JOURNAL OF INTERNET LAW
VOLUME 23
NUMBER 7
JANUARY 2020
EDITED BY DLA PIPER

When Online Political Trickery and Gamesmanship Morph into Standard Practice: Victim Blaming, Do-It-Yourself Cybersecurity, and Wild West Retribution

By Jo Ann Oravec

INTRODUCTION

Forms of political trickery have been critical factors in elections for decades (whether or not computers were utilized), with many political operatives and parties involved (Bassil-Morozow, 2014; Frost-Arnold, 2014; McIntyre, 2013; McLeod, 2015; Philipps, 2015). Political pranksters either infiltrated campaigns or worked from a distance for the benefit of competing campaigns, often in attempts to expose the managerial weakness of their opponents' organizers and candidates. Today, such infiltrations can take place online as Internet resources are manipulated or compromised. This paper explores an assortment of recent concerns and related mitigation efforts involving online information distortion and political gaming in the contexts

Continued on page 15

Jo Ann Oravec *is a full professor in the College of Business and Economics at the University of Wisconsin at Whitewater in the Department of Information Technology and Supply Chain Management. She received her MBA, MS, MA, and PhD degrees at the University of Wisconsin at Madison and is affiliated with the Holtz Center for Science & Technology Studies at UW-Madison.*

Wolters Kluwer

When Online Political Trickery from page 1

of electioneering and voting, with a focus on how recent elections that have apparent manipulations have been framed in political discourse. Campaigns that fall prey to such trickery are often construed as failing to be diligent in response to potential security threats and "harden" their candidacies, although cybersecurity best practices may indeed have been followed by campaign managers and candidates. Failures of campaigns to deal with damaging cybersecurity and manipulation issues are often hidden from public view (to the extent and length of time that is possible), which can embolden perpetrators and make comprehensive and systematic mitigation attempts more difficult. Although this paper focuses on the United States and United Kingdom, political trickery has been widely observed, as in the reported hijacking of the Twitter accounts of Turkish political leaders and the subsequent dissemination of unapproved messages (Fontana, 2017).

Many recent claims about election manipulation and gaming have focused on international propaganda and infiltration, with foreign governments acting strategically and opportunistically (Hyde, 2017; Bjola, 2018). Widely-disseminated narratives emerged from such popular publications as Malcolm Nance's (2016) *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*, Nance's (2019) *The Plot to Betray America*, and Michael Isikoff and David Corn's (2018) *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*. Wirth (2016) declares that "The Cyber Arms Race Is On," with Russian hackers being implicated in some US election security breaches and related online information distortion. Nance, Isikoff, Corn, Wirth, and many others generally frame online political trickery in stark Cold War terms rather than in a more nuanced formulation involving crowdsourcing and multilayered online inputs and disseminations. As discussed in this paper, these large-scale, international-level security concerns sometimes overshadow the growing number of smaller-scale modes for online attack of campaigns, including "Google bombing," wiki-wars, and domain name-jacking; however, these generally less-publicized, emergent practices are part of the environment in which the larger-scale, internationally-rooted attacks are interpreted and framed by the public. These sophisticated international attempts can indeed inform the efforts of campaign managers, volunteers, and candidates, but more locally situated attempts can also materialize (and perhaps eventually gain broad influence). Many of the political information distortion practices emerging in the past decades online can have a collaborative and diffuse nature, with various individuals developing and forwarding "fake news" and participating in Google bombing or cybersecurity attacks often without direct, central coordination (Morgan, 2018) or with targeted harmonization through local parties and campaigns. Efforts to counter these homegrown trickeries can be rather unsophisticated and sometimes rely on accidental discovery or the dogged attempts of local journalists and bloggers to develop their politically-themed stories (Chang, Zhong, & Grabosky, 2018).

A number of corporate and nonprofit organizations have faced security breaches and pranks of the kinds that are being described here for political entities, with reputations and financial issues at stake (Lucas, 2017; Kollár & Poór, 2016). Many individuals and households have encountered security breaches and attacks of various sorts as well, resulting in financial and reputational losses without substantial means for countering these violations (Dodel & Mesch, 2018). The political sphere, however, presents a different kind of context. For example, the impacts of many political trickeries and security breaches have been framed in positive terms for the public good as well as more critical perspectives: political campaigns can be construed as being combative "contests" (Bennett & Segerberg, 2012). In this formulation, political trickery and gaming can serve to test the competitors involved, with the appropriation and sequestering of domain names linked to candidates by their opponents (or domain name-jacking) as major examples (Low, 2016). One case of this is carlyfiorina.org, which was purchased by someone who did not support the candidate Carly Fiorina; it was used to convey extensive anti-candidate propaganda during her 2015-6 Republican presidential nomination run. Many accounts of this situation characterized Fiorina (who was once an executive at the technology-related US corporation Hewlett-Packard, HP) as being clearly incapable of handling even trivial aspects of her own campaign's technological and security matters (Frizell, 2015). Kauffman (2018) describes comparable concerns about the Web site bobstefanowski.co:

> Search for gubernatorial candidate Bob Stefanowski on Google, and high on the list of hits will be his campaign's official website at bobforgovernor.com. But higher than that link may be an ad for bobstefanowski.co, a website registered two weeks ago that has nothing nice to say about the Republican candidate — and appears courtesy of Stefanowski's Democratic rival, Ned Lamont. "The Stefanowski Plan: Radical. Wrong," the website declares, above a lengthy list of catastrophes the Lamont campaign says would befall the state if Stefanowski were to follow through on his pledge to eliminate the state income tax. At the bottom, below 26 footnotes, is the message: "Paid for by Ned for CT. Richard Smith Treasurer. Approved by Ned Lamont and Susan Bysiewicz."

In this Connecticut race, both sides subsequently incorporated domain name-jacking as a strategy, creating a "wild West" retributive scenario:

> Lamont, meanwhile, can likewise find his name in the web address of an unflattering site controlled by others — and prominently featured in Google searches. Click on www.nedlamont.fyi, registered last month and run by a Republican political action committee, and you'll see Lamont described as a "top enabler for failed Governor Dan Malloy," with information under the categories "Enabler," "Tax-And-Spend" and "Families Pay More." The website is the work of Change PAC, which is financed by the Republican Governors Association, but is required by law to operate independently of the Stefanowski campaign.

The notion that trickery is good for campaigns in the long run is often rooted in how it may reveal the weaknesses of individual candidates, exposing potential deficits that could be related to their future performance in office. The playing fields however, involved in these supposed contests can rarely be construed as level and the attacks often spearheaded by individuals with biases toward particular races, genders, or religions (Noble, 2018). An example is the aspect of technological competence (whether sufficiently strong passwords were selected, etc.), which can have a gender or ethnic bias as security violations and political trickeries are framed by the press, bloggers, or opponents. The notion that Carly Fiorina was in some way not manifesting technical competence hit her campaign very hard, leading to appearances on talk shows and other *mea culpa* venues to explain how the situation occurred; Wisconsin gubernatorial candidate Mary Burke encountered similar attacks (described shortly). Corporations have faced comparable issues through the years (Erb, 2017; "How 'username squatting' became," 2018), but often have a longer timeframe and considerably more legal and public relations assistance with which to deal with the aftermath (Oravec, 2013).

Controversies have been salient involving bias and opportunism on the part of the managers of platforms on which political information is shared *via* social media; for example, Google (Alphabet Corporation) and Facebook have both been criticized in US Congressional hearings and other public policy forums for reportedly allowing opportunistic advantages to emerge that can disempower citizens who want basic information about a candidate's popularity and current positions (Kulshrestha *et al.*, 2019). For example, some gaming and manipulation efforts are designed to present candidates in a positive light in relation to their popularity and relation to various social trends; for instance, Twitter and Facebook followers can be "purchased," creating a sense of momentum in a campaign. Other platform-related controversies involve their possibly-inadvertent support of fake news generation and dissemination, which has presented tough challenges concerning the role of Internet-related corporations and the government in political communications (Nicas, 2016).

POLITICAL TRICKERY AND GAMING AS COLLABORATIVE COMMUNICATION ACTS

As computer networks play larger roles in everyday discourse, Internet-related tricks and treacheries have emerged in many arenas of interaction besides the political, including commercial and even religious venues (Akerlof & Schiller, 2015). The kinds of communication acts involved are expanding in variety, resulting in potential confusions as well as coordination potentials (Linell, 2009) Political campaign managers have available to them techniques that

have been developed for use in giving unfair advantage to rival nation states, competing corporations, or organizations involved in various public projects (such as those described in Collins, 2015). Political trickery and gaming can be framed as communication acts involving an assortment of audiences; these acts often have similarities in communications structure to acts of terrorism in how the parties involved are identified by others or self-identified. The question of whether or how terrorists claim credit for particular acts, or are even incorrectly associated with the acts by various political or journalistic figures, can play important roles in the meaning of the acts and the overall effect of terrorism (as discussed in the context of Sinn Féin and the PIRA by Alonso, 2016). Some campaign organizers may find it appropriate to claim credit for certain manipulations and trickeries, often at later points in the campaign when the trickeries are shown to be effective and as legal claims concerning the trickeries are not a large factor. As particular tricks, pranks, and gaming efforts show their effectiveness to professional campaign organizers, these methods often become normalized and part of the standard arsenal through which campaigns operate; volunteer organizers can also acquire certain practices through observing and modeling.

The consequences of such political trickery can be substantial for citizens in their quests to learn about candidates and issues. Consider the following fictional scenario, rooted in the themes outlined in this paper:

> You are a citizen who is interested in a particular candidate. You hear about the candidate on the radio: what is supposedly the candidate's website, terrysmith.com, is often mentioned; the website is owned by the candidate's opposition, however, and has incorrect and generally negative information. You go on social media to find out about the candidate on Twitter, and are amazed at the amount of attention the candidate's tweets are receiving; you later learn that much of this attention was engineered through the purchase of Twitter followers and the maintenance of "bots." You read material about Terry Smith that is posted in political blogs and news websites and find various, possibly-fictitious news stories and negative themes across the platforms possibly linked to a few sources.

The kinds of problems just outlined for individuals in obtaining basic information about candidates are widespread (Morgan, 2018). Added to these concerns are the prospects that citizen engagement and voter turnout could be affected by warnings that political campaign materials could somehow be tainted by online manipulation. In the US and UK elections in 2016 (the US Presidential and UK Brexit votes, respectively), the question of the extent of international influence (intervention from beyond the borders of the country) had a major role in discourse during and after the election (Howard & Kollanyi, 2016; Wingfield, Isaac, & Benner, 2016). The assumption that "some legal or political force would have stopped these abuses if the concerns would be important enough" often dampens the fervor of those who are trying to spearhead specific political communications reforms. The structure of campaigning and elections, however, provides timeframes through which various forms of information and search engine manipulation can be conducted with little chance for detection and mitigation (Coleman, 2015). Even though campaigns can be lengthy in duration (especially in US contexts), the legal and social mechanisms through which trickery and manipulations can be mitigated and reputational matters changed can take even longer to put into motion.

The "victim" theme takes a variety of dimensions in the online political trickery arena. Many traditional broadcast as well as social media sources have targeted campaigns that have been beset by online trickery and cyberattacks as being incompetent or culpable of campaign management malpractice, which can be seen as a kind of "victim blaming." Also, a great deal of recent political discourse construes individuals receiving manipulated or fabricated political information as being somehow victimized (Mejias & Vokuev, 2017), and not empowered to participate in the processes involved. Social media are drawing individuals into direct participation into the kinds of deceptive and disruptive practices that can potentially further dilute the quality of political communications. The platforms that support social media (such as Facebook and Twitter) often provide economic and reputational incentives to participate in such problematic practices, providing advertisement revenue for popular Web sites that disseminate fake news (Epstein & Robertson, 2015). Some of these organizations have recently stated their resolves to rectify this situation,

but overall changes that would be of benefit to voters are only slowly materializing.

WHAT CONSTITUTES ONLINE POLITICAL TRICKERY AND GAMING?

Political interactions are often hard-fought, and the positions individual candidates take can be heavily distorted in the course of political discourse, both computer-mediated and traditional. Construing a particular campaign as engaging in online political trickery may be a judgement call as many practices described in this paper become normalized and affect the various platforms through which potential voters find out about and discuss candidates. Some of the strategies discussed in this paper are borderline in terms of legality, involving unauthorized access to networks. Hacking into another campaign's Web sites and engaging in other more obviously illegal activity has often been supported in indirect ways by political parties in certain circumstances. In the US 2016 Presidential campaign, for example, electronic mail messages that were taken illegally from the Gmail account of a major campaign organizer played considerable, open roles in political discourse (Isikoff & Corn, 2018). A number of political trickery and gaming initiatives involve stretching existing rules and perhaps dealing with aspects of online interactions that have not yet been well mapped by legislation or international treaty.

Computer networking and social media have opened new channels for the exchange of problematic or corrupted information about candidates, issues, and voting mechanisms. For example, the identities of candidates can be readily affixed to statements (including tweets or posts) that they never produced or which were strategically edited; these communications can subsequently be disseminated in social media platforms (Malachowski, 2010). As previously mentioned, domain name piracy (or "name jacking") can have a strong impact on whether or how potential voters obtain information about candidates: "without any legitimate affiliation, people nab rights to web sites that evoke politicians' names" (Sanderson, 2009, p.3). Such piracy is generally legal, although there can be some attempts by those whose names are involved to make intellectual property-related claims against the squatters. Along with these candidate-related issues have emerged new opportunities for diminishing the integrity of basic voting processes and mechanics. For example, information about voting registration and election schedules has often been compromised; such schemes have been uncovered as providing the wrong election dates and polling locations to certain, targeted potential voters as well as establishing bogus voter registration systems that ultimately serve to disenfranchise citizenry (Oravec, 2005; Paulo & Bublitz, 2019).

Online practices that have often been construed in terms of trickery have increasingly been put into use as political operatives and candidates observe them in action, often spread by political operatives who market their skills to campaigns. The normalization of these practices can be rapid as people learn of their effectiveness. Many of these practices have been placed under the rubric of "computational propaganda" with bots and other artificial intelligence programs participating (Bessi & Ferrara, 2016), such as the roles of bots in steering the direction of many 2016 US presidential election political discussions on Twitter and other social media platforms. Below are descriptions of other commonly-known as well as emerging online political manipulation and trickery practices:

GOOGLE BOMBING

"Google bombing" can be used to denigrate candidates by associating demeaning information with their names as part of a browser search, or otherwise affecting the order of information retrieved by a Web browser (Oravec, 2013). According to McNichol (2004), once the basic mechanisms behind Google bombing were ascertained and shared, the practice spread among politically-minded activists of an assortment of parties and interests:

> The unlikely electoral battle is being waged through "Google bombing," or manipulating the Web's search engines to produce, in this case, political commentary. Unlike Web politicking by other means, like hacking into sites to deface or alter their message, Google bombing is a group sport, taking advantage of the Web-indexing innovation that led Google

> to search-engine supremacy. The perpetrators succeed by recruiting a small group of accomplices to link from their Web sites to a target site using specific anchor text (the clickable words in a link). The more high-traffic sites that link a Web page to a particular phrase, the more Google tends to associate that page with the phrase…

Victims of Google bombing have included David Cameron of the UK and Congressperson Rick Santorum of the US (Noble, 2013). Google bombing can have a considerable impact as individuals share information about the attacks through social media.

WIKI-WARS

Repeated "vandalism" attempts on Wikipedia sites (often weaponizing particular gender- or racial-related themes and images) can also serve to drain attentional resources of some political campaigns (Martellozzo & Jane, 2017). Bahrami, Touiserkani, and Momeni (2015) state that "Since everybody is allowed to edit Wikipedia entries, observing impartiality is practically and mostly dependent on the good will of the Wikipedian" (p.113). When this good will erodes or other partisan factors intercede, online battles in altering Wikipedia information in ways negative to specific candidates or issues can occur. Berghel (2014) relates that "Wiki wars (or edit wars) result when mini-crowds become mobs, and empirical truth degenerates into opinion and ideology" (p.90).

FAKE NEWS

Fake news stories expanded in their impacts in the 2016 US and UK elections (Frank, 2015), with "clickbait" headlines and image tags attempting to attract attention (Hurst, 2016). Many of these stunts and manipulations have a strong humorous or comedic dimension, sometimes being crafted for entertainment as well as political advantage (Sørensen, 2013). Extensions of the fake news themes are bogus interviews of candidates with planned stunts or trick scenarios (Kroon & Angus, 2017; Reilly, 2018). Some fake news developers and disseminators have acquired some level of celebrity (Ohlheiser, 2017), including the late Paul Horner in the United States.

POLITICALLY-RELATED CYBERBULLYING AND COORDINATED HARASSMENT:

As previously related, online political activism often involves a playful component (McCaughey & Ayers, 2013; Yates, 2015), and some of the motivation of political trickery participants can simply be to have fun. The abuses involved in some kinds of political harassment, however, can be devastating: "prominently, the cultural public sphere is a terrain of contest characterised by mockery, pity and hostility towards celebrities, particularly women" (Eronen, 2014). Bal *et al.* (2016) describe "caricatures, cartoons, spoofs and satires" as playing critical roles in political communication through the centuries. However, especially damaging and sustained online harassment of women politicians and individuals identifying themselves in some way as female is common, and is often not countered by those in positions to mitigate the situation (Kuzma, 2013). Geismar (2014) states that "the extent to which public hate speech against women is tolerated by both politicians and mass media alike might be construed as bizarre and hypocritical."

SWATTING AS POLITICAL EXPRESSION:

One example of potential physical danger involving political trickery is the "swatting" involved in some political situations (Enzweiler, 2014), which involves the inappropriate and generally anonymous summoning of emergency services to appear at campaign offices or rallies, or even at the homes of candidates. As related by Enzweiler, such practices have had a growing role in political spheres:

> The use of swatting as a form of political intimidation against the ideals of another by placing them in potentially dangerous situations is of grave concern and must be addressed. Such politically motivated swatting activities bring to the fore a sinister application of this phenomenon, in which it is aimed at silencing particular viewpoints in political discourse. Such actions threaten not only the safety of

> the parties involved, but at a deeper level pose a threat to the viability and integrity of the American political system, which is heavily reliant upon free expression.

The "swat" in "swatting" stems from the potential summoning of SWAT teams to various political settings. Swatting can have especially tragic consequences when mistaken identities and inaccurate locations are involved.

ASTROTURFING AND SOCKPUPPETING

Construction of "astroturf" public sentiment is also facilitated by some social media platforms. As previously described, Facebook and Twitter both allow for the purchase of followers, entities that can serve as signals or as proxies for political activity. Zhang, Carpenter, and Ko (2013) place astroturfing in a corporate context: "astroturfing occurs when people are hired to present certain beliefs or opinions on behalf of their employer through various communication channels. The key component of astroturfing is the creation of false impressions that a particular idea or opinion has widespread support" (p.2259). Sockpuppeting involves constructing and disseminating fake reviews, ratings, and other commentary online as to simulate positive public opinion (Fornaciari & Poesio, 2014). Even broadcast and online talk shows have reportedly been affected by synchronized calls in efforts to simulate citizen engagement with particular issues or candidates (Kerby & Marland, 2015).

DISTRIBUTED HASHTAG SPOILING

Twitter has been playing growing roles in shaping political discourse (Freelon & Karpf, 2015). Various Twitter users, however, have worked to "distract" people from the flow of latest news about certain political issues by posting "irrelevant" tweets at high frequency with particular hashtags; Najafabadi and Domanski (2018) categorize these efforts as akin to spam. The #IranTalks hashtag was reportedly damaged in its use and overall impact by such distractions, which could be seen as disrupting discourse on the important nuclear negotiations between Iran and other countries that began in September 2013.

Analyzing political trickery and gamesmanship from a media ecology perspective can illuminate some interactions and related complexities. Some of the problematic trickery and manipulation strategies just described are not easily mitigated with mechanical toolkits (such as wiki-wars and swatting); labor-intensive human intervention would be needed for effective mitigation, providing a drain of campaign resources and attention. Online trickery can interact with and have impacts on political communication in other forms of media (including traditional print and broadcast media). For example, narratives created and disseminated through social media can migrate to more traditional news services (Bennett & Segerberg, 2012; Oravec, 2020) and are often used for sources with little vetting or background analysis by journalists. Overwhelming levels of political trickery may place daunting barriers to citizens who seek to be engaged with the political process, although the question of what constitutes such high levels and subsequent overload is still open.

Placing the burden of countering and mitigating political trickery on the shoulders of individual campaigns is skin to distributing anti-virus software to households and small businesses with the aim or eradicating virus attacks; some benefits can indeed be forthcoming, but there is still a strong likelihood that various slippages and disruptions will occur. Google (with Alphabet as the parent company and Jigsaw as the public policy arm), Facebook, and Microsoft have all developed specific approaches and toolkits designed for small- and medium-sized political campaigns to counter the kinds of attacks they are likely to come across in the course of electoral processes:

> … steps include an ID verification program for anyone seeking to buy a federal US election ad from Google, in-ad disclosures attached to election ads across Google's products, a transparency report specific to political ads on Google and a searchable ad library that allows anyone to view political ads for candidates in the US. As we previously reported, that database does not include issue-based ads or any ads from state or local races so its utility is somewhat limited though new ads will be

> added on an ongoing basis… In the statement to Congress, Google also touted its Advanced Protection Program, an effort to discourage spear phishing campaigns, and Project Shield, a free DDoS protection service for US campaigns, candidates and political action committees. (Hatmaker, 2018, para. 6-7)

Lack of trust of the organizations that are developing and distributing the tools can exacerbate the issues involved rather than mitigate them (Meserve & Pemstein, 2018). Development of these tools is designed to provide some sense that the social media and search engine giants who are profiting in some ways from online political disruptions are indeed attempting to assist in mitigation efforts (Hawkins, 2018). Broeders and Taylor (2017) ask the rhetorical question "Does great power come with great responsibility?" describing the current characterizations of responsibilities of online platform and service providers as expanding as public awareness of their current and potential influences enlarges.

RIGHTEOUS HACKERS, RIGHTEOUS TRICKSTERS? POTENTIAL IMPACTS OF ONLINE POLITICAL TRICKERY AND GAMING ON DEMOCRATIC PROCESSES

The long history of political trickery, pranks, and gaming includes narratives about political campaigns that have been crushed through probably-illegal but ultimately unpunished prankstering (Bassil-Morozow, 2014; Frost-Arnold, 2014; McLeod, 2015). Campaigning, voting, and the election cycle as a whole have gone on even through citizens are often aware of what is transpiring but have few means of countering these practices or mitigating their effects. The phrase "wild West" (referring to the 19th century period of frontier exploration in the United States) has been used to characterize the arena of Internet trickery, manipulation, and security breaches in which political campaigns are currently operating online (Oppliger, Pernul, & Katsikas, 2017; Park, 2018), with responsible oversight and governance often not applicable factors. The possibility that voters will no longer be as involved in the election process because of their awareness of and concerns about online trickery is growing (Wirth, 2016). The impacts of any particular political communications practice or event may not be large (Bennett & Iyengar, 2008), but over time such interactions may have cumulative impacts that deeply affect citizen participation in democracy. Bublitz and Merkel (2014) have outlined a basic human right of individuals to be free from overwhelming barrages of emotionally-involving information that they are forced to assimilate, comparable to the steady stream of negative and convoluted information about electoral matters.

Competence in campaigns continues to be a theme in discourse on political trickery. For example, Mary Burke, a Democratic candidate for governor of Wisconsin, was given comparable treatment to that afforded Republican Carly Fiorina. The Web site maryburke.com was purchased by someone who used it to "hammer" Mary Burke, a relative newcomer to elective politics; her previous political position had been on the Madison, Wisconsin School Board (DeFour, 2013). Burke's supposed neglect in obtaining the maryburke.com domain may have been the kind of mistake made by those who do not spend their lives in pursuing public office. The notion that new candidates can be damaged by political trickery, however, is matched with accounts of how "legacy" candidates are also treated. The 2000 Bush presidential campaign ran into difficulties in dealing with supposed online trickery:

> The George W. Bush presidential campaign experienced even greater problems in dealing with twenty-something graduate student Zack Exley, who purchased sites such as www.gwbush.com and www.gbush.org. Exley vexed the Bush camp with his anti-Bush postings and the vast amount of press he received, prompting Bush officials to file a complaint with the Federal Election Commission (FEC). In April 2000, more than eleven months after the filing, FEC commissioners determined that the Bush complaint did not warrant consideration and dismissed it without considering the merits. Exley was thus left free to continue his activities without fear of running afoul of federal election regulations." Nevertheless, the Exley controversy has raised difficult issues that are likely to resurface as cyber-politics

become more prevalent and more necessary for electoral success. (Coleman, 2015, p.236)

The notion of the "righteous hacker" is often associated with "hacktivism." The term is generally applied to those who engage in various online break-ins so as to push forward the state of cybersecurity and improve computing technology as a result; hacktivism has roots in the early days of computing (Clarke, 1996; Gorham, 2015). In comparable ways, the righteous "political trickster" may also play a continuing role in subsequent political campaigns, endeavoring to test current and potential candidates through various manipulations. Political parties can work together to lessen the impacts of such trickery, so that at least newer candidates can have the possibility of running effective campaigns without overwhelming obstacles. Legal actions against those involved in election-related manipulation and gaming (mobs) include tort liability (Hua, 2017), though after-the-election penalties may dim in significance since the election results themselves will rarely be overturned. Occasionally, the candidates involved in trickery suffer bad publicity, as in the case of a politician in Guelph (in Ontario, Canada) who reportedly collected current and projected opponents' domain names in excess (May, 2014), but this is not automatic.

The needs for individuals to extend their current levels of civic literacy are growing in light of the extents of political trickery they may encounter in everyday political communications. Even while individuals obtain information through formal political debates and candidate-approved materials they may be accessing second- or even third-screen communications that can be doctored and manipulated (Freelon & Karpf, 2015). Case studies and analyses of such trickery may help in attempts to understand how online communications can be manipulated by interested parties (Dahlgren, 2009); in turn, these studies can demonstrate how many social media participants have often played proactive roles in disseminating the distorted or manipulated information. One difficulty in conducting such studies is presenting the resulting material in ways that are not politically steered in various partisan directions; some descriptions of online trickery and manipulations can also take on the appearance of "conspiracy theories" and be rejected as quasi-fictional intrigue.

SOME CONCLUSIONS AND REFLECTIONS: TAKING POLITICAL TRICKERY AND MANIPULATION SERIOUSLY

Major public policy questions arise from the emerging varieties of online political trickery and manipulation, some of which pertain to the character of democracy and the potentials for damaging intervention into electoral systems. For instance, the propriety of political campaigns striking back at each other with political trickeries in a "wild West" style can certainly be unsettling as Internet communications become essential to electoral discourse and as some forms of partisanship become more intense. In an age in which entertainment and politics are becoming more tightly fused (Wells et al., 2016), the humorous and even voyeuristic aspects of online manipulation and gaming in electoral contexts can be especially problematic as participants battle for reputational gains. It can indeed be amusing for many to watch people in current or potential positions of power be humiliated in some way, if only through online manipulations that expose the lack of cyber savvy on the part of their (often amateur) staffs. New manipulation and trickery practices are surfacing as applications of artificial intelligence (such as bots) and "big data" methodologies along with the individual human efforts of everyday fake news writers spread into various election settings, both national and local. Some of the methods of manipulation are becoming democratized to some extent, more easily accessible to those who want to become involved somehow in the political process regardless as to whether they have the means to contribute monetarily to campaigns or become candidates themselves. The potential of well-funded and coordinated efforts to subvert democratic processes, however, is becoming more intense as online manipulation and trickery practices become more sophisticated.

The hacking of the Democratic National Committee (DNC) in the United States in 2016 brought some attention to these issues but only shone lights on one part of a complex set of phenomena. Framing political manipulation and gaming issues as occurring largely in the national and international arenas can diminish the impacts of smaller yet significant incursions on everyday political interactions. Speculation about whether or how

the political infrastructure in the United States and United Kingdom could be somehow "hardened" to withstand the emerging forms of computer-assisted trickery, either locally-generated or implemented at international levels, often incorporates concerns about freedom of speech, although many of the gaming and trickery incidents themselves effectively disable or impair needed channels of political communication. Technological advances that can target fake news and related policies and legislation that are expressly designed to diminish the potentials for political trickery are a start, but sustained attention will be needed to mitigate potential damages (Dupont, 2016; Shackelford *et al.*, 2017). Legislative efforts to reinforce the ownership of certain kinds of online intellectual property (such as the name "Carly Fiorina" in association with related domain names) presents serious issues relating to intellectual property on the Internet (Odinet, 2016).

Whether or not individual political campaigns are somehow culpable in allowing online attacks to occur (for example, by not engaging in "proper" cyber hygiene and security hardening, with practices in synch with what high-tech leaders promote), allowing political trickery to proceed without some checks may serve to weaken confidence in democratic processes over time. The overall impacts of the practices described in this paper on citizenship activities are complex, and damages as well as some benefits are likely. On the positive side, social media have served to democratize political trickery and gaming to some extent, providing capabilities for some kinds of political stunts and manipulations to those with fairly few financial and personnel resources. Bell and Ippolito (2011) relate some of the "equalizing tendencies" of networks, which can empower new and emerging actors in political and social contexts. Political trickery, however, can also demoralize and drain the resources of some less-well-funded and less-politically savvy candidates. The need for conscientious reputation management on the part of candidates can place considerable burdens on campaigns, possibly detracting from the overall value of these online political communications to democracy. Responses to these trickery practices may also underpin the attitudes of citizens as well as traditional media outlets to politically-related international security breaches, possibly desensitizing and numbing them as to potential dysfunctions with political communications as a whole.

Political trickery and gamesmanship are likely to take new forms as potential voters increasingly utilize online sources to access information about candidates as well as obtain polling numbers (Tremayne, 2015), with increased personalization and artificial intelligence support (Oravec, 2019). Campaigns that do not have sufficient resources and savvy to project potential problems with their online presences can find that their messages are misread and communications misdirected. Corporations facing comparable issues often gain more sympathy and obtain more assistance from the legal system in countering invasions of their networks and damage to their systems (Erb, 2017). Even with corporations, a "wild West" approach in which aggrieved parties retributively attack those suspected of hacking and manipulation is emerging, exacerbating partisanship and ill will. Maintaining fairness and nonpartisanship while countering attacks upon the deliberative processes of voters will be difficult but essential for the health of democracies.

REFERENCES

Akerlof, G. A. & Shiller, R. J. (2015). *Phishing for phools: The economics of manipulation and deception*. Princeton University Press.

Alonso, R. (2016). Terrorist skin, peace-party mask: The political communication strategy of Sinn Féin and the PIRA. *Terrorism and Political Violence*, *28*(3), 520–540.

Bahrami, S., Touiserkani, M., & Momeni, M. R. (2015, October). An examination of the culture of impartiality in Wikipedia, A case study of the Islamic World representation in the English and Persian versions of the Wikipedia. In *Culture and Computing (Culture Computing), 2015 International Conference* (pp.113–118). IEEE.

Bal, A., Campbell, C. L., Payne, N. J., & Pitt, L. (2010). Political ad portraits: A visual analysis of viewer reaction to online political spoof advertisements. *Journal of Public Affairs*, *10*(4), 313–328.

Bal, A., Pitt, L., Berthon, P. & DesAutels, P. (2009). Caricatures, cartoons, spoofs and satires: political brands as butts. *Journal of Public Affairs*, 9(4), 229–237.

Bassil-Morozow, H. (2014). *The trickster and the system: Identity and agency in contemporary society*. New York: Routledge.

Bell, J., & Ippolito, J. (2011). When the rich don't get richer: Equalizing tendencies of creative networks. *Leonardo*, *44*(3), 260–261.

Bennett, W. L., & Iyengar, S. (2008). A new era of minimal effects? The changing foundations of political communication. *Journal of Communication*, *58*(4), 707–731.

Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics. *Information, communication & society*, *15*(5), 739–768.

Berghel, H. (2014). Sticky Wikis. *Computer*, *47*(9), 90–93.

Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 US Presidential election online discussion. *First Monday*, *21*(11).

Bishop, J. (2014). Representations of 'trolls' in mass media communication: a review of media-texts and moral panics relating to 'internet trolling'. *International Journal of Web Based Communities*, *10*(1), 7–24.

Bjola, C. (2018). The ethics of countering digital propaganda. *Ethics & International Affairs*, *32*(3), 305–315.

Broeders, D., & Taylor, L. (2017). Does great power come with great responsibility? The need to talk about corporate political responsibility. In *The Responsibilities of Online Service Providers* (pp.315–323). Springer, Cham.

Bublitz, J. C. & Merkel, R. (2014). Crimes against minds: On mental manipulations, harms and a human right to mental self-determination. *Criminal Law and Philosophy*, *8*(1), 51–77.

Cardona, A. M. (2015). *Vitriolic voices: Political candidates and the incivility gender gap online* (Doctoral dissertation, University of Texas-Austin).

Chang, L. Y., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, *12*(1), 101–114.

Clarke, C. T. (1996). From CrimINet to CyberPerp: Toward an inclusive approach to policing the evolving criminal mens rea on the internet. *Orlando Law Review*, *75*, 191–215.

Coleman, M. (2015). Domain name piracy and privacy: Do federal election regulations offer a solution? *Yale Law & Policy Review*, *19*(1), 235–263.

Collier, J. (2017). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. In *Ethics and Policies for Cyber Operations* (pp.187–212). Springer International Publishing.

Collins, M. L. (2015). Still standing, new branding: Corporate crossroads of shaping a modern brand while protecting intellectual property. *Duq. Bus. LJ*, *17*, 197.

Dahlgren, P. (2009). *Media and political engagement*. Cambridge: Cambridge University Press.

DeFour, M. (2013, Oct 07). Democrat Mary Burke announces bid for governor. *McClatchy - Tribune Business News*.

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712–728.

Dupont, B. (2016). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, *67*(1), 97–116.

Enzweiler, M. J. (2014). Swatting political discourse: A domestic terrorism threat. *Notre Dame L. Rev.*, *90*, 2001.

Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences*, *112*(33), E4512–E4521.

Erb, K. P. (2017). When a name isn't just a name: Securing and protecting your domain. *Computer and Internet Lawyer, 34*(4), 10–11.

Eronen, M. (2014). "It's so wrong yet so funny": Celebrity violence, values and the Janus-faced cultural public sphere online. *Celebrity Studies*, *5*(1–2), 153–174.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59*(7), 96–104.

Frizell, S. (2015, May 4). Carly Fiorina Can't Be Happy With CarlyFiorina.Org. *Time*. Retrieved from *https://time.com/3845232/carly-fiorina-webpage-domain-name/*

Fontana, I. (2017). Disentangling the cyber politics–cyber security nexus: the new challenge of global politics. *Global Affairs*, *3*(1), 99–104.

Fornaciari, T. & Poesio, M. (2014). Identifying fake Amazon reviews as learning from crowds. In *Association for Computational Linguistics Conference Proceedings*, 279–287.

Frank, R. (2015). Caveat lector: Fake news as folklore. *Journal of American Folklore*, *128*(509), 315–332.

Freelon, D., & Karpf, D. (2015). Of big birds and bayonets: Hybrid Twitter interactivity in the 2012 presidential debates. *Information, Communication & Society*, *18*(4), 390–406.

Frost-Arnold, K. (2014). Imposters, tricksters, and trustworthiness as an epistemic virtue. *Hypatia*, *29*(4), 790–807.

Geismar, H. (2015). Tricksters everywhere. *HAU: Journal of Ethnographic Theory*, *5*(2), 375–381.

Gillespie, T. (2017). Algorithmically recognizable: Santorum's Google problem, and Google's Santorum problem. *Information, Communication & Society*, *20*(1), 63–80.

Gorham, A. (2015). Does information want to be free? Hacktivism and the democratization of information. *The Journal of International Relations, Peace Studies, and Development*, *1*(1). Retrieved from *https://scholarworks.arcadia.edu/agsjournal/vol1/iss1/7/*

Hatmaker, T. (2018). Instead of Larry Page, Google sends written testimony to tech's Senate hearing. *Techcrunch*. Retrieved from *https://techcrunch.com/2018/09/04/larry-page-google-senate-intel-hearing/?ncid=txtlnkusaolp00000616*

Hawkins, D. (2018, May 18). Google to help political campaigns thwart attacks. *The Washington Post*.

Hill, C. (2018, Sep 09). Indianapolis dad helps expose Russian trolls. *Journal & Courier*.

Hindman, M. (2008). *The myth of digital democracy*. Princeton University Press.

How 'username squatting' became a digital real estate nightmare for brands and celebrities. (2018, Mar 30). *Telegraph.Co.Uk*. Retrieved from *https://www.telegraph.co.uk/technology/2018/03/30/username-squatting-became-digital-real-estate-nightmare-brands/*

Howard, P. N., & Kollanyi, B. (2016). Bots, #StrongerIn, and #Brexit: Computational propaganda during the UK-EU Referendum. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2798311

Hua, W. (2017). Cybermobs, civil conspiracy, and tort liability. *Fordham Urban Law Journal*, *44*(4), 1217–1265.

Hurst, N. (2016). *To clickbait or not to clickbait? An examination of clickbait headline effects on source credibility* (Doctoral dissertation, University of Missouri--Columbia).

Hyde, S. D. (2017). *The pseudo-democrat's dilemma: Why election observation became an international norm*. Cornell University Press.

Isikoff, M., & Corn, D. (2018). *Russian roulette: The inside story of Putin's war on America and the election of Donald Trump*. New York: Twelve.

Jane, E. A. (2015). Flaming? What flaming? The pitfalls and potentials of researching online hostility. *Ethics and Information Technology*, *17*(1), 65–87.

Kauffman, M. (2018). The website is bobstefanowski.co - but it doesn't belong to bob stefanowski. *Hartford Courant (Online)*, Hartford: Tribune Interactive, LLC. Sep 10, 2018.

Kerby, M. & Marland, A. (2015). Media management in a small polity: Political elites' synchronized calls to regional talk radio and attempted manipulation of public opinion polls. *Political Communication*, *32*(3), 356–376.

Kollár, C., & Poór, J. (2016). Organisations in digital age–Information security aspects of digital workplaces. *Management, Enterprise and Benchmarking in the 21st Century*, 73–82.

Kroon, Å., & Angus, D. (2017). Microphone pokes as prank or political action? *Journal of Language and Politics*, 17(2), 222–240.

Kulshrestha, J., Eslami, M., Messias, J., Zafar, M. B., Ghosh, S., Gummadi, K. P., & Karahalios, K. (2019). Search bias quantification: investigating political bias in social media and web search. *Information Retrieval Journal*, *22*(1–2), 188–227.

Kuzma, J. (2013). Empirical study of cyber harassment among social networks. *International Journal of Technology and Human Interaction (IJTHI)*, 9(2), 53–65.

Larson, S. (2018, February 20). Facebook to use postcards in anti-election meddling effort. *CNN Wire Service*. Retrieved from *https://money.cnn.com/2018/02/20/technology/facebook-postcards-identity-elections/index.html*

Lev-On, A. (2014). Campaigning online, locally. *International Journal of E-Politics (IJEP)*, 5(3), 16–32.

Linell, P. (2009). *Rethinking language, mind, and world dialogically*. Information Age Press.

Low, S. (2016). Hey that's mine: What to do when political candidates are unable to register their names as the domain name for their website. *Tul. J. Tech. & Intell. Prop.*, *19*, 135.

Lucas, G. R. (2017). *Ethics and cyber warfare: The quest for responsible security in the age of digital warfare*. Oxford University Press.

Malachowski, D. (2010). Username jacking in social media: Should celebrities and brand owners recover from social networking sites when their social media usernames are stolen. *DePaul Law Review*, *60*, 223–270.

Martellozzo, E., & Jane, E. A. (2017). Gendered cyberhate, victim-blaming, and why the internet is more like driving a car on a road than being naked in the snow. In *Cybercrime and its victims* (pp.77–94). Routledge.

May, W. (2014, Dec 02). Guthrie wants to put cybersquatting in past. *The Guelph Mercury*.

McCaughey, M., & Ayers, M. D. (Eds.). (2013). *Cyberactivism: Online activism in theory and practice*. Routledge.

McIntyre, I. (2013). *How to make trouble and influence people: Pranks, protests, graffiti & political mischief-making from across Australia*. PM Press.

McLeod, K. (2015). *Pranksters: Making mischief in the modern world*. New York: New York University Press.

McNichol, T. (2004, January 22). Engineering Google results to make a point. *New York Times*.

Mejias, U. A., & Vokuev, N. E. (2017). Disinformation and the media: The case of Russia and Ukraine. *Media, Culture & Society*, *39*(7), 1027–1042.

Mercuru, R. (1993). Corrupted polling. *Communications, 36*(11), 122.

Meserve, S. A., & Pemstein, D. (2018). Google politics: The political determinants of Internet censorship in democracies. *Political Science Research and Methods*, *6*(2), 245–263.

Moore, M., & Tambini, D. (Eds.). (2018). *Digital dominance: The power of Google, Amazon, Facebook, and Apple*. Oxford University Press.

Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, *3*(1), 39–43.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. PublicAffairs.

Najafabadi, M. M., & Domanski, R. J. (2018). Hacktivism and distributed hashtag spoiling on Twitter: Tales of the# IranTalks. *First Monday*, *23*(4).

Nakayama, M., & Wan, Y. (2017). Exploratory study on anchoring: Fake vote counts in consumer reviews affect judgments of information quality.

Nance, M. (2016). *The plot to hack America: How Putin's cyberspies and WikiLeaks tried to steal the 2016 election*. Skyhorse Publishing, Inc.

Nance, M. (2019). *The plot to betray America*. Hachette Books.

Nicas, J. (2016, Nov 14). Google pulled into debate over fake news on the web; The company's search engine highlighted a right-wing blog that erroneously claimed Donald Trump won the popular vote in last week's election. *Wall Street Journal (Online)*.

Noble, S. U. (2013). Google search: Hypervisibility as a means of rendering black women and girls invisible. *InVisible Culture*, *19*.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

Odinet, C. K. (2016). Bitproperty and commercial credit. *Washington University Law Review*, *94*(3), 649–706.

Ohlheiser, A. (2017, September 27). Who do you believe when a Internet hoaxer is said to be dead? Retrieved from *https://www.washingtonpost.com/news/the-intersect/wp/2017/09/27/who-do-you-believe-when-a-famous-internet-hoaxer-is-said-to-be-dead/?utm_term=.aac0fdb4b915*

Oppliger, R., Pernul, G., & Katsikas, S. (2017). New frontiers: Assessing and managing security risks. *Computer*, *50*(4), 48–51.

Oravec, J. A. (2005). Preventing e-voting hazards: The role of information professionals. *Journal of Organizational and End User Computing*, *17*(4).

Oravec, J. A. (2013). Gaming Google: Some ethical issues involving online reputation management. *Journal of Business Ethics Education*, *10*, 61–81.

Oravec, J. A. (2015). Gamification and multi-gamification in the workplace: Expanding the ludic dimensions of work and challenging the work/play dichotomy. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *9*(3), 57–69.

Oravec, J. A. (2019). Artificial Intelligence, Automation, and Social Welfare: Some Ethical and Historical Perspectives on Technological Overstatement and Hyperbole. *Ethics and Social Welfare*, *13*(1), 18–32.

Oravec, J. A. (2020, forthcoming). Online social shaming and the moralistic imagination: The emergence of Internet-based performative shaming. *Policy & Internet. https://doi.org/10.1002/poi3.226*

Park, J. (2018). Three decades of digital security. In *Women in Security* (pp.59–67). Springer, Cham.

Paulo, N., & Bublitz, C. (2019). Pow (d) er to the People? Voter manipulation, legitimacy, and the relevance of moral psychology for democratic theory. *Neuroethics*, *12*, 55–71. *http://dx.doi.org/10.1007/s12152-016-9266-7*

Philipps, A. (2015). Defacing election posters: A form of political culture jamming? *Popular Communication*, *13*(3), 183–201.

Reagle, J. M. (2015). *Reading the comments: Likers, haters, and manipulators at the bottom of the Web*. MIT Press.

Reilly, I. (2018). F for Fake: Propaganda! Hoaxing! Hacking! Partisanship! and Activism! in the fake news ecology. *The Journal of American Culture*. *41*(2), 139–152.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.

Rojecki, A. & Meraz, S. (2016). Rumors and factitious informational blends: The role of the web in speculative politics. *new media & society*, *18*(1), 25–43.

Rowe, I. (2015). Civility 2.0: A comparative analysis of incivility in online political discussion. *Information, Communication & Society*, *18*(2), 121–138.

Rowe, N. C., & Rrushi, J. (2016). *Introduction to cyberdeception*. New York: Springer.

Sanderson, M.T. (2009). Candidates, squatters, and gripers: a primer on political cybersquatting and a proposal for reform. *Election Law Journal*, 8(1), 3–29.

Shackelford, S., Schneier, B., Sulmeyer, M., Boustead, A.E., Buchanan, B., Craig, A., Herr, T. & Malekos Smith, J. Z. (2017). Making democracy harder to hack: Should elections be classified as 'critical infrastructure?' *Michigan Journal of Law Reform, 50*, 629–648.

Shifman, L., Coleman, S. & Ward, S. (2007). Only joking? Online humour in the 2005 UK general election. *Information, Community and Society*, *10*(4), 465–487.

Social media companies increase political ad transparency (2018, May 29). *CQ News & Schedules*. MWashington: CQ Roll Call.

Sørensen, M. J. (2013). Humorous political stunts: Speaking "truth" to power? *The European Journal of Humour Research*, *1*(2), 69–83.

Thackray, H., & McAlaney, J. (2018). Groups online: Hacktivism and social protest. In *Psychological and Behavioral Examinations in Cyber Security* (pp.194–209). IGI Global.

Tremayne, M. (2015). Partisan media and political poll coverage. *Journal of Information Technology & Politics*, *12*(3), 270–284.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, *19*(7).

Wells, C., Shah, D., Pevehouse, J., Yang, J., Pelled, A., Boehm, F., Lukito, J., Ghosh, S., & Schmidt, J. (2016). How Trump drove coverage to the nomination: Hybrid media campaigning. *Political Communication 33*(4), 669–676.

Wingfield, N., Isaac, M., & Benner, K. (2016, November 15). Google and Facebook use ad policies to take aim at fake news sites. *New York Times*, p.B1.

Wirth, A. (2016). "The cyber arms race is on:" Lessons from the US presidential election. *Biomedical Instrumentation & Technology*, *50*(6), 463–465.

Yates, C. (2015). Introducing emotion, identity and the play of political culture. In *The Play of Political Culture, Emotion and Identity* (pp.1–21). London: Palgrave Macmillan UK.

Zhang, J., Carpenter, D., & Ko, M.(2013). Online astroturfing: A theoretical perspective. In *19th Americas Conference on Information Systems (AMCIS)*, Chicago, 2259–2265.

Zhang, Y., Ruan, X., Wang, H., Wang, H., & He, S. (2017). Twitter trends manipulation: A first look inside the security of Twitter trending. *IEEE Transactions on Information Forensics and Security*, *12*(1), 144–156.