Routledge
Taylor & Francis Group

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Countering foreign interference: election integrity lessons for liberal democracies

Adam Henschke, Matthew Sussex & Courteney O'Connor

To cite this article: Adam Henschke, Matthew Sussex & Courteney O'Connor (2020) Countering foreign interference: election integrity lessons for liberal democracies, Journal of Cyber Policy, 5:2, 180-198, DOI: 10.1080/23738871.2020.1797136

To link to this article: https://doi.org/10.1080/23738871.2020.1797136

Published online: 28 Jul 2020.

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 2, 180–198
https://doi.org/10.1080/23738871.2020.1797136

Routledge
Taylor & Francis Group

OPEN ACCESS

Countering foreign interference: election integrity lessons for liberal democracies

Adam Henschke, Matthew Sussex and Courteney O'Connor

College of Asia and the Pacific, National Security College, Australian National University, Canberra, Australia

ABSTRACT

Liberal democracies and their allies are facing a generational challenge from increased and evolving efforts by foreign actors to undermine public trust and degrade democracy. This article examines the problem of foreign interference with particular reference to the US midterm elections of 2018 as a case study, to draw potential lessons for liberal democracies in advance of future democratic processes. These lessons are centred upon five vulnerabilities to malicious actors, which – if exploited, either partly or wholly – can potentially degrade a democratic political system. The five vulnerabilities incorporate democratic institutions, election infrastructure and private industry. They also include individuals, and the core ideas that underpin democratic norms and values. We call these the 'Five Is'. The paper outlines the challenges facing the integrity of elections for liberal democracies and fills out the concept of the 'Five Is'. We note that the 'Five Is' are causally linked and overlapping. Having discussed the 'Five Is', we then look at the US 2018 midterms as a way to clarify and specify the 'Five Is' in practice. The paper then offers eight recommendations for policymakers to increase the resilience of electoral processes to such threats and attacks.

ARTICLE HISTORY
Received 4 November 2019
Revised 20 February 2020
Accepted 15 May 2020

KEYWORDS
Election integrity; cybersecurity; foreign interference; liberal democracies

Increased and evolving efforts by foreign actors to undermine public trust and degrade democracy are creating a generational challenge to liberal democracies and their allies. Recent history provides numerous examples of hostile interference: the US 2016 presidential election (CNN Library 2019; Masters 2018; Yourish, Buchanan, and Watkins 2018); the 2018 US midterms (Gerstein 2018; Goldman 2018; Seligman 2018); the 2016 Brexit referendum (House of Commons Digital, Culture, Media and Sport Committee 2019; Field and Wright 2018; Wintour 2018; Seligman 2018); elections in France and Germany (Brattberg and Maurer 2018; Conley and Vilmer 2018; Greenberg 2017; Reinbold 2017; Stelzenmüller 2017); increased social unrest in France and Spain (Dalton 2018; Martineau 2018; Matlack and Williams 2018; Committee on Foreign Relations United States Senate n.d.; Palmer 2017; Wintour 2019); and attacks on Australian political infrastructure (Remeikis 2019; Westcott 2019; Wroe and Uhlmann 2019). Parallel to this is the increased interest in, and public concern about, political instability. One study of the media search engine, Factiva, saw that there were more articles

CONTACT Adam Henschke adam.henschke@anu.edu.au

published on 'the threat to democracy' in the period 2010–2018 than there were in the period 1970–2010. In public discourse the notion that democracy is now fundamentally threatened has arisen again after being dormant for at least 40 years. The Economist Intelligence Unit's annual democracy index finds that in 2019, 'the average global score has fallen from 5.48 in 2018, to 5.44. This is the worst average global score since The Economist Intelligence Unit first produced the Democracy Index in 2006' (Economist Intelligence Unit 2019). Parallel to this, public trust in government is in significant decline. 'For example, in 1958, 73% of Americans reported that they trusted their government at least most of the time; by 2019, that percentage had fallen to 17%' (Buell, Porter, and Norton 2019).

This article examines the problem of foreign interference with particular reference to the US midterm elections of 2018 as a case study, to draw potential lessons for liberal democracies in advance of future democratic processes. In doing so, we do not claim to identify all threats stemming from foreign interference to democracies. Nor are we seeking to offer a deep theoretical analysis as a way to conceptually triage the burgeoning literature on the topic. Rather, the article attempts to develop a practical policy framework whereby some of the more potent challenges associated with foreign interference might be understood by practitioners in democratic nations. In seeking to define the magnitude of the problem, the article then attempts to identify some potential solutions.

The lessons we identify are centred upon five vulnerabilities, which – if exploited either partly or collectively – can potentially degrade a democratic political system. The five vulnerabilities incorporate democratic *institutions*, election *infrastructure* and private *industry*. They also include *individuals* and the core *ideas* that underpin democratic norms and values. At the end of this paper we offer some specific prescriptions to address each of these vulnerabilities. Some are public-facing, while others are best conducted by agencies. In presenting our findings we stress that democracies face the most danger from foreign influence campaigns in the cybersphere, *via* disinformation and misinformation targeting individual voters or social groupings. Given difficulties around information assurance and election integrity, the most efficient way forward is to encourage resilience in the structures and processes underpinning democratic electoral processes, including the voting community. And further research on our identified vulnerabilities will help us to recognise when these vulnerabilities are under attack, to respond to the particular threat event, and to learn from experience to mitigate and reduce the impacts of such events into the future.

We also need expertise in order to ascertain the extent to which each of the vulnerabilities may affect democratic processes in future, as well as how each one interacts with, and may affect, the others. This is important given that, in order to build and maintain robust democratic systems, we will need a strong and independent evidence base to develop community engagement guidelines aimed at promoting social coherence and resilience.

The scope of the challenge

It is mistaken to assume that liberal democracies are somehow inherently enduring. Democracies are said to produce robust societies, but they are not immutable. Being open and free, democracies depend on debate, transparency, multiple ways of expressing preferences and multiple sources of information. But in doing so, they also rely significantly on trust and accountability (Diamond and Morlino 2004). With public confidence and trust in core democratic institutions and ideas declining across the West, the potential for hostile foreign actors to exploit existing vulnerabilities and pressure points is enhanced (Chua 2018; Deudney and John Ikenberry 2018). Yet paradoxically, some of the potential vulnerabilities of democracies are also some of their chief sources of resilience.

As with democracies like the US, the UK and EU member states, the challenge to liberal democracies from foreign actors is being significantly assisted by the evolution of a range of disruptive technologies (Brechenmacher 2018). In a data-rich environment, the size, speed, diversity and potential unreliability of information – not to mention the fact that anyone can disseminate and share it – leads to a plethora of information sources that can be manipulated. This is often referred to as the 'Five Vs' of big data: volume, velocity, variety, veracity and value (BBVA 2017; Marr 2014).

Addressing this problem with conventional practical measures is difficult. While it is customary to distinguish between *foreign influence* (activities that may be unwelcome but are nonetheless legal) and *foreign interference* (activities that violate the law), such distinctions are unhelpful outside a strict regulatory context. This is because hostile actors can use both influence and interference efforts to undermine democratic processes. As the 2016 US presidential election demonstrated, influence activities can pose as many challenges to democracies as those that cross over into illegal practices (Blank 2017; Brattberg and Maurer 2018). The repercussions of the Russian influence over, and interference in, the 2016 presidential elections affected not only the attitudes toward, and concerns surrounding, the 2018 midterm elections in the United States, but general trust in the integrity of democratic institutions (Morgan 2018). Hostile actors are also well aware of the grey spaces between legal influence and illegal interference and adapt their approaches accordingly through the use of proxies, viral mechanisms and other tactics with varying degrees of plausible deniability (Schmitt 2017).

Viewed in this way, foreign influence covers a number of challenges – from espionage and information operations, all the way through to interference in elections. And depending on where one concentrates attention in the scholarly literature, it is possible to identify a complex web of state, non-state and commercial players who participate in acts that are complex in themselves: misinformation, disinformation, hybrid war, information operations, psychological operations, computational propaganda and political war (Jack 2017). Indeed, whereas the motives for such activities might be political influence or financial gain, online technology that allows messaging to strategic populations is a common enabler. What has been called 'cyber-enabled information warfare' (Lin 2019) allows hostile actors to manipulate traditional and social media using automated bots (Rizoiu et al. 2018) and trolls to shape public opinion and electoral results (Woolley and Howard 2019).[1] Hence, while foreign influence is not new, many more actors – either large or small – are now better able to exploit domestic discourses and processes in democratic countries.

Foreign interference and influence are also regularly developed with local rules in mind. Indeed, in the example of the 2016 US presidential election, the 'lawfare' undertaken in that case demonstrates that legal activities can have even wider-reaching implications than foreign interference strategies that are illegal (Brattberg and Maurer 2018). Given that proxy networks, viral dissemination of information and citizen curation of information increase the distance between the external state agent and its transmission belts, it is difficult to establish direct culpability (Golovchenko, Hartmann, and Adler-Nissen 2018).[2] This makes public attribution difficult, and therefore hard to punish.

Here we can potentially differentiate between foreign interference and foreign influence in terms of how each type of activity affects the political process. For instance, efforts to deliberately change the calculus of political elites are highly targeted, in contradistinction to broader information campaigns that seek to gradually alter the perceptions of citizens, policy elites or powerful stakeholders, like businesses and other influential constituencies, in civil society over time. In this way, giving incentives to politicians through inducements (or even the implied threat of releasing compromising information) is a direct form of *interference*, even though it may not be illegal.[3] So too is tampering with election results, because this directly and negatively affects voting integrity. Conversely, activities like seeking to shape curricula in tertiary institutions, performing propaganda and messaging campaigns to influence specific sections of the population, or backing lobby groups in their attempts to bring about political change, are a longer-term form of *influence*. Of course, each of these can be damaging to liberal democracies. But in framing interference and influence activities in terms of their targets and objectives, we can potentially shed more light on how policymakers might understand the problem of foreign influence, as opposed to interference, and at the same time to assess how effective – in terms of the specific vulnerabilities each state faces – the available suite of countermeasures might be.

This means that foreign interference – as defined here – also reaches well beyond a *voting security* threat, which can be defined as a disruption or distortion of voting processes through electronic or more conventional means, such as ballot-rigging (Smith 2013). Instead it becomes an *election integrity* challenge, potentially encompassing all aspects of a democratic nation's politics, society and economy. Nations with well-developed capabilities in the manipulation of information, such as the Russian Federation and the People's Republic of China, can now reach into democratic societies to conduct information warfare operations directly against a population (Brattberg and Maurer 2018).

Doing so is not only relatively simple, given the array of digital media in the ecosystem, but also cheap. During the 2016 US presidential elections, Russia's Internet Research Agency was able to reach an estimated 120 million Americans with targeted Facebook advertisements that cost only a little over US$100,000 (Solon 2018). And although these may have been the least successful aspect of Russian disinformation, the overall US $1.25 million per month that Russia's Internet Research Agency received from Kremlin confidante, Yevgeny Prigozhin's Concord Management and Catering groups, to hijack identities and act as a troll farm, suggests that the operation was extraordinary value for money (Tamkin 2018). Indeed, in the weeks prior to that election, public engagements with digital fake news stories actually exceeded engagement with news from mainstream media outlets (Lee 2016; Price 2016).

Protecting democratic elections from such interference is therefore a critical national security policy challenge. We will need to envisage a future 'information conflict environment' in which hostile actors seek to attack our core institutions, carry out intrusions into data repositories, manipulate information and compromise our critical infrastructure. Our responses will need to reflect a whole-of-society approach, seeking to turn our democracy's vulnerabilities into sources of resilience. Fundamentally, the common element in all these arenas is ensuring that we encourage public trust: not only by having secure systems and infrastructure, but also by encouraging debate that is linked to evidence and fact. While it is important in certain cases to maintain secrecy surrounding specific events and capabilities in the interests of national security, we must recognise that, to acquire and maintain public trust, it is essential to keep the public informed as a key duty of effective public policy.

How do we ensure that our elections are free and open, whilst assuring voters of the integrity of the processes and outcomes? What are the main challenges that we can pre-emptively address, and what lessons can we learn from the experiences of other nations? To answer these questions, we identify five pressure points central to election security, before turning to the 2018 US midterm election as a case study in foreign interference. While we acknowledge the differences between liberal democracies, in the remainder of this article we nonetheless identify some important common lessons.

The 'Five is' of foreign interference

Institutions

The *institutions* of democracy can be either formal or informal, but typically include components that have both a physical presence as well as functions, norms and practices that endure beyond those who make up its workforce at any given time. Thus, the term covers the agencies and departments responsible for carrying out the work of government, as well as the parliament, the judiciary and the media. Serving as both the architecture of a democracy, as well as the places where its main principles are put into practice, institutions are vulnerable to an array of potential attacks (Rid and Buchanan 2018). This includes, for instance, the 2019 hack on Australia's Parliament House, which reportedly targeted email and other data systems (Remeikis 2019; Westcott 2019; Wroe and Uhlmann 2019). But it can also include viral public campaigns to undermine trust in elections, as well as the judiciary. Foreign agents themselves are not the only potential culprits here. For instance, Donald Trump noted on numerous occasions in 2016 that he might not accept the result of the presidential election unless he was the victor (Gambino 2016; Johnson 2016; Lewis, Jacobs, and Siddiqui 2016; Nelson 2016).[4] Attacks on court judgments on the grounds that they are biased or unfair, or attacks on individual judges, are all activities that undermine trust in institutions. Likewise, notions such as 'fake news' undermine the media and degrade public trust in the very idea of shared truths.[5] Given that institutions are large and complex, and hence often inscrutable, attacks on them often have broader, whole-of-society effects than attacks against individuals.

Infrastructure

Democratic *infrastructure* differs from institutions in that it is often highly automated and comprised of systems (rather than humans) performing key tasks. In critical infrastructure, there are often many commonalities between nations, depending on how supply chains are regulated and the extent to which agencies and private companies are responsible for maintaining data security. But this can also be highly variable across democracies. In the US, a plethora of different companies, organisations and processes at local, state and federal levels are all stakeholders in the voting process (National Conference of State Legislatures 2020; Pastor 2014). By contrast, voting infrastructure in Australia – the process of conducting elections, tallying votes and certifying results – is highly centralised *via* the Australian Electoral Commission (AEC) (Australian Electoral Commission 2019a; 2019b).

This leads to a fundamentally different calculus for assessing risk in each case: in the US there are multiple points of vulnerability, while Australia has a main point of vulnerability. And, in the case of data breaches or manipulation, these are frequently traceable and identifiable. Yet this also demonstrates how democracy's pressure points are interlinked: to attack a nation's institutions, for instance, it is often most convenient to attack its infrastructure.

Industry

Private, for-profit *industry* is both crucial to the health of a democracy's economy as well as a source of much of its ability to innovate and prosper in a globalised marketplace. However, the security of personal data has become a chief threat that requires urgent attention. Industries and companies that collect personal data (including those who collect data as a public good, such as census data, for instance) are at risk of having that data manipulated or stolen, or access to their platforms compromised. The role of private, for-profit companies like Facebook in ongoing election integrity, how they work with governments, and what oversight processes can be introduced whilst maintaining their independence from political interference, presents a complex, evolving relationship that frequently relies on trust between government and industry (Gordon 2019; Lomas 2019; Paul 2019; Rodriguez 2019; Rosen et al. 2018). But because it is responsive (and susceptible) to market forces, industry often has different sets of interests, incentives and obligations in comparison to democratic institutions. And since industry can be self-regulating, or less closely regulated in order to encourage competition, it tends to be less transparent or accountable than other aspects of democracies. This, too, leads to potential threats in a voting and election security context. Industrial espionage that successfully steals a patent from a mining company, for example, would undermine trust in a core national industry in addition to its ability to compete with others, with real implications for its standing and its shareholders.[6]

Individuals

Central to any democracy are its *individuals*. These make up a democracy's voting population, its workforce, the public servants and the nation's political leaders. With political power in democratic nations coming from the ballot box, individuals are vital causal actors, independently and as blocs and coalitions. More than any other category identified in this paper, though, individuals act on a complex set of beliefs, incentives and motivations. They are therefore the hearts, as well as the minds, of a democracy. This makes them especially vulnerable points for the integrity of elections. Distortions of fact, and false or misleading information, can potentially have a significant effect on political outcomes. Here, hostile actors can seek to nudge fringe ideas towards the political centre, undermine specific parties or candidates in the eyes of the electorate, or tarnish trust in core democratic institutions (Rid and Buchanan 2018). The success of firms such as Cambridge Analytica is testament to the ability of today's digitally aware voter to be manipulated through appeals to tribalism and emotion (Chua 2018; Guardian 2019). In a 'post-truth' age, forces like tribalism and emotion can be more powerful than appeals to facts and reason.

We draw attention to the importance of political leaders here, in their capacity to set, evolve or undermine standards of behaviour that impact democratic resilience. Any effective response will require a whole-of-government approach. And this approach must include efforts to educate political leaders in how they can be threat vectors and victims, as well as a safeguard for resilience. Any approach here would need to be bipartisan, and to actively and equally engage with government and opposition. For education to have true social reach, this effort should also include key community leaders.

Ideas

Equally important to a democracy's institutions and its individuals are its core *ideas*, which underpin a democracy's legitimacy. Ideas reflect how a concept like democracy is understood (as a system of belief), as well as how it is used (as a system of motivations for representing voter's preferences). We could not answer the question, 'Why does someone vote the way they do?' without having some understanding of that person's ideas. Crucially, ideas can be realised in different ways, which makes them vulnerable to attack. In particular, they can undergo rapid change, where the basic part of the idea remains constant, but shifts occur in the context in which it applies. An example of this can be found in the ongoing and sustained efforts to undermine the integrity of the media. Insofar as good journalism is geared towards uncovering and expressing truth and facts, the long-term effect of repeated use of phrases like 'fake news' by political leaders is to degrade the very idea that there is a shared, objective truth (Anderson and Rainie 2017). Other examples can be found in state-sponsored campaigns by the Russian Federation marking the US as a warmonger with a foreign policy designed to dominate all others (Williams 2014), or in the PRC's numerous information campaigns around issues like human rights, or the historical sovereignty of the South China Sea (McDevitt 2017; Kuo 2018). Finally, we see the idea of elections themselves being vulnerable to public perceptions as attacks on electoral infrastructure 'undermine public trust in the election process' (Shackelford et al. 2017, 643) due to the problem that one cannot 'patch this psychological vulnerability' (Thomas Rid, quoted in Greenberg 2017).

The 'Five Is' of foreign interference are causally linked and overlapping. Presenting the threat in this way encourages policymakers to think about each threat arena as a distinct vulnerability, but also to consider what effect a potential policy response might have in other arenas. It can be visualised thus:

Figure 1 In presenting threats to democracy as the 'Five Is' of foreign interference, we do not claim to capture all potential challenges to elections, or to democracy. Nor do we intend it to represent an academic thought experiment. Rather, we believe it is a useful model for practical policy responses to a very complex problem. In other words, by better understanding some of the key vulnerabilities that democracies face, we will be better placed to develop countermeasures to ensure our democracy is resilient to these challenges in the future. One of the chief examples of this was the interference in the 2018 US midterm elections. Which vectors were targeted? How did they interact with others? What was the overall effect? And, crucially, what can we learn from them? It is to this issue that we now turn.

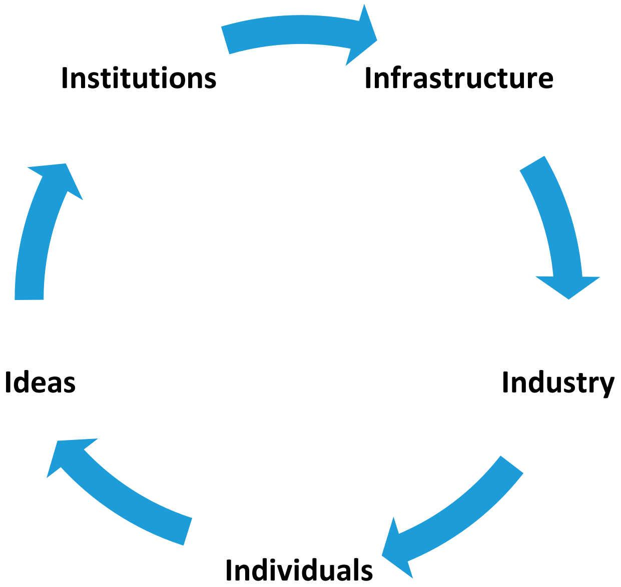

Figure 1. 'Five Is' of foreign interference.

The 'Five is' and the 2018 US midterm election

Institutions

Voting is an integral institution of the democratic political process, and following the controversial 2016 US presidential election, the electoral process suffered a loss of public trust (Pope 2018). In the 2018 midterm election, the state of Florida – in particular Broward County – undertook vote recounts and legal battles concerning the outcome. Importantly, trust in those processes and the election outcome was not displayed by Republicans, Democrats, or even by the White House (Durkin 2018; Thrush and Peters 2018). The contravening information surrounding those processes from these three entities further politicised the interference issue in the domestic context and reduced public faith in the integrity of the electoral process, the fundamental democratic institution. The effect on the public was potentially further exacerbated by the ongoing Russian disinformation and social media influence campaign, as outlined in a criminal complaint laid against a Russian national by the US Department of Justice (2018b). Despite concerns regarding the security of electoral institutions during and following the 2016 US presidential election, and an investigation of more than two years' duration into Russian interference by the Senate Select Committee on Intelligence (Samuelsohn 2019), it appears that no significant improvement has been made to further secure electoral institutions in the United States or to repair public trust in the same (Zetter 2018b).

A key lesson for liberal democracies here, is that social media campaigns alluding to the illegitimate nature of voting may be foreign disinformation efforts – or at least assisted by them. This can occur in certain areas, focus on encouraging certain (minority) groups among the voting citizenry not to vote, or can take the form of strident and persistent voices which question the legitimacy of the outcome. A key potential marker for foreign influence or interference can be found in relatively new social media accounts, those that post solely political content, or those whose content has changed significantly. To address this vulnerability prior to elections, first and foremost, an organisation should be identified created to oversee and coordinate intelligence on threats and nationwide responses (**Recommendation 1**). Next, an education and positive messaging campaign around voting (**Recommendation 2**) would be useful. Ideally this would involve both relevant electoral oversight bodies (where such bodies exist) and civil society leaders to potentially reduce the negative effect of such disinformation tactics. A particularly important task here concerns post-election audits, where suspected and reported cases of interference can be investigated objectively, especially in elections with disputed outcomes.

Infrastructure

In the lead-up to the 2018 US midterms, concerns were articulated about the relative security of electronic voting machines, some of which are known to have remote access control software installed (Hay Newman 2018; Zetter 2018a). Officials admitted that there had been a number of phishing and DDoS attacks, some of which seem to have targeted election software and hardware manufacturers, whose equipment is in use in counties throughout the United States (Hay Newman 2018). At the other end of the spectrum, centralisation of voting in nations like Australia both reduces the vulnerabilities of a more diffused electoral system, such as in the US, but also presents a larger target at which hostile parties can aim. In parallel to the lack of increased securing of electoral institutions and public trust in those institutions, election infrastructure in the United States remained vulnerable to hostile parties prior to, and throughout, the midterms in 2018, having retained the pre-existing hardware, software and policies utilised in 2016 (Zetter 2018b). Moves have been made following the 2018 midterms to overhaul election systems in several US states, but it remains to be seen whether those new systems will increase or decrease the security and integrity of election infrastructure (Pratt and Undark 2019).

A thorough review of both hardware and software involved in voting specifically, and electoral processes generally, should be undertaken in order to ensure the greatest level of resilience possible in future elections. But a significant element here would also focus on training staff associated with elections (**Recommendation 3**), including but not limited to officials overseeing voting processes, so that they are aware of and able to respond to potential influence or interference. This will need to be undertaken on a recurring basis, at both national and local levels, as regional elections might pose an opportunity for foreign agents to test new methods in advance of federal elections, and *vice versa*.

Industry

Facebook has been the subject of scrutiny for its involvement in the diffusion of misinformation and disinformation during elections as a distributional social media platform with comparatively little regulatory control of content. Russian actors posing as Americans, and utilising a variety of personas with disparate political persuasions, attempted to affect domestic political opinion on certain issues or candidates through advertising and support of domestic political groups during both the 2016 and 2018 elections in the United States (US Department of Justice 2018a). One such campaign was discovered, shut down and announced by Facebook in the lead-up to the 2018 midterms. It was described as a 'sophisticated disinformation operation … that engaged in divisive messaging', with evidence of adaptive tactics by the operators and use of proxies to purchase advertising (Dwoskin and Romm 2018).

All nations with democratic political systems need to engage in education and awareness programmes with the domestic populace that will provide voters with the tools to identify potential influence and interference campaigns. Moreover, given that many of these events occur in or through cyberspace, and that much of the relevant architecture involves private industry, governments must develop and maintain cooperative working relationships with key industry players (**Recommendation 4**) to ensure that both parties can and should trust each other with what could be, at times, extremely sensitive information.

Individuals

Individuals in specific social groups are also targets for foreign influence and interference operations. In the lead-up to the 2018 US midterms, Russian operators posing as Americans delivered election-related material designed to affect and influence, for example, African-Americans, by implying that, since there were no ideal candidates for their interests, they should either not vote or vote for a third-party candidate unlikely to win. In addition, Democratic campaigns during the midterm were subject to ongoing cyber interference campaigns designed to gather intelligence, spread disinformation, degrade trust and potentially steal campaign funds (Wofford 2018).

What is particularly relevant for liberal democracies around the world is that many of those targeted in the 2018 midterms were legitimate US citizens, voicing legitimate beliefs and concerns about the US democratic processes and outcomes. We must therefore be vigilant about ways in which foreign actors can seek to exploit those within liberal democracies, to encourage and amplify what may be legitimate concerns, but in a way that degrades the integrity of the elections and overall democratic processes. Political leaders are of particular concern here as they already have large and, at times, motivated audiences. The role of foreign agents as covert funders of political campaigns, for instance, needs to be carefully monitored. But equally important is that politicians can unwittingly amplify ideas and material that are linked to foreign influence campaigns, and unintentionally cause further breakdowns in public trust. Accordingly, we propose that greater effort be devoted to helping political leaders identify at-risk behaviour, and to strive for a set of conduct-based 'red-lines' to avoid (**Recommendation 5**).

Ideas

Public trust in the idea of ballot integrity was also a source of discord in the 2018 US midterm elections, with accusations of double counting; suppression of legitimate mailed ballots; and discounting of valid ballots (Durkin 2018; Thrush and Peters 2018). Additionally, electoral commission and state election websites were the subject of ongoing DDoS attacks apparently meant to reduce trust in the idea of a secure election as it became clear that results were unavailable to either officials or the public (Wofford

2018). Following the information released about interference in the 2016 presidential elections and the concerns surrounding a fundamentally similar, and thus vulnerable, electoral process for the 2018 midterms, going forward, it is crucial to invest in not only the infrastructure, but also the idea that the result of an election is accurate and trustworthy.

Even nations that have compulsory voting and a centralised voting system with few opportunities to meddle with individual ballots are vulnerable to attacks on ideas. And like many other liberal democracies, there is a significant digital element to both voting and tallying, which, subject to a campaign of significant size and influence, could reduce public trust in the integrity of the ballot. It is important to provide information and education on potential interference to both the public service and the general public in order to reduce public discord in the event that an attack does occur. This could have two components. The first is to form a trusted experts group from civil society, academia, government and industry to identify challenges to election security and offer ways to mitigate these risks in future (**Recommendation 6**). Second, to achieve whole-of-government responsiveness to these challenges, there would need to be discussion about which organisation would be the best-placed to provide inter-agency monitoring and pre-emptive action to safeguard democratic ideas and ideals (**Recommendations 1 and 7**). While challenging, such an integrated and coordinated response is necessary.

Recommendations

In presenting our recommendations, we caution against a common response to threats from a national security paradigm: to draw on regulation as the most robust instrument of democracy. Regulation is a top-down and generally coercive instrument that can serve to further undermine public trust if it is not incorporated carefully alongside other measures. Instead, we suggest that forthcoming elections be used as a way to see which of the ‘Five Is’ of foreign interference are targeted; what means are used in this targeting; what the responses to these attacks are, and that intelligence and threat sharing across liberal democracies are strongly encouraged (**Recommendation 8**).

In order to achieve an end result where our democratic systems are resilient, we need a set of measures that ensure and assure the integrity of election outcomes. As the analysis above has demonstrated, the following recommendations should be considered as part of the broader whole-of-society challenge from hostile actors to degrade elections and democracy.

(1) Electoral operations should be centralised around the collation of foreign interference data. Where such a central organisation does not exist, funding needs to be increased to deal with these new roles, and effective training and staffing practices are engaged with in order to maximise resilience. We note here that in countries like the US, with the tradition of states having the authority over electoral processes, this may be socially and politically hard to achieve. ‘State policymakers are particularly concerned that federal efforts to secure the election process may invite further federal involvement in election activities that have traditionally been regulated on the state level’ (Shackelford et al. 2017, 644). However, ‘all fifty states accepting DHS assistance in identifying and repairing weaknesses in their election infrastructure by early

November 2016' (644-645). Moreover, presenting this centralisation as being concerned with combatting foreign interference, rather than a federal takeover of the state's electoral processes, might find more support.

(2) Positive messaging campaigns around voting security need to be undertaken. These would be centrally led by the relevant national electoral organisation, and enlist civil society champions to reinforce this message. Ryan Buell, Ethan Porter and Michael I. Norton call attention to what they call 'submerged state' and note that a lack of public awareness about what government services are being offered and being done well can lead to a decline in trust. They 'propose that the public's deteriorating relationship with government – manifested in declining levels of trust, support, and engagement – may arise in part from what is not publicly salient … we suggest that government increasing the transparency of its operations – literally, showing its work – can influence citizens' trust in and engagement with government' (Buell, Porter, and Norton 2019). Here we see a necessary connection between recommendations 1 and 2. Insofar as the threats posed by foreign interference gain greater publicity, and knowledge of the effectiveness of centralised responses increase through effective positive messaging campaigns, we would anticipate that that opposition and antipathy to some centralisation would decrease.

(3) Recurrent and adaptive staff training is needed to help prevent threats to voting infrastructure. We note here that recommendation matches recommendations 6.2 and 6.3 of the National Academies Of Sciences, Engineering and Medicine report, *Securing The Vote: Protecting America's Democracy,* which states that '[p]roper training of election administrators is a key component in ensuring well-run elections and in the mitigation of disruptions in the voting process' (National Academies Of Sciences Engineering Medicine 2018, 107). As such, they recommend that '[t]he U.S. Election Assistance Commission, with assistance from the national associations of state and local election administrators, should encourage, develop, and enhance information technology training programs to educate state and local technical staff on effective election administration' and that '[u]niversities and community colleges should increase efforts to design curricula that address the growing organisational management and information technology needs of the election community' (National Academies Of Sciences Engineering Medicine 2018, 10). The point here is that not only is training of local election administrators vital to ensure and assure the integrity of the outcomes, but that this training needs to extend beyond just those staff involved in processing and monitoring elections to engage with the voting community more generally.

(4) Strong engagement with key industry peak bodies and members as collaborative partners are needed, to both enable up-to-date monitoring and communication of emerging threats and trust between government and industry. Again, the recommendations in the *Securing The Vote* report provide a good starting point here, where recommendations 6.4–6.8 look at the need to secure the voting technology marketplace (National Academies Of Sciences Engineering Medicine 2018, 10). However, on the 'Five Is' approach, given the increased role of social media in foreign interference, industry must be seen in a broader way than just voting infrastructure. Moreover, by identifying individuals and ideas as further points of vulnerability, the relations between industry and the voting populace need to be included as part of industry engagement.

(5) Engagement with political leaders is needed to identify when and how they are at risk of being vectors or victims of manipulation and to develop 'red-lines' of behaviour that all political leaders can agree to. This follows Recommendations 2 and 3 – that education about threats must not only be wide-ranging, but deliberately engaged with key causal players in electoral processes. Political leaders are likely targets for foreign interference, both as individuals and as parts of institutions. Further, they must be made aware of how actions that may bring them short-term political success can act to undermine the integrity of elections more generally. US President Trump's public statements about Hillary Clinton receiving 3–5 million illegal votes, for instance, are indicative of bad public behaviour. In these increasingly partisan political times, where politics is seen as a zero sum game, we consider this education of, and co-operation between, political leaders as essential to election integrity. This also goes to the ways that political leaders engage with the public more broadly about threats to election integrity. '[O]ur leaders must speak candidly and apolitically about threats to our election systems. Transparent communication about threats to the integrity of our elections is vital. Openness is the most effective antidote to cynicism and distrust' (National Academies Of Sciences Engineering Medicine 2018, xii). To put it simply, in representative democracies, the 'people must have confidence that their leaders place the larger interests of democracy above all else' (xii).

(6) Governments need to form Trusted Experts Groups (TEG), comprising qualified representatives from government, academia and civil society, to examine examples of challenges to election security and make recommendations on future actions. Here, again, we seek to extend the recommendations of the National Academies that universities and colleges and voting technology providers (National Academies Of Sciences Engineering Medicine 2018, 10) are engaged in the efforts to protect electoral integrity, to recommend a deeper and more formalised process where such engagements are long-lasting and ongoing.

(7) Governments need to form interagency working groups to identify threats, prioritise them, develop responses and assess the effectiveness of responses. 'The ensuing network of jurisdictions, competences and responsibilities is what makes a whole of government approach and interagency collaboration on cybersecurity in elections essential' (van der Staak and Wolf 2019, 25). Such cooperation is no easy task, as there 'may also be a need to mitigate misgivings or hostility regarding national-level oversight in local affairs' (van der Staak and Wolf 2019, 30). In decentralised contexts like the US, for example, 'a key role of interagency collaboration is often coordination and trust-building between local election administrations and a range of state-level agencies, from the national [electoral management bodies] to security agencies' (van der Staak and Wolf 2019, 30). As each nation has significant variation in how their elections are conducted and subjected to oversight and assurance, there is not a one-size-fits-all model for the composition and processes of interagency working groups. What we suggest is that, following the five points of vulnerability we have identified: institutions, infrastructure, industry, individuals and ideas, a comprehensive interagency response would look to ongoing knowledge about how foreign actors are targeting the 'Five Is', and determine which local agencies are the most appropriate to monitor the threats, respond to events and resolve the vulnerabilities.

(8) Liberal democracies and their allies should actively gather and share intelligence on threats to their democratic processes such that one nation's experience can be used to assist other nations. 'Information sharing is another important component of mitigating the risk to voting machines … These sharing centers provide a mechanism for stakeholders to share data on vulnerabilities and threats with one another to more quickly and effectively guard against emerging threats' (Shackelford et al. 2017, 664). Given their earlier discussion of the need for building minilateral cybernorms (Shackelford et al. 2017, 659-661), we understand the approach on information sharing to include international cooperation. However, as per our attention on the 'Five Is' as points of vulnerability, in contrast to Shackelford et al. (2017), we would extend the need for information sharing to go beyond vote hacking to the larger issues of election integrity.

Even several years ago, it would have seemed paranoid to suggest that liberal democracies were at risk of fraying or collapsing. Moreover, to propose that foreign actors could undermine the integrity of our elections through well-placed disinformation on social media would have seemed almost absurd. However, recent history shows that foreign actors are indeed making the attempts, and these attempts have had some success. In this paper we proposed that the 'Five Is' of institutions, infrastructure, industry, individuals and ideas, present five points of vulnerability for foreign interference. In an effort to increase their resilience in the structures and processes underpinning democratic electoral processes, we have presented eight recommendations. We also suggest that ongoing research into the identified vulnerabilities is needed to help us recognise when these vulnerabilities are under attack, to respond to the particular threat event and to learn from experience to mitigate and reduce the impacts of such events into the future.

Notes

[1] For a global survey of these efforts, See Samantha Bradshaw and Philip N. Howard, 'The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.' Working Paper, 19 September 2019. Oxford, UK: Project on Computational Propaganda https://comprop.oii.ox.ac.uk/research/cybertroops2019/

[2] On lawfare, see Mosquera and Dov Bachmann (2016).

[3] On this point, see Schmitt (2017).

[4] Trump stated in the final candidates' debate on 19 October 2016 that he would consider filing a legal challenge if candidate Clinton won and he felt the election was 'rigged against him' ('3rd Presidential Candidates' Debate' 2016).

[5] For an exploration on the effects of misinformation on trust, see Anderson and Rainie (2017).

[6] For example, articles released from 2015 onward trace the production of new Chinese stealth aircraft to a hack that captured technological data and blueprints on the technologies of the JF 35 fighter from Lockheed Martin, and then from an Australian contractor (Goldman 2017; Gady 2015).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by European Research Council [Grant Number Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies]; Australia research council [Grant Number DP180103439]; Australian Department Of Defence [Grant Number Strategic Policy Grants Program Category 1, 2019].

Notes on contributors

Adam Henschke is Senior Lecturer at the National Security College, ANU.

Matthew Sussex is Associate Professor at the National Security College, ANU.

Courteney O'Connor is a doctoral candidate at the National Security College, ANU.

ORCID

Adam Henschke http://orcid.org/0000-0002-2956-0883
Courteney O'connor http://orcid.org/0000-0002-8598-7478

References

'3rd Presidential Candidates' Debate'. 2016. United States of America.

Anderson, Janna, and Lee Rainie. 2017. *The Future of Truth and Misinformation Online*. Washington, DC: Pew Research Centre for Internet & Technology.

Australian Electoral Commission. 2019a. "Counting the Votes." Australian Electoral Commission. https://www.aec.gov.au/Voting/counting/index.htm.

Australian Electoral Commission. 2019b. "Voting Options." Australian Electoral Commission. https://www.aec.gov.au/Voting/ways_to_vote/.

BBVA. 2017. "The Five V's of Big Data | BBVA". *NEWS BBVA* (blog), May 8. https://www.bbva.com/en/five-vs-big-data/.

Blank, Stephen. 2017. "Cyber War and Information War a La Russe." In *Understanding Cyber Conflict: 14 Analogies*, edited by George Perkovich and Ariel E. Levite, 81–98. Washington, DC: Georgetown University Press.

Brattberg, Erik, and Tim Maurer. 2018. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Washington, DC: Carnegie Endowment for International Peace.

Brechenmacher, Saskia. 2018. *Comparing Democratic Distress in the United States and Europe*. Washington, DC: Carnegie Endowment for International Peace.

Buell, Ryan W., Ethan Porter, and Michael I. Norton. 2019. "Surfacing the Submerged State: Operational Transparency Increases Trust in and Engagement with Government." *Harvard Business School Marketing Unit Working Paper 14-034*.

Chua, Amy. 2018. "Tribal World: Group Identity Is All." *Foreign Affairs* 97: 25–33.

CNN Library. 2019. "2016 Election Hacking Fast Facts." CNN, May 2. https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Committee on Foreign Relations United States Senate. n.d. "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." US Government Publishing Office.

Conley, Heather A., and Jean-Baptiste Jeangene Vilmer. 2018. "Successfully Countering Russian Electoral Interference." *Center for Strategic & International Studies*, June 21. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

Dalton, Matthew. 2018. "France Probes Any Moscow Role in Yellow-Vest Movement." *Wall Street Journal*, December 14. Sec. World. https://www.wsj.com/articles/france-probes-any-moscow-role-in-yellow-vest-movement-11544826863.

Deudney, Daniel, and G. John Ikenberry. 2018. "Liberal World: The Resilient Order." *Foreign Affairs* 97: 16–24.

Diamond, Larry, and Leonardo Morlino. 2004. "The Quality of Democracy: An Overview." *Journal of Democracy* 15 (4): 20–31.

Durkin, Erin. 2018. "Trump Claims "honest Vote" Not Possible in Florida as Counties Rush to Recount." November 13. https://www.theguardian.com/us-news/2018/nov/12/florida-recount-governor-senate-trump-response-honest-vote.

Dwoskin, Elizabeth, and Tony Romm. 2018. "Facebook Says It Has Uncovered a Coordinated Disinformation Operation Ahead of the 2018 Midterm Elections." *Washington Post*, August 1. https://www.washingtonpost.com/technology/2018/07/31/facebook-says-it-has-uncovered-coordinated-disinformation-operation-ahead-midterm-elections/.

Economist Intelligence Unit, 2019. "EUI Democracy Index." The Economist, May 15.

Field, Matthew, and Mike Wright. 2018. "Russian Trolls Sent Thousands of Pro-Leave Messages on Day of Brexit Referendum, Twitter Data Reveals." *The Telegraph*, October 17. https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/.

Gady, Franz-Stefan. 2015. "New Snowden Documents Reveal Chinese Behind F-35 Hack." *The Diplomat*, January 27. https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

Gambino, Lauren. 2016. "What Would Happen If Donald Trump Refused to Concede This Election?" *The Guardian*, January 21. https://www.theguardian.com/us-news/2016/oct/20/donald-trump-refuse-concede-election-electoral-college.

Gerstein, Josh. 2018. "U.S. Brings First Charge for Meddling in 2018 Midterm Elections." *POLITICO*, October 19. https://politi.co/2Ajbubq.

Goldman, Adam. 2018. "Justice Dept. Accuses Russians of Interfering in Midterm Elections." *The New York Times*, October 19. Sec. U.S. https://www.nytimes.com/2018/10/19/us/politics/russia-interference-midterm-elections.html.

Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen. 2018. "State, Media and Civil Society in the Information Warfare Over Ukraine: Citizen Curators of Digital Disinformation." *International Affairs* 94 (5): 975–994.

Gordon, Marcy. 2019. "Facebook Working on Addressing Election Threats Ahead of 2020 Vote, U.S. Lawmakers Told." *Global News*, September 20. https://globalnews.ca/news/5931797/facebook-us-election-threats/.

Greenberg, Andy. 2017. "The NSA Confirms It: Russia Hacked French Election "Infrastructure"." *Wired*, May 9. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.

Guardian, The. 2019. "The Cambridge Analytica Files." *The Guardian*. http://www.theguardian.com/news/series/cambridge-analytica-files.

Hay Newman, Lily. 2018. "The Midterm Elections Are Already Under Attack." *Wired*, July 20. https://www.wired.com/story/midterm-elections-vulnerabilities-phishing-ddos/.

House of Commons Digital, Culture, Media and Sport Committee. 2019. "Disinformation and 'Fake News': Final Report". https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm.

Jack, Carolyn. 2017. "Lexicon of Lies: Terms for Problematic Information." *Data and Society*. August 9. https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf.

Johnson, Jenna. 2016. "Donald Trump Says He Will Accept Results of Election — "If I Win"." *Washington Post*, October 21. https://www.washingtonpost.com/news/post-politics/wp/2016/10/20/donald-trump-says-he-will-accept-the-results-of-the-election-if-i-win/.

Kuo, Lily. 2018. "China Says UN Criticism of Human Rights Record Is "Politically Driven"." *The Guardian*, November 7. https://www.theguardian.com/world/2018/nov/06/china-un-criticism-human-rights-record.

Lee, Timothy B. 2016. "The Top 20 Fake News Stories Outperformed Real News at the End of the 2016 Campaign." *Vox*, November 16. https://www.vox.com/new-money/2016/11/16/13659840/facebook-fake-news-chart.

Lewis, Paul, Ben Jacobs, and Sabrina Siddiqui. 2016. "Donald Trump Says He Will Accept US Election Result "If I Win"." *The Guardian*, October 21. https://www.theguardian.com/us-news/2016/oct/20/donald-trump-us-election-result.

Lin, Herb. 2019. "The Existential Threat From Cyber-Enabled Information Warfare." *Bulletin of the Atomic Scientists* 75 (4): 187–196.

Lomas, Natasha. 2019. “Facebook Accused of Blocking Wider Efforts to Study Its Ad Platform.” *TechCrunch* (blog), April 30. https://social.techcrunch.com/2019/04/29/facebook-accused-of-blocking-wider-efforts-to-study-its-ad-platform/.

Marr, Bernard. 2014. “Big Data: The 5 Vs Everyone Must Know | LinkedIn.” *LinkedIn*, March 6. https://www.linkedin.com/pulse/20140306073407-64875646-big-data-the-5-vs-everyone-must-know/.

Martineau, Paris. 2018. “The Co-Opting of French Unrest to Spread Disinformation | WIRED.” *Wired*, December 11. https://www.wired.com/story/co-opting-french-unrest-spread-disinformation/.

Masters, Jonathan. 2018. “Russia, Trump, and the 2016 U.S. Election.” Council on Foreign Relations, February 26. https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

Matlack, Carol, and Robert Williams. 2018. “France to Probe Possible Russian Influence on Yellow Vest Riots – Bloomberg.” *Bloomberg*, December 8. https://www.bloomberg.com/news/articles/2018-12-08/pro-russia-social-media-takes-aim-at-macron-as-yellow-vests-rage.

McDevitt, Michael. 2017. “The South China Sea Seven Years On.” *East Asia Forum*, July 19. https://www.eastasiaforum.org/2017/07/19/the-south-china-sea-seven-years-on/.

Morgan, Susan. 2018. “Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy.” *Journal of Cyber Policy* 3 (1): 39–43. doi:10.1080/23738871.2018.1462395.

Mosquera, Munoz Andres B., and Sascha Dov Bachmann. 2016. “Lawfare in Hybrid Wars: The 21st Century Warfare.” *Journal of International Humanitarian Legal Studies* 7(1): 63–87.

National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

National Conference of State Legislatures. 2020. “Election Administration at State and Local Levels.” *National Conference of State Legislatures*, February 3. https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx.

Nelson, Libby. 2016. “Donald Trump Just Said He Might Not Concede the Election If Clinton Wins.” *Vox*, October 19. https://www.vox.com/2016/10/19/13341712/presidential-debate-donald-trump-concede.

Palmer, Ellis. 2017. “Spain Catalonia: Did Russian ‘Fake News’ Stir Things up in Catalonia?” *BBC News*, November 18. Sec. Europe. https://www.bbc.com/news/world-europe-41981539.

Pastor, Robert A. 2014. “The United States Administration of Elections: Decentralized, Pre-Modern and Contented.” http://aceproject.org/ace-en/topics/em/annex/electoral-management-case-studies/the-united-states-decentralized-to-the-point-of.

Paul, Kari. 2019. “Facebook Says It Can’t Handle Election Misinformation Crisis Alone.” *The Guardian*, June 27. http://www.theguardian.com/technology/2019/jun/26/facebook-constitution-supreme-court-zuckerberg.

Pope, Amy E. 2018. “Cyber-Securing Our Elections.” *Journal of Cyber Policy* 3 (1): 24–38. doi:10.1080/23738871.2018.1473887.

Pratt, Timothy, and Undark. 2019. “Computer Scientists Make the Case Against an Expensive New Voting System.” *The Atlantic*, July 13. https://www.theatlantic.com/technology/archive/2019/07/computer-scientists-worry-over-election-security-georgia/593497/.

Price, Rob. 2016. “The Fact Fake News ‘Outperformed’ Real News on Facebook Proves the Problem Is Wildly out of Control.” *Business Insider*, November 17. https://www.businessinsider.com.au/fake-news-outperformed-real-news-on-facebook-before-us-election-report-2016-11.

Reinbold, Fabian. 2017. “How Germany Is Preparing for Russian Election Meddling - DER SPIEGEL.” *Der Spiegel*, July 9. https://www.spiegel.de/international/germany/how-germany-is-preparing-for-russian-election-meddling-a-1166461.html.

Remeikis, Amy. 2019. “Australian Security Services Investigate Attempted Cyber Attack on Parliament.” *The Guardian*, February 8. https://www.theguardian.com/australia-news/2019/feb/08/asio-australian-security-services-hack-data-breach-investigate-attempted-cyber-attack-parliament.

Rid, Thomas, and Ben Buchanan. 2018. “Hacking Democracy.” *SAIS Review of International Affairs* 38 (1): 3–16. doi:10.1353/sais.2018.0001.

Rizoiu, Marian-Andrei, Timothy Graham, Rui Zhang, Yifei Zhang, Robert Ackland, and Lexing Xie. 2018. "The Role and Influence of Socialbots on Twitter during the 1st US Presidential Debate". *The 2018 International AAAI Conference on Web and Social Media (ICWSM)*.

Rodriguez, Salvador. 2019. "The FBI Visits Facebook to Talk about 2020 Election Security, with Google, Microsoft and Twitter Joining." *CNBC*, September 4. https://www.cnbc.com/2019/09/04/facebook-twitter-google-are-meeting-with-us-officials-to-discuss-2020-election-security.html.

Rosen, Guy, Alex Stamos, Samidh Chakrabarti, Tessa Lyons, and Rob Leathern. 2018. "Hard Questions: What Is Facebook Doing to Protect Election Security?" *About Facebook* (blog), March 29. https://about.fb.com/news/2018/03/hard-questions-election-security/.

Samuelsohn, Darren. 2019. "Senate's Russia Reports to Start Publishing in July." *POLITICO*, June 27. https://politi.co/2Ni0Aeg.

Schmitt, Michael N. 2017. "Grey Zones in the International Law of Cyberspace." *Yale Journal of International Law Online* 42 (2): 1–21.

Seligman, Lara. 2018. "Mattis Confirms Russia Interfered in U.S. Midterm Elections." *Foreign Policy* (blog), January 12. https://foreignpolicy.com/2018/12/01/mattis-confirms-russia-interfered-in-us-midterm-elections-putin-trump/.

Shackelford, Scott, Bruce Schneier, Michael Sulmeyer, Anne Boustead, Ben Buchanan, Amanda N. Craig Deckard, Trey Herr and Jessica Malekos Smith. 2017. "Making Democracy Harder to Hack." *University of Michigan Journal of Law Reform* 50 (3): 629-668.

Smith, Rodney. 2013. *Internet Voting and Voter Interference*. Sydney: New South Wales Electoral Commission.

Solon, Olivia. 2018. "Facebook Deletes Accounts over Signs of Russian Meddling in US Midterms." *The Guardian*, August 1. https://www.theguardian.com/technology/2018/jul/31/facebook-russia-election-midterms-meddling.

Stelzenmüller, Constanze. 2017. "The Impact of Russian Interference on Germany's 2017 Elections." *Brookings* (blog), June 28. https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

Tamkin, Emily. 2018. "This Is What $1.25 Million Dollars a Month Bought the Russians – Foreign Policy." *Foreign Policy*, February 16. https://foreignpolicy.com/2018/02/16/this-is-what-1-25-million-dollars-a-month-bought-the-russians/.

Thrush, Glenn, and Jeremy W. Peters. 2018. "Charges of Vote Stealing in Florida Portend More Distrust in System for 2020." *The New York Times*, November 18. Sec. U.S. https://www.nytimes.com/2018/11/18/us/politics/florida-recount-voter-fraud.html.

US Department of Justice. 2018a. United States of America v. Internet Research Agency LLC and others. District Court for the District of Colombia.

US Department of Justice. 2018b. United States of America V. Elena Alekseevna Khusyaynova.

van der Staak, Sam and Peter Wolf. 2019. *Cybersecurity in Elections: Models of Interagency Cooperation*. Stockholm: International Institute for Democracy and Electoral Assistance. https://doi.org/10.31752/idea.2019.23.

Westcott, Ben. 2019. "Australian Parliament's Computer Network Targeted by Unknown Hacker." *CNN*, February 8. https://www.cnn.com/2019/02/07/australia/australia-parliament-hack-intl/index.html.

Williams, Carol J. 2014. "Putin Lashes out at U.S. as Warmonger That Has "deformed" World Order." *Los Angeles Times*, October 24. https://www.latimes.com/world/europe/la-fg-russia-putin-us-20141024-story.html.

Wintour, Patrick. 2018. "Russian Bid to Influence Brexit Vote Detailed in New US Senate Report |The Guardian". *The Guardian*, January 11. https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

Wintour, Patrick. 2019. "Spain Says 'Disinformation' Surrounds Catalan Separatists' Trial The Guardian." *The Guardian*, February 12. https://www.theguardian.com/world/2019/feb/12/spain-disinformation-surrounds-catalan-separatists-trial.

Wofford, Benjamin. 2018. "The Hacking Threat to the Midterms Is Huge. And Technology Won't Protect Us." *Vox*, October 25. https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting.

Woolley, Samuel C., and Philip N. Howard, eds. 2019. *Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media*. Oxford: Oxford University Press.

Wroe, David, and Chris Uhlmann. 2019. "Federal MPs' Computer Network Hacked in Possible Foreign Government Attack." *The Sydney Morning Herald*, February 8. https://www.smh.com.au/politics/federal/federal-mps-computer-network-hacked-forcing-passwords-to-be-changed-20190208-p50wgm.html.

Yourish, Karen, Larry Buchanan, and Derek Watkins. 2018. "A Timeline Showing the Full Scale of Russia's Unprecedented Interference in the 2016 Election, and Its Aftermath." *The New York Times*, September 20. https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-trump-election-timeline.html.

Zetter, Kim. 2018a. "Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States." *Vice*, July 17. https://www.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states.

Zetter, Kim. 2018b. "The Crisis of Election Security." *The New York Times*, September 26. Sec. Magazine. https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.