democratic shipwreck" as Emmanuel Macron emails leaked before poll', *Sydney Morning Herald*, 7 May 2017, online.

60 Jigsaw & Google, 'Protect your election', online.

61 Lily Hay Newman, 'A cybersecurity arsenal that'll help "protect your election"', *Wired*, 21 March 2017, online.

62 James Vincent, 'Facebook tells UK users how to spot fake news in full-page print ads', *The Verge*, 8 May 2017, online.

63 Stegan Nicola, Brigit Jennen, 'Germany gets really serious about fake news on Facebook', *Bloomberg*, 5 April 2017, online.

ELECTION SECURITY POLICY CONSIDERATIONS FOR DEMOCRACIES

This multifaceted vulnerability isn't going to disappear overnight, and it's a challenge that all modern democracies should consider and address. While every national context is different, several high-level policy considerations need to be taken up in all democracies. The framework put forward in this report includes several key recommendations on election cybersecurity and information security.

CYBERSECURITY OF ELECTION INFRASTRUCTURE

- **Reconceptualise critical national infrastructure to include election systems.** US Secretary of Homeland Security Jeh Johnson added election systems to the 'government facilities' critical infrastructure sectors list in January 2017.[64] While this is only a conceptual change, it affords the systems a level of significance that justifies federal oversight and greater response options should a system become compromised.
- **Improve the cybersecurity of existing election systems.** Invest in improving the cybersecurity of existing systems and demonstrate vigilance with necessary updates.
- **Prioritise security when considering expanding the digital elements of the election process.** Pause for thought about how much to digitise, how quickly, and the role of traditional recording methods to retain verification assurance.
- **Increase public awareness of election cybersecurity measures.** Develop a dedicated communications strategy to elevate and sustain public confidence in the security of the system. Convincing the public that an election is secure is just as important as making the election secure.

INFORMATION SECURITY OF ELECTION CAMPAIGNS

- **Increase dialogue with private sector.** Support and incentivise industry innovations, such as fact-checking technology that helps prevent the spread of fake news and overcome the artificial consensus factor in social media.
- **Bring political organisations into the tent.** While not directly part of government, political parties hold sensitive information that makes them targets for those hoping to influence an election through targeted disclosures. Educating and supporting the cybersecurity of political organisations is a step towards national election security.
- **Consider whether existing legislation is sufficient to cover election security concerns.** Developing clarity on the distribution of responsibility for election security will improve national understanding and coordination. For example, how responsible, if at all, are social media companies for the content disseminated on their platforms?
- **Educate the public on identifying reliable information sources.** Work with the private sector to ensure that citizens are equipped with the necessary knowledge to protect them from the influence of information operations.

NORMATIVE RESPONSES

- **Share election security threat information with international partners.** Inform allies about threats to election infrastructure to generate greater collective situational awareness.
- **Communicate best practice ways of responsibly managing election information flows.** Liberal democracies have a shared interest in securing the integrity of elections without suppressing freedom of speech and the openness of the internet.
- **Prepare a suite of policy responses.** Consider different potential election interference scenarios and prepare proportionate diplomatic responses that the government would take in each. For example, does election interference ever become an international act of force and, if so, when?

64 Department of Homeland Security, 'Statement by Secretary Jeh Johnson on the designation of election infrastructure as a critical infrastructure subsector', 6 January 2017, online.

ACRONYMS AND ABBREVIATIONS

CIA	Central Intelligence Agency
DNC	Democratic National Committee
DRE	direct recording electronic
FBI	Federal Bureau of Investigation

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au
facebook.com/ASPI.com
@ASPI_ICPC
https://www.aspi.org.au/icpc/home


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE