Compendium on Elections Cybersecurity and Resilience

NIS Cooperation Group Publication

Updated version (2024)

First edition was published on 03/2018

ABOUT

This document has been drafted and endorsed by the NIS Cooperation Group.

The NIS Cooperation Group, composed of representatives of EU Member States, the European Commission, and the European Union Agency for Cybersecurity ('ENISA'), has been established by Article 14 of the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). The NIS Cooperation Group supports and facilitates strategic cooperation and the exchange of information among Member States, as well as strengthens trust and confidence between the EU Member States regarding cybersecurity issues.

Table of Contents

1. Introduction

During the last decade, elections across the globe have become a frequent target of cyberattacks. Cyber threat activity targeting elections has increased worldwide. These cyberattacks are often combined with information operations and other hybrid threats. Even when the actual vote is often carried out with pen and paper, electoral processes increasingly depend on network and information systems, and it is therefore important to take cybersecurity measures to protect the integrity of elections. **Cyber-attacks against the core functions of our democratic processes could undermine the safeguards in place to protect them, the participants in this best moment of the democratic process and the very legitimacy of democratic institutions.**

In the case of the elections for the European Parliament, a successful campaign of cyberattacks against one EU Member State could threaten to compromise the entire parliamentary election. For instance, the disruption of the network and information systems underpinning the elections in one Member-State, or even the perception of it, could impact vote counting and tabulation processes at the national level and cause a delay in Member States notification of the names of the elected Members to the Parliament resulting in affecting the proper functioning of the European Parliament or even its democratic legitimacy.

This compendium aims to support elections management bodies, national electoral authorities and cybersecurity bodies involved in cybersecurity and resilience of elections in the EU Member States. The present document is an updated version of the document published by the NIS Cooperation Group in March 2018. This living document provides guidelines and practical measures based on relevant experiences and best practices identified by its contributors. Contributions have been made by most EU Member States as well as the European Commission and the European Union Agency for Cybersecurity (ENISA). The European External Action Service (EEAS) as well as the European Cooperation Network on Elections (ECNE) also assisted in drafting this document.

However, the organization and security of elections is ensured at national level, with significant variation across EU Member States. Therefore, this compendium has been designed to allow EU Member States select approaches and measures they consider appropriate for their national context and provide them with good practices identified through the sharing of experiences by the EU Member States.[1] In addition, a number of checklists and case studies are included to offer further practical guidance.

2. Elections threat landscape

It is important to take an all-hazard approach[2] and to take into account **all potential cybersecurity threats and incidents,** which could impact election technology, including cyber-attacks (see below), system failures (such as software bugs, hardware failures, etc.), human errors (such as software

[1] The Recommendation on inclusive and resilient electoral processes in the European Union invites EU Member States to continue and deepen their cooperation and exchange of information and best practices in ECNE and the NIS Cooperation Group.You can access the Recommendation at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H2829

[2] Note that also the NIS directive requires this all-hazard approach, and also the widely used ISO27K1 standard uses an all-hazard approach to risk management.

misconfigurations, mistakes with maintenance or software updates), natural disasters and similar contingencies such as power cuts and network outages.

2.1 Cyber attacks

The following cybersecurity threats have to be taken into account in the electoral context.

- **Ransomware and wiperware attacks**

Ransomware and wiperware can have a material impact on the conduct of elections, for example by rendering voters' registration data unavailable and hence blocking the very conduct of elections. Ransomware has ranked first among the threats described in the ETL 2023 (31,32% of analysed cases) and it has been pointed out as a growing trend, with the industrial and manufacturing sector being the primary target of top-tier ransomware groups. The high recurrence of ransomware makes it a very relevant threat for elections, as electoral infrastructure can become a random target of financially motivated ransomware[3]. Usually, before files encrypting, data is exfiltrated in order to be further exploited for financial advantages or to exert influence on elections.

- **Distributed Denial-of-Service (DDoS) attacks[4]:**

Although it has been observed that lately the duration of DDoS attacks has generally decreased to less than one hour[5], they can still be very effective in undermining the public's trust in the electoral process, especially if affecting its most critical and visible phases – that is the transmission, aggregation and display of voting results. DDoS attacks have ranked second in the ETL 2023 (21,4% of analysed cases) with trends that make them particularly relevant for elections. For example, the increased availability of "DDoS-for-hire" services allowing unskilled users to launch DDoS, as well as the use of DDoS in conflicts by hacktivists. DDoS attacks can be volumetric or application-specific, and effective defense usually requires multiple tools.

- **Social engineering and phishing attacks**

The access to sensitive information made possible by phishing can affect the electoral process in several ways, such as: spreading ransomware that can block communication or access to critical data (see above); granting access to voter to harvest personal data used to address misleading messages; exfiltrating internal party or governmental documents that can be used in disinformation campaigns. The ETL 2023 reports that phishing, in particular via e-mails, is one of the top initial infection vectors and points to the risks of AI applied to social engineering, which can make phishing cheaper, easier to scale-up and more effective e.g. the use of AI for crafting more convincing phishing emails and messages and deepfakes for voice cloning and AI-driven data mining. Similar cyber-attacks are Smishing, phishing via SMS and Vishing, phishing via a phone call.

- **Website defacement**:

Although not identified as a top threat in 2023, in an electoral context, public-facing websites (for example, displaying elections results or party-related information) are an obvious target of these types of attacks, since they are not particularly sophisticated and can be very effective. Altering their content in support of specific disinformation narratives pollutes the information environment and, most importantly, the perceived integrity of elections.

[3] For more information check out https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

[4] To better understand this threat as well as how to better protect against it please check out https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks

[5] Microsoft observed that most of the attacks (89%) had short durations (less than an hour) and 26% lasted between one and two minutes [Quoted in ETL 2023].

- **Supply-chain attacks:**

Supply-chain attacks combines a first attack on a supplier that is then used to attack a target to gain access to its assets[6]. Electoral infrastructure is vulnerable to these types of attacks because of its reliance to externally sourced components and services, also including commercial-off-the-shelf hardware and software[7]. The ETL 2023 registers an increased interest by threat actors in these types of attacks, and in particular by using employees – preferably with elevated privileges - as entry points.

- **Cybersecurity attacks facilitating the creation and spread of manipulated information,** for example:
  - Attacks exfiltrating and leaking data or documents can be used to harm the reputation of a party or candidate. To this aim, forged documents can also be added to the leaked information.
  - Attacks affecting the functioning of the digital infrastructure/technologies for the elections can be used to undermine the public's trust by seeding doubts on the integrity of the electoral process and/or discredit the ability of States to run it.

In the case of elections, it is important to note that cyber-attacks can have an impact even if they did not take place or if they were unsuccessful (completely or partially). Alleged cyberattacks against public institutions can add legitimacy to forged documents. Also, cyber-attacks that have been claimed but that have not occurred (or occurred without substantial consequences) might impact the public opinion anyway, since they can alter the public's perception of the electoral context and processes.

State/state-sponsored threat actors are often mentioned in the context of elections. Still, it is important to note that financially motivated cyber-criminals as well as self-proclaimed hacktivists can also play a role (see ransomware and DDoS above). Also, insider threats (whether intentional or unintentional) should be considered as they are also a source of concern.

2.2 Past cyberattacks affecting elections

Multiple incidents have affected elections organized worldwide. The following table[8] contains examples of noteworthy electoral incidents.

	Region	Year	Method used	Target
1	North-America	2020	Data breach (voter data); Defacement of campaign website; ransomware	State and election-related websites; candidates' campaign websites; voter verification system
2	Europe	2021	Attempted spear phishing for data theft	Members of parliament
3	Europe	2023	Attempted DDoS, attempted phishing campaigns	Unspecified targets
4	Latin America	2023	Unspecified attack	On-line voting system for citizens living abroad
5	Global	2023	Spear phishing; data breaches; unspecified (attempted) attacks	Members of Parliament; universities, journalists, public sector, non-government organisations and other civil society organisations

[6] To better nderstand this threat as well as how to better protect against it please check out https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[7] Center for Internet Security, Managing cybersecurity supply chain risk in election technology

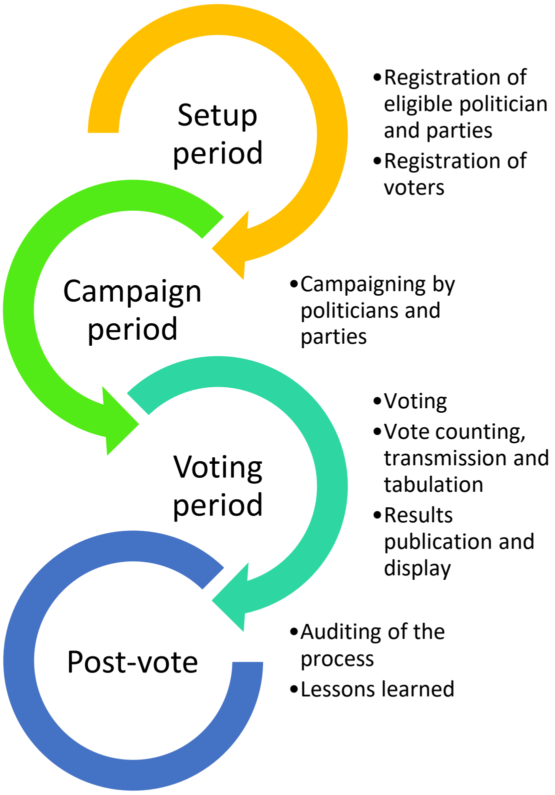
[8] It is by no mean a comprehensive chronological list of electoral incidents. Nevertheless, it contains different types of attacks and incidents that could provide important lessons for election organizers.

2.3 The attack surface - assets and processes at stake throughout the electoral cycle

The use of digital technologies across the electoral cycle varies from country to country. In most EU countries the actual vote is carried out with pen and paper, mainly due to security and transparency concerns. However, ICT is widely used and is critical for voter registration and the transmission and aggregation of election results. For example, a recent ENISA survey of national authorities in charge of cybersecurity of elections or electoral matters conducted across 22 EU countries, indicates that digital technologies are used mostly for voter registries and the transmission and display of election results[9].

In addition, most candidates and parties heavily rely on technology for their campaigning. Also, news outlets and media rely on ICT for reporting on elections. Although not under the direct responsibility of EMBs, cyber-attacks on this ICT could have an impact on the actual or perceived integrity and fairness of elections.

We can broadly break down the electoral cycle into four main phases – each of which involves to some extent election technology:


Setup period
•Registration of eligible politician and parties
•Registration of voters
Campaign period
•Campaigning by politicians and parties
Voting period
•Voting
•Vote counting, transmission and tabulation
•Results publication and display
Post-vote
•Auditing of the process
•Lessons learned

Case Study: Estonian I-voting Estonian National Election Committee[10]

"In Estonia, elections are overseen by the seven-member Estonian National Election Committee. The State Electoral Office is the country's top-level EMB. It is institutionally independent but falls under

[9] The ENISA survey was done in preparation of the exercise for the European Elections ELEX 2023. 41 organisations (national authorities with competence on either cybersecurity or electoral matters) from 22 EU countries took part in the survey.

[10] https://www.idea.int/publications/catalogue/cybersecurity-in-elections - Estonia case study page 57 Internet voting in Estonia 2005–2019: Evidence from eleven elections.

the Chancellery of the Parliament. It conducts elections, and organizes and ascertains the results of Internet voting. It also supervises the activities of election managers and is responsible for the development and management of the technical solutions necessary to organize elections.

The State Electoral Office uses a range of election technologies:

- *Internet Voting System—operational since 2005, with about one-third of votes cast electronically from 116 countries.*
- *Election Information System—operational since 1998 as an electronic tool for managing electoral preparations and processing electoral actors, candidates, statistics and results. However, the official results are still the ones from the paper protocols.*
- *Electoral Results Webpage—publishes the results and statistics from the Election Information System.*
- *Voters' Register—voters have been drawn from the centralized state population register and maintained by the Ministry of Interior since 2000. An Electronic Voters' Roll (which will allow all polling stations to connect to a single information system) is planned from 2021. The system will draw data from the voter register, but will be the responsibility of the EMB.*

Election technologies are part of a broad range of Estonian e-government applications based on public and private sector (energy, telecom, banking) systems. All Estonian citizens carry an electronic ID card to access and use these systems. While election technologies are the responsibility of the EMB, it is not responsible for electoral campaigns, including social media. However, any illegal social media activities are immediately referred to the police."

2.4 Mapping cyberattacks to election phases

In the table below we match the threat to the assets, and give some specific examples on how threats could materialize to affect the four different phases of the electoral cycle explained in the previous section.[11]

Phase(s)	Assets	Examples of Threats
Setup	Party/candidate registration	• tampering with registrations; • DoS or overload of party/campaign registration, causing them to miss the deadline; • fabricated signatures from sponsors.
Setup	Electoral rolls	• identity fraud during voter registration; • Deleting or tampering with voter data; • DoS or overload of voter registration system, suppressing voters.
Campaign	Campaign IT	• Hacking candidate laptops or email and social media accounts; • hacking campaign websites (defacement, DoS); • misconfiguration of a website; • leak of confidential information.
All phases	Government IT	• hacking/misconfiguration of government servers, communication networks, or endpoints; • hacking government websites, spreading misinformation on the election process, registered parties/candidates, or results;

[11] Some of the reconnaissance and preparation may happen in advance of the electoral cycle. Therefore, considering these potential cyberattacks not only during the electoral cycle but also in advance is recommended.

		• DoS or overload of government websites.
Voting period	Election technology	• tampering or DoS of voting and/or vote confidentiality during or after the elections; • software bug altering election results; • tampering with logs/journals; • breach of voter privacy during the casting of votes; • tampering, DoS, or overload of the systems used for counting or aggregating results; • tampering or DoS of communication links used to transfer (interim) results; • tampering with supply chain involved in the movement or transfer of data.
Campaign, public communication	Media/press	• hacking of internal systems used by media or press; • tampering, DoS, or overload of media communication links; • defacement, DoS, or overload of websites or other systems used for publication of the results.

3. Hybrid threats to elections cybersecurity and resilience[12]

There are a number of hybrid threats, which may mislead, deceive and destabilise democratic processes such as elections. These threats have to be considered carefully - especially during the electoral life-cycle - because they could materialise and used to affect the outcome, the fairness and integrity of the elections. Below we highlight a few important and emerging ones in order to raise awareness.

3.1 Hybrid threats and foreign information manipulation and interference (FIMI)

Hybrid threats[13] and in particular FIMI in the context of elections combine traditional and technological tactics and techniques of state and not-state actors to manipulate public opinion, threaten electoral systems and undermine trust in the democratic process with the intention of influencing the outcome of the electoral process or undermining their integrity.

- Election infrastructures can be weakened by threat actors targeting certain systematic vulnerabilities in a coordinated way. Threat actors can also use multiple techniques simultaneously, for example they could launch hybrid attacks including a cyber component, an information manipulation operation and an attack on physical infrastructure;
- By exploiting the interfaces between formally declared war and state of peace, regulated and non-regulated actions, virtual and real, internal and external, etc;
- Cognitive warfare — influence decision making, attitudes and behaviours;
- Overlap between threat actors, for example the same threat actors may be behind cyber and disinformation campaigns;
- Use of salami tactics – this refers to a strategy where a series of small actions are taken to achieve a larger goal, while each individual step is small enough to be unnoticed or deemed insignificant.

[12] This chapter was drafted based on contribution made exclusively by EEAS in order to provide to the reader a more complete compendium on elections cybersecurity and resilience. Hybrid and emerging threats, and especially disinformation and social media platforms are outside the scope of the NIS directive and consequently of the mandate of the NIS Cooperation Group who is the author and copyright holder of this document.

[13] https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

- Use of Foreign information Manipulation and Interference (FIMI), including disinformation.
- Development of Hybrid Hacktivism, with cyber-attack campaigns combined with digital propaganda impersonating ideological motivations.

Foreign Information Manipulation and Interference (FIMI), including disinformation, is closely connected to both hybrid threats and cyber threats. Foreign actors, who engage in intentional, strategic and coordinated attempts to manipulate facts, to confuse, sow division, fear and hatred.

Cyber-enabled operations can be used both to attack physical infrastructure and to reinforce threat actors' operations. In the context of FIMI attacks, cyberattacks can be followed by an information manipulation component, as it is the case for some of the analysed incidents, thereby constituting a form of hybrid attack.

In 2023 the EU adopted the FIMI Toolbox[14] to address foreign information manipulation and interference[15]. The Toolbox, developed by the EEAS in close cooperation with the Commission and Member States, is built upon four dimensions (situational awareness; resilience building; disruption and regulation; EU external action) that comprise different instruments. The EEAS presented a proposal for a common analytical framework and methodology to analyse FIMI in its 1st EEAS Report on Foreign Information Manipulation and Interference Threats[16] in 2023. The 2nd report on FIMI threats[17] outlines how to collectively activate threat-informed countermeasures in a network of FIMI defenders. This report sets out a conceptual outline of a Response Framework. The Response Framework is then applied to the analysis of election-related FIMI incidents and outlines a possible workflow to address FIMI and disinformation during elections.

3.2 Social media networks and disinformation

Social media networks have introduced both opportunities and risks to the election process. While social media can facilitate political engagement, voter mobilization, and information sharing, it also poses several significant risks. The risks indicated below are subject to ongoing research and an evolving understanding of the level of actual harms they entail, the effectiveness of risk mitigating interventions, as well as the proportionality of the latter in relation to the exercise of fundamental rights like freedom of expression and information:

- False or misleading information can spread rapidly on social media platforms, potentially influencing voter opinions, behavior, and election outcomes.
- Social media algorithms can create echo chambers where users are exposed to information that aligns with their existing beliefs, reinforcing confirmation bias.
- False or misleading content can go viral quickly, making it challenging to counteract even after it has been debunked.
- Social media accounts of candidates, political parties, and election authorities can be hacked, leading to the spread of false information or interference in the electoral process.
- Hostile foreign actors may use social media to manipulate public opinion, sow discord, and interfere in domestic elections.

[14] The development of the Foreign Information Manipulation and Interference (FIMI) toolbox was part of the actions presented in the EU Strategic Compass for Security and Defence. Read more at https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

[15] https://www.consilium.europa.eu/media/68967/europeancouncilconclusions-14-15-12-2023-en.pdf

[16] https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

[17] https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

- Micro-targeted political ads on social media can be used to influence specific voter demographics in potentially unethical ways.
- The collection and misuse of user data by political campaigns and third-party entities can infringe on user privacy.
- Social media can be a platform for harassment, hate speech, and divisive rhetoric, contributing to polarisation. This can contribute to polarization, but it can also stimulate verbal and physical intimidation and abuse of politicians or candidates, and their families. This can have a paralyzing effect on democracy, which cannot thrive in a context where democratically elected representatives are unsafe.[18]
- Disinformation campaigns as well as FIMI on social media may aim to suppress voter turnout by spreading false information about polling locations, voter eligibility, or election dates.
- Bots - can run in the browser and are built to mimic actions, from logging into the app, clicking the menu button, and posting. This can create a clear image of a bot of a real person posting.
- Online deception – done via social media it implies content that is shared by an account intended to spread false information either on a targeted public or to a wide public.
- Online impersonation – can be done by political adversaries as well as by any random person via hands-on posting or automated programs. The felony incident here is identity theft, as the purpose is dissimulating the identity of a certain candidate and affect his public image by posting certain messages on the impersonating account to mislead the electorate.
- Deceptive influence operations – there are many other forms of deceptive influence operations which can be carried out on social media platforms. Deceptive operations on social media platforms could mislead users to believe that an account, group, or group chat is not political, while it is set up for political influence, to impact the elections.

3.3 Artificial Intelligence (AI)

The 2024 elections will see the power of AI being harnessed by stakeholders across the electoral ecosystem, including politicians and campaigns, but also malicious actors aiming to attack the integrity and fairness of elections. Below we outline some benefits as well as risks posed from AI involvement in the electoral process:

Benefits of AI include:

- Enhanced security: AI can be used to bolster cybersecurity measures, detect and respond to cyber threats, and protect sensitive election data.
- Voter engagement: AI-powered chatbots and virtual assistants can engage with voters, answer questions, provide information, and even help voters choose a party or candidate, , enhancing voter participation. Large language models can be used for translation or simplification of text.
- Data analysis: AI algorithms can analyze large datasets to identify trends, voter preferences, and potential irregularities, helping election officials make data-driven decisions.

Technology risks associated with AI include:

- Security Vulnerabilities - AI systems, datasets and models can themselves be vulnerable to cyberattacks, leading to potential manipulation of election results or data breaches.
- AI poisoning -in an AI poisoning attack, adversaries tamper with the AI training dataset to taint the learning process to manipulate the behavior of the systems in the way they desire

[18] CoE Report on Hate Speech and fake news: the impact on working conditions of local and regional elected representatives

- Bias and Fairness - AI systems can inherit biases present in training data, potentially leading to unfair or discriminatory outcomes in voter registration, candidate selection, or data analysis.
- Cyber-attacks leveraging AI - One use that has already been observed and it is likely to increase is the use of AI for more targeted and effective social engineering attacks, both relying on AI-driven data mining to identify potential targets and vulnerabilities and to create “baiting” content accordingly
- AI-generated image-, video- and text-based content: AI-generated content and other forms of synthetic media can be used to spread disinformation or manipulate public opinion. In addition, AI can be used by threat actors seeking to pollute the information environment to influence the outcome of the vote (e.g., ahead of the parliamentary elections in Slovakia a fake audio appeared online where a party leader and a journalist discussed election rigging. In addition, it can also be used by parties and candidates for campaigning (e.g., AI-generated content was widely used by presidential candidates in Argentina. While the latter might not contain fake content, the lack of adequate labelling could contribute to the pollution of the information environment

Case Study: Spanish General Elections in 2023 - Disinformation with a fake website

Two days before the elections, a domain was registered imitating the official website of the Community of Madrid and its content. The cloned site published an article, warning about a possible attack on polling stations by the former terrorist group ETA on July 23. No amplification was found on open sources, likely indicating that the FIMI operation was possibly carried out on encrypted private channels or chats. According to third-party information, URLs to the domain were received by private Russian Telegram users residing in Spain.[19]

Case Study: Polish parliamentary elections in 2023 - Disinformation with a deepfake video

Two days before the elections, Polish media published a video of a police intervention in one of the three polling stations in Poland, where an anonymous bomb threat had been sent before the day of the vote[20]

Accounts belonging to the Russian FIMI infosphere presented the video in a reframed context, alleging that explosions had already occurred. This misleading framing was amplified by some unattributed pro-Russia accounts on social media. This incident shows an intentional attempt to escalate fears around the alleged bomb threats to the polling stations and thereby dissuade people from going to vote

The above two case studies show the interconnection between cyber, FIMI and disinformation threats in the realm of hybrid threats to elections. Both examples have been taken from the *2nd EEAS Report on FIMI Threats* published in January 2024 by the EEAS.[21]

4. Specifics and particularities of the European Parliament elections

Elections for the European Parliament, which take place every 5 years, are rather specific compared to national or regional elections within an EU Member State and their cross-border nature creates

[19] ECD Confidencial Digital (July 2023) *Una web que suplanta a la Comunidad de Madrid se inventa que ETA amenaza con atentados este 23 de julio* https://www.elconfidencialdigital.com/articulo/seguridad/web-que-suplanta-comunidad-madrid-inventa-que-eta-amenaza-atentados-23-julio/20230723143844613758.html

[20] Post on X from Polish media outlet Onet @OnetWiadomosci https://archive.ph/OQsSt

[21] https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

unique challenges. An incident in any stage of the electoral process anywhere in the EU may have spill-over effects and affect the legitimacy of the overall election results. EU Member States and European institutions therefore have a common interest in addressing the cybersecurity challenges of elections together, facilitating the sharing of experience and good practices, including through this compendium.

Elections for the European Parliament are organized by each Member State across the EU, using their own processes and technologies. All EU Member States organize this vote within a designated week, but the exact timing and day of the vote may vary depending on the Member State. Usually, the voting starts on a Thursday morning and ends on the following Sunday, but the exact date and times are fixed by each EU Member State.[22] This rolling nature of elections creates unique challenges for those tasked with securing the elections as there is additional potential for spill-over effects. EU Member States may not make the results of their count public, until after the polls close in the Member State whose electors are last to vote. Keeping the confidentiality of that vote results in the Member States voting earlier requires additional security measures or procedures.

4.1 Election organisation and possible threats

The EP elections are subject to both European legislation and specific national laws. The common EU rules lay down the principle of proportional representation and the specifics of the mandate of members of the European Parliament. The exact electoral system, including the number of constituencies, is governed by national rules. Therefore, to a great degree, the European Parliament elections reflect national election procedures and rely on similar rules, regulations, processes, and election managers as local, federal (where applicable) and national elections.

In the European Parliament elections most countries function as a single constituency, but Belgium, Ireland, Poland, and Italy have divided their national territory into a number of regional constituencies. This means that for registration of voters and candidates and the management of the relevant databases the European Parliament elections in a country may differ from national, federal, state or municipal elections.

In general EU citizens can vote and stand as candidate in the EU country where they reside[23]. Therefore, EU Member States have to address issues such as voter and candidate registration of Union non-nationals and the exchange of information to avoid multiple voting or instances where the same person would stand as a candidate more than once at the same elections. The Crypto Tool made available to Member States by the European Commission supports their exchange of data aimed at ensuring that mobile EU citizens can only vote and stand as candidates once.

4.2 Relevant legal and policy documents

Different sets of rules apply to elections at EU and national level including General Data Protection Regulation, the Network and Information Systems Directive, the Digital Services Act, etc. Below we list some directly relevant legal and policy documents for elections organized in the EU, including non-binding instruments.

- Commission Recommendation on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament, C(2023) 8626[24]

[22] https://www.europarl.europa.eu/ftu/pdf/en/FTU_1.3.4.pdf

[23] Article 3 of Council Directive 93/109/EC https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31993L0109

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302829

- Communication on protecting election integrity and promoting democratic participation, COM (2021) 730[25]
- Compendium of e-voting and other ICT practices (non-paper from the Commission services)[26]
- Guide on good electoral practices in Member States addressing the participation of citizens with disabilities in the electoral process, SWD (2023) 408[27]
- Regulation 2022/2065[28] on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)[29] - in particular the DSA crisis protocols (Art. 48) and crisis response mechanisms (Art. 36)
- Commission guidance on the application of Union data protection law in the electoral context. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM (2018) 638[30]
- Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949[31]
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Securing free and fair European elections, COM (2018) 637[32]
- Commission Recommendation on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament, COM (2018) 234[33]
- Commission Recommendation /EU of 29 January 2014 addressing the consequences of disenfranchisement of Union citizens exercising their rights to free movement, COM (2014) 53[34]
- Commission Recommendation on enhancing the democratic and efficient conduct of the elections of the European Parliament, COM (2013) 142[35]
- Council Directive 94/80/EC laying down detailed arrangements for the exercise of the right to vote and to stand as a candidate in municipal elections by citizens of the Union residing in a Member State of which they are not nationals[36]
- Council Directive 93/109/EC laying down detailed arrangements for the exercise of the right to vote and stand as a candidate in elections to the European Parliament for citizens of the Union residing in a Member State of which they are not nationals[37]

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0730

[26] https://commission.europa.eu/document/download/b0898ba3-c7ad-4af5-8467-5e23a0469a78_en?filename=compendium.pdf

[27] https://commission.europa.eu/system/files/2023-12/SWD_2023_408_1_EN_document_travail_service_part1_v4.pdf

[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0638

[31] https://cyberpolicy.nask.pl/wp-content/uploads/2018/09/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0637

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0234

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014H0053

[35] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013H0142

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31994L0080

[37] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31993L0109

4.3 Existing EU networks and initiatives on securing elections

Since the 2019 elections, a number of networks were set up at EU level with a direct impact on ensuring the security of elections:

- **European Cooperation Network on Elections (ECNE)**: This network brings together representatives of Member States' authorities with competence in electoral matters and allows for concrete and practical exchanges on a range of topics relevant to ensuring free and fair elections, including data protection, cyber-security, transparency and awareness raising.
- **NIS Cooperation Group (NISCG):** The Group's overall mission is to achieve a high common level of security for network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States. A full list of the Group's task is presented in Article 11 of the NIS Directive.
- **Rapid Alert System (RAS):** Set up among the EU institutions, Member States and international partners, the RAS facilitates the sharing of information analysis and others insights (such as trends, reports, best practices) related to FIMI, including disinformation, and coordinate response including ahead of the EP Elections 2024.
- **Joint Mechanism for Electoral Resilience:** Organised and coordinated through the European Cooperation Network on Elections in close cooperation with the Network and Information Systems (NIS) Cooperation Group and the EU's Rapid Alert System. Its primary operational focus is to support deployment of joint expert teams and expert exchanges with the aim of building resilient electoral processes, in particular in the area of online forensics, disinformation and cybersecurity of elections.
- **EU CSIRTs (Computer Security Incident Response Team) Network:** This network is composed of EU Member States' appointed CSIRTs, ENISA, and CERT-EU and allows for cooperation at technical level between Member State, in case of cybersecurity incidents.
- **EU Cyber Crisis Liaison Organisation Network (EU-CyCLONe)**: formalized in 2023, this Network ensures the coordination between Member States and the European level in case of large-scale cybersecurity incidents.
- **DSA Digital Services Coordinators:** Designated as part of the implementation of the Digital Services Act (DSA), national Digital Services Coordinators will have direct responsibility in implementing and enforcing the provisions of the DSA on illegal content and disinformation.
- **CyberCOM Informal Network**: this informal network at EU institutions, bodies and agencies can exchange relevant information and key public messages to ensure a coordinated EU public communication mechanism. This activity is done in line with the mandates of the EUIBAs and the expectations and limitations of their respective stakeholder communities in the EU Member States.
- **European Expert Group on Electoral Matters**: national expert implementation group for Directives 93/109/EC and 94/80/EC concerning the voting rights of mobile EU citizens.
- Other cooperation frameworks may also be relevant including for instance on **data protection**

4.4 Communication of preliminary and final results

The last mile of the EP elections has two steps:

1. **Communication of preliminary results to the European Parliament for information purposes** which is done as polls close at the end of the election week, to provide data to the website with preliminary results, showing the preliminary allocation of seats in the future European Parliament hemicycle.
2. **Communication of the binding national results from the capitals to the European Parliament** which is treated as the official communication by the Member State of the election results.

Projecting the European Parliament's future composition on election night is an operation consisting of several factors. Including the collection and distribution of available national results of the European elections to the media and the general public as early as possible on election night and the projection of Parliament's future composition, based on an evolving data mix consisting of, for instance, available national results, exit polls or partial results. These results are displayed and visualised as quickly as possible for public communication purposes, as polls have closed but are not the binding results for the composition of the European Parliament. The staff of European Parliament website representing the allocation of seats in the future hemicycle has to ensure that they receive true and unaltered results from the national capitals, verifying all the results through an independent communication channel with the national authority tasked with vote tallying.

Case Study: Collecting and verifying national results for the Hemicycle

The election years 2014 and 2019: In the months preceding election night, the European Parliament, together with an external contractor selected based on a public call for tender[38], produced internal projections based on an ongoing voting intention monitoring in all Member States. Moreover, and in addition to the work of collecting and sourcing both voting intention data and actual election results through its network of institutes, the tenderer was required to contact and communicate with the official national bodies in charge of counting and disseminating the results of the European elections in each Member State concerned. The tenderer established a liaison with each of these bodies to ensure the collection of results during the European elections period. Special attention had been given to obtaining results from the official bodies in an appropriate digital format. In addition, this liaison had to remain operational until the official announcement of the results in the Member States.

The steps for doing so were as follows for the 2014 and 2019 elections:

1. The contractor's 28 national institutes collected data on turnout, estimates and results. These were collected using either the national institutes' own data (e.g. in France and Germany where their own estimates and exit polls results were used) as well as via the official websites of the national electoral commissions.

2. The data collected was transferred via a dedicated intranet and email to the coordination centre team located in the contractor's Brussels office. A dedicated telephone line had been installed as a back-up option in the case of failure but was not used in 2014.

3. Data was checked and validated by the coordination centre team located in the contractor's Brussels office. Several standard error checks were also performed (for example that end sums were not higher than 100%, templates set in advance with party lists that cannot be modified, etc.)

4. Data was transferred by the coordination centre team to the team located in the European Parliament using a dedicated intranet. A private and dedicated connection was used to ensure rapidity, security and fluidity of the transfer. Email was used as a secondary channel with a dedicated phone line as a back-up option.

5. Data was gathered, validated and used to build the projections by the team located in the European Parliament. Data was then transferred to the second contractor in charge of feeding the results website, formatting the data and publication. At this step, the database was cross-checked against that from the European Parliament External Offices. The contractor's team and the EP team then decided together what data to use for the next projection/publication (more up to date, more official sources). Any data had to be double validated by both the contractor and the EP team before use.

[38] Call for tender for the European Parliament elections 2019, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=3334

***Case Study: IT-Grundschutz – protection profile for preliminary election results - Security concept for the secure transmission of preliminary election results*[39]**

For the determination and forwarding of the preliminary election results for Bundestag and European elections information technology is generally used from municipal level onwards. Any use of information technology can pose risks to the confidentiality, authenticity, integrity and availability of data. be associated.

To ensure information security in the transmission of absentee ballots for Bundestag and European elections in accordance with the current state of the art, a federal state working group, together with the Federal Office for Security and Information Technology, has drawn up this IT basic protection catalog for absentee ballots. The IT baseline protection profile is primarily aimed at electoral bodies and authorities at municipal and district level. In addition, the requirements can also be used at state and federal level.

***Target group -** The IT-Grundschutz profile for rapid notifications is aimed at electoral bodies and authorities that are involved in the process of quick notifications pursuant to Section 71 BWO and Section 64 EuWO up to and including the district and municipal municipal electoral administrations.*

***Objective -** The IT-Grundschutz profile is intended to facilitate the adaptation of the security process in accordance with IT-Grundschutz for the rapid reporting of nationwide parliamentary elections to the district electoral administrations. It is intended to support users in increasing information security when determining the provisional election results. The aim is to use the requirements described in this profile requirements set out in this profile and the corresponding measures introduced, to ensure the availability and integrity of the rapid reports. In addition, the protection of the confidentiality of the data during election preparation is also covered.*

This IT-Grundschutz profile is intended to help users to check the security level in a relatively resource-efficient manner and to meet the requirements for level of security and implement the requirements for securing parliamentary elections in a relatively implement. Building on the IT baseline protection profile, security concepts for information networks, specialist tasks or processes can also be mapped. The IT-Grundschutz profile can be continuously supplemented by the electoral bodies and authorities involved in the electoral bodies and authorities involved in the rapid notifications.

5. Cybersecurity good practices

The previous sections illustrate the challenge and importance of proactively protecting the integrity and resilience of electoral processes in a continually evolving threat landscape. Best practice considerations are now presented to assist those charged with mitigating the risk of cyberattack throughout the electoral process in achieving that goal. These should be tailored to meet the specific circumstances of each EU Member State.

5.1 Collaboration and information sharing

It is a good practice to establish a national electoral network, including election taskforces or election ISACs, ahead of the elections, involving all the relevant stakeholders, for collaboration and information sharing. In Recommendation C(2018) 5949[40], the European Commission also encouraged Member States to set up national election networks.

[39] The IT-Grundschutz profile is not for public use. Further information is available on request from the German Federal Office for Information Security at sicherheitsberatung-politik@bsi.bund.de

[40] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0637&from=EN

An election network may include, depending on the national setting, the EMB, the national CSIRT, relevant ministries, IT organizations responsible for election technology and/or relevant vendors providing such technology, data protection authority, law enforcement, media regulators, entities in charge of addressing disinformation, intelligence services, etc. It is important to kickstart a process of information sharing within this network, to ensure that all the relevant stakeholders know about threats to the elections and keep each other informed about potential issues. This network can help with collaboration and information sharing between stakeholders in the run up to the election, as well as during an election as a 24/7 support, coordination and incident handling resource.

Depending on the national setting, vendors, contractors, or the software developers of the election technology may be invited to join such a taskforce. The taskforce should involve government spokespersons and senior-management, decision makers. It is essential that within the taskforce communication channels are up-and-running, and that there are backup channels, for example, lists of phone numbers and backup messaging apps.

In setting up the network, it is beneficial to consider and document:

- a single point of contact for the network,
- a ladder of crisis escalation, detailing levels of criticality and modus operandi,
- roles and responsibilities within the taskforce and backups,
- communication channels and backup channels,

Case Study: Spanish incident response team - Monitoring the security situation during the elections

On the day of the elections in Catalonia, a team was deployed to supervise and manage every incident of the day. The team had direct communication with the systems, development, communications, security, forensic, and DOS teams.

Regular meetings were established every 3 hours to review the security status and concentrate on a brief report. When the counting of votes began, the meetings were held every hour. If any suspicious equipment was detected, it was included in a quarantine network for forensic review.

For all teams, a limited number of fully operational back-ups were available to replace any suspect equipment.

5.2 Awareness raising

It is important to raise awareness about potential cybersecurity incidents, including cyber-attacks, with all relevant stakeholders, including not only the government entities involved, the media organizations, the politicians, and campaigns. End-user awareness campaigns should explain potential cyber threats and cover basic cyber hygiene (good passwords, two-factor authentication on email and social media accounts, phishing (by email), vishing/smishing (by telephone or SMS), the importance of software updates, etc.

Target audience[41]

- Officials working at the election management body
- Employees at IT organizations and/or vendors responsible for election technology
- Municipalities and local government involved in organizing and counting the vote
- Officials and citizens working at polling stations

[41] Awareness raising about cyber threats is important for all election stakeholders.

- Campaign organisations, parties and politicians
- Media and journalists

Awareness raising topics to cover[42]

- Phishing, spear-phishing, vishing and smishing attacks, i.e. cyber-attacks where an attacker sends fake messages, often emails, pretending to be a bank or an otherwise trusted company, to get the end-user to reveal a password or to run malicious software. Attackers also use fake SMS (smishing), fake customer support phone calls (vishing).
- Password security, i.e. the importance of not using easy to guess or non-default passwords, to avoid attackers taking over the devices of the end-user. Where possible, the importance of multi-factor authentication should be emphasized.
- Device and software updates, i.e. the importance of keeping end-user devices, like PCs, smartphones and tablets updated to the latest software version and to install security updates when available, to avoid that cyber-attackers exploit software vulnerabilities.
- Ransomware, malware and other viruses.

Sometimes it is also important to raise awareness with more expert roles, such as software developers, who may be very technical but not fully aware of cybersecurity threats. In these cases, a wider range of topics needs to be covered – see for example the other topics covered in this section. ENISA provides a set of material to support the creation of awareness raising campaigns, called Awareness raising in a box.[43]

5.3 Identifying risks and managing threats and crisis

As the elections in the Member States are different, it is important to perform a cybersecurity risk assessment, to understand what are the threats and what are the appropriate measures to protect the election and e-voting technology. To ensure good operational collaboration and preparedness in the face of large incidents and crises, it is important to develop contingency plans, with crisis management procedures and playbooks, including communication plans, and continuity plans, when there are large scale incidents.

Risk management

It is important in cybersecurity risk assessment to consider all potential cybersecurity threats and incidents (including the cyber-attacks listed in Section 2), but also other types of cybersecurity incidents which are not malicious such as configuration errors, software bugs, overloads, network outages, power outages, etc. This is called a so-called all-hazard approach – any potential threat which could impact the election or e-voting technology should be taken into account. Note that also the NIS directive requires an all-hazard approach, and also the widely used ISO27001 standard uses an all-hazard approach to risk management.

The risk management can be divided in three steps

1. Identifying the assets, the election and e-voting technology which needs to be protected
2. Risk assessment, assessing likelihood and potential impact of threats, the risk for each asset

[42] Awareness raising explains to a non-technical audience, how potential cyber threats could materialize, when using technology, in the capacity of end-user.
[43] You can access it at https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box

3. Security measures, appropriate to the risk, to protect these assets from the threats

When assessing risks, the following threats should be considered

- Cyber-attacks (including for example some of the threats listed in Section 2).
- System failures, including software bugs, hardware failures, configuration errors, etc.
- Human errors, including software misconfiguration, or mistakes in carrying out hardware maintenance or software update procedures.
- Natural disasters and similar contingencies such as power cuts, network outages

While the risks and potential attack vectors are often specific to elections, widely used risk assessment and risk management standards can be used.[44] In addition, scenario planning can be a useful tool for dealing threats that have a high impact but a low probability, so called black swan scenarios.

Case Study: French risk management approach - Generalities and objectives

The French cyber risk framework, EBIOS Risk Management (RM), published by the French National Cybersecurity Agency (ANSSI), provides a shared understanding of digital risks between decision-makers, operational actors and IT experts. The key objective of EBIOS RM is to enable decision-makers to fully understand these risks in order to take appropriate decisions in the same way as for the other usual types of strategic risks

EBIOS RM enables organisations to perform and manage cyber risk assessment. This method synthesises compliance and scenarios-based approaches. Firstly, it is based on a solid security baseline focused on compliance with applicable guidelines and regulations. Secondly, the scenario-based approach focuses on sophisticated threats, which target the studied perimeter (organization, information system…) through the business and technical ecosystem.

How it works? *Divided into five sucessive workshops, the EBIOS Risk Manager method adopts a risk management approach which starts from the organization's point of view at the highest level (major missions of the object studied). Progressively, business and technical inputs are studied to identify possible vulnerabilities through end-to-end operational attack path that are designed from the attackers point of view, with cyber threat intelligence support and taking into account the critical stakeholders of the organization's ecosystem. Security measures are therefore identified to improve efficiently the level of security and are monitored in a risk treatment plan. Above all, the assessment is subject to regular review in the light of technology and business developments as part of a continuous improvement cycle.*

Proof of concept - *Fully compliant with ISO 27005 (2022) standard, EBIOS Risk Manager follows a dynamic model which is inspired by agile development methods, constantly challenged and adapted to different employment contexts by an open, connected and responsive community. It is the result of close internal collaboration, because it makes digital security an integral part of strategic and operational organization's challenges. Released in 2018, EBIOS Risk Manager has passed the test of reality and is now praised by risk managers in France as a practical, educational and collaborative tool for integrating digital technology into risk management and also as an efficient communication and decision-making tool to better understand technical issues.*

Case study: IT-Grundschutz -Objectives, concept and design

[44] See the NIS Cooperation group guideline on risk management and security measures, which can be found at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

In the IT-Grundschutz Compendium, standardised security requirements for typical business processes, applications, IT systems, communication links and rooms are described in the individual IT-Grundschutz modules.[45]

It is updated and published on a regular basis by Germany's Federal Office for Information Security (BSI). T-Grundschutz is comprised of a set of standards, a modular compendium of cyber security controls, and various supporting documents. The standards cover information security management (compatible with ISO/IEC 27001), methodology, and risk management.

The objective of IT-Grundschutz is to enable organisations to attain an adequate level of protection for all their information. The IT-Grundschutz Methodology is characterised by a holistic approach. By implementing a suitable combination of standard organisational, personnel-related, infrastructural, and technical security requirements, it is possible to attain a security level that is adequate for the relevant protection needs and appropriate for protecting information relevant to the organisation. Furthermore, the requirements of the IT-Grundschutz Compendium not only form a security basis for business processes, applications, IT systems, communication links and rooms that are highly sensitive; in many instances they also explain how a higher security level can be reached.

IT-Grundschutz follows a modular approach to enable improved structuring and planning in an area as heterogeneous as information technology, including regarding operational environments. The individual modules address typical business process workflows and areas of IT use – for example, emergency management, client/server networks, buildings, and communication and application components. The modules of the IT-Grundschutz Compendium reflect the state of the art based on the latest knowledge at the time of their publication. The requirements formulated in the modules describe what generally should be implemented to achieve the state of the art by means of appropriate security safeguards. The requirements and safeguards that reflect the state of the art correspond both to what is technologically advanced at the time of publication and what has proven successful in practice. In particular, IT-Grundschutz provides in-depth guidance and best practices on the following questions:

- *What are the key elements of information security management?*
- *How can organisations identify relevant threats and risks for the processing of information?*
- *What are the technical and non-technical means to protect IT systems and networks against intrusions and tampering?*
- *How can organisations protect the availability of vital IT services?*
- *How can organisations detect cyber-attacks, mitigate their impact, and restore services swiftly?*

Incident detection and response

Incident detection and response requires:

- **Situational awareness** – it is important to understand the cyber threats for the election and e-voting technology that needs to be protected. Up-to-date threat intelligence can be obtained from a variety of government and commercial sources.
- **Incident detection through logging and monitoring** – it is important to monitor the election and e-voting technology for incidents, through logging and monitoring of the logs. Automated tools, such as a SIEM, connected to threat intelligence information, should be used to effectively process logs and detect anomalies, and raise an alert if there is a suspicious case.

[45] IT-Grundschutz A systematic basis for information security: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

- **Triage** – Alerts raised by the SIEM should be followed up and analysed by experts. If an alert turns out to be an incident the alert should be forwarded to an incident response team. At this point an incident response procedure is triggered.
- **Incident response plan/procedure** which describes how the organization responds after an incident is detected, specifying:
    - Response phases including scoping phase, to understand the size of the incident, containment phase, to contain the attacker, recovery phase, to start eradicating and cleaning the system
    - Roles and responsibilities in the incident response phase
    - Reporting procedures and communication plans, specifying who should be notified about the incident;
    - Crisis management procedures and contingency plans, which are triggered when there are major/catastrophic incidents.

Crisis management

Crisis management procedures are needed for an adequate response to large-scale incidents[46] and crises. Crisis management plans and procedures should include

- Standard Operational Procedures, which describe actions and steps for different roles, to be able to act swiftly when a crisis occurs.
- Contact lists, to be able to reach out in case of a crisis or large-scale incident
- Communication plans should be part of the crisis management plan. Good communication is essential to maintain trust in the election process.
- Contingency plans, to be able to activate a backup solution, a backup network connection, for example.

At EU level, EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level.

Crisis and incident response procedures should be tested in table-top or technical exercises, in which decision-makers but also more technical level operators practice their response to events.

5.4 Exercises and training

It is important to test crisis management and contingency plans, to understand if these plans are adequate and working, in case of an incident or crisis. Relevant stakeholders to be involved in such cyber exercises and dry-runs include the security roles in the EMB, experts from the national CSIRT, the data protection authority, law enforcement, etc. These roles need to receive adequate training ahead of time.

Exercises can be carried out at different levels and in different formats. A scenario-based table-top exercise or dry-run can be useful to prepare decision makers for potential incidents and contingencies. More technical exercises can be used for more technical roles. For example, a technical exercise could prepare incident responders for a technical response to an incident.

Exercises can have multiple objectives, such as:

- to grasp the complexities of crisis management and how to overcome the crisis;

[46] The NIS2 Directive (EU 2022/2555) defines large-scale cybersecurity incidents as an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States

- to understand the implications of losing trust in an IT/communication system;
- to understand the implications of an election process being compromised by an adversary;
- to test existing processes and crisis procedures for possible incidents connected with the election process;
- to point out weaknesses in existing procedures;
- to simply allow all stakeholders to become acquainted with each other, to learn names and exchange contact details.

Involving all election stakeholders in such exercises is desirable, as it helps to ensure that the exercise is as realistic as possible. The critical training audiences include:

- decision-makers involved in the election process from a variety of institutions;
- operational-level representatives who are deeply involved in election process (from technical and non-technical units);
- spokespersons and governmental STRATCOM experts;
- representatives of the teams responsible for incident handling;
- representatives of private sector companies involved as vendors, developers or consultants.

A realistic scenario allows taking best advantage of the training opportunity of any exercise, and an evaluation session (or other format of after-action review) allows the discussion of the outcomes with the target audience; leading to realistic recommendations.

Case study: EU ELEx23, EU-level table-top exercise for the European Elections 2023

On November 2023, the European Parliament, the European Commission and the EU Agency for cybersecurity (ENISA) organised a cybersecurity exercise, named EU ELEX23, as one of the measures being implemented by the European Union to ensure free and fair elections in June 2024. The exercise was funded by the joint mechanism for electoral resilience in the framework of the European Cooperation Network on Elections. The drill allowed participants to exchange experiences and best practices, and helped them enhance their capacity to respond to cybersecurity incidents as well as to contribute to the update of existing guidelines and good practices on the cybersecurity of technology used in the election process. The exercise brought together representatives from national electoral and cybersecurity authorities. EU ELEX23 is the second exercise organised by ENISA, the European Parliament and the European Commission on the European Elections process. The first exercise was organised in 2019.

Case Study: Training the employees of Czech statistical office

In 2017 and 2018, with regard to the parliamentary and presidential elections, the National Cyber and Information Security Agency (NCISA) provided two training sessions to the Czech Statistical Office (CSO).

Training session before the parliamentary election

Training was focused on relevant incidents and events during elections in foreign countries. The target audience included the employees of CSO that were involved in securing the election process, ranging from IT workers to spokespersons and management. The training session took form of a presentation with discussion guided by the NCISA cyber security experts to steer the audience towards desired areas of interest.

The following incidents were introduced and thoroughly described:

- *the cyber campaign during Ukraine's presidential election in 2014;*
- *cyber-attacks launched on the Emmanuel Macron campaign during the French presidential election in 2017;*

- *multiple cyber-attacks during the US presidential campaign in 2016;*
- *the Netherlands' preparations before the 2017 parliamentary election.*

The examples were selected due to their relevance for the Czech election process. They provided valuable examples, lessons learned and cases to study. The CSO employees were steered towards discussing the security of the Czech election process in light of the presented events and incidents to examine if there were potential vulnerabilities and contingency plans in place.

The greatest advantage of the selected approach was the combination of introducing new knowledge to the audience and engaging them in active participation. However, as this was not an exercise there was no connection between the incidents and there was also a lack of time pressure. Therefore, the selected form did not represent environmental features of the real world.

Training session before the presidential election

After the 2017 parliamentary election, when CSO faced a DDoS attack disabling the official website of the election results, the NCISA prepared another training session in January 2018. This time, the target audience was not only CSO employees, but also included the representatives of suppliers (primarily private companies). In order to simulate a real-world environment, the session was designed as non-technical table-top exercise.

The topics in focus were:

- *public communication to maintain the credibility of CSO and the presidential election per se;*
- *effective communication inside CSO and with partners and suppliers in order to prevent miscommunication and contradictory public statements, leading to the loss of credibility;*
- *to identify and point out to weak spots and potential attack vectors, this was enabled by previously acquired knowledge of the election process in Czech Republic and by studying select case studies.*

Since this exercise was scheduled a short time before the presidential election, the focus was on areas with possible shortcomings that could be fixed in a quick manner, in order to maximise the outcomes of the session.

The primary focus was on cyber-attacks attempting to negatively affect the credibility of the election in the eyes of citizens. Such an attack can cause massive damage to the election process and democratic values, even if it does not directly affect election outcomes. The secondary areas of focus were the actions of possible attackers using cyber-attacks as a means to influence peoples' preferences; such as by defaming candidates via leaks or defacements. The biggest advantage of the exercise was its emulation of a real-world environment; meaning time pressure, a continuous and evolving campaign in cyberspace, and inciting interactions among various entities and their employees. A disadvantage of this approach was the high demand on organisers in terms of time and requiring a deep knowledge of the processes.

The collaboration between CSO and the NCISA continued in subsequent years. In 2021, in the context of Czech parliamentary elections, a comprehensive audit was conducted, covering the range of services provided by the NCISA including inspections, scans and penetration tests. The audit also involved a table-top exercise, through which the CSO could test its preparedness for crisis situations relating to the processing and presentation of election results, including in the media. A new infrastructure was put in place which required external and internal testing to be carried out by the NCISA. Additionally, a phishing campaign with the theme of the upcoming elections was executed, including the possibility of passive vishing, where users called the provided number.

5.5 Supporting campaigns, parties, and candidates with cybersecurity

It is important to offer support and advice to the election stakeholders, including campaign organisations, parties and politicians. This support should include awareness raising (see below), guidance on protection measures, for example on DDoS protection, practical support, for example by offering security quick scans, etc.

A democratic electoral process should be based on equal and fair opportunities for all contestants and their supporters to campaign in an environment free from limitation and obstruction. However, past attacks on parties and candidates have shown that cyber-attacks can affect the ability of parties and campaigns to engage in political discussions, which, in turn can delegitimise the entire democratic process.

Parties and candidates however might not directly approach the government for advice on maintaining their cyber security.

It is good practice to have a programme of outreach and direct engagement towards parties and campaigns to support them with taking the necessary cybersecurity measures.

Awareness raising activities and measures to ensure resilience could include regularly distributing information to party members and candidates on cybersecurity risks related to their activities and activities of other entities close to them, delivering training on cybersecurity, as well as supporting them in improving monitoring of the security of digital platforms and tools used for electoral campaigns.

Case Study: Anticipate actions, raise awareness and build trust in France

Regarding the information systems supporting elections, ANSSI does not consider that they represent specific challenges for cyber security agencies as classical information system "hygiene" applies here too. However, greater attention must be paid to systems mapping and the setup of a functioning relationship with the various stakeholders (political parties, ministries and agencies, etc.)

Firstly, in order to oversee ANSSI's possible involvement in assisting political parties while complying with its political neutrality, only the National Commission for the Control of the Electoral Campaign for the Presidential Election (here after designated as CNCCEP) was entitled to decide whether ANSSI should be involved in the response to an incident affecting candidates. The involvement of the CNCCEP itself could be sought only by political parties.

Moreover, prior to the elections, a great deal of attention was paid to awareness-raising measures with ANSSI addressing a range of first-line players and "at risk" users. Two meetings intended for campaign directors and people accountable for the cyber security of political parties were held, and a two-pager intended for general elections with examples of attack scenarios and corresponding good practices and recommendations was issued.

Even more challenging to technical agencies like ANSSI, is how to deal with information systems within political parties, as these systems are often heterogeneous (a large use of personal accounts and devices). This heterogeneous nature, therefore, makes them unsuitable for the application, in its full extent, of an information security policy relying on detection devices and the sharing of indicators of compromise (IoC).

In order to properly address this matter, which is out of the usual spectrum of activities covered by cyber security agencies, an important recommendation would, therefore, be to anticipate actions, raise awareness, and build trust. As well as, if needed, to adapt the legislative and organisational *framework to oversee the intervention of the relevant state entity toward political parties that are not traditional and well-known partners.*

Target audience - As candidate and party IT resources and solutions as well as methods of managing them can be rather diverse, engaging with both **party IT departments and party officials** could be the best combination. IT departments or outsourced service providers are to implement much of the advice, however party officials are likely to be ones who manage the budget, can release resources, and mandate the implementation of certain improvements.

When active engagement begins there are several ways to proceed, individually, by party, or as a collective. **Collective engagement** has the advantage of guaranteeing commonality of message and is probably better from an impartiality as well as resource effectiveness perspective. The downside is that parties may be unwilling to contribute to the conversation in the presence of their rivals and a party-by-party approach may mitigate against this.

Topics to cover - The topics to cover depends on the level of maturity of the target audience. Each campaign or party will have a different level of maturity and experience with cybersecurity, depending on the size of the party, their available ICT resources, their understanding of the threat, and may linked to whether they have recently been in government. and their political outlook. As a result, advice will need to be tailored, and fit the individual needs of a parties or campaigns. Individual politicians running a small campaign may need different advice than a large incumbent political party which has been in the parliament or even the government for years.

The amount of time between engagement and election will also affect the depth of advice and guidance the parties are able to digest. If only weeks are available, then there is only time to go over the absolute basics and to explain how support can be requested for example from the national CSIRT. If months or even years are available, it is possible – depending on the overall maturity of the parties being engaged – to go to a much deeper level and treat the parties in a similar manner to providers of critical infrastructure.

- General awareness raising – see above in Section 5.2.
- Cybersecurity good practices – see the NIS Cooperation group guideline on risk management and security measures [47]
- How to notify and report about cybersecurity incidents to the national CSIRT, and how to get their support with incident response

5.6 Organizational and technical measures to secure election and e-voting technology

The electoral process in the EU member states depends on a wide range of different ICT systems, also known as election technology, for example for monitoring the vote, counting the vote, or communicating the results, even if in most EU countries the actual voting is done with a pen and paper. In some EU countries the voting itself is done electronically, so-called electronic voting or e-voting. For both the election technology and the e-voting technology it is important to use state of the art ICT, to use trusted vendors, to include cybersecurity requirements in procurement and outsourcing contracts, and to audit the election and e-voting technology.

The EMBs should ensure that appropriate organizational and technical measures are taken to secure the election and e-voting technology. See the NIS Cooperation group guideline on risk management

[47] Available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

and security measures for an overview of organizational and technical measures which should be considered [48.]

In this section we discuss testing and auditing of these measures in more detail.

Testing and auditing

Testing and auditing are the cornerstones of network and information system security, because when security controls are implemented, it is important to test and audit that these controls are working in practice. Testing and auditing can be

- Organizational – of processes, procedures, roles, responsibilities, standard operating procedures, documentation, etc.
- Technical – of networks and information systems, security controls, software, hardware, etc.

Below we some tests and audits which should be considered.

Continuous automated functional (or unit) tests of systems and software during development (also called integration testing) should be an integral part of any software development setup. Modern software development methods (like Agile) place constant testing at the heart of the development process allowing low-level tests, typically called "unit-tests", to address each small piece of functionality or code. Usually, security testing tools need to be added to continuous integration tools, they are not built in. The most significant tests are integrated tests that test the entire system or solution in unison, as it would be run during elections. A public dummy test is occasionally used for an electronic solution that is widely deployed, while a more common approach would be full test run of election procedures, with fictitious candidate and voter data through the full election cycle, deploying every related system.

Source code review allows other teams within the organisation responsible for development to offer important feedback through internal audit and code review. Source code review is important to spot vulnerabilities before they get found by attackers. It is good practice to use automated tools, and/or external testers.

Load tests are designed to understand how well the systems cope with intense use (high load). This test is particularly appropriate for election technology as usage peaks for a short period of time during elections. This specific type of test also indicates the resilience to DoS attacks, which are often used against election systems, including on public-facing websites.

Security tests are separate and distinct from functional tests (functionality tests, unit tests, and load tests) that focus on whether the system does what it needs to do, and what it is expected to do. However, attacks on security often exploit the fact that systems also do things that are not wanted or intended. System security tests focus on ensuring that systems cannot be compromised by forcing it to act in unintended or unwanted ways. The problem with these non-functional tests is that there is often an endless list of assets, conditions and circumstances to test to see if the system behaves in unexpected or unintended ways. As non-functional testing is thus close to endless, testers often use a combination of known vulnerabilities, common coding mistakes (buffer overflows), and random testing, also called fuzz testing. Regardless of the approach, security testing is best undertaken by independent teams that report to the election management body or those responsible for the cyber security of elections but are not related to the developer.

Vulnerability scans are a specific and simplified form of security testing for "known" vulnerabilities. Vulnerability scans are particularly fitting for standard, commercial or open-source software. For

[48] Available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

custom developed software, they are useful for testing infrastructure and libraries, but not the custom software itself.

Penetration testing aka red-teaming: Penetration testing combines an organisational test/audit with a system test/audit. It is one of the ultimate security tests as testers are given permission to try to attack the organisation and its network and information systems "by any means necessary". In these broad and creative tests, testers try to mimic real attackers, using a combination of attack methods. Penetration tests can be very useful to reveal weaknesses in the set-up, connections, systems, and organisation. However, they do not serve as a substitute for other tests and audits.

The outcomes of penetration testing, by nature, depend on the creativity and skills of the testers. The final reports from penetration tests should also suggest solutions to the identified vulnerabilities.

Case study: Testing the security of political parties' websites in Lithuania

Lithuania provides a good example of regular reviews of political parties' websites. The Lithuanian National Cyber Security Centre (NCSC) conducts regular security testing of the websites of political parties and election infrastructure systems and provides online training and education programmes for politicians and candidates. Ensuring the security of political party websites is a largely unique measure given that most of the countries included in this research do not have any such measures in place. It is important to note that the NCSC is trusted to implement such measures.[49]

Auditing the organization: As mentioned already, software and system testing are important; but the organisation, the individuals operating the systems and the processes, can have weaknesses that cause incidents. Regardless of whether the network and information systems are developed and implemented securely. A common framework for organisational audits is the ISO27001 standard and the associated audit framework.

Security research, hackathons, and bug bounties: Inviting a wide group of experts or the public to examine technology can take many different forms.

This level of openness is appropriate for mature organisations and systems to complement, not replace, security and functionality testing. Firstly, it is expensive and not reasonable to offer (financial) incentives for simple errors and vulnerabilities that basic testing would have revealed. Secondly, open testing only fulfils its purpose if the owner of the technology can fix the issues reported. Thirdly and perhaps most importantly, this level of transparency when the technology lacks maturity is likely to create opportunities for well-resourced adversarial actors, which means that the potential risks could outweigh the benefits.

Case Study: French organisational and technical recommendations post-audit

A major contribution from ANSSI to the cybersecurity of elections was delivered through a critical system audit, hardening, and additional ad hoc measures meant to improve protection from incidents. The initiative started in February 2017 at the request of the Ministry of the Interior and was reinforced in 2022 preparing for the presidential and legislative elections, which involved a security audit and a hunting campaign on the nation-wide information system linked to the election

[49] https://www.hybridcoe.fi/wp-content/uploads/2023/09/20230912-Hybrid-CoE-Research-Report-10-PEI-WEB.pdf (pp.10- 13)

process. ANSSI provides a full support to protect and secure every information system at the technical and organizational level, as in the process of crisis management:

- First, ANSSI makes recommendations to secure administration of IT systems which are often targeted by attackers. In that perspective, ANSSI has developed a set of technical and non-technical measures to maintain the IS in operational and security condition, and to manage minor changes or major evolutions. This includes security objectives and principles for administrators, measures for administration station, network and tools but also regarding access management or security maintenance.

- Then, ANSSI provides prevention and awareness-raising to the administrations concerned by the election process to ensure that all actors are involved and ready to meet and implement ANSSI's requirements. Each entity must mobilize the necessary resources, including human resources to work on these audit and security campaign. Moreover, ANSSI produces numerous guides on communication and crisis management for all entities involved in the electoral process.

- ANSSI helps prepare these entities for post-incident response through different actions such as threat analysis (always for presidential and legislative elections) and on call-duty within the agency at various level (crisis communication procedure, crisis management etc).

Additionally, a range of less critical systems are also addressed due to their connection with the election process. ANSSI specifically recommend the implementation of the following essential measures to improve security:

Deploy capabilities to ensure a continuity of activities in the event of an incident (mitigation of impact from a possible sabotage or intrusion);

Implement a journalizing (logs) and detection mechanism;

Implement efficient network filtering (prevention of intrusions);

Implement the effective back-up of data deemed critical and corresponding recovery capabilities (business continuity plan);

Improve system robustness to withstand an increase in the volume of requests (denial of service attacks);

Ensure the comprehensive application of security updates on the components exposed on the internet (patching policy);

Report incidents on the exposed information systems to the cyber security authority without delay.

Case Study: Response to testing in the Netherlands

Case Study: use of software in the tabulation of election results in the Netherlands

The voting process in the Netherlands is a manual process: eligibility to vote is manually checked by the electoral committees at the polling stations, citizens vote by ticking a box with a red pencil on a paper ballot, and after the polls close each electoral committee counts the votes by hand and determines the votes that have been cast for each list and for each candidate (decentralised counting) or for each list (centralised counting). On the day after the election the municipal electoral committees (MEC) counts the votes for each candidate (centralised counting) and performs some checks as set out in a protocol by the Electoral Council. Voters may attend the manual counting of the votes by the electoral committee and the MEC.

The electoral committees at the polling stations and the MEC record its results on an official paperreports (called proces-verbaal).

The MEC determines the result on municipal level by adding up the votes. They use software named Ondersteunende Software Verkiezingen 2020 (OSV2020) of the Electoral Council to add up the votes. Copies of this form and the official reports of the polling stations are available for inspection at the town hall and can also be consulted on the municipality's website.

When a voter misses a vote in the official reports, the voter can notify the Electoral Council. In response to that the Electoral Council can request the MEC to investigate the notification, and if necessary, adjust the results in the official reports via a so-called corrigendum. The corrigendum will be made public alongside the official reports.

The result of this calculation by the MEC is recorded on a (paper) form that will be taken to the principal electoral committees (PEC) in person, together with the official reports of the electoral committees. Also, the results will be transmitted digitally via a secured online platform.

The PEC of all districts checks if the results transmitted digitally and brought in person match. When that is the case the PEC determine the total number of votes cast, the number of votes cast per list, and per candidate. The PEC draw up an official report of the total number of votes cast in the electoral district. The PEC take the official report of their session to the central electoral committee (the Electoral Council) in person and transmit the results digitally via a secured online platform. The official reports of the PEC are published on the internet.

The Electoral Council checks if the results transmitted digitally and brought in in person match. When that is the case the Electoral Council calculates the seat allocation at party level manually, based on the official reports (paper report of the results) of the PECs. In addition, the results are worked out at candidate level by means of a calculation tool (OSV2020). After allocation of the seats and residual seats to parties, the Electoral Council determines which candidates have been elected. The Electoral Council announces the result of the elections in a public session. The official report of this session is published on the Electoral Council's website.

Case Study: DDoS attacks against government websites in Spain

During the general elections to the Parliament in Spain in July 2023, distributed denial of service (DDoS) attacks targeted government websites in Spain, which did not impair the electoral infrastructure connected to the Internet but were claimed as targeted actions to disturb the operations of the "Spanish Internet segment" during election day.

The DDoS actions were carried out by an actor attached to the pro-Russian hybrid hacktivism cluster, a cluster that was organized as a cyber-threat infrastructure after the military invasion of Ukraine by Russia in February 2022. We call hybrid-hacktivism a cluster of cyber-threats that, generally through content spread through social media and also by carrying out cyber-attacks on computer systems, they impersonate an apparent ideological narrative to justify their actions, a narrative that in fact aims to cover up actions based on geopolitical interests in favour of a State.

In the case of pro-Russian hybrid-hacktivism, this type of cyber-threat is configured through a diverse set of digital identities that spread pro-Russian, anti-Western, anti-European and anti-NATO propaganda content on social media, while deploying their own botnet-type infrastructures to organize, on a daily basis, DDoS attacks in order to disturb the normal functioning of government and strategic economic sectors web services in European Union and NATO countries.

In this context of a cyber-threat cluster aligned with Russia's geopolitical interests, pro-Russian hybrid hacktivism could operate in coordination with another typology of cyber-threats of alleged Russian origin acting in more sophisticated and dangerous cyber-operations targeting European computer systems.

Case Study: Dual system of result transmission in Austria

In Austria there is a strict reporting chain of results from local polling stations up to the highest level, the Federal Electoral Board. Preliminary (non-binding) results are delivered through a system of ad-hoc reports (email, text message, fax, etc.) The use of IT solutions provided by the Federal Ministry of the Interior, which acts as the Federal Electoral Board's secretariat, only starts at the provincial level (the second highest administrative level in the country). The provinces feed the data into a secure system.

Data transmission is carried out in an encrypted format. The system is run on secure servers of the Federal Ministry of the Interior. The software is constantly improved and modernised and the system is tested before every election (through pilots with involved authorities). The public presentation of (preliminary) results starts after the closing of the last polling stations (from 17:00 onwards). An elaborate IT solution is provided over the internet.

Once the data from all polling stations is in, the Federal Minister of the Interior, in his capacity as Chair of the Federal Electoral Board, usually announces the preliminary final results on Election Day. As this announcement is not compulsory, a press release is also possible. Before the preliminary final results are presented, the figures tabulated in the IT system are double-checked with the respective provincial reports arriving via email.

While the preliminary final results are eagerly awaited by the public on Election Day, they have no final legal relevance as two processes coin the dual system of result transmission in Austria. On the one hand, non-binding ad hoc reports are delivered and accumulated on Election Day, and on the other hand, minutes on paper are passed by the competent electoral boards within the framework of official meetings shortly after the election.

The Austrian Constitutional Court only considers paper records as legally relevant. All binding results have to be determined and decided by electoral boards. A recount could be ordered by the Constitutional Court. Therefore, ballot sheets have to be kept until the final results remain uncontested.

Case Study: DDoS - preparations to improve the security in Sweden

The Swedish Election Authority wrote following in its report after the 2022 elections:

''Based on the experience of the 2018 elections – when the agency's website was subjected to a denial-of-service attack and thus inaccessible for most of the election night - much preparation had been put into improving the security, capacity and resilience of the system against feared attacks during the 2022 elections.

The agency's website was subjected to at least three serious denial-of-service attacks in connection with election day 2022, including one attempt on the day before election day and two attempts on election day and election night. After the initial attempts, a series of measures were implemented to secure the website to close possible loopholes. The overall preparations were successful as all attack attempts could be repelled. The website was accessible throughout the election night and it was possible to follow the preliminary vote count on val.se without interruption.

Experience shows that the IT-security for the Authority's website and its digital environment in general requires extensive work and an ongoing systematic maintenance between the election occasions, both in terms of technical security and cooperation with other authorities."

Case Study: Electoral rolls in Germany

The municipality keeps a register of voters for Bundestag and European elections. The electoral roll determines the group of persons formally entitled to vote. The basis for this is the population register kept by the municipality. When drawing up the voters' register, only persons with German citizenship *who are registered with the registration authority on the 42nd day before the election are considered ex officio.*

Anyone entered in a voters' register must have received a polling card from the local authority by the 21st day before the election at the latest.

To check the data of other persons entered in the voters' register, eligible voters only have a right to inspect the voters' register if they can credibly demonstrate facts which may show that the voters' register is incorrect or incomplete. Anyone who considers the electoral roll to be incorrect or incomplete may lodge an objection with the municipal authority within the inspection period.

Case Study: Use of digital identity in Elections

Digital ID as an authentication method in elections can come to play where it is recognised as secure by the government authorities. Estonia, with its unique I-voting, relies on a secure government-backed digital identity. There have been experiments with distributing credentials through mail, email or SMS message, all of which were considered less secure; while a few Member States have attempted identification through online banking, creating dependencies on a private sector service.

A choice of SMS or email in particular raises the issue of the choice of the third party generating the mail and/or SMS, which potentially provides access to the credentials of the voter and their identity (emails or phone number). Regardless of the approach to voter ID and rolls (including no-compulsory identification and fully paper-based elections), election organisers have to recognise it as a (often live) dependency and an attack vector.

Case Study: From paper ballots to results in the news in Finland

Paper ballots are first counted at polling stations (with few exceptions) on election Sunday. The initial results are input to the election data system and written on paper forms that are then sealed in envelopes and transported to central election committees in municipalities. Results are published to two systems. One is the official results system and the other is for media (not on the internet) so they can get raw data immediately when they are published to the system. Citizens mostly view results from the web pages of the media. However, a number still use the official result page.

The ballots are recounted and corrections are made if there are changes to the initial results. Usually, confirmed results are ready on the Tuesday or Wednesday following the election Sunday.

6. Conclusion

This document aims to support all actors involved in elections to navigate the evolving elections threat landscape. It offers useful insights and proposes good practices, in order to help interested parties and those involved in all the phases of the electoral process to step up their awareness and resilience against security threats and incidents throughout the electoral cycle. By sharing the case studies, which are included throughout this document, EU Member States highlight the commitment in the EU to information sharing, collaboration and overall, to enhancement of safeguards to keep elections in the EU secure, free and fair. By strengthening cybersecurity preparedness and resilience, this resource helps ensure the integrity of European democratic processes.

The relevance and completeness of this compendium might be reviewed by the actors involved in the 2024 electoral year, by further compiling and analyzing their observations and assessing the necessity to update this document to ensure its quality, level of accuracy and usefulness.

Annex I: Terminology and Abbreviations

Table of Abbreviations	
Backdoor	A method, often secret, of bypassing normal authentication or encryption in an IT system.
CDN	A content delivery network or content distribution network (CDN) is a geographically distributed network of proxy servers and their data centres. The goal is to distribute service spatially relative to end-users to provide high availability and high performance.
CSIRT **CERT**	Computer security incident response team (CSIRT), often called a computer emergency response team (CERT) or computer emergency readiness team is an expert group that handles computer security incidents.
CTI	Cyber Threat Intelligence (CTI) is based on the collection of intelligence on cyber security from various sources including open-source intelligence, social media, technical intelligence and others.
Cyber-attack	A digital attempt targeting availability, confidentiality and integrity of data, systems or networks.
DoS **DDoS**	A denial-of-service attack (DoS) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.
Web Defacement	An attack on a website that changes the visual appearance or content of the site or a webpage.
ENISA	The European Union Agency for Cybersecurity (ENISA) tasked with improving network and information security in the European Union.
European Parliament (EP)	The European Parliament (EP) is the directly elected parliamentary institution of the European Union.
FIMI	Foreign Information Manipulation and interference (FIMI) is defined as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory
Hactivism	Hacktivism, or hactivism, is the use of computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change. With roots in hacker culture and hacker ethics, its ends are often related to free speech, human rights, or freedom of information movements.
Hybrid threats	Political use of Hybrid Threats refers to manipulative, unwanted interference through a variety of tools: spread of disinformation/misinformation, creation of strong (but incorrect or only partially correct) historical narratives, election interference, cyber-attacks, economic leverage etc.

HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network, and is widely used on the internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or formerly, its predecessor, Secure Sockets Layer (SSL). The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication.
IP	An Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite. Its routing function enables the internet to work and essentially establishes the Internet. An Internet Protocol (IP) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
IT	Information technology.
Malware	Malicious software (malware) is any software intentionally designed to cause damage to a computer, server or computer network.
MEP	Member of the European Parliament.
MP	Member of Parliament.
NGO	Non-governmental organisation.
NIS Directive	The Directive on Security of Network and Information Systems (NIS Directive) set into policy by the European Parliament in 2016 in order to create an overall higher level of cyber security in the European union.
Ransomware	Ransomware is a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability.
SIEM	Security information and event management (SIEM) are software products and services that provide the real-time analysis of security alerts generated by applications and network hardware.
SOC	Security Operations Centre
Spear phishing	Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Spear phishing is directed at specific individuals or companies, where attackers typically gather personal information about their target to increase their probability of success.
STRATCOM	Strategic communication (STRATCOM) means organizational communication and image management that satisfies long-term strategic goals of an organisation or individual.
TTP	Tools, techniques and protocols.
VLAN	A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building. A virtual LAN (VLAN) is any communication layer that is partitioned and isolated in a computer network at the data flow layer.
VPN	A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. To ensure security, data travel through secure tunnels and VPN users use authentication methods – including passwords, tokens and other unique identification methods – to gain access to the VPN.

Wiperware	Wiperware is a variation of ransomware which is technically similar, but while in a ransomware attack the attacker aims to get a ransom, and then restores (decrypts) the data, in a wiperware attack, the attacker does not request a ransom and never intends to restore (decrypt) the data.

Annex II: Overview of case-studies

Table of Case Studies

Case Study	**Chapter**	**Main lesson learned / area of focus**
Estonian National Election Committee - Estonian I-voting	2.3	Best practice for the organization of election supervision and result control
Spanish General Elections in 2023 - Disinformation with a fake website	3.3	Example of disinformation attack on polling station without security incident.
Polish parliamentary elections in 2023 - Disinformation with a deepfake video	3.3	Example of disinformation Attack on polling station without security incident.
Collecting and verifying national results for the Hemicycle	4.4	Best practice for the transmission of election results
IT-Grundschutz – protection profile for preliminary election results - Security concept for the secure transmission of preliminary election results	4.4	Best practice for the transmission of election results
Spanish incident response team - Monitoring the security situation during the elections	5.1	Monitoring the security situation and responding
French risk management approach - Generalities and objectives	5.3	Best practice for cyber risk managment
IT-Grundschutz -Objectives, concept and design	5.3	Standard and best practices for information security management
EU ELEx23, EU-level table-top exercise for the European Elections 2023	5.4	Exercise to improve ability to respond to cyber security incidents
Training the employees of Czech statistical office	5.4	Awareness campaigns for employees of the electoral authority
Anticipate actions, raise awareness and build trust in France	5.5	Awareness campaigns for electoral authority and political parties
Testing the security of political parties' websites in Lithuania	5.6	Best practice for ensuring the security of political party websites

French organisational and technical recommendations post-audit	5.6	Best practice for the protection of information systems related to the electoral process
Response to testing in the Netherlands	5.6	Proven procedure for determining election results
DDoS attacks against government websites in Spain	5.6	Example of hybrid hacktivism in the context of elections
Dual system of result transmission in Austria	5.6	Best practice for ensuring the transmission of election results
DDoS - preparations to improve the security in Sweden	5.6	Proven method for protecting election websites against DDOS attacks
Electoral rolls in Germany	5.6	Electoral roll as best practice to ensure the identity of eligible voters
Use of digital identity in Elections	5.6	Digital identity as a best practice for authenticating electors
From paper ballots to results in the news in Finland	5.6	Best practice for the transmission and publication of election results