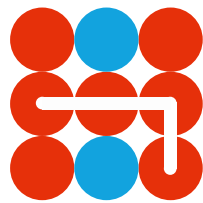


AUGUST 2018

Hybrid CoE Strategic Analysis 10
**Cyberspace - Just another
domain of election interference?**

LIISA PAST



Hybrid CoE

Cyberspace - Just another domain of election interference?

Cyberspace, and particularly election technology, has become a new domain for those who wish to suppress or interfere with the key processes of democratic societies in order to further their own ends, writes Liisa Past, Next Generation Leader at the McCain Institute for International Leadership and former Chief Research Officer at the Cyber Security Branch of the Estonian Information System Authority.

Influence, social media and information campaigns against elections and election campaigns are no longer an unexpected occurrence. Rather, they have become a planning assumption. Cyber attacks against the essential functions of democratic systems, as well as those who are involved in election campaigns, are often integrated with such operations.

In the case of elections, the networks, data and machines used, as well as the IT systems of those involved in politics, have been targeted. These cyber attacks seek to compromise the confidentiality, availability or integrity of the very systems that underpin the key processes of democracy.

Hence, it is imperative to build tactics, techniques and procedures to deter, detect, combat and mitigate the effects of attacks that can effectively delegitimize electoral outcomes. In addition to the US November 2018 midterms, which are likely to be closely observed by adversarial actors and cyber defenders alike, direct elections across Europe will lead to the election of a new European Parliament in May 2019.

Universal reliance on technology

Elections form the very core of a democratic system. Regardless of the specific electoral system, all elections rely on some elements of information technology. Even those election management bodies that rely exclusively on paper and often postal ballots to gather votes are nonetheless likely to take advantage of IT solutions in voter and candidate registration and the corresponding databases, preparation of voter and candidate lists, and in tallying results or publishing the outcomes.

It should be noted that election interference and fraud, in themselves, are not new phenomena. Neither digital nor analogue (pen and paper) technology is essentially secure or not secure per se. Rather, the specific risks of any election organization have to be assessed and mitigated case by case. It is up to the election management bodies and legislators to find and implement solutions – digital or analogue – that technically and legally fulfil the requirements of democratic elections: free, fair and open, as well as guaranteeing a secret ballot.



2016 - Breaking a taboo?

Attempts to influence politics, and elections in particular, are not a result of the deployment of digital technologies; efforts to delegitimize these processes have always been part of the adversary's playbook. Rather, cyberspace, and particularly election technology, has become a new domain for those who wish to suppress or interfere with the key processes of democratic societies in order to further their own ends.

At the same time, it was – perhaps naively – believed in the Western world that the key processes of democracies would not become a target of state-backed or politically inspired cyber attacks, at least not during peacetime. The 2016 French and US presidential elections highlighted that cyberspace has become a domain of influence over democratic processes in which states and other political actors can assert their power opportunistically, methodically, and sometimes indiscriminately. These attempts now form an ever-present and sustained environment that nations as well as international organizations and election management bodies will need to treat as a planning assumption if the legitimacy and sanctity of elections are to be upheld.

While the central functions of the electoral process – the gathering and counting of votes – are not impervious to attack, it would be extremely difficult and costly to scalably compromise that process and go undetected. Instead, auxiliary targets such as candidates, parties, campaigns, as well as the systems and vendors that elections

rely on, have been the preferred target of cyber attacks. Given the strategic goal of delegitimizing the process and the typically opportunistic behaviour of the attacker, their cost-benefit calculation is likely to favour this low-hanging fruit of lesser consequence and not the central functions of the electoral process, where stricter security procedures and clear legal requirements are in place.

In the case of the 2019 European Parliament election, the potential attack surface also includes the transfer of both the indicative and binding results. This is particularly significant as it is the first European election in the changed security environment, while national electoral procedures have been tried and tested since 2016.

Patterns in the adversarial strategy behind election interference

The most notorious attempts to meddle in elections, specifically the 2016 US presidential race, have been attributed to Russia. Only national governments are likely to have both the resources and the motivation to systematically discredit democratic processes over a sustained period of time, even if proxies and privateers are deployed. Such an adversarial strategy seeks to sow doubt and mistrust towards democratic systems to advance the adversary's own national interests and strategic goals.

To be able to counter election interference in the most effective way, the patterns of digital interference need to be understood.



To this end, the following factors and features have been identified in connection with state-backed cyber attacks against elections:

- **Opportunistic and reactive:** while pursuing a strategic goal, the adversary is agile and willing to experiment at the operational level. They seem, for example, to be constantly pushing ahead and assessing the potential intelligence and influence value of the information gained.
- **Wide attack surface:** the cyber attacks attributed to nation-state or related actors extend across sectors and targets, highlighting an integrated approach where no target is out of scope at any given time. Targets have included a variety of political actors, including major parties and candidates, campaign staff as well as election organizers and technology vendors. Similarly, the media or other solutions used to display and publish results are likely to be targets, as disrupting the announcement of the outcomes creates the confusion needed to delegitimize the whole process.
- **Using all or any tools and techniques:** in pursuing their goals and constantly monitoring opportunities, malicious actors driven by political motivation are likely to deploy both widely-known and openly available (albeit often through the dark web) tools (including exploits), as well as those custom-developed for their particular use.
- **Better-resourced:** to be able to take advantage of a wide range of tools and techniques as well as talent, these actors need to have a reasonable supply of resources at their disposal, both

human and capital, with a high level of flexibility in how they can be deployed.

- **Patient:** as the goal is strategic, the attackers are persistent and often proceed slowly to avoid detection. The DNC hack demonstrated the patience and the timescale involved: a US analysis has revealed that Russian actors had been compromising the system for about a year and a half and continued to do so right up to election day. This approach is distinct from the grab-and-go mindset of criminals motivated by profit. Taking a longer-term view, a system may be compromised over an extended period of time. This type of action is consistent with the priming phase in the conceptual work on hybrid threats.

Comprehensive defences

Resilience and security by design, comprehensive risk-based approaches, good development practice, and prudence in introducing innovation as well as cyber hygiene are key when it comes to successfully protecting the cyber security of elections. Furthermore, at no point should any innovation be introduced into electoral procedures at the expense of security; if the security principles are followed, digital technology can, in fact, bolster security.

As an example of a comprehensive approach, the *Compendium on Cyber Security of Election Technology*, published by a work stream of the Cooperation Group of the Network and Information Security (NIS) Directive, reviews the complete lifecycle of elections. It offers comprehensive, practi-

cal and actionable guidance on bolstering cyber security for election organizers and cyber security agencies alike, based on the contributions of around two dozen EU member states and a number of European institutions.

In summary, the following aspects need to be considered if election interference in the cyber and digital domain is to be countered successfully.

First of all, cyber security of **election technology needs to be viewed in a wider context**, allowing for risk-driven decision-making that also encompasses the full spectrum of hybrid threats, as well as risks arising from technology, management, decision-making and resource allocation. Where appropriate, elections could be viewed as critical national infrastructure or essential services, which would result in mandated standards and extra protection automatically being extended to them.

Secondly, it is important to note that **the election management bodies are not likely to be empowered and resourced to lead the effort alone**, so a cross-government approach is called for.

Thirdly, while **we have not yet seen collective international response to cyber attacks against elections, the international coordination efforts are promising**. The EU Cyber Diplomacy Toolbox allows for Common Foreign and Security Policy (CFSP) measures in response to aggression in cyberspace, and could be used in the case of election meddling. Furthermore, experience and operational-threat sharing among like-minded nations is already underway since similarities exist in the adversary's attack tools and behaviour.

Fourthly, **attribution and public discussion of cyber attacks are essential tools**

when deterring election interference in the digital and cyber domains.

It should be noted, however, that further standardization of election procedures and organization is not desirable and is unlikely to lead to increased cyber security of democratic processes. Nations should fundamentally maintain their sovereignty over democratic processes, including election organization, as long as the principles of open, free and fair elections are complied with. **The diversity of election systems itself serves as a powerful protection mechanism in that the spillover effect of potential election compromises is limited, and hence attacks are unlikely to be scalable internationally.**



Author

Liisa Past (MA)) is a Next Generation Leader at the McCain Institute and former Chief Research Officer at the Cyber Security Branch of the Estonian Information System Authority, where she designed, led and carried out an analysis related to cyber security, including risk, threat and impact assessments. She has been one of the driving forces behind the Estonian comprehensive risk assessment of elections and the *Compendium on Cyber Security of Election Technology*, published by the Cooperation Group of the Network and Information Security Directive.

Literature:

Alperovitch, D. (2016). Bears in the Midst: Intrusion into the Democratic National Committee. *CrowdStrike*. Available at: <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>

Cooperation Group of the Network and Information Security Directive, *Compendium on Cyber Security of Election Technology*, CG Publication 03/2018, Brussels. Available at: https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Department Of Homeland Security, Office of the Director of National Intelligence (2016). Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security, Department of Homeland Security. Available at: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>

Director of National Intelligence (2017). Assessing Russian Activities and Inten-

tions in Recent US Elections, Director of National Intelligence. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Fuchs, M. H., Kenney, C., Perina, A., & VanDoorn, F. (2017). Why Americans Should Care About Russian Hacking, Center for American Progress. Available at: <https://cdn.americanprogress.org/content/uploads/2017/02/13093554/Russian-HackingWhyItMatters-brief.pdf>

Kelly, M. (2018). Megyn Kelly's extended interview with Russian President Vladimir Putin in Kaliningrad for NBC News. Available at: <https://www.nbcnews.com/video/watch-megyn-kelly-s-extended-interview-with-russian-president-vladimir-putin-in-kaliningrad-1182806083818?v=raila>

Martin, C. (2017). 'Cyber security: fixing the present so we can worry about the future', an address to the Times Tech Summit, National Cyber Security Centre. Available at: <https://www.ncsc.gov.uk/news/cyber-security-fixing-present-so-we-can-worry-about-future>

Nurse, J., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., . . . Creese, S. (2016). An Independent Assessment of the Procedural Components of the Estonian Internet Voting System. University of Oxford, Cyber Studies Programme. Oxford: University of Oxford.


Past, L. (2017). All Elections are Hackable: Scalable Lessons from Secure I-Voting and Global Election Hacks. *European Cybersecurity Journal*, 3(3), 34–47, Available at: https://www.riaa.ee/sites/default/files/content-editors/kuberturve/ecj_volume3_issue3_extract_past.pdf

Past, L. (2018). 2016–2018 – Breaking the Cyber Security Taboos. *Netherlands' Military Law Review*, Cyber Special Edition. Available at: https://puc.overheid.nl/mrt/doc/PUC_248137_11/

Priestap, B. (2017). Statement of Bill Priestap, Assistant Director Counterintelligence Division Federal Bureau of Investigation Before the Select Committee on Intelligence United States Senate For a Hearing Entitled "Assessing Russian Activities and Intentions in Recent Elections" Presented June 21, 2017, US Senate Select Committee on Intelligence. Available at: <https://www.intelligence.senate.gov/sites/default/files/documents/os-bpriestap-062117.pdf>

Singer, P. (2017). Prepared Testimony and Statement for the Record at the hearing on 'Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities' Before the House Armed Services Committee. Available at: <https://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Wstate-SingerP-20170301.pdf>

United States of America v. Viktor Netyksho, Boris Antonov, Dmitriy Badin, Ivan Yermakov, Aleksey Lukashev, Sergey Morgachev, Nikolay Kozachek, Pavel Yershov, Artem Malyshev, Aleksandr Osadchuk, Aleksey Potemkin, Anatoliy Sergeyevich Kovalev, Case 1:18-cr-00215-ABJ, The United States District Court for the District of Columbia July 13, 2018. Available at: <https://www.justice.gov/file/1080281/download>



US Election Assistance Commission (2017). Starting Point: U.S. Election Systems as Critical Infrastructure (Whitepaper), US Election Assistance Commission.
Available at: https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

Vassil, K. & Solvak, M. (2016). E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005–2015) Tartu: Johan Skytte Institute of Political Studies, University of Tartu.

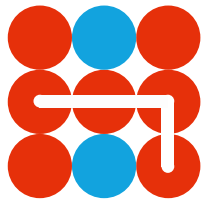
The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-51-9
ISSN 2670-2282

Second version of the publication. Previously published as "Strategic Analysis August 2018: Cyberspace - Just another domain of election interference?"

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

The responsibility for the views expressed ultimately rests with the authors.



Hybrid CoE