IDSA
Issue Brief

INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

Voter's Dilemma: Data Leaks and Electoral Interventions

Munish Sharma

May 22, 2017

Summary

Two much anticipated elections in the recent past, those in the US and France, were marred by massive leaks of data from the campaigns of presidential candidates. Even as new dimensions to these hacking attempts are unfolding, they certainly mark the onset of cyber means of electoral interventions. Given the uncertainty involved in attribution, the myriad of actors involved and the enigma of their motivations, such interventions are here to stay. This Issue Brief analyses these recent cases and brings out the contrasts between them in terms of perspectives, modalities and outcomes.

A few hours before the campaign for the French presidential elections came to an end on May 12, data obtained through a hack from Emmanuel Macron's campaign was published on WikiLeaks with the intention of influencing the outcome. However, the leak failed to damage Macron and he emerged the winner, possibly owing to the timing of the leak. In contrast, a few months earlier, data retrieved from a hack into the Democratic National Committee's (DNC) election campaign was meticulously leaked and leveraged to sabotage Hillary Clinton's prospects in the US presidential elections. These two episodes mark the onset of cyber means of electoral interventions. This certainly does not augur well for democratic systems.

Free and fair elections are the bedrock of the democratic system of governance. People elect their own representatives, and their faith in democratic values gets reaffirmed when the electoral process is transparent. Changes of governments through elections also lead to major shifts in domestic and foreign policies. Campaigning by both individual candidates and political parties is a cornerstone of the preparations for the electoral contest. Perception management is an integral part of electoral campaigning. Building and maligning perceptions about candidates play an important role in the outcome of the electoral process.

Voters' decision to choose one among several candidates or parties is influenced or moulded by perception. Election campaigns are specifically designed to mould voters' perceptions in order to convince them to vote for a particular candidate. With election campaigns turning digital in terms of their execution, outreach and communications, a whole range of activities and internal communications have become cyber enabled. This has opened up opportunities for hackers to gain access to private email communications of the team members of election campaigns. A simple phishing/spear-phishing attack is all it takes to break into the network and exfiltrate classified information pertaining to personal communication, contracts, bank accounts or wealth information and even internal discussions. Any contentious evidence could thereupon be used to sabotage an election campaign, or worse, mould a negative public opinion about the candidate.

The DNC and *En Marche* cases might look similar with an alleged Russian hand behind them. But in terms of timing, management, preparation and outcomes, both exhibited stark differences. Nevertheless, both hacking instances offer a peek into the future: data leaks and cyber means of electoral intervention are likely to become an unfortunate and inevitable part of the electoral processes and campaigns.

DNC Case: The Surprised Ones

Owing to the massive data leak from the DNC, the 2016 US presidential election became controversial; and it continues to be a subject of two congressional

investigations. The first of its kind and scale, the DNC hack was an attempt to sway the outcome of the US presidential elections. After accessing thousands of emails related to the election campaign of Hillary Clinton, the hackers passed on the cache to WikiLeaks, which published it in October 2016.[1] This data leak featured extensively in the mainstream media and was exploited by the then presidential candidate Donald Trump to attack his contender Hillary Clinton.

The US intelligence community - Central Intelligence Agency, Federal Bureau of Investigation and National Security Agency - subsequently analysed the incident and issued an assessment report, some parts of which were declassified and made public in January 2017. The report collated expertise and information from all three agencies to assess the motivation and scope of Russia's intentions regarding the US elections and the use of cyber tools and media campaigns to influence public opinion, but stumbled on the key challenge of attribution.[2] In brief, the report assessed that Russian President Putin had ordered an influence campaign in 2016 to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. The report assessed Putin and the Russian Government to have developed a clear preference for Donald Trump.[3]

The hackers had been on the DNC's systems since the summer of 2015, but the latter announced the breach only in mid-June 2016. Presumably, the DNC never assessed the modalities of cyber-attacks. The laxity could also be on the part of the DNC staff, who ignored breach warnings[4] or fell prey to spear-phishing attacks.[5]

En Marche Case: The Prepared Ones

The leaked data from Emmanuel Macron's election campaign - around nine GB of mails as well as accounting and contracts documents - was dumped on the anonymous document sharing website Pastebin just 36 hours before the French elections. *En Marche*, the political platform of candidate Emmanuel Macron, acknowledged the hacking of personal and professional mailboxes in a public

1 Luke Harding, "Top Democrat's emails hacked by Russia after aide made typo, investigation finds," *The Guardian*, December 14, 2016, available at https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds, accessed on May 9, 2017.

2 Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017, available at https://www.dni.gov/files/documents/ICA_2017_01.pdf, p. 1, accessed on May 9, 2017.

3 Ibid.

4 Dmitri Alperovitch, "Hunting the DNC hackers: how Crowdstrike found proof Russia hacked the Democrats," *Wired*, March 5, 2017, available at http://www.wired.co.uk/article/dnc-hack-proof-russia-democrats, accessed on May 9, 2017.

5 Note. 1.

statement, asserting that false documents had been added to the leaked data in order to sow doubt and misinformation.[6]

Newspapers and broadcasters in France also played a constructive role by consciously avoiding any mention of the details of the pre-election hack.[7] The French electoral authority, CNCCEP, issued a statement the next day that it may be a criminal offence to republish the data and warned social and traditional media not to publish the hacked content. It called upon everyone to show responsibility and not to pass on the content, so as not to affect the vote.[8] The leaks failed to gain traction in the mainstream media, possibly because the information came online just before the campaigning came to an end on Friday and France entered a quiet period, with politicians effectively forbidden from commenting on the leak.

The digital campaign team of *En Marche* was better prepared for cyber-attacks from the beginning, drawing upon lessons from the DNC hack. In December 2016, when Emmanuel Macron emerged as the anti-Russian, pro-NATO and pro-European Union candidate in the presidential race, *En Marche* began receiving the first round of phishing emails[9] - the usual tactic of hackers to gain access to email communications.

In an interview, Mounir Mahjoubi, who led the digital campaign for Macron, discussed at length his experiences with the sustained onslaught, and insinuated a Russian hand. With limited resources, Mahjoubi's 18 member team adopted a "cyber-blurring" strategy and created false email accounts and filled them with phony documents.[10] According to Mahjoubi, the five compromised personal mail accounts reveal no secrets, as most of the emails and documents were associated with the day-to-day functions of a normal election campaign.[11]

---

6 *En Marche*, "Communiqué de presse - En Marche a été victime d'une action de piratage massive et coordonnée," May 5, 2017, available at https://en-marche.fr/article/communique-presse-piratage, accessed on May 10, 2017. (Translated from French using Google translation).

7 Rachel Donaldio, "Why the Macron Hacking Attack Landed with a Thud in France," *The New York Times*, May 8, 2017, available at https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html?_r=0, accessed on May 10, 2017.

8 Jon Henley, "France goes to the polls as country decides between Macron or Le Pen," *The Guardian*, May 7, 2017, available at https://www.theguardian.com/world/2017/may/07/voting-begins-in-final-round-of-french-presidential-election, accessed on May 11, 2017.

9 Adam Nossiter, David E. Sanger and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *The New York Times*, May 9, 2017, available at https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html?_r=0, accessed on May 11, 2017.

10 Antoine Bayet, "Macronleaks: le responsable de la campagne numérique d'En marche! accuse les "supports" du Front national," *Radio France*, May 8, 2017, available at http://www.francetvinfo.fr/politique/emmanuel-macron/video-mounirmahjoubi-patron-de-lacampagne-numerique-d-emmanuel-macron-le-macronleaks-ca-pue-la-panique_2180759.html, accessed on May 11, 2017. (Translated from French using Google translation).

11 Ibid.

There is a clear division among experts on the issue of the actual perpetrators of the *En Marche* hack. In a US Senate hearing, the Director of the National Security Agency, Admiral Michael S. Rogers, accused Russia of hacking into Macron's election campaign. A number of private cyber security enterprises have also carried out their own independent investigations. Trend Macro, a Japanese firm, has pointed at the Russian-government-linked hacker group Fancy Bear, also known as Pawn Storm.[12] Flashpoint, a US-based cyber intelligence firm, also named Fancy Bear as the perpetrator of the leaks, since the cache had links to some of the websites set up by the group.[13] But some experts have argued against this analysis and assessed the operation to be too amateurish for an adept hacker group like Pawn Storm. For instance, the group would certainly not have left any traces, and the 38 links to Pawn Storm in the leaked emails do not necessarily establish definitive attribution to the group.[14]

The way France has handled an incident of this magnitude and gravity is exceptional. The swift action on the part of CNCCEP as well as the moral standards adopted by the media and the citizens ensured that the repercussions of the electoral intervention were warded off. The hack failed to influence the outcome of the elections with Macron winning by a 66 to 34 per cent margin. The French might have got it right this time, but the hacks into the Macron and Clinton election campaigns have raised alarm for political parties, politicians and election watchdogs across the world. Electoral interventions are not new, but cyber means of electoral interventions have unveiled a whole new dimension.

Electoral Intervention in the Digital Age

Interventions in the election process could either be covert or overt, with both having their own attendant costs and benefits. Covert means encompass the use of intelligence services for "plausible deniability" of any kind of involvement, while overt intervention is carried out openly through the media, news outlets and social media. The latter also involves monetary support, training programmes, media know-how, public relations assistance, etc. The digital age has opened up both these intervention options. Through espionage and hacking attempts, it is operationally easy to gather electronic documents or communication messages stored on

12 Andy Greenberg, "Hackers hit Macron with Huge Email Leak Ahead of French Election," *Wired*, May 5, 2017, available at https://www.wired.com/2017/05/macron-email-hack-french-election/, accessed on May 16, 2017.

13 Adrian Croft and Geert De Clercq, "France fights to keep Macron email hack from distorting election," *Reuters*, May 7, 2017, available at http://uk.reuters.com/article/uk-france-election-idUKKBN1820BM, accessed on May 17, 2017.

14 Andrew Rettman, "Russian spies or US neo-Nazis: Who hacked Macron?" *EU Observer*, May 12, 2017, available at https://euobserver.com/elections/137884, accessed on May 16, 2017.

computers or mail boxes of staffers. Sensitive and classified information shared over email is susceptible to data theft and its leak thereafter in the public domain.

The more influential or effective means of electoral intervention is through the media. Various media stories and intelligence assessments (that have been made public) have accused Russia of influencing public opinion through its media arms, *Russia Today* and *Sputnik*,[15] in the case of both the US and French presidential elections. But with a significant proportion of the population using social media platforms, cyber means have opened a virtual Pandora's Box to influence voters. Targeted news channel content on YouTube or instant blogging and trolling over Twitter have a far reaching impact, in comparison with traditional media. Moreover, with paid services, it is quite easy to generate content, indulge in trolling, or propagate an agenda. On top of this, social media platforms have enhanced participation of citizens on political issues of importance. Trends on social media are also a prominent factor now, which could also be handily enhanced or fudged. With the rise of social media in shaping the decisions of individual voters and their inclination towards populist politics - leaning both towards the extremes of right and left - a whole new dimension of electoral intervention is unfolding in the digital era.

Direct foreign intervention in elections to favour a candidate or a party has been a common phenomenon since the end of the Second World War. Foreign intervention in national elections is definitely not new for the US or Russia. In a 2016 research paper, Dov H. Levin of Carnegie-Mellon University concluded that, between 1946 and 2000, the US and the USSR/Russia intervened in this manner 117 times.[16] With statistical evidence, Levin has demonstrated that electoral interventions increase the chances of the aided candidate, and that moreover, overt interventions are usually more effective than covert interventions.[17]

A third country is more likely to intervene in a national election when it perceives that a particular candidate or political party, if elected to power, will seriously undermine its own interest; in other words, there has to be a clear motive to intervene. Also, there needs to be an opportunity, a recipient or a candidate willing to accept help and act in accordance with the interests of the intervening state. To take the examples of the alleged Russian intervention in the US and French elections: Russia had a clear motive to alter the electoral outcomes to ensure that a pro-

---

15 Note 2, p. 11, and "Europe is trying to keep Russia from influencing its elections," *The Economist*, April 15, 2017, available at http://www.economist.com/news/europe/21720665-france-and-germany-fear-propaganda-and-espionage-favouring-pro-kremlin-candidates-europe-trying, accessed on May 11, 2017.

16 Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly*, Vol. 60, Issue 2, 2016, pp. 189-202, https://academic.oup.com/isq/article-lookup/doi/10.1093/isq/sqv016, accessed on May 11, 2017.

17 Ibid.

Russian candidate got elected. However, given the absence of an opportunity to actually aid the preferred candidate, Russia appears to have aimed at undermining the chances of the candidate with a proven or stated anti-Russian stance. Hence, its principal target was the election campaign of Hillary Clinton, and undermining her reputation was the best option. If the alleged Russian intervention is indeed true, then the Kremlin can be said to have successfully moulded the American public perception.

On the other hand, in the French case, possibly due to the proactive measures adopted by better prepared and alerted digital campaigners, or because of the inappropriate timing of the leak, the alleged intervention failed to alter the electoral results in Russia's favour. Again, in such a scenario, Russia's chances for success lay in undermining the credibility of the anti-Russian candidate. However, substantial evidence of any Russian involvement in the French elections is yet to be established, and the investigation has already been initiated under the aegis of the Information Technology Fraud Investigation Brigade, better known as BEFTI, with support from the National Cybersecurity Agency of France, the ANSSI.

As various independent and governmental investigations are underway, a new dimension to the French election hacking case has unfolded. One of the investigations, published by *Le Monde*, conducted in collaboration with the independent media support organization Virtualroad.org, highlights that the spread of these fake documents (about the offshore account of Macron) could have emanated from the American neo-Nazi sphere.[18] This indicates that these efforts may have been directed to help Marine Le Pen in the election. There are discreet evidences of far-right individuals popularising the leaks and one of them, who had created a website to host the leaked document, also happens to be the administrator of the neo-Nazi website, the Daily Stormer.[19] The links between far-right activists in the US, the campaign team of Trump, and Russia are all under scrutiny as part of an FBI investigation.[20]

Cyber has been an operationally useful option in these cases. At one end, it enables covert operations to gather secret private communications or documents and release them over the Internet for public consumption, with complete anonymity and

---

18 Martin Untersinger and Damien Leloup, "MacronLeaks, offshore account: the shadow of the American neo-Nazis," *Le Monde*, May 11, 2017, available at http://www.lemonde.fr/pixels/article/2017/05/11/macronleaks-compte-offshore-d-emmanuel-macron-l-ombre-des-neonazis-americains_5126389_4408996.html#kXSwYJ6bWm1r6AG3.99, accessed on May 16, 2017.

19 David Gauthier-Villars, "U.S. Hacker Linked to Fake Macron Documents, Says Cybersecurity Firm," *The Wall Street Journal*, May 16, 2017, available at https://www.wsj.com/articles/u-s-hacker-linked-to-fake-macron-documents-says-cybersecurity-firm-1494929136, accessed on May 17, 2017.

20 Andrew Rettman, "US neo-Nazis linked to Macron hack," *EU Observer*, May 12, 2017, available at https://euobserver.com/foreign/137882, accessed on May 17, 2017.

deniability. Leaked data could contain both legitimate as well as phoney documents for the specific purpose of sabotage. At the other end, social media platforms are increasingly being exploited for propaganda, election campaigning, perception management and narrative development. Moreover, attribution remains a lingering issue, and any intelligence or technical investigation in such instances cannot establish attribution beyond a certain probability. Intervening states can absolutely deny their involvement, and that is exactly the posture Russia has maintained in the DNC case.

The Two Cases in Perspective: Modalities and Outcomes

In the DNC case, the agenda behind the leaks was clear, as the leaked documents were thoroughly analysed and carefully placed to ensure maximum damage to the election campaign and integrity of Hillary Clinton. The perpetrators had sufficient time to do so. In contrast, the cache of leaked documents from Emmanuel Macron's campaign was dumped as it was just before the election campaign came to an end.

The investigations in the case of the DNC hack have primarily been state led. The US intelligence community has also made some parts of its classified report public. All the subsequent analyses and investigations have unanimously accused Russia of meddling in the US elections. The French case has been investigated by different independent agencies and firms, implying multiple dimensions and actors. There is less unanimity in these reports about Russian involvement. Moreover, some evidence points to US based neo-Nazi groups having been part of the operation.

The starkest difference lies in the outcome of the sabotage by these two leaks. The DNC hack caused damage as it revealed the funding details of Hillary Clinton's presidential campaign and a plethora of personal email communications related to political issues such as migration, borders, Syria, etc. as well as internal discussions about many individuals. These worked to the advantage of her opponent. On the other hand, the revelations from the *En Marche* hack were limited to the documents/notes or email communications related to the execution of the campaign. The only troublesome content was the offshore bank account of Emmanuel Macron, which did not attract much attention. As a result, while the victim of the leaks in the case of the US elections lost, the victim in the French case actually won the elections. Irrespective of the contrasting results of these two elections, cyber breaches and their resultant leaks have eroded the integrity of the very process of campaigning and voting in electoral contests.

Difficulty and uncertainty of attribution also contribute to the audacity of foreign governments and non-state actors in engaging in such nefarious activities. Moreover, unidentified or unpunished perpetrators could further compel other actors to jump

into the fray. Two developed nations and vibrant democracies have already fallen victim so far to cyber based electoral intervention. Two more elections are due this year, in the UK (June) and Germany (September). If any intervention were to occur in these forthcoming elections, many fingers would be automatically pointed at Russia. Theresa May with her conservative and anti-immigration stand contests against anti-war activist Jeremy Corbyn who has been highly critical of the role of NATO[21] and President Donald Trump.[22] These differences in political inclinations and viewpoints are possibly factors which could drive the motives of external powers to intervene in the UK elections.

Germany is also gearing up for federal elections, and there has already been a reported instance of cyber-attack at think-tanks affiliated with the ruling coalition of the Christian Democratic Union (CDU) and Social Democratic Party (SPD). Pawn Storm has been dubbed to be behind this attack.[23] Angela Merkel has pushed to maintain sanctions on Russia over the Crimea crisis.[24] The hacking incident has been associated with this and is considered to be an attempt to impair Merkel's election campaign. Germany's political dynamics are also being shaped by the immigration issue and right-wing populism. In this regard, it is important to note that one of the investigations into the Emmanuel Macron's leaks has unearthed the role of neo-Nazi groups. Germany also has right-wing extremists, out of which one-quarter are neo-Nazis.[25] Given the strong ties between the American and European neo-Nazis, these groups could be one of the probable spoilers working to undermine the September elections in Germany.

In the digital age, cyber means of electoral intervention may be here to stay. If these activities continue unchecked, they would undermine the faith of voters in the overall electoral process, thus endangering the very fabric of a healthy democracy. Voters

---

21 Jeremy Corbyn, "Nato Belligerence Endangers u all," *Morning Star*, April 17, 2014, available at http://www.morningstaronline.co.uk/a-972b-Nato-belligerence-endangers-us-all#.WRwabZKGPcs, accessed on May 17, 2017.

22 Rob Merrick, "Jeremy Corbyn: Donald Trump's state visit to the UK should be scrapped," *Independent*, February 9, 2017, available at http://www.independent.co.uk/news/uk/politics/jeremy-corbyn-donald-trump-uk-state-visit-banned-entry-us-president-muslim-ban-labour-leader-a7570641.html, accessed on May 17, 2017.

23 Reuters, "Cyber Spies Attacked German Think-Tanks Ahead of National Elections", *Fortune*, April 25, 2017, available at http://fortune.com/2017/04/25/cyber-hack-election/, accessed on May 17, 2017.

24 Andrea Shalal, "Germany confirms cyber-attacks on political party think tank", *Reuters*, April 27, 2017, available at http://www.reuters.com/article/us-germany-election-cyber-idUSKBN17T2Y1, accessed on May 17, 2017.

25 The 2015 Annual Report on the Protection of the Constitution by the German Federal Ministry of Interior estimates that more than one-quarter of all right-wing extremists (22,600) in Germany are neo-Nazis, at around 5,800 persons. See Federal Ministry of the Interior, "2015 Annual Report on the Protection of the Constitution," 2015, available at https://www.verfassungsschutz.de/embed/annual-report-2015-summary.pdf, p. 8, accessed on May 16, 2017.

would continue to grapple with the dilemma of making the right choice; the one they perceive to be correct or the one they have been falsely made to believe is correct. This elevates the stakes for digital election campaigners as well. The ones who pick up the warning signals on time, train their staff well, learn from the practices and mistakes of others will be better prepared to overcome attempted electoral interventions.

About the Authors

Munish Sharma is a Associate Fellow (Cyber Security Project) at the Institute for Defence Studies & Analyses, New Delhi.

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/InstituteforDefenceStudiesAnalyses