Cybersecurity and democracy

Hacking, leaking and voting

by Jakob Bund

In early October, the Obama administration publicly attributed a series of leaks containing troves of emails stolen from various US political organisations and influential political figures to the Russian government. The US Department of Homeland Security (DHS), in a joint statement with the intelligence community, went on to describe the leaks as an attempt 'to interfere with the US election process' through the manipulation of public opinion. The joint statement also mentioned scanning and probing activities targeting voter registration databases in more than 20 US states.

In mid-August, after confirmed intrusions of voter registries in Arizona and Illinois, the FBI alerted state authorities and shared technical details about the threat. The attackers ultimately failed to breach the networks in Arizona but were able to extract the voting records of up to 200,000 people in Illinois. While tracing these operations back to Russia, the US government declared it was not yet prepared to officially link these incidents directly to the Russian government. Prior to attributing the leaks, however, a US official had referred to the two intrusions as the closest the US administration had 'come to tying a recent hack to the Russian government'.

Later in October, US intelligence officials revealed plans by the Obama administration to task the CIA with covert cyber operations in response to the Russian activities. The unusual practice of announcing looming covert action appears to be a stopgap measure to encourage Russian restraint before the elections: public signalling avoids that the silence surrounding the planning and implementation of a forceful but carefully calibrated response is construed as a nod to Russia to continue.

Why does this matter?

This is not the first time US election campaigns have become the targets of espionage operations: the McCain, Romney, and Obama campaigns were hacked in the run-up to the 2008 and 2012 elections – although not in all cases by Russia.

Undertaken for the purpose of gaining a 'deep understanding' of the incoming administration, these intelligence-gathering activities can, in fact, act as stabilising factor. During transition periods, miscommunication is bound to occur as past policies are reviewed: a clearer picture of a potentially new administration's roadmap can smooth over initial frictions. The US accepts this practice between states as part of strategic espionage, yet draws a line between collecting information and using it to sway public opinion. Leaking this information to the public crossed this line and fundamentally changed

the quality from a legitimate *intelligence* operation to an *influence* operation interfering in domestic affairs.

Non-democratic intrusions from abroad that shake popular confidence in the fairness of US elections have yet to occur. The same lack of exposure can, however, nurture a false sense of security. Only with trust in the outcome does the opposition accept defeat and confers legitimacy to the winning party. Sowing doubts about the credibility of election results – or the impartial process of opinion-forming that precedes them – undermines the very foundation of democracy.

Why are democracies vulnerable?

The US is not alone in facing cyber-enabled political influence campaigns. The UK's signals-intelligence agency – GCHQ – reportedly already fended off attempts by Apt28, the same Russian hacker group that had penetrated political networks in the US, to compromise government and media networks during the 2015 election. Apt28 is believed to be affiliated with the Main Intelligence Directorate (GRU), Russia's foreign military intelligence service. And last September, the German Office for Information Security (BSI) warned parliamentarians of all parties about widespread efforts targeting political groups in cyberspace. Again linking the intrusion attempts to Apt28, the BSI raised concerns about the use of inside information to potentially manipulate public opinion ahead of the 2017 parliamentary elections. And similar concerns are spreading across other EU countries before the beginning of a protracted electoral season on the continent.

Yet, the US exhibits a set of distinct features that make it a particularly appealing target because of its vulnerability. Effectively a two-party system, the US political landscape is unfamiliar with the concept of coalition governments. This binary logic makes the impact of vote manipulation easily calculable for an attacker. The winner-takes-all principle most states follow in allocating their delegates to the electoral college (who then go on to elect the president) gives small, majority-changing interventions an outsized effect. Marginally interfering with votes for one party or moving votes from one camp to the other – just enough to tip the scales – can change the outcome for a whole state.

The wealth of historical data on party preferences in past elections also facilitates the identification of key battleground states. In practice, the US presidential elections are decided by the results in this handful of 'swing states', where no one party commands an overwhelming majority. On the basis of this information, targeted efforts could seek to manipulate votes or voting behaviour in a few strategically important locations, translating into a disproportionate effect on the elections overall.

In the US, administering elections – including federal ones – falls within the remit of state and local governments. Involvement of the federal government, even if to ensure the integrity of elections, is regarded as encroachment. Not least for this reason, the DHS was careful to stress the voluntary nature of the assistance it has offered to states in light of concerns about voting systems becoming a target of manipulation. With the technical and legal environment varying from state to state, individual vulnerabilities require time to be assessed. While several states have taken laudable precautions, some swing states, like Georgia, have moved entirely to electronic voting – with some foregoing an auditable paper trail and/or relying on outdated voting computers.

In 32 states and the District of Columbia, certain absentee ballots can be submitted by email, online, or by fax. Communications through these channels could be easily intercepted. Even without direct control over its effect on the elections outcome, spreading reasonable doubts on successful vote blocks could compromise trust in the elections. Lingering uncertainty would, in turn, hamstring US capacity to project power internationally. Domestic distraction and brief paralysis of US decision-making organs may be all the *marge de manœuvre* an adversary needs to change the facts on the ground before the US can react.

'Even without direct control over its effect on the elections outcome, spreading reasonable doubts on successful vote blocks could compromise trust in the elections. Lingering uncertainty would, in turn, hamstring US capacity to project power internationally.'

The US is no stranger to challenged elections. The race between George W. Bush and Al Gore in the 2000 presidential elections eventually required a ruling from the Supreme Court to be settled. Bush took the presidency by the slimmest of margins, acquiring only the minimum number of votes in the electoral college, even though Gore won the popular vote. Were the same contested scenario to play out with the added suspicion of vote tampering in the background, the consequences could

be severe. Any meddling with the electoral process would not have to be sophisticated or successful to undermine confidence in the vote. News of an attempt would be enough to discredit the elections – at least in the perception of certain segments of popular opinion.

Fast forwarding to 2016, months before the election one major-party candidate (albeit for wholly different reasons) refuses to declare whether he would accept the outcome of the presidential elections. Depriving the democratic process of the legitimacy awarded by the opposition's concession of defeat feeds into the downward spiral of dwindling confidence in the elections' integrity. Add to this the already polarised atmosphere in which these elections will be held. An October poll by Politico captured the deep divisions that separate the US along ideological lines: more than 41% of survey respondents thought that victory 'could be stolen from Trump because of voter fraud.' That number rises to 73% if limited to Republicans.

'If a government fails to react, how can it deter an attacker from stepping up probing to an actual attack? Yet, acknowledging an organised campaign against the elections' integrity lends credence to the seriousness of the threat and risks harming confidence on its own.'

All the while, the current administration finds itself in a dilemma. The White House long held back any official statement on authorship and intent of the (attempted) breaches and leaks it later linked to Russia – even after private firms had identified and traced back the threat. Prudent abstention from comment to not inadvertently assist attackers in their efforts to undermine trust, however, easily blends with an outside perception of hesitation and a lack of strategy. If a government fails to react, how can it deter an aggressor from stepping up probing to an actual attack? Yet, acknowledging an organised campaign against the elections' integrity lends credence to the seriousness of the threat and risks harming confidence on its own.

How can cyber influence elections?

Broadly defined, there are four ways of influencing elections through cyber means: 1) changing the vote, 2) manipulating opinions that inform the vote, 3) interfering with the act of voting, and 4) undermining confidence in the integrity of the vote.

The first and perhaps most intuitive way – the actual hacking of voting machines – is at the same time the least likely to occur, if only because there are more cost-effective ways to compromise elections. Security researchers have demonstrated for years the porous protections of electronic voting equipment. Until last year, for example, Virginia had voting computers in use that required an active Wi-Fi connection to tally the votes. Not only did the internet connection offer a vector to infiltrate the machine remotely, but it allowed anyone in the vicinity to freely connect to the network.

While all Wi-Fi-connected machines have been replaced, this is not to say that voting computers stay permanently unconnected, or air-gapped. Prior to the election, all machines will be fed with updates and ballot information from the election management system that could function as the central launch pad for malware. In similar fashion, malicious code could be uploaded to individual machines by an agent on site, although this is much heavier in terms of resources and therefore likely prohibitive due to cost. In many ways, the rugged landscape of US voting systems both causes trouble and offers protection. Different standards and systems make it difficult to stage nationwide manipulation. But the technological diversity also adds complexity that makes it more difficult to audit votes and easier to manipulate them locally.

Second, influencing a vote does not necessarily require tampering with ballots or tallying machines. Shaping opinions that inform the vote may well prove to be the subtler approach. Selectively publishing sensitive documents stolen from a party or candidate on the ballot to hurt one side in the elections could be deceptively marketed as public service to warn voters, especially if the leak is orchestrated by a self-appointed anti-secrecy organisation. Such influence operations come with additional disquieting side effects: leaks provide perfect camouflage for fabricated documents and enhance their credibility. If a leak contains 99 authentic but innocuous documents and one incriminating but forged file, how can the fake insertion be credibly explained to the public?

Third, election outcomes could also be altered by preventing certain groups from participating in the first place. The majority of voters in the US declare a party affiliation upon registration. Hacking into networked voter registration databases and deleting voters identified with a certain party would

significantly disrupt the process on election day. In 2006, Maryland experienced malfunctions with its electronic poll books, causing several polling stations to open late. Considering the age of many US poll workers (the average is above 70), lack of IT literacy could compound the problem – both as technical failures occur and as additional security measures are implemented. Even if enough provisional ballots were available to cover all affected voters, long waiting times would be inevitable. Reluctant voters and those without the time to wait or return would effectively be taken out of the political equation.

Turning elections into a trial of patience could substantially harm voter mobilisation rates in the current climate where, despite strong polarisation, many voters are also left disillusioned by the choice they can make. But a lower turnout and unusually large amounts of provisional ballots have wider reverberations. Reduced voter participation lowers the bar for targeted vote fixing and malicious activity to tip results in strategic precincts in the desired direction. Unexpected delays in the voting process and a massive number of provisional ballots do their part in hurting confidence in the outcome.

Lastly, vote manipulation is just one possible means to influence elections. Given the challenges to detecting foul play and auditing procedures, confidence in the outcome may be more important than the outcome itself. Well publicised probing attempts in the run-up to an election could inflate fears of manipulation capabilities and ultimately erode confidence in the integrity of elections. An isolated incident of outside intervention could let confidence collapse. Attackers could precipitate this process by leaking information about alleged vote manipulation to the media. These accounts could also be made up altogether. Assurances of the government to the contrary might not be taken seriously by the population, as governments might want to keep incidents secret to prevent turmoil. 'The hack that wasn't' can nonetheless have serious consequences, making confidence a far easier target than the vote itself.

Who would do it and why?

With all the cyber vulnerabilities in electoral processes (particularly those related to the e-voting systems in broad use in the US), it is important to keep in mind that, while much is possible in the cyber realm, not all is reasonable, and many capabilities remain unexercised. But whatever the method, two questions driving the threat assessment remain fundamentally the same: who would interfere with democratic elections, and for which purpose?

Most malicious cyber activity is linked to cybercrime. Yet, targeting elections offers no direct financial gain. In terms of attribution – which, despite recent improvements, remains a challenge in cyberspace – this narrows down the circle to state and terrorist organisations (bar the 'lone wolf' hacker who may have a limited impact). In terms of motivation, undermining democratic elections could form part of a general attempt to prove theories about the fragility of democracies or at least harm their capability to project 'soft' power internationally. Influence operations may also be specifically designed to wrestle the target into a condition of temporary political paralysis. Prolonged uncertainty domestically draws attention and resources away from foreign policy issues that rely on active leadership, leaving room to fill and manoeuvre for other actors.

The high stakes involved in targeting a country's democratic process make it hard to imagine a scenario where outright vote manipulation takes place without significant diplomatic fallout. Under circumstances of strained but still workable relations, fair confidence in attribution capabilities and strong expected retaliation outside of cyberspace can act as deterrent. For now, states still have to find a response to popular alarm about probes and leaks that, as far as elections are concerned, threaten to subvert confidence in democracy. Building defence and resilience against the threats democracies face from cyberspace starts with improving people's understanding of the role cyber elements play in elections: voters need to be aware of the vulnerabilities in the voting process.

The same applies to efforts by foreign players to steer public opinion through the adept exploitation of media channels to circulate leaked documents (fake or real). The indiscriminate use of technical terms like probe, intrusion, and breach in news reports blurs important distinctions, describes escalatory progression that has not taken place, and thereby reinforces popular sentiments of uncertainty. As unintended consequences, they underscore the importance of standardised dictionaries and awareness about the effect language choices have on public confidence and threat perception. All these are crucial steps to improve cybersecurity in their own right – but the stakes of failure just got higher.

Jakob Bund is a Junior Analyst at the EUISS.

 | QN-AK-16-030-2A-N | ISBN 978-92-9198-463-3 | ISSN 2315-1110 | doi:10.2815/9916