THE EU CYBERSECURITY AGENCY

ELECTION CYBERSECURITY: CHALLENGES AND OPPORTUNITIES

February 2019

In a democratic society, a high level of cybersecurity is key for safeguarding the whole election lifecycle.

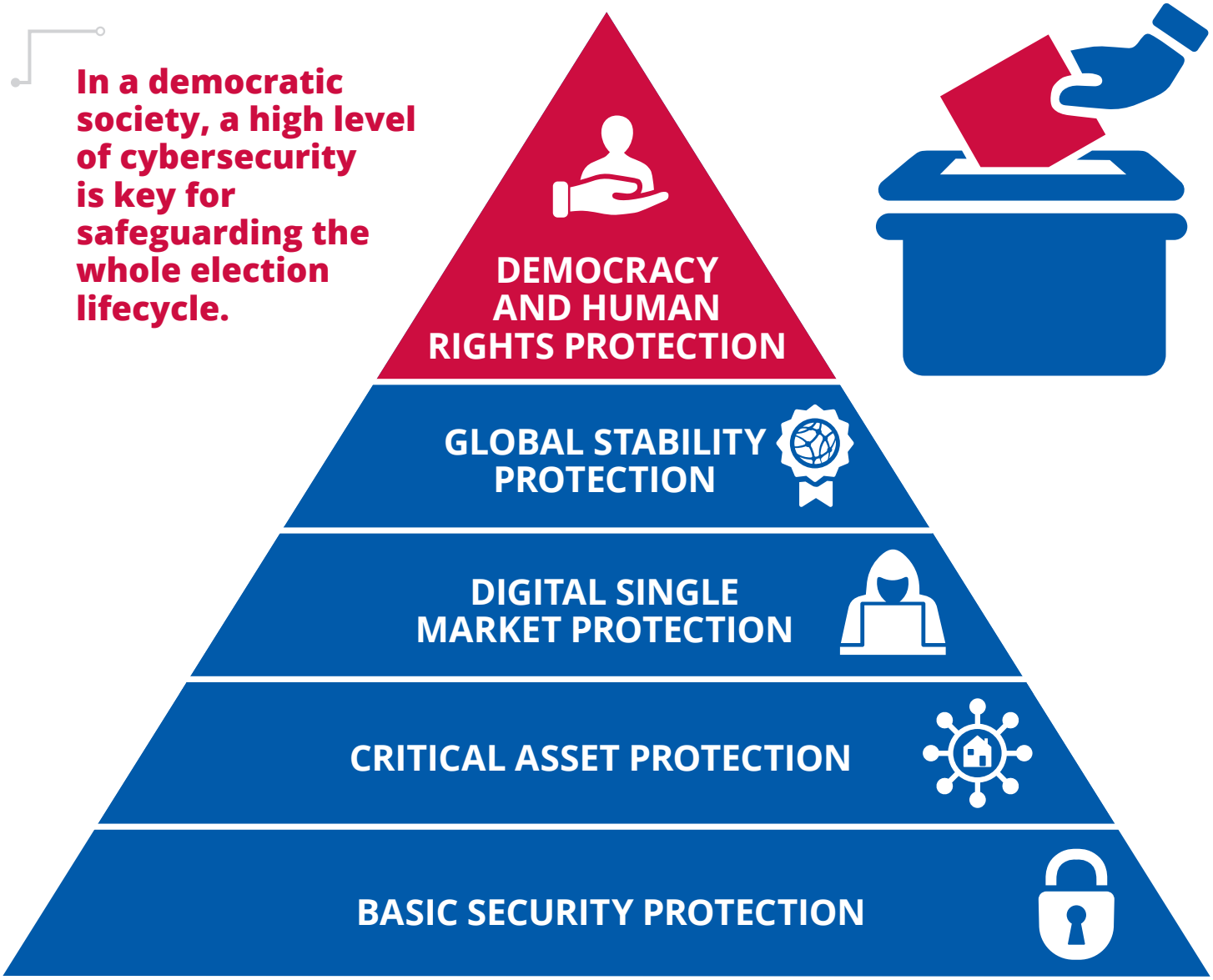


TABLE OF CONTENTS

Picture on the cover: "Cyber space and layers of protection", European Union Agency for Network and Information Security (ENISA) , "ENISA overview of cybersecurity and related terminology" available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

1. RECOMMENDATIONS

1.1 Digital Service Providers, social media, online platforms and messaging service providers are advised to deploy technology that will identify unusual traffic patterns that could be associated with the spread of disinformation or cyberattacks on election processes.

1.2 While it is recognised that some of the above players have agreed to self-regulate and introduce disinformation policies, consideration should be given to regulation of these platforms at an EU level to ensure a consistent and harmonised approach across the EU to tackling online disinformation aimed at undermining the democratic process.

1.3 Member States should continue to actively work together with the aim to identify and take down botnets.

1.4 ENISA supports the general and specific technical proposals to mitigate the risks that are documented in the Compendium on the Cyber Security of Election Technology.

1.5 Developing more exercises aimed at testing election cybersecurity will help improve preparedness, understanding and responding to possible election-related cyber threats and attack scenarios.

1.6 Official channels/technologies for the dissemination of the results should be identified. Additionally, back-up channels/technologies should be available to validate the results with the count centres. Where websites are being used, DDoS mitigation techniques should be in place.

1.7 A legal obligation should be considered to classify election systems, processes and infrastructures as critical infrastructure so that the necessary cybersecurity measures are put in place.

1.8 A legal obligation should be put in place requiring political organisations to deploy a high level of cybersecurity in their systems, processes and infrastructures.

1.9 Member States should consider introducing national legislation to tackle the challenges associated with online disinformation while protecting to the maximum extent possible the values set down in the Treaty of Lisbon and the Charter of Fundamental Rights of the EU.

1.10 The cybersecurity expertise of the state should be used to assist political practitioners in the securing of their data and their communications. For example, CSIRT expertise can be leveraged to support political parties.

1.11 Political parties should have an incident response plan in place to address and counter the scenario of data leaks and other potential cyber-attacks.

1.12 Increased cooperation and exchange of best practices and experiences between the Member States and at EU-level can contribute to strengthening cybersecurity across the EU, including the cybersecurity of the election process. Member States should also make use of the existing frameworks and structures that are in place.

2. INTRODUCTION

If we look at modern history, the term "cyber" was first coined by the French physicist André-Marie Ampère who suggested that "the future science of governments should be called "la cybernétique".[1] In the 1940s, the term was taken up again by Norbert Wiener who defined "Cybernetics" as "the science of control and communication in the animal and the machine".[2] However, the word originally comes from the Greek word 'Κυβέρνηση' (pronounced 'Kyvérnisi'), which means government.

In a democratic society, 'Cybersecurity'[3] may also involve ensuring the transparent operation of a governance or election system. This protection should include the integrity, availability and confidentiality of election processes.

The original root of the word cyber takes on renewed importance, as there are increasing reports of cyber-enabled threats with a potential to undermine democratic processes across the EU and beyond.[4] Of particular significance is the possibility of interference in elections by cyber means, due to the widespread use of digital technology to support electoral processes. For example, digital technology is used to support:

- Confidential communications of politicians and political parties;
- Political campaigns;
- Communication via the media;
- The electoral register;
- The casting of votes;
- The counting of votes;
- The dissemination of the results.

Vulnerabilities in relation to any of these elements may form a target for exploitation by malicious actors seeking to interfere in and undermine the legitimacy of democratic elections. As a result, promoting a high level of cybersecurity across the EU plays an important role in safeguarding the whole election lifecycle. In this context, the 2019 European Parliament elections, which involve election processes at national level in all EU Member States, are fast approaching. Due to their scale and the different electoral systems used in the various Member States, these elections are susceptible to interference by cyber means.

The original root of the word cyber takes on renewed importance, as there are increasing reports of cyber-enabled threats with a potential to undermine democratic processes across the EU and beyond.

A recent Eurobarometer survey on democracy and elections demonstrates public concern surrounding election interference. In particular, 61 percent of respondents expressed some level of concern about the possibility of elections being manipulated through cyberattacks.[5]

This paper presents ENISA's opinion on the cybersecurity of elections and provides concrete and forward-looking recommendations to improve the cybersecurity of electoral processes in the EU.

1 Ampère, AM, *Essai sur la philosophie des sciences, ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines.* Première partie, Paris, Bachelier, 1834.

2 Wiener, N, *Cybernetics or Control and Communication in the Animal and the Machine.* Technology Press, 1948.

3 Defined in the European Commission Proposal for a Cybersecurity Act (COM/2017/0477) as *"[...] all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;"* available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A0477%3AFIN

4 See: European Union Agency for Network and Information Security, *"ENISA Threat Landscape 2018"*, January 2019, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

5 European Commission, *Special Eurobarometer 477 "Democracy and elections"*, September 2018, available at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2198

3. MOTIVATIONS AND ACTORS

With the increase in the digitalisation of our lifestyles, information can be transferred across the globe in seconds. With regard to elections, the traditional sources of information in the form of national broadcasters, and paper media are diminishing and content is often being provided and uploaded into the digital ecosystem by individuals, e.g. on digital platforms and social media.

The threat actors often associated with cyber interference in the election process include:[6]

- Black hat hackers;
- Terrorists;
- Criminals;
- Nation states / nation state sponsored actors;
- Insiders;
- Hacktivists;
- Politically motivated groups.

Additionally, an evolving threat is the motivation behind the actors interfering with the due process of elections by cyber means. The motivation for the actors can be manifold. Examples include:[7]

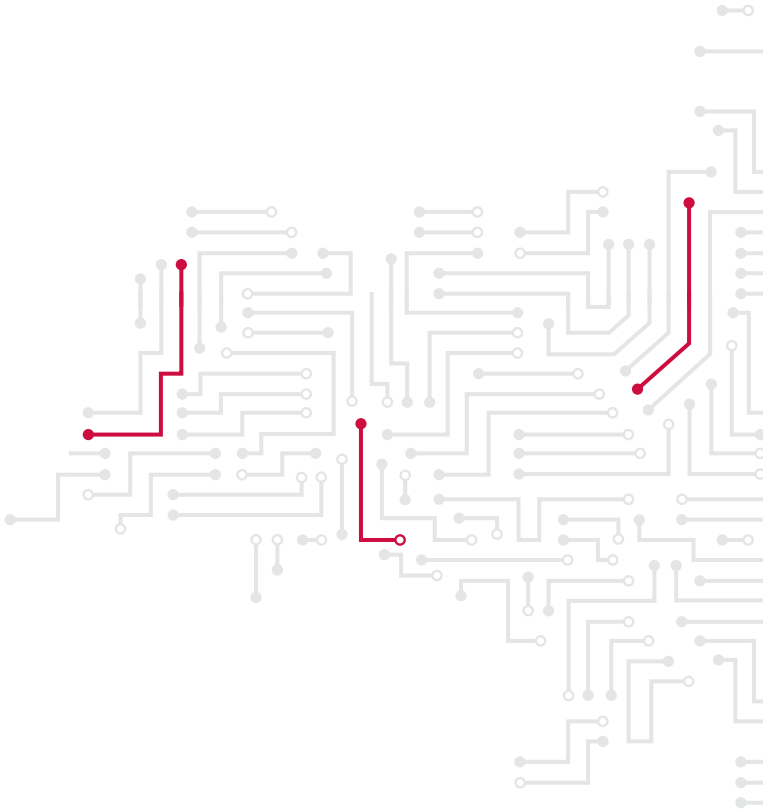
- Financial gain;
- Fame and reputation;
- Provoking chaos / anarchy;
- Foreign policy / national interests;
- Vengeance;
- Sowing social division;
- Subverting political opposition;
- Undermining trust in democracy.

The analysis of any cyber incident has to take into account both the motivation and the type of actor, as well as their associated capabilities. An additional complication is that these actors with their motivations can generate cyber interference using automated tools such as botnets.[8] Botnets are now readily available at very low cost to actors on the dark web and their potential effect should not be underestimated. Another effect from using botnets is that attribution can be difficult.

Recommendation 1: Digital Service Providers, social media, online platforms and messaging service providers are advised to deploy technology that will identify unusual traffic patterns that could be associated with the spread of disinformation or cyberattacks on election processes.

Recommendation 2: While it is recognised that some of the above players have agreed to self-regulate and introduce disinformation policies, consideration should be given to regulation of these platforms at an EU level to ensure a consistent and harmonised approach across the EU to tackling online disinformation aimed at undermining the democratic process.

Recommendation 3: Member States should continue to actively work together with the aim to identify and take down botnets.



6 Defending Digital Democracy Project (D3P), *"The State and Local Election Cybersecurity Playbook,"* Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018, available at: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

7 Ibid.

8 Supra note 4, at p. 59-63.

4. AN EVOLVING THREAT LANDSCAPE FOR CYBER ATTACKS ON ELECTION SYSTEMS AND PROCESSES

Several methods can and have been used to influence or undermine the integrity of electoral processes by cyber means. As a result of the large attack surface that is inherent to elections, the risks do not only concern government election systems, but also extend to individual candidates and individual political campaigns. Examples of attack vectors that affect election processes include:

- Spear phishing;
- Data theft;
- Online disinformation;
- Malware; and
- (Distributed) Denial-of-Service (DDoS) attacks.

The *"Compendium on the Cybersecurity of Election Technology"* prepared by the Cooperation Group set up under the 2016 Network and Information Security Directive, to which ENISA has contributed, contains detailed information on examples of cyberattacks on election processes. In recent years, there have been an increasing number of reports of these techniques being used to interfere with election processes.[9]

The risks are by no means limited to electronic voting or voting machines. For example, DDoS attacks have been reported targeting the Central Election Commission in Bulgaria, and electoral websites in the Czech Republic.[10] Other reported examples illustrate that politicians and political campaigns may also form a target. These examples include the 2016 Democratic National Committee (DNC) email leak in the run-up to the US presidential elections[11] and the reported cyber meddling in the 2017 French presidential elections[12].

As the agency tasked with contributing to the network and information security of the Union, ENISA is prepared to support and advise on efforts that aim to improve the resilience and preparedness of the election process across the EU. In particular, in view of the upcoming European Parliament elections, ENISA also supports the preparedness at Member State level by working with the national electoral commission to test simulations of cybersecurity incidents and disinformation campaigns aimed at disrupting the electoral process[13]

Recommendation 4: ENISA supports the general and specific technical proposals to mitigate the risks that are documented in the *Compendium on the Cyber Security of Election Technology*

Recommendation 5: Developing more exercises aimed at testing election cybersecurity will help improve preparedness, understanding and responding to possible election-related cyber threats and attack scenarios.[14]

As the agency tasked with contributing to the network and information security of the Union, ENISA is prepared to support and advise on efforts that aim to improve the resilience and preparedness of the election process across the EU.

9 NIS Cooperation Group, *"Compendium on Cyber Security of Election Technology"*, CG Publication 03/2018, July 2018, p. 49, available at: https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

10 Ibid.

11 See e.g. Geller, E, *"Inside the race to hack-proof the Democratic Party"*, Politico, 17 October 2018, available at: https://www.politico.com/story/2018/10/17/democrats-hacking-cybersecurity-dnc-909883

12 BBC News, *"French election: Emmanuel Macron condemns 'massive' hack attack"*, 6 May 2017, available at: https://www.bbc.com/news/world-europe-39827244

13 ENISA 'ENISA supports Portuguese National Cybersecurity Exercise on electoral process', 26 February 2019, available at https://www.enisa.europa.eu/news/enisa-news/jenisa-supports-portuguese-national-cybersecurity-exercise-on-electoral-process

14 See: Wolf, P, *"Cybersecurity and Elections: An International IDEA Round-table summary"*, International Institute for Democracy and Electoral Assistance (IDEA), 7 August 2017, available at: https://www.idea.int/news-media/news/cybersecurity-and-elections-international-idea-round-table-summary

5. LIFECYCLE OF THE ELECTION

The election process and the risks associated with it can be divided into a number of sections. These include:

- The maintenance of the electoral register;
- The public political campaigning process;
- The voting process;
- The delivery of the results.

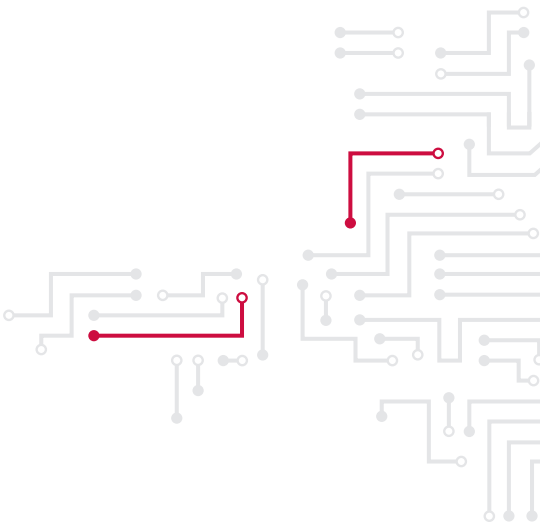
The electoral register is a list of persons eligible to vote in elections. Registration in the electoral register is generally managed by the local authorities. Where enrolment is not automatic, voter registration frequently takes place through the action of physically registering at the authority in question. As a result, many countries are not dependent on a central registry. Postal distribution is often used to notify registered persons of the election process. In view of these factors, the cybersecurity risk level associated with the electoral register is considered medium.

As follows from the analysis provided in this opinion paper, the public political campaigning process is susceptible to cyber interference. Due to the high complexity of this step in the election lifecycle, the different attack vectors, and the reported examples of disinformation and data leaks (see section 6), the cybersecurity risk level in this area is considered high.

Given that the majority of Member States have either postponed or discontinued the use of electronic voting, the risk associated with the voting process can be considered to be somewhat reduced. Examples of countries that have postponed or discontinued electronic voting include Ireland,[15] the Netherlands,[16] France,[17] Finland[18] and Germany.[19] In the Netherlands in 2017, the government also decided to return to counting votes by hand instead of the electronic counting due to cybersecurity concerns.[20] Examples of countries that make use of electronic voting technology include Estonia[21] and Belgium[22].

Taking into consideration that, as noted above, the roll-out of electronic voting has been either discontinued or postponed in a number of Member States, the cybersecurity risk level in relation to the voting process is considered medium. This cybersecurity risk level is likely to be higher in countries where e-voting systems are being implemented. A distinction should also be made between online and offline e-voting systems, where the former is likely to entail a higher cybersecurity risk level than the latter.

Results are generally counted in election count stations, which are accessible to the public in some jurisdictions. The dissemination of the results is covered by the media and typically takes place via several channels of communication, including broadcast television, online media, and print media. In view of these factors, the cybersecurity risk level is considered medium. The cybersecurity risk level is likely to be higher in jurisdictions which use digital technology to count votes.



15 O'Halloran, M and O'Regan, M, *"E-voting machines to be disposed of"*, The Irish Times. 6 October 2010, available at: https://www.irishtimes.com/news/e-voting-machines-to-be-disposed-of-1.865193

16 Ritzen, G, *"Kabinet: stemmen worden bij verkiezingen met de hand geteld"*, NRC, 1 February 2017, available at: https://www.nrc.nl/nieuws/2017/02/01/kabinet-stemmen-worden-bij-verkiezingen-met-de-hand-geteld-a1544017

17 Reuters, "*France drops electronic voting for citizens abroad over cybersecurity fears*", 6 March 2017, available at: https://www.reuters.com/article/uk-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUKKBN16D235

18 Ministry of Justice Finland, *"Working group: Risks of online voting outweigh its benefits"*, 19 December 2017, available at: https://oikeusministerio.fi/en/article/-/asset_publisher/tyoryhma-nettiaanestyksen-riskit-suuremmat-kuin-hyodyt

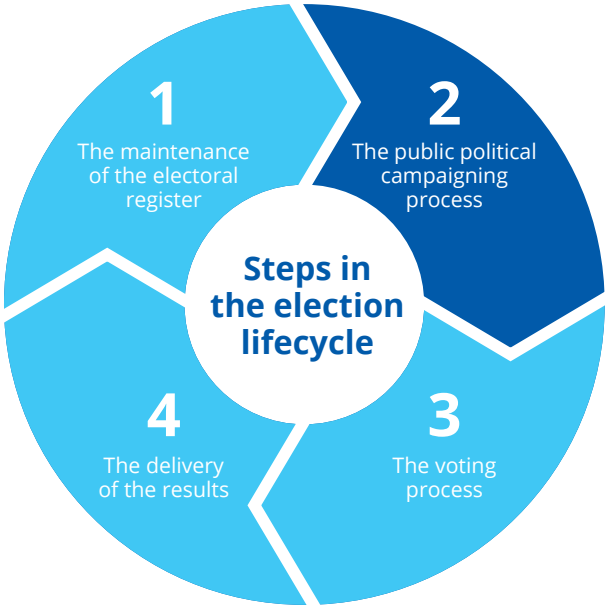
19 Deutsche Welle, *"German Court Rules E-Voting Unconstitutional"*, 3 March 2009, available at: https://www.dw.com/en/german-court-rules-e-voting-unconstitutional/a-4069101

20 Supra note 16

21 Valimised.ee (Estonian elections website), "Internet voting in Estonia", available at: https://www.valimised.ee/en/internet-voting/internet-voting-estonia

22 Flemish Parliament, *"Digitaal Stemmen"*, available at: https://www.vlaanderen.be/nl/vlaams-parlement/verkiezingen/digitaal-stemmen

Taking into account the above, from a cybersecurity perspective, ENISA considers the cybersecurity risks as follows:



Cyber risk level: High Medium Low

Recommendation 6: Official channels/technologies for the dissemination of the results should be identified. Additionally, back-up channels/technologies should be available to validate the results with the count centres. Where websites are being used, DDoS mitigation techniques should be in place.

6. THE ROLE OF HUMAN FACTORS AND ONLINE DISINFORMATION

In addition to the technical aspects of election cybersecurity, a number of human factors have to be taken into account. For example, human error and poor cyber hygiene[23] (weak passwords and poorly configured IT systems) can result in vulnerabilities that may be exploited thereby resulting in interference to elections, e.g. through data leaks.

Online disinformation represents another tool that may be used by malicious actors in an attempt to influence human decision-making. So-called "fake news" has gained the attention of the media and policymakers due to reports of its misuse in both the media and on social networks with the intention to influence the opinions of citizens, which potentially have a consequential effect on voting choices. Examples include the alleged interference in the British EU membership referendum[24], the 2016 US presidential elections[25], and the 2017 French presidential elections[26]. Other documented examples include the use of social media profiling to target voters without either their knowledge or their consent.[27]

6.1 ADDRESSING ONLINE DISINFORMATION

In April 2018, ENISA published an opinion paper outlining a number of policy recommendations in relation to online disinformation[28], which was provided as input to the European Commission's Communication on this topic. Subsequently, a number of online platforms, social networks and advertisers endorsed a self-regulatory Code of Practice on Disinformation proposed on the initiative of the Commission.[29]

In its fake news opinion paper, ENISA provided two recommendations that are of particular importance in the context of elections:

Recommendation 7: A legal obligation should be considered to classify election systems, processes and infrastructures as critical infrastructure so that the necessary cybersecurity measures are put in place; and

Recommendation 8: A legal obligation should be put in place requiring political organisations to deploy a high level of cybersecurity in their systems, processes and infrastructures.

In relation to the designation of election systems as critical infrastructure, the US Department of Homeland Security has recently implemented such a policy.[30] ENISA also noted the potential of Artificial Intelligence (AI) in combating online disinformation. However, AI alone is not a silver bullet. AI will have difficulty in addressing cultural differences, political humour, cynicism, satire, and other non-literal means of communication. Consequently, the results of any AI analyses must be validated by humans.

23 See: European Union Agency for Network and Information Security, *"Review of Cyber Hygiene Practices"*, December 2016, available at: https://www.enisa.europa.eu/publications/cyber-hygiene

24 See e.g. House of Commons Digital, Culture, Media and Sport Committee, *"Disinformation and 'fake news': Interim Report"*, July 2018, available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

25 See e.g. Faris, R, et al. *"Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election"*, August 16 2017, available at: https://cyber.harvard.edu/publications/2017/08/mediacloud

26 See e.g. Ferrara, E, *"Disinformation and social bot operations in the run up to the 2017 French presidential election"*, 2017, available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.00086.pdf

27 See e.g. The Guardian, *"The Cambridge Analytica Files"*, available at: https://www.theguardian.com/news/series/cambridge-analytica-files

28 ENISA, *"Strengthening Network & Information Security & Protecting Against Online Disinformation ("fake news")"*, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/fake-news

29 European Commission, *"Code of Practice on Disinformation"*, Commission News Article, 26 September 2018, available at: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

30 Since January 2017. See: Congressional Research Service, *"The Designation of Election Systems as Critical Infrastructure"*, updated January 28, 2019, available at: https://fas.org/sgp/crs/misc/IF10677.pdf

6.2 NATIONAL LEGISLATIVE APPROACHES

Approaches by different Member States to the problem of online disinformation can be observed in the 2017 German Network Enforcement Act[31], and the 2018 French law against manipulation of information[32]. The use of legislation to tackle this problem is challenged by the need to balance the freedom of expression with the risk associated with the effects of disinformation on the public interest. For example, the French legislative proposal was declared constitutional following a challenge before the Constitutional Council.[33]

Recommendation 9: Member States should consider introducing national legislation to tackle the challenges associated with online disinformation while protecting to the maximum extent possible the values set down in the Treaty of Lisbon and the Charter of Fundamental Rights of the EU.

6.3 IMPROVING DATA PROTECTION AND PRIVACY

Human factors also play a role from the perspective of privacy and data protection, where the emails of politicians and political campaign staff were targeted. Reported examples include the 2016 Democratic National Committee (DNC) email leak in the US and the recent leak of politicians' data in Germany[34].

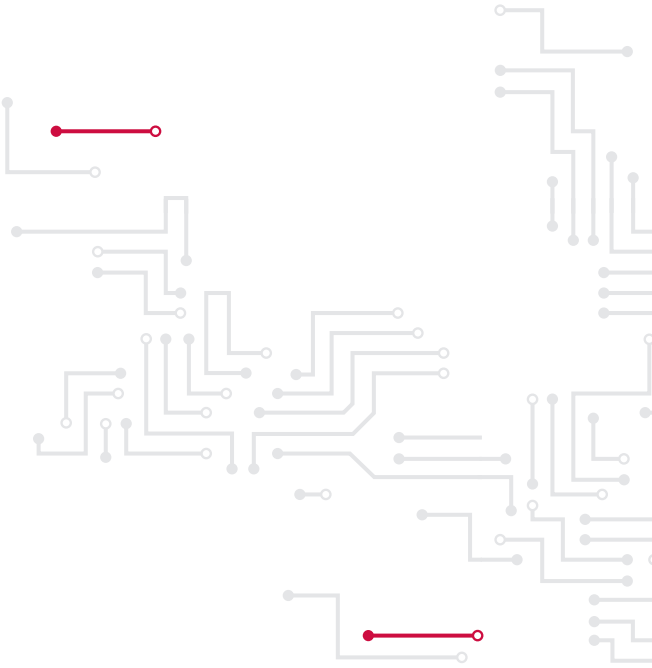
Appropriate trainings and guidance for politicians and their personnel in terms of securing their data and their communications contribute to addressing this issue. Examples that represent good practices in this area in some Member States include:

- the French initiative where ANSSI (the National Cybersecurity Agency of France) held a workshop on cybersecurity for political parties and MPs.[35]
- The UK, where the NCSC is working with political parties to better protect their data and communications, for example by providing guidance for political parties and their staff on protecting their digital systems and online profiles.[36]
- In Belgium, a guide for candidates and political staff has been developed on joint initiative of the State Security Service, the Centre for Cyber Security and the General Information and Security Service.[37]

One notable example of an active measure used to respond to cyber interference in the election process was the Macron campaign's use of counter-attack methods to misdirect hackers in the context of the 2017 French presidential elections.[38]

Recommendation 10: The cybersecurity expertise of the state should be used to assist political practitioners in the securing of their data and their communications. For example, CSIRT expertise can be leveraged to support political parties.

Recommendation 11: Political parties should have an incident response plan in place to address and counter the scenario of data leaks and other potential cyber-attacks.



31 See: Engels, S and Fuhrmann, T, *"Network Enforcement Act in A Nutshell"*, DLA Piper IPT Germany Blog, 31 January 2018, available at: https://blogs.dlapiper.com/iptgermany/2018/01/31/network-enforcement-act-in-a-nutshell/

32 Loi n° 2018-1202 relative à la lutte contre la manipulation de l'information, 22 December 2018, available at: http://www.senat.fr/dossier-legislatif/ppl17-623.html

33 Constitutional Council of France, Decisions n° 2018-773 and 2018-774 of 20 December 2018, available at: https://www.conseil-constitutionnel.fr/actualites/communique

34 The Guardian, *"German politicians' personal data leaked online"*, 4 January 2019, available at: https://www.theguardian.com/world/2019/jan/04/german-politicians-personal-data-hacked-and-posted-online

35 Baezner, M and Robin, P, *"Cyber and Information Warfare in elections in Europe"*, December 2017, available at: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf

36 UK National Cyber Security Centre, *"Statement: Guidance for political parties and their staff"*, 17 May 2017, available at: https://www.ncsc.gov.uk/news/statement-guidance-political-parties-and-their-staff

37 VSSE, CCB, and SGRS/ADIV, *"Veilig online tijdens de verkiezingscampagne/ Surfer en toute sécurité pendant la campagne électorale"*, February 2019, available at: https://www.ccb.belgium.be/fr/actualit%C3%A9/surfer-en-toute-s%C3%A9curit%C3%A9-pendant-la-campagne-%C3%A9lectorale

38 Logeswaran, A, *"How Macron's team thwarted the hackers with one simple trick"*, World Economic Forum, 11 May 2017, available at: https://www.weforum.org/agenda/2017/05/how-macrons-team-thwarted-the-hackers-with-one-simple-trick/

7. FOSTERING EUROPEAN COOPERATION IN ELECTION CYBERSECURITY

The cybersecurity of elections is a common issue that affects all the EU Member States. The cross-border relevance of working towards more cyber secure elections is all too evident in the context of the European Parliament elections, where cyber interference in one or more Member States has the potential to undermine the legitimacy of the full European election process. If malicious actors manage to give only the impression that the election process has been tampered with or has been conducted unfairly in one Member State, this could be enough to create the illusion that the whole European election process has been compromised. Therefore, cooperation amongst Member States is even more important.

In addition to cooperation between services within the Member States, further investing in European cooperation and information exchange efforts can play an important role. Such efforts can facilitate effective responses to cyber incidents, promote mutual learning between Member States, and help tackle and coordinate the issue of attribution.

Recommendation 12: Increased cooperation and exchange of best practices and experiences between the Member States and at EU-level can contribute to strengthening cybersecurity across the EU, including the cybersecurity of the election process. Member States should also make use of the existing frameworks and structures that are in place.

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For media enquires about this paper, please use press@enisa.europa.eu.

LEGAL NOTICE

AUTHORS

Aidan Ryan, ENISA
Olivier Van Geel, ENISA
Florian Pennings, ENISA
Rodica Tirtea, ENISA
Valerie Follmer, ENISA

COPYRIGHT NOTICE

Vasilissis Sofias Str 1
151 24 Maroussi, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu