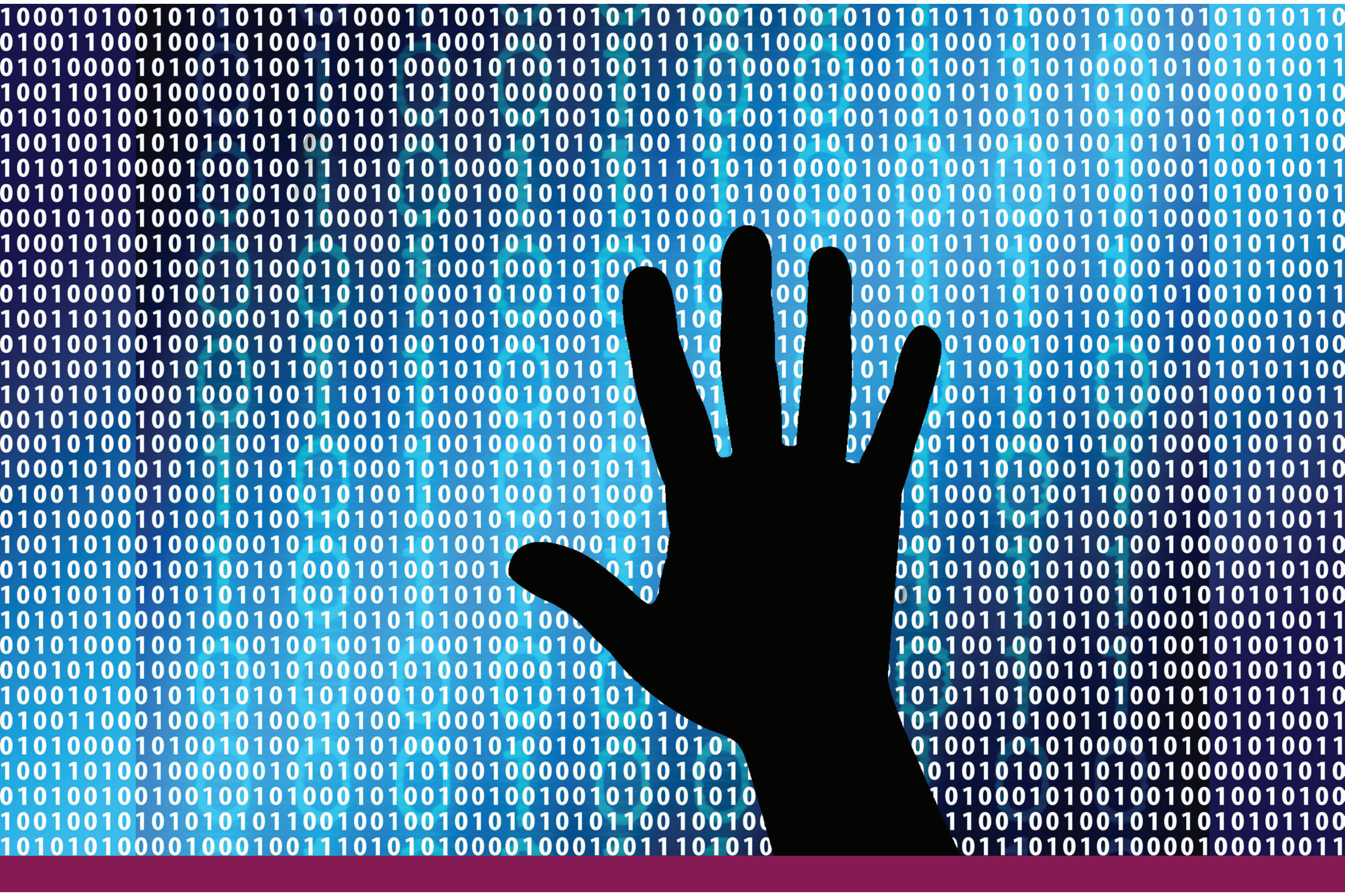
ELECTION HACKING IN DEMOCRACIES

204

THE EXAMPLE OF THE U.S. 2016 ELECTIONS

Mika Aaltola & Mariita Mattiisen

FIIA BRIEFING PAPER 204 • October 2016



ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

ELECTION HACKING IN DEMOCRACIES

THE EXAMPLE OF THE U.S. 2016 ELECTIONS

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

FIIA Briefing Paper 204
October 2016

Mariita Mattiisen
Independent analyst, Project Manager
Estonian Atlantic Treaty Association

- The US, as a highly digitalized state, depends on different cyber platforms for election campaigning, political discussions, forming popular opinions, and – in some cases – the voting process itself.

- Geopolitically motivated election hacking can aim to influence the direction of foreign policy debates, to promote/demote candidate(s), and to instigate disruptions, suspicions, and distrust towards the election process or the democratic system. The strategic aim is to lower the democratic appeal and to increase the attraction of autocratic "stability".

- A state sponsor of hacking can demonstrate that it has sophisticated cyber capabilities, thereby promoting its own major power standing. Even if its efforts raise suspicions, it gains visibility, as its efforts are discussed in the media and it manages to insert itself into the election discussions.

- The state sponsor can subtly promote the images of its own type of political system as being comparatively more resilient and stable than the US democratic system.

- The relative success of the election hacking targeting the US might motivate scaling up the intensity and scope of similar operations in future democratic elections. At a minimum, the election-hacking incidents point to a scenario that has to be taken seriously.

Western democratic institutions have been relatively durable throughout the Cold War years up to the present time, despite external political challenges. It seems that the democratic stability has perhaps been taken for granted. Influence operations have gained potency through the digitalization of political debates and processes. In particular, cyber-based tools, in combination with older methods of operations, can be used to place additional strains on Western political systems at key moments. Any problems in seeking consent according to regular established procedures will undermine the legitimacy of the democratic government. This can cause uncertainty and, to a degree, undermine the legitimacy of the elected government in the eyes of its own population.

As the US presidential election is approaching, there have been enough signs of election-related cyber hacking for the question of specific democratic vulnerabilities to be taken seriously. What kind of motives and capabilities are needed in order for an outside politically motivated actor to influence an election in the digital age? This paper examines possible objectives, the evidence for such operations to date, and perpetrator states' ostensible motives and resources. The main question is whether the US election-related hacking indicates an increasingly serious vulnerability in the highly digitalized liberal democracies.

The context of destabilizing and influencing US debates

Potentially antagonistic major powers, such as China and Russia, have traditional methods of exerting influence on the US. They can pressure the US through diplomatic means, and through carrot and stick policies. On the softer side, they can, for example, fund opportune projects in the influential Washington D.C. think-tanks or hire lobbying firms to press for certain policies. However, it can be argued that the contemporary age has opened up other temptingly efficient and alarmingly easy cyber-related influence vectors.

The election period is critical in the transition of power between successive administrations. As an already tense period, elections can be more sensitive to foreign influences as the main candidates' teams are just maturing and developing their policy options. On the other hand, "October surprise" is an often-used scenario in the US that refers to the vulnerability of election processes during the final election stretch. Unexpected turns of events can influence the election during the last intense weeks of campaigning.

The US has a vast and diverse public whose political views range from mainstream to fringe. The often paranoid fringe is no longer as marginal and isolated as it used to be. The entrenched suspicions of the far-right and the radical left fuel a cacophony of domestic disinformation campaigning – arising from paranoia, suspicion, ignorance and fear – that blends with unintentional and intentional foreign influences. Deliberate foreign disinformation campaigning and attempts to co-opt the domestic elements can be especially effective in social media, where no moderating and editorial filters prevail. Social media is also transnational by nature. The fringes can be mobilized by inundating it with outrageous, misleading, or false information. This can legitimize fringe suspicions and elevate them to semi-legitimate election issues.

On the one hand, the myriad of different controversies and scandals can draw attention away from the underlying changes in the foreign policy debates. With so many simultaneous spectacles, scandals and moral dilemmas, more traditional topics do not come under critical scrutiny by the media or by the wider audiences, as they are otherwise preoccupied. Previously unorthodox foreign policy views can be expressed because the public discussions are so saturated with other trending topics. Adding more messiness to the already volatile election context can be beneficial for the political aims of foreign actors.

Besides "messing up" the debates, the cyber environment can be used to lend support to candidates with favourable policy stances and to undermine candidates who have unfavourable policy proposals affecting the outside state actor. The overall effect can be one of shifting the content of the debates in ways and to a degree that are beneficial for the outside influencer. Gatekeeping that separates the "serious" foreign policy debates from the increasingly fringe ones can fail.

During the 2016 election cycle, points of view have been expressed that fall outside of the customary long-term foreign policy fluctuation. For example, it is noteworthy that the Republican candidate Donald Trump has been praising Russian President Vladimir Putin as an example of a strong and committed leader. This language in itself is a clear departure from the overall Washington consensus when it comes to Russia.

An additional harbinger of disarray has been the debate over the depth of US support for Ukraine. Some have stressed that the US needs to go beyond non-lethal military aid besides the economic sanctions against Russia. Others have called for the US to stand firmly behind the sanctions regime and to push the European allies to do the same. A shift in this balance towards a more neutral position could be in the interests of a major power competitor. It is noteworthy that Donald Trump has at times acknowledged the legitimacy of Russian interests in Ukraine and over Crimea. His campaign surrogates have even stated that the US should not go to war over places like Estonia, which are "suburbs of St. Petersburg". Positions and statements like these indicate an unusual deviation from the long-established norm.

Upholding the commitments towards allies has enjoyed the support of the Washington foreign policy elite. However, the Republican candidate has been notably critical towards NATO. His rhetoric rendering US responsibilities under Article 5 of NATO radically more conditional is something that no major party candidate has adopted since the signing of the Atlantic treaty. However, these exceptional policy stances might not be anything more than the Trump campaign making explicit its opposition to the Washington establishment. The anti-establishment stance has, after all, been the key to his candidacy.

It can be argued that the supposed election-hacking operation may be based on more conditioning tactics. Tactics can depend on co-opting and influencing the existing discursive dynamics in the US, or in any other similar democratic system. By demonstrating an active capability to influence, an outside actor can change the evolutionary dynamics of the campaign in ways that make it increasingly likely that candidates will be tempted to co-opt these influences for their own benefit. What is needed are favourable dynamics that can be reinforced and accentuated. In this scenario, favourably disposed actors in the target state can learn to "surf with" or even "adapt to" the underlying operations without any need to directly and explicitly participate in the operation.

Evidence-based anatomy of US election hacking

The spectrum of election-hacking efforts ranges from general influence operations where cyber plays an increasingly key role to direct election hacking, such as the hacking of voting machines or giving the impression of such a capability. The hacking of electronic voting machines might be easier than thought since they often use outdated insecure platforms. Although there is no evidence of direct hacking of the e-voting machines, there are indications that several state boards of elections were breached.[1] The US voting system is relatively decentralized, which, in theory, makes hacking operations more complicated.

The most significant efforts to influence the election have been the hacking of the formal governing body of the Democratic Party, the Democratic National Congress (DNC), to steal leakable data – such as messages, audio recordings and images – and to monitor emails, phone calls, and chat traffic. The effectiveness of election hacking is partly due to the notorious difficulty of attributing illicit cyber-activity to its actual perpetrators. In the case of the DNC hacking, the attribution has been strong enough for the US authorities to draw a formal conclusion. The US government has claimed that the aim of this operation was to "interfere with the US election process" and that the hack was committed with the authorization of "Russia's senior-most officials".[2] The supposed aim was to create a steady stream of

[1] Wired (2016): Hack brief: As FBI warns election sites got hacked, all eyes are on Russia, 29.8.2016, *https://www.wired.com/2016/08/hack-brief-fbi-warns-election-sites-got-hacked-eyes-russia/*, last accessed 26.10.2016. AP (2016): US official: Hackers targeted election systems of 20 states, 30.9.2016, *https://www.apnews.com/c6f67fb36d-844f28bd18a522811bdd18/US-official:-Hackers-targeted-election-systems-of-20-states*, last accessed 26.10.2016.

[2] Reuters (2016): U.S. formally accuses Russian hackers of political cyber attacks, 9.10.2016, *http://www.reuters.com/article/us-usa-cyber-russia-idUSKCN12729B*, last accessed 26.10.2016.

embarrassing and negative publicity to undermine one presidential campaign.

The suspected operational logic has been as follows: gaining access to the email systems of the Democratic Party to steal data, setting up allegedly fake hacktivist profiles (e.g. Guccifer 2.0), establishing links with existing leak sites (e.g. WikiLeaks), leaking the data through this network, getting data published in the mainstream media, and then releasing further authentic or altered data in a tactically timed manner to promote certain themes and candidates.

The DNC was compromised by two sophisticated cyber operations known as COZY BEAR (probably initiated during the summer of 2015) and FANCY BEAR (from March 2016 until summer 2016): one targeted the internal communications while the other went after the DNC's and the Clinton campaign's research on Donald Trump. The highly sophisticated techniques and agile tactical moves indicate a nation-state-level origin for the two "bears". The cyber-security company, SecureWorks, investigated the group behind the hack and concluded "with moderate confidence" that "the group is operating from the Russian Federation and is gathering intelligence on behalf of the Russian government".[3] Cyber- security company CrowdStrike determined that the two operations "are believed to be closely linked to the Russian government's powerful and highly capable intelligence services".

COZY BEAR campaigning is also known by the name CozyDuke, which cyber-security company F-Secure examined in their 2015 report. F-Secure's conclusion based on years of historical evidence is that "the Dukes are a well-resourced, highly dedicated and organized cyber espionage group that we believe have been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making".[4] In the case of the Bears and Dukes, the actor behind the operations had a clear geopolitical motive, which was to cause distrust and instability in highly digitalized societies.[5]

FANCY BEAR (also known as Pawn Storm, Sofacy or APT 28) is an operation whose roots can be traced back to 2008 at least. FANCY BEAR operations have allegedly been carried out against the German Bundestag and France's TV5 in the past. Whereas COZY BEAR is supposedly associated with the Russian domestic intelligence (FSB), FANCY BEAR has been linked with the Russia military intelligence service, GRU.[6]

No interaction and synchrony has been detected between the two BEAR campaigns. This might indicate that the two cyber operations are running without much awareness of each other. The other option might be that there is clearly a shared geopolitical motive and, although the operations are separate or even competitive, they are aimed at similar goals, are different phases of one overall process, complement each other opportunistically or work in tandem as mutual back-up campaigns.

The DNC breach can be regarded as a key phase in a wider influence operation. Most likely the emails and other documents were handed over to actors in the next phase of the overall operation. The subsequent phase used a supposedly independent hacktivist. This alias was used to leak the data to the US media. So far, many of the leaks appear to have taken place through an entity called Guccifer 2.0. or, ultimately, through known sites such as WikiLeaks.

It should be noted that one key characteristic of the FANCY BEAR operation in particular has been its use of "false flag" tactics. Operations are disguised to appear as if they were carried out by someone other than the actual perpetrators. A denial and deception

[3] SecureWorks (2016): Threat Group-4127 Targets Hillary Clinton Presidential Campaign, 16.6.2016, https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign?_ga=1.211064981.1830189129.1474006576, last accessed 26.10.2016.

[4] F-Secure (2015): The Dukes: Seven years of Russian cyberespionage, https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf, last accessed 26.10.2016.

[5] Aaltola, Mika (2016): Cyber Attacks Go Beyond Espionage: The Strategic Logic of State-sponsored Cyber Operations in the Nordic-Baltic Region, 29.8.2016, http://www.fiia.fi/en/publication/606/cyber_attacks_go_beyond_espionage/, last accessed 26.10.2016.

[6] CrowdStrike (2016): Bear in the Midst: Intrusion into the Democratic National Committee, 15.6.2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee, last accessed 26.10.2016.

effort provides the foundation for any successful election-hacking campaign: "In cyberspace, the strategic goal is straightforward: hack everything, deny everything, and make counter-accusations".[7] If this theory is correct, the operations would have been designed to attract media attention, distract the official investigation, and arouse indecision over the use of counter-measures.[8]

Challenger's motives and means

Any politically motivated election hacking has to be consistent with the motivation and resources of certain perpetrator states. Although suspicions have centred on Russia, this does not mean that other major illiberal powers have not or could not abuse the same democratic vulnerabilities in the future. For example, there are strong suspicions that a Chinese actor – the so-called APT16 campaign – hacked the website of a major political party and collected data on users in connection with the 2016 national elections in Taiwan.[9]

If Russian geopolitically motivated actors have been behind the main US election-hacking operations, it leads to questions concerning possible motives, advantages, and resources. The use of election-related cyber-attacks should be seen as a part of Russia's wider efforts aimed at creating social divisions, undermining trust in institutions, and polarizing societies along ethnic and religious lines. Against this perceived pattern, it is understandable that election-hacking concerns have been expressed recently in Germany with regard to the country's approaching elections.[10] In the UK it was revealed that an alleged Russian cyber-hacking operation was thwarted in the run-up to the May 2015 parliamentary elections.[11] Whether or not these allegations against Russia in connection with the cyber hacking of elections can be proved, two potential political motives present themselves:

Revival of past super-power status: After the collapse of the Soviet Union, which has been described by President Vladimir Putin as the greatest catastrophe of the 21st century, the Russian role in world politics was reduced to a more regional position. Solidification of the democracies to the west of Russia and NATO's attractiveness to the Eastern European states were interpreted as threats to Russia. There seems to be a desire to upgrade the regional and even the global position of the country, as well as to demonstrate its capabilities and to give at least a semblance of parity with the US.

Worries that the West is engaged in similar regime destabilization: More general strategic planning and national security thinking stems from (the perceived) Western illicit anti-regime activities in Russia and its neighbourhood (e.g. Maidan), as Article 17 of the Russian National Security Strategy states: "The West's stance aimed at countering integration processes and creating seats of tension in the Eurasian region is exerting a negative influence on the realization of Russian national interests". More specific to the cyber domain, there have also been internal concerns about the spreading Western influence as a cause of regime instability. There have been long-held suspicions in Russia that the West has instigated regime changes via Twitter and Facebook in connection with the Arab Spring and Euromaidan, for instance. The cyber capabilities of the US and its allies, such as the so-called Five Eyes – the US, the UK, Canada, Australia, and

[7] Council on Foreign Relations (2016): Net Politics: Lessons From the Cold War to Combat Modern Russian Disinformation campaigns, 20.9.2016, http://blogs.cfr.org/cyber/2016/09/20/lessons-from-the-cold-war-to-combat-modern-russian-disinformation-campaigns/, last accessed 26.10.2016.

[8] E.g. Pomerantsev, Peter (2014): Russia and the Menace of Unreality: How Vladimir Putin is revolutionizing information warfare, *The Atlantic*, 9.9.2014, http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/?_ga=1.43497893.1830189129.1474006576, last accessed 26.10.2016.

[9] FireEye (2016): Redline Drawn – China recalculates its use of cyber espionage, June 2016, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf, last accessed 26.10.2016.

[10] SecurityWeek (2016): German Political Parties hit by Cyber-Attacks, 21.9.2016, http://www.securityweek.com/german-political-parties-hit-cyber-attacks, last accessed 26.10.2016.

[11] The Times (2016): GCHQ spooks thwarted Russian cyber-attack on general elections, 25.9.2016, http://www.thetimes.co.uk/edition/news/gchq-spooks-thwart-russian-cyber-attack-on-general-election-62zdk9mnb, last accessed 26.10.2016.

New Zealand – are seen as hostile. This motivates counter-measures to target the perceived Western vulnerabilities.

Besides the gains, Russia, as a major power competitor with the US, can benefit from using a cyber vector against the US for three primary reasons:

Cyber-reach of influence operations: One of the most advantageous characteristics of cyber is that it negates geographical distance. This facilitates reaching societies and states that are highly digitalized but further away from methods requiring geographical or cultural proximity. For example, in Western Europe, these kinds of operations have allegedly co-opted the refugee crisis in order to catalyze turbulence in the political systems.[12] It may be that the idea is to exploit the vulnerabilities within the key states that are further away, but which are crucial for one's own geopolitical goals, insomuch as the objectives themselves seem to be focused on the geographically adjunct states bordering Russia.

Opportunity for relative soft power gains: US soft power depends, to a significant degree, on its image as the oldest continuous democracy. Any perception of instability would likely further hamper its democracy promotion efforts and the attractiveness of the Western model. The potential competitor states that have felt threatened by these efforts would benefit from the perceived weakness in the US democratic appeal.

More integrated and hybrid cyber practices: For Russia, cyber is not only a separate technical category. Rather, cyberspace is seen in a synergic context as comprising the practices of informational and psychological operations.[13] These wider information technology practices are considered to be cheap and effective methods of influencing a target for strategic added value. This means that the opportunities – such as advanced capabilities in cyber hacking – can act seamlessly in tandem with other more traditional methods such as disinformation campaigning and trolling.

Furthermore, evidence of two sets of past practices provides indications for contemporary and future geopolitical actions.

Contemporary evidence for geopolitical cyber operations: During Ukraine's 2014 presidential elections, Russian cyber-attacks were found to have destroyed software and damaged hard drives and backup systems.[14] However, the Ukrainian case did not rely on a cyber vector. There were many other means of carrying out operations in Ukraine. A telling case concerning interference in the electoral process was the Scottish 2014 referendum for independence. In this case, supposed Russian election observers provided legal assistance for the 'yes' campaign. Propaganda and trolling was also detected.[15] Even though the results of the Scottish referendum were not favourable to the supposed Russian interests, they still managed to question the cohesion of the EU, and more widely the West. The election was framed by Russian propaganda as a pivotal opportunity to reclaim national rights from the EU.

Evidence of general election operations: The Russian government has claimed to have provided moral support and, in some cases, even financial support for rising far-right movements to help them propagate their views. Marine Le Pen from France's far-right National Front has admitted taking loans from Russia. The Russian 'hand' can also be seen in the 2016 Dutch Ukraine treaty referendum. As Anne Applebaum has stated, in the case of the Dutch referendum, "Many of the 'no' campaign's

[12] See for example: Nato Review (2016): The "Lisa case": Germany as a target of Russian disinformation, http://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/, last accessed 26.10.2016.

[13] Mattiisen, Mariita (2016): "What Russia Wants in Regulating the IT Field", June 2016, *Diplomaatia*, http://www.diplomaatia.ee/en/article/what-russia-wants-in-regulating-the-it-field/, last accessed 26.10.2016.

[14] Coker, Margaret; Sonne, Paul (2015): "Ukraine Cyberwar's Hottest Front", 9.11.2015, *The Wall Street Journal*, http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671, last accessed 26.10.2016.

[15] Ostanin, Iggy; Rose, Eleanor (2016): "Brexit: How Russian Influence Undermines Public Trust in Referendums", 20.6.2016, Organized Crime and Corruption Reporting Project, https://www.occrp.org/en/investigations/5368-brexit-how-russian-influence-undermines-public-trust-in-referendums, last accessed 26.10.2016.

themes, headlines and even photographs were lifted directly from Russia Today and Sputnik, Russia's state propaganda website". Anti-EU sentiments were effectively co-opted for the strategic purpose of hindering the free trade agreement between the EU and Ukraine. Many of these sentiments were endogenous to the Netherlands, but Russian disinformation may have had the effect of exogenously accentuating these tendencies.

Democratic election-hacking vulnerability

For any outside actor, the operation to somehow manipulate the US debates in order to allow a suitable candidate to win a major party's candidacy seems far too complicated to carry out. It would require massive efforts, unseen strategies and tactics, and extreme luck. However, a more modest and qualified hypothesis can be suggested. It is possible that once a candidate emerged whose views were different from the long-standing consensus in the US, an opportunity opened up to undermine the other candidate's campaign. The US election debates have shown that a major power's decades-old foreign policy debates can change. What is more, radical disagreements can result.

An election-hacking campaign can be an increasingly effective part of the overall effort to disrupt the election process, stir up trouble in liberal democracies, and decrease the appeal of the democratic model. The growing sentiment that there is something seriously wrong with the elections, that they are biased towards one candidate, or that they are somehow rigged can be seen as the main goal of any election hacking operation. External actor(s) can try to sow widespread distrust of the election process and, in so doing, cause legitimacy challenges for the democratic succession. This, in turn, can further accentuate anti-establishment sentiments and complicate the coherent formulation of policies after the "challenged" elections.

Evidence of at least some level of interference in several important elections and referendums should be a clear danger signal that calls for situational awareness and, possibly, counteractions. These include increasing cyber-security counter-measures as well as political-level strategic decision-making on how to respond to serious threats without escalating the situation too much. For an illicit outside actor, a deep understanding of the overall quirks and asymmetries of the connected political life of Western democracies provides opportunities for strategic influence and destabilization. For the authorities in the democratic states, similar in-depth knowledge is needed in the future to secure election processes and to establish a strong degree of election-related cyber-deterrence through measures such as economic sanctions and de-escalatory counter-hacking. The key is to attribute the election hacking to the correct actor(s), to understand how these actors can best be held at bay and, if an attack has already occurred, how they can be conditioned in a lasting way to stay out of future elections.

There is still a degree of naivety in the West over the self-preserving nature of the democratic process. The digital dimension and cyber hacking are clearly becoming more deeply and widely established parts of the overall election influence operations. However, cyber is not the meat of the matter. The crux of the operations still lies in the more traditional methods of influence, and will continue to do so until the cyber influence operation has proved to be effective. This threshold might have been crossed during the US 2016 elections.

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

ISBN 978-951-769-507-7
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.