DEMOCRACY'S ELEVENTH HOUR

226

SAFEGUARDING DEMOCRATIC ELECTIONS AGAINST CYBER-ENABLED AUTOCRATIC MEDDLING

Mika Aaltola

FIIA BRIEFING PAPER 226 ▪ November 2017

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

DEMOCRACY'S ELEVENTH HOUR

SAFEGUARDING DEMOCRATIC ELECTIONS AGAINST CYBER-ENABLED AUTOCRATIC MEDDLING

Mika Aaltola
Programme Director
Global Security Research Programme
The Finnish Institute of International Affairs

FIIA Briefing Paper 226
November 2017

- Recent elections in the US, France and Germany indicate an emerging practice whereby autocracies meddle in democratic elections by hacking data, scandalizing it through leaks, and amplifying the effect by creating intense cognitive flows of disinformation and distrust across social media.

- Election meddling now has a recognizable five-stage pattern, which allows for the development of algorithms that can detect signs of machined foreign operations in real time in cases of similar meddling patterns.

- The meddling toolbox is reusable. However, increasing awareness about its practices can mitigate the impact in subsequent elections: There are clear signs of the meddling having shifted from the US to the French, and especially the German elections. Election meddling can also backfire, and hence deter further meddling.

- Democratic oversight of data is lacking for the most part. Voters should be better equipped with defensive tools that tackle manipulative algorithmic and future AI-based tactics. These tools can be provided by governments. However, more agile market or society-based solutions could also be made available through different forms of cyber-based election monitoring.

Introduction

Data, content, and their flows have geopolitical importance similar to the territorial control of key natural resources, or functional control over their flows. Data and content flows can be weaponized against democracies by domestic actors and hostile states working alone or in collusion. These flows influence the extent to which people trust their governments and recognize news as trustworthy. Furthermore, people are increasingly developing their political awareness and patterns of trust through social media flows.[1] However, trust in governments has been steadily but also alarmingly eroding. The trend has been similar in most OECD countries, where only 43% of people on average currently trust their governments; in the US, the figure is even lower at about 20%.[2] Amplified by the spread of social media, trust is being diffused and is drifting away from top-down relationships towards a vertical identification with one's 'we groups' and like-minded people.[3]

A broader geopolitical game underlies the election meddling against the West. Election meddling by autocratic actors challenges expectations that have prevailed since the fall of the Berlin Wall. Democracies have enjoyed considerable appeal. However, the other side of the coin is that autocracies have come to view democratic appeal as a destabilizing threat to themselves, as a driver behind internal democratic movements and colour revolutions. A more active strategy for some autocratic governments may be to induce weaknesses in democracies, changing the prevailing geopolitical balance and strengthening the domestic stranglehold of autocratic regimes. Influencing and manipulating cognitive flows through cyber methods and algorithmic social media tactics provides a natural toolbox for autocratic operations from the outside.

Democratic trust was the key target of the recent election hackings in the major Western democracies. For the most part, social media flows were meddled with and manipulated in order to engender distrust and polarization, and to reduce the cohesion in (and between) Western democracies. This briefing paper examines the likely pattern that external meddling took in the 2016 United States presidential elections, 2017 French presidential election, and 2017 German federal elections. Meddling by corruptive and other more traditional means is omitted from the analysis, although it can be used in tandem with an election hacking operation. The strategies and tactics of election hacking are reviewed in order to develop more viable recommendations on how to alleviate the alarming democratic vulnerability.

The five stages of election meddling

The 2016 US presidential election provides a reference case for understanding how contemporary elections can be meddled with. Several components of the following five-stage chain of events can also be detected in the French and German elections.

First stage – using disinformation to amplify suspicions and divisions: Deliberate widespread foreign disinformation campaigning can be used to lay the groundwork for effective election meddling; however, more often than not, the objective is a more general weakening of trust in democracies. The objective is to abuse and heighten existing societal, economic, and political enmities, deepen polarization, and establish tactical links to useful parties and/or find colluding candidates. Disinformation campaigning can be particularly effective in social media, where the main platform providers, such as Facebook and Twitter, have yet to establish effective moderating and editorial filters. In the dramatic pre-election context, the professional media's ability to fact- check leaks and differentiate between whistleblowing and mere cunning ploys is lower than usual. Gatekeeping that separates "serious" policy debates from marginal and fringe ones may fail as election campaigning heats up and the media hunt down scandals and scan the horizon for any hint of potential game changers. By default, the agitated and hectic election environment may be further inflamed, paving the way for marginal groups and viewpoints to break away from the outer edges of the political debate.

[1] The Media Insight Project (April 2016). A New Understanding: What Makes People Trust and Rely on News. http://www.mediainsight.org/PDFs/Trust/TrustFinal.pdf, accessed 12 October 2017.

[2] OECD. Trust in Government. http://www.oecd.org/gov/trust-in-government.htm, accessed 12 October 2017.

[3] *The Atlantic* (1 July 2016). Trust in Government is collapsing around the world. https://www.theatlantic.com/international/archive/2016/07/trust-institutions-trump-brexit/489554/, accessed 12 October 2017.

Second stage – stealing sensitive and leakable data: If opportunities permit, and a geopolitically important election is approaching, the overall operation can adopt the more precise objective of election meddling, either to cast an election into disarray or to promote particular candidates or policies. The hacking of confidential campaign discussions can be useful for generating negative, scandalous publicity. Campaigns try to maximize their visibility, raise funds, build political networks with manifold actors, and make their message consistent yet appealing to specific constituencies. These efforts involve tactical decisions and discussions on different options that are often confidential and sensitive if leaked in their 'raw' form. The stolen data can appear even more viral and scandalous in the context of an effective disinformation operation that has already painted an undesired candidate as a controversial and untrustworthy figure. For a resourceful state actor, the hacking of campaign data, such as messages, phone calls, chat traffic, audio recordings and images, can be a relatively easy task. For example, Hillary Clinton's campaign emails were evidently hacked by two sophisticated cyber operations know as COZY BEAR (similar to the variants of DUKES) and FANCY BEAR (also called PawnStorm, Sofacy or APT 28). The highly sophisticated techniques and agile tactical moves indicate a nation-state-level origin for the two 'bears', commonly associated with the Russian intelligence services FSB and GRU. The same allegedly Russia actors have also been suspected of stealing confidential data before important elections in France and Germany.

Third stage – leaking the stolen data via supposed 'hacktivists': During the second phase of the operation, the emails and other documents were likely given to supposedly independent hacktivists. These may be mere fronts set up by an illicit actor. For example, the US election leaks involved an actor named Guccifer 2.0, which was likely a front set up by Russian state actors. The use of a deceptive front confounds attribution, distorts situational awareness, and hinders counter-measures.[4] Whereas denial and deception facilitate the success of an election meddling campaign, the use of known whistleblower and leak sites captures the attention of the professional media. An established and well-known site, WikiLeaks, was actively leaking stolen materials during the US elections. Although the reputation of WikiLeaks' founder, Julian Assange, is controversial, he still has credibility and numerous followers that can increase the dissemination and mainstreaming of controversial stolen information.

Fourth stage – whitewashing the leaked data through the professional media: The information obtained through this cyber breach is leaked to the mainstream media. In the US elections, this was done mainly through WikiLeaks. In the heated election environment, leaks are easily judged newsworthy by the professional media. The professional US and international media are generally eager to publish such material after the worldwide attention achieved by the Manning and Snowden leaks. These initial leak episodes were highly regarded by the US and international press and even led to the awarding of prestigious prizes in the media world – the *Guardian* and *Washington Post* won Pulitzer prizes based on Edward Snowden's leaks in 2014. Leaks are considered to be revelatory, and any speculation concerning the strategic intent of the possible actors behind the leaks is often omitted from the stories, thereby opening up opportunities for more effective deception and denial.

Fifth stage – secret colluding in order to synchronize election efforts: A candidate, party, or a background group can create links and establish coordination with a foreign state to change the election dynamics. The coordination can be willing and conspiratorial in nature. The links of collusion can be established and nurtured over many years, or they can be brief and tactical. Collusion can also be opportunistic and may even lack direct contact between the domestic and foreign entities.

Targeting, timing, and agility

Based on the five-stage scenario, the key to the effectiveness of election meddling is not so much the stealing of sensitive information *per se*, but finding ways to use the data (1) to demographically and geographically target the right voters with divisive disinformation, and (2) release the stolen data and the distorted content in a tactical and well-timed way. The leaking of data to the media at well-timed intervals creates and sustains a scandalous election

[4] ThreatConnect (2016). Shiny Object Guccifer 2.0 and the DNC Breach. 29 June 2016. https://www.threatconnect.com/blog/guccifer-2-0-dnc-breach/, accessed 12 October 2017.

environment that can further amplify the mobilizing impact of hysteria and paranoia.

Targeting: In the US case, it is relatively well-established that extreme ideological content – devoid of any relevant political information – targeted the key swing states. Much of the content was produced by domestic actors, and some by foreign ones. On Facebook, ads linked to the alleged Russian influence operation were targeting voters in Michigan and Wisconsin. Both proved to be key states in the elections. Facebook has acknowledged that an estimated 10 million people saw the ads before and after the elections. Many of these ads were bought by a Russian entity called the Internet Research Agency (IRA). The content focused on "divisive social and political messages across the ideological spectrum, touching on topics from LGBT matters to race issues to immigration to gun rights".[5]

It is also important to note that social media ads provide effective platforms for the testing of videos, posters, and stories for their virulent potential. The number of likes and shares provides an indication of the kind of material that agitates voters most effectively and where. Such content can then be further engineered and promoted by fake accounts and bots to maximize its impact.

On the one hand, locally situated events can be sustained and stirred up by strong national cognitive flows and their ad hoc publics that suddenly become transfixed by the dramatic events and turn them into national hot-button issues. For example, contrary Facebook ads, bought by the troll farm NRA, targeted different groups to spread mutual animosity in localities with local violent events and clashes – for instance in Baltimore and Ferguson over questions concerning police brutality. Both sides of a divisive issue were agitated, and the animosities between the groups were deepened.

On the other hand, wider agitation and national cognitive flows can be used to create the appearance of dramatic local events in the complete absence of factual events. During the US elections, the best example of this was the so-called Pizzagate, a viral episode which claimed that the hacked emails of Hillary Clinton's campaign manager contained secret messages about a child sex ring run by the alleged New World Order elites from a Washington D.C. pizza restaurant. In Germany, there were some notable virulent rumours of sexual violence committed by refugees that turned out to be baseless.[6]

Timing: The effectiveness of a strategic election meddling campaign depends very much on the tactic of timed releases of stolen data. The method is simple: If the campaign discussion trends away from the strategic message intended by the illicit actor, then new content can be released to refocus attention on the strategic message. Well-timed content maintains the focus on certain polarizing issues or sustains attention on scandals advantageous to the meddler's intent.

Timing sometimes seems to be the key to the anticipated impact of hacking and leaks. Effective timing can highlight the surprise value of the content. It can even make otherwise relatively non-scandalous material seem just as newsworthy and relevant because the timing is right and the event occurs during a very sensitive period just before the elections.

The French and German elections: Downstream and blowback effects

After the US elections, concerns mounted that the French election in particular would be the next target. The key question was whether tactical patterns similar to those applied during the US elections, namely the hacking of emails, their well-timed leaking to the mainstream press and fake news sites, and targeted misinformation campaigning – would be attempted in these elections as well.

[5] Facebook (2 October 2017) "Hard Questions: Russian ads delivered to Congress. https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress, accessed 12 October 2017.

[6] Spiegel Online (5 February 2016). Russia's Propaganda Campaign Against Germany. http://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html, accessed 12 October 2017.

French presidential elections 2017

There was a sense that France, which has recently experienced reactionary and populist political sentiments, was similarly vulnerable and that targeting the country might be geopolitically beneficial for an outside autocratic actor. In the past, there had already been signs that France was high on the hit list. For example, the same campaign that hacked Hillary Clinton's campaign email was allegedly already active in 2015 when French TV5 was hacked. Furthermore, fake documents claiming that the leading candidate, Emmanuel Macron, had a secret offshore bank account had already surfaced in early spring 2017. In the same vein, campaigning of the "whatever sticks" variety took the form of personal insults and sexual insinuation to besmirch Macron.

The underlying polarizing and mean campaign dynamics similar to those witnessed in the US were in place. Moreover, as in the US case, the first and second stages – disinformation campaigning and hacking operations – were carried out. Macron campaign emails were hacked a few days before the presidential elections. The third stage was also achieved as a huge trove of campaign emails and other materials were leaked to the internet.[7] Macron's campaign made information about the hack public, but did not point out who was behind it. Trend Micro, a Tokyo-based security firm, had earlier identified PawnStorm – APT 28 – as being behind the attempts to infiltrate the Macron campaign servers.[8] This finding would implicate the same external actor that had been behind the US and French hackings, namely Russia

On the other hand, the US case resulted in greater awareness, attention, and vigilance in respect of the issue of outside election meddling. To a degree, the suspicions concerning the US election results and President Trump's controversial standing in Europe engendered an immunizing trend. Macron was helped by the anti-Trump sentiments in France, which highlighted that Western democracies were under threat. The French security authorities were also highly vigilant and had been forewarned by other Western security services. The impact of the French election law is also significant. The law prohibits electoral polling, publications, and broadcasts during the final weekend of the elections. However, the last-minute leak could have been timed to stop the Macron campaign from reacting to the posting of the data online. Nevertheless, the impact of the leak remained low and was not subjected to whitewashing by the French professional media.

Finally, the publicized fears that the leaks contained tainted information also undermined the legitimacy of the leaks. This deliberate seeding of the leak with distorted or fake content was also pointed out by the Clinton campaign. However, the Macron campaign expressed these delegitimizing fears more strongly and strategically, thereby mitigating the virulence of the leaks if they were to be publicized. It can be said that the transparent and timely communication of the initial fears of hacking and leaks and, subsequently, of the actual break-in was well executed by the French authorities and by the Macron campaign. In comparison, the US authorities and the Clinton campaign were caught unawares, taken by surprise, and left without a clear plan for effective counter-measures.

Furthermore, the attempted French election meddling can be deemed to have backfired on the alleged perpetrator. The misinformation campaign directed against Macron and the hacking of the emails failed to damage the candidacy. Macron was targeted, but still won by a landslide. Nonetheless, a foreign power succeeded in obstructing Macron's path to the presidency, which might cast a shadow over the Franco-Russian relationship in a way that was not the strategic intent of the election meddling campaign.

Overall, the evidence points to a downstream effect whereby external meddling becomes less effective in subsequent elections when its tactics and impact are widely publicized after one notable case. As the immunity strengthens down the stream of a series of elections, the successful utilization of the same tactic can even lead to opposite and more detrimental

[7] Enisa (15 June 2017). Disinformation operations in cyber-space. *https://www.enisa.europa.eu/publications/info-notes/disinformation-operations-in-cyber-space*, accessed 12 October 2017.

[8] Guardian (25 April 2017). Hackers have targeted election campaign of Macron, says cyber firm. *https://www.theguardian.com/world/2017/apr/25/hackers-have-targeted-election-campaign-of-macron-says-cyber-firm*, accessed 12 October 2017.

strategic results from the perspective of the illicit actor.

German federal election 2017

The German security authorities were on high alert for any signs of foreign attempts similar to those that had taken place in the US and French elections.[9] The weeks leading up to the German election were often characterized as relatively undramatic although the debates had previously been intense, especially related to migration issues. For the election meddling to work, a more agitated political climate would have been needed. Divisive messages do not stick when the emotional charge is calmer and more consensual.

However, one key feature of an effective election meddling operation was in place in Germany. In 2015, the computer network and email system of the Bundestag was hacked. Key targets included the parliamentary offices of Chancellor Angela Merkel and several leading figures in her CDU/CSU party. The Bundestag hack has been strongly attributed to a Russian intelligence operation.[10]

The German parliamentary hack was discovered relatively quickly compared to how long it took for the US intelligence services to detect the intrusion into the Clinton campaign and DNC servers. One reason for this is that, in the US, the legacy of the Nixon years makes it harder for campaigns to trust the arms of the federal government for their data protection. However, the German security agencies have more centralized and coordinated practices and tools. The American relatively compartmentalized system did not respond as quickly as the French and German systems.

Retaliating with offensive cyber attacks – namely hackback – was one of the response options that the German government considered in order to establish some degree of cyber deterrence and to increase the costs for a potential election meddler. However, the main efforts focused on a legislative process whereby Germany can legally and effectively respond in the event of future offensive actions.

Warnings and attempts to highlight the costs of any election meddling can be read in the speeches of the key intelligence heads in Germany. For example, Hans-Goerg Maassen, president of the domestic intelligence group, stated that, "We recognize this as a campaign being directed from Russia. Our counterpart is trying to generate information that can be used for disinformation or for influencing operations. Whether they do it or not is a political decision".[11] The pointed reference to the top-level political decisions indicates clarity regarding the attribution and an implicit warning directed at the leadership of the implicated actor.

The key reasons for the relative lack of election meddling in the German case were both domestic and international. Firstly, the recent German elections have not been as closely contested as the US elections for decades. This time around, it was relatively likely that Merkel would remain Chancellor. The cost of going after the likely winner could have been high. The American and French polities are more polarized than in Germany. Germans also rely more on the professional media than on social media sites. The authorities had been aware of different suspicious and verified hacking attempts for a long time. Lessons had been learned from previous elections and hence they were prepared.

Secondly, international intelligence assistance was also prominent, as was the case in France as well. Moreover, the backfiring of the US meddling operations was already becoming apparent, as US foreign policy towards the suspected illicit actor had toughened, not softened. Similarly, the French elections highlighted the blowback risks involved in meddling in complex democratic processes. Perhaps there were clearer geopolitical, economic, and trade risks in destabilizing the relationship with Germany.

[9] E.g. Spiegel Online (7 September 2017). Is Moscow Planning Something? *http://www.spiegel.de/international/germany/how-germany-is-preparing-for-russian-election-meddling-a-1166461.html*, accessed 12 October 2017.

[10] Zeit Online (12 May 2017). Cyberattack and the Fancy Bear. *http://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia*, accessed 12 October 2017.

[11] Quoted by Reuters (4 May 2017). Germany challenges Russia over cyberattacks. *http://www.reuters.com/article/us-germany-security-cyber-russia/germany-challenges-russia-over-alleged-cyberattacks-idUSKBN1801CA*, accessed 12 October 2017.

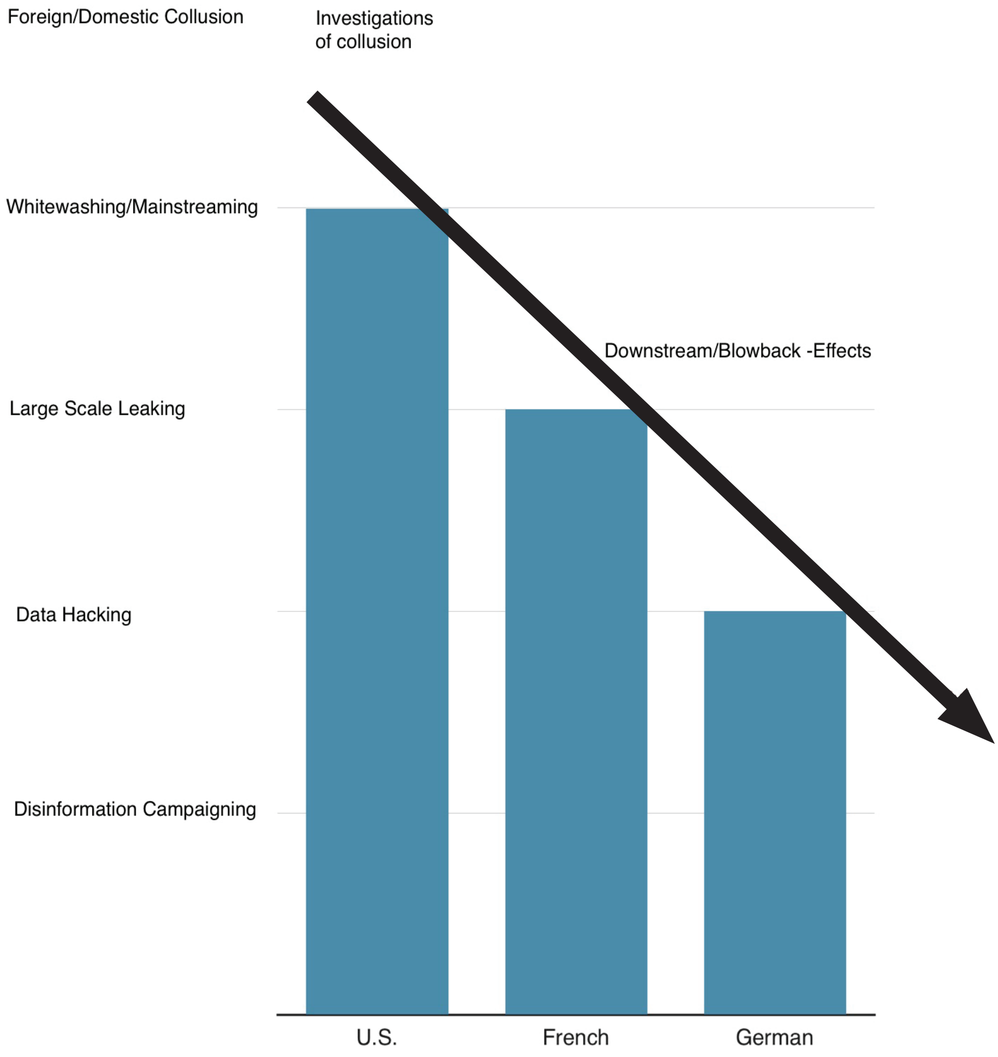

Figure 1. The five stages of election meddling in the three elections

The downstream and backfire effects might have been among the key reasons why there were less noticeable attempts to meddle with the German parliamentary elections.

What can be done?

Relying on maximizing the downstream effect and increasing the perpetrator's blowback concerns is too risky in the absence of more proactive internal instruments and deterrence-enhancing external tools. The key problem is that the democratic oversight regarding data and content flows is largely missing. The problem with accountability in the use of algorithms is going to become even more pressing with the emerging utilization of artificial intelligence in political campaigns, and in future forms of external election meddling. In order to maintain election legitimacy, democratic institutions should demonstrate sustained functional control over externally induced and amplified influence flows prior to, during, and after elections.

The key lies in procuring digital remedies for fighting back. One pressing issue concerns the updating of existing election laws in democracies. Election laws should better cover and regulate the use of known meddling tactics on the major social media platforms during elections. Companies such as Facebook and Twitter should also agree to reveal more of their own data and algorithmic techniques, and develop more effective self-regulation, especially when it comes to autocratic actors' interference in elections. The social media providers should also allow for enhanced and more transparent self-regulation in the interests of their customers, who are also, in many cases, voters in the democratic states that should have oversight over the emerging business practices.

Moreover, voters should also be equipped with defensive tools provided by governments, civic activists, or private sector actors. Since governments are often behind the curve, the private sector is quicker to embrace the latest technologies and should be able to offer solutions to monitor, detect and counteract election meddling. The cognitive flows in social media that are induced by outside actors use means that should be recognizable by humans or machine learning algorithms. The toolbox of a meddler that is based on hacking, leaking, the use of bots, disinformation amplifiers, tactical timing, and clever targeting leaves behind a recognizable pattern. The effects of cyber-enabled meddling can be stopped or mitigated if recognized quickly enough.

The Finnish Institute of International Affairs
tel. +358 9 432 7000
fax. +358 9 432 7799
www.fiia.fi

ISBN 978-951-769-546-6
ISSN 1795-8059
Language editing: Lynn Nikkanen
Cover photo: Pixabay. Used under Creative Commons license.

The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decision-making and public debate both nationally and internationally.

All manuscripts are reviewed by at least two other experts in the field to ensure the high quality of the publications. In addition, publications undergo professional language checking and editing. The responsibility for the views expressed ultimately rests with the authors.

This briefing paper was drafted as a part of a broader research project titled Societal Resilience in the Age of Competitive Interdependency: Prospects and Challenges, funded by the Finnish Scientific Advisory Board for Defense.