Compendium on Cyber Security of Election Technology

CG Publication 03/2018

NIS Cooperation Group

July 2018

ABOUT

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

The Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), has been established by Article 11 of the Directive (EU) 2016/1148 'concerning measures for a high common level of security of network and information systems across the Union' (NIS Directive). It facilitates strategic cooperation between the Member States regarding the security of network and information systems.

Table of Contents

1. Executive Overview

Elections are crucial to the functioning of representative democracy and election processes being compromised can delegitimize a whole political system. At the same time, elections have become an increasingly frequent target in the modern digital era, coming under attack across the globe. Cyber-attacks – most likely combined with information operations and other hybrid threats – are therefore a reality in elections and must be reflected in planning assumptions and risk management.

In the case of the elections to the European Parliament, a successful campaign against one Member State that includes cyber-enabled elements could mean that the assignment of seats cannot be confirmed thus compromising the entirety of election processes. This could impact the ability of the European Parliament to convene and thus could affect the very functioning of the European Union.

All elections are expected to be free, open and fair, and based on secret ballot; technology cannot be introduced at the cost of compromising these requirements. Digital solutions, or election technology in itself, are no more or less secure than paper-based voting solutions but rather need to be introduced prudently while making sure that the digital solutions meet the same legal requirements for elections as traditional solutions. Additionally, technology can ensure that these requirements are met, so this compendium details a number of methods to harness innovation to ensure the legitimacy of electoral outcomes.

State-backed cyber-attacks, often coupled with information operations, appear to be aimed at sowing doubt and discord with the possible objective of disrupting and influencing the democratic processes. Even electoral systems that exclusively rely on pen and paper in voting, take advantage of digital tools and services in compiling voter rolls, candidate registration or result tabulation and communication.

Therefore, a work stream focusing on the cyber security of election technology has been set up under the auspices of the Cooperation Group established by the NIS Directive in order to share experiences and provide guidance as well as an overview of tools, techniques and protocols to detect, prevent, and mitigate such threats.

While the processes of elections themselves – the registering of voters and candidates, the gathering and counting of votes, and the communication of the election results – are by no means impervious to attack, recent events highlight the need to also defend the auxiliary systems – for example IT used by parties and candidates or those communicating the elections results, including the media.

As such, this living document is a broad sum of guidelines that are based on the experiences and best practices of its contributors, and is a compendium of practical and workable measures that can be taken by cyber security organisations and election management bodies as well as those advising or overseeing them to secure the technology involved in elections. Contributions have been made by a majority of Member States as well as the European Commission, ENISA and the staff of the European Parliament's Secretary General.

As the organisation of elections is a national prerogative and there is a great degree of variation across Member States, the compendium offers all Member States the opportunity to select the approaches best fitting their specific situation and needs.

A number of appropriate checklists and case studies offer further practical guidance. To be of efficient use, cyber security measures are reviewed as pertaining to:

- the specifics of European Parliament elections;

- universal development and security principles as applicable to election technology, including testing and auditing;
- security measures specific to elections;
- voter and candidate registration and databases;
- electronic tools used in gathering or aiding the gathering of votes;
- digital tools to transmit, process and count votes;
- systems to publish or communicate election results;
- relevant auxiliary systems and services.

In line with the focus of the NIS directive, this compendium specifically focuses on events that are cyber-enabled or relate to the security of network and information systems in the context of elections. **Social media, information operations, and disinformation are outside of the scope of this initiative**, while internet/remote voting solutions are not at its heart, but can inform the practices discussed.

2. 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.
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 Network and Information Security (ENISA) tasked with improving network and information security in the European Union.
European Parliament	The European Parliament (EP) is the directly elected parliamentary institution of the European Union.
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.
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 a long term strategic goals of an organization 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.

3. The Increasing Cyber Threat to Elections

In recent years, the international security environment has changed dramatically and the European Union has expressed serious concern about the increased motivation and capability of state and non-state actors to pursue their objectives by engaging in malicious cyber activities,[1] often integrated with other operations or campaigns. **These cyber-enabled attacks, when aimed against the core functions of our democratic institutions, including elections, undermine the very legitimacy of these institutions, the safeguards in place to protect them, and the participants of the democratic process. Therefore, the robust cyber defences of the technology involved in elections cannot be overestimated.**

Politically motivated (including state or state-backed) actors can be opportunistic, well-resourced, persistent, and strategic as they engage in cyber-enabled sabotage as well as economic and political espionage. In the former, they have often focused on swaying the democratic processes to delegitimise the target or for potential geopolitical influence.

Several EU Member States, as well as other countries, are paying close attention to the digital influencing of democratic institutions, particularly in the light of several high-stakes presidential races impacted in 2016. For example, the German political party CDU, the En Marche! movement of French President Emmanuel Macron, and the US Democratic Party have been the victims of cyber-attacks.

These activities appear to be aimed at sowing doubt and discord with the possible objective of disrupting and influencing the democratic process. While attacks on the processes of the elections themselves (the registering of voters and candidates, the gathering and counting of votes, and the communication of the election results) are by no means impossible, these events highlight the need to bolster cyber security not just through the election life cycle but also of auxiliary systems. In France, data from the campaign of presidential candidate Macron was leaked shortly before the elections in May 2017. The security company Trend Micro announced in May 2016 that German Chancellor Angela Merkel's party had been the victim of cyber-attacks. Employees of the CDU received spear phishing emails that linked to a copied login screen for the webmail service that they used. The attacker had hoped to acquire login details this way. The same year, it appeared that the US Democratic National Committee had been the victim of a number of attacks that resulted in the theft and publication of politically sensitive materials. According to the US intelligence services, the attacks, attributed to a state-backed actor, were part of a campaign aimed at influencing the presidential elections.

These events highlight the dependence of electoral processes on technology and therefore, the need to bolster the cyber security of election technology. Even Member States that exclusively use paper ballots in voting can rely on electronic solutions for voter and candidate registration, vote counting or the communication of the results.

As with any novel solution, election technology needs to be introduced prudently while making sure that the digital solutions meet the same legal requirements for elections as traditional solutions. While the language of national norms can vary, all elections are expected to be free, open and fair, and based on secret ballot; technology cannot be introduced at the cost of compromising these requirements, as set out in a constitution or election legislation. However,

[1] Council Conclusions on malicious cyber activities, http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf (16 April 2018, accessed 18 June 2018)

technology can ensure that these requirements are met, so this compendium looks at ways – such as logging and monitoring – to harness innovation to ensure the legitimacy of electoral outcomes.

3.1 Need for Experience Sharing

Elections are necessarily and uniquely a national prerogative. However, the cyber-enabled threats are likely to be global. Experience sharing across Member States benefits all as the attack vectors and adversaries are often similar. This is particularly true in the case of the elections to the European Parliament in May 2019 where an incident or threat affecting the legitimacy of election results in one Member State inevitably affects the legitimacy of the election results of the whole of the Parliament, possibly impeding its ability to convene.

The elections to the European Parliament have a strong international component and the impact of incidents and threats is EU-wide. The European Council has received a strong mandate from Member States "to shore up the integrity of our free and democratic societies in the digital age, by protecting the citizens' constitutional rights, freedoms and security online as well as the integrity and legitimacy of democratic processes, in particular of our elections" in 2017.[2]

Similarly, the Secretary General of the European Parliament wrote to the Chair of the Cooperation Group established under the NIS Directive in October 2017, asking to address the cyber security of elections with a view of securing the 2019 European Parliament elections, as "elections are a particularly sensitive process in a Union that has democracy as one of its founding values." The highest official of the European Parliament highlighted in his letter that an incident during the elections "could create major disruptions to the constitution of the next Parliament."

The European institutions can possibly facilitate such experience sharing. Thus, "with a view to the 2019 European Parliament elections, the Commission has encouraged the competent national authorities to identify best practices for the identification, mitigation and management of risks to the electoral process from cyber-attacks and disinformation."[3]

Furthermore, it is not only the central functioning of the systems controlled by the election management bodies that need to be addressed. As demonstrated in a plethora of elections and campaigns, the auxiliary systems related to elections (including other government networks and databases as well as the IT of candidates, parties and media) can be targeted, and successful attempts can similarly undermine elections.

Cyber-attacks – most likely combined with information operations and other hybrid threats – are a reality in elections and must be reflected in planning assumptions and risk management.

The Cooperation Group established by the NIS Directive supports and facilitates strategic cooperation and the exchange of information among Member States to develop trust and confidence amongst them. Therefore, on 28 November 2017, the Cooperation Group agreed to focus on the cyber security of election technology and asked Estonia to map similar existing European initiatives and advance the process. The initiative is co-chaired by the Czech Republic; and

[2] *Preliminary conclusions of the Prime Minister of Estonia from the Tallinn Digital Summit,* *https://www.eu2017.ee/news/press-releases/preliminary-conclusions-prime-minister-estonia*

[3] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling online disinformation: a European Approach, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804 (26 April 2018, accessed 18 June 2018)

a majority of Member States as well as ENISA and the staff of the European Parliament's Secretary General have contributed to the discussions or parts of this text.[4]

3.2 Existing Initiatives

There are a number of initiatives to secure elections nationally, as well as internationally between the election organisers, such as the European Commission for Democracy through Law of the Council of Europe ("the Venice Commission") that works closely with the Electoral Management Bodies (EMBs) of its 61 Member States[5] and has also dedicated its annual conference in 2018 to election security.[6]

As of mid-2018 there are also a number of EU initiatives to address election security across the European Union. In particular, the Commission expert group on electoral matters focuses on remote voting in the context of bolstering turnout and could benefit from a set of best practices on securing the electoral process. Elections are embedded in the very fabric of representative democracy, so a number of EU institutions are planning election security related events and initiatives in the run-up to the elections to the European Parliament. Additionally, major effort has been delivered, most notably by the Friends of Presidency Group focusing on hybrid threats.

However, none of these focus on the cyber security of the electoral process and therefore are complementary to the work in the current document. Furthermore, in drafting these guidelines, the work stream has regularly exchanged information with the relevant working groups as to best benefit from each other's work.

[4] Liisa Past of Estonian Information System Authority (liisa.past@ria.ee) and Viktor Paggio of Czech National Cyber and Information Security Agency (v.paggio@nukib.cz) were in charge of the first draft of this document. Please contact the European Commission (CNECT-NIS-DIRECTIVE@ec.europa.eu), secretariat of the NIS Cooperation Group, or the respective national authorities for further information, contributions or comments.

[5] The Venice Commission assisting Electoral Management Bodies towards genuine electoral processes, https://www.coe.int/en/web/electoral-management-bodies-conference/about-us

[6] Read more on https://www.coe.int/en/web/electoral-management-bodies-conference/emb-2018

4. Specifics of Elections to the European Parliament

Elections to the European Parliament are rather specific compared to elections within a Member State and their cross-border nature creates unique challenges. Most importantly, as has been highlighted already, a compromise of any stage of the electoral process anywhere in Europe can have spill-over effects to the legitimacy of the whole election. Therefore the Member States and European institutions have a common interest to address the challenges of election organisation together, facilitating experience sharing, including through this compendium.

The importance of the last mile of these elections – the communication of the results from capitals to Brussels and the display of the results – cannot be overestimated. While municipal, federal state, and national elections are organised at close intervals allowing election management bodies within Member States to practice the appropriate procedures, including those relating to security, regularly, the elections to the European Parliament take place every 5 years.

Therefore the 2019 campaign and elections are the first time that the last mile shall be put into practice in a changed security environment in terms of the attacks on digital infrastructure, potentially creating an attractive attack surface. **Pan-EU cooperation and a comprehensive view of election security are necessary steps in ensuring the legitimacy – both in terms of public trust and legal procedures – of the 2019 European Parliament elections.**

Two distinct but connected layers of technology are at play in the international element – or the last mile – of the elections to the European Parliament:

- **The communication of preliminary results for information purposes** as polls close at the end of the election week, through a website representing the allocation of seats in the future European Parliament hemicycle.
- **The communication of the binding national results from capitals to the European Parliament** is treated as the official communication of any election results and, regardless of the specific mode of transfer, has to be secured and verified as per best practice. Including using the advice laid out in this document.

The European Parliament will set a system allowing the collection of the national results provided by Member States as well as the calculation of the composition of the hemicycle and the distribution of all these results on the internet from the electoral night and until the constitutive session. After reviewing the specific regulations and organisational details pertaining to the elections of the European Parliament, this chapter will then review the security measures taken to secure the communication layer.

4.1 Election Organisation and Regulations

Both European legislation defining rules common to all Member States and national law govern elections to the European Parliament. These common rules lay down the principle of proportional representation and the specifics of the mandate of a Member of the European Parliament. The exact electoral system, including the number of constituencies, is governed by national regulation.

Therefore, to a great degree, the European Parliament elections mimic national election procedures and rely on similar rules, regulations, processes, and election managers as local, federal (where applicable) and national elections. Unlike with national elections, however, most Member States function as single constituency, with Belgium, France, Ireland, Italy and the United

Kingdom having divided their national territory into a number of regional constituencies.[7] Constituencies of merely administrative interest or distributive relevance within the party lists also exist in the Netherlands, Poland, and, to a degree, in Germany.[8] This means the registration of voters and candidates and the management of the relevant databases can differ from that during national, federal state or municipal elections.

With a few limitations or extra requirements across Member States, the nationals of a Member State can vote and stand as candidate[9] in their Member State of residence, should those be different. Therefore, the European elections have to address cross-border voter registration; an initiative led by DG JUST focuses on that issue in the 2019 election cycle.

Elections to the European Parliament take place every 5 years. While elections to the European Parliament are held within the same period starting usually on a Thursday morning and ending on the following Sunday, the exact date and times are fixed by each Member State.[10]

This rolling nature of elections creates unique challenges for those tasked with securing the elections as there is additional potential for spill-over effects. Member States may not make the results of their count public until after the closing of polls in the Member State whose electors are last to vote; maintaining the confidentiality of results in Member States that vote earlier might require additional security measures or procedures.

4.2 Security of Communication of the Preliminary Results for Information Purposes

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**.

The selection of the company in charge of the platform representing the preliminary results on-line was made via a call for tender.[11] References are required, along with team composition in order to be able to assess the capability to carry out such a project. Weekly follow-up meetings, on-site visits,

[7] The European Parliament: electoral procedures, available on http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.3.4.html#_ftn1, accessed on 19 March 2018

[8] The European Parliament: electoral procedures, available on http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.3.4.html#_ftn1, accessed on 19 March 2018

[9] Article 3 of Council Directive 93/109/EC

[10] The European Parliament: electoral procedures, available on http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.3.4.html#_ftn1, accessed on 19 March 2018

[11] Call for tender for the European Parliament elections 2019, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=3334, accessed on 18 June 2018

precise lists of the technical and functional documents to be produced, and assurances that key members remain the same throughout the project are required.

Advanced security measures should be taken in order to make this operation a success. Access to back-office tools should only be reserved to the operational team with an enhanced double authentication system. Similarly, the publication system should be highly protected and a secure Content Delivery Network used in order to accommodate great numbers of visitors and to prevent a

Case Study: Collecting and Verifying National Results for the Hemicycle

The year 2014: In the months preceding election night, the European Parliament, together with an external contractor selected on the basis of a public call for tender, produced internal projections based on an ongoing voting intentions monitoring in all Member States. The same procedure will be enacted for the 2019 elections. 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 will be 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 is expected to establish a liaison with each of these bodies to ensure the collection of results during the European elections period. Special attention should be given to obtaining results from the official bodies in an appropriate digital format. In addition, this liaison will have 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 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.

The 2014 elections results were published on http://www.europarl.europa.eu/elections2014-results/en/election-results-2014.html.

denial of service. Annex 2 of this compendium offers outtakes of the call for tender in terms of the security requirements.

5. Universal Development and Security Guidelines as Applicable to Election Technology

There are several established methodologies on the selection and implementation of security controls for IT-based processes.[12] However, it is a common understanding that the identification of relevant assets and threats — at least on an abstract level — is a prerequisite. This particularly applies to election processes, as the threat landscape is not necessarily standard in its integrated and fast-moving nature.

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 sponsor.
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 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; • DoS or overload of government websites.
Voting	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.

[12] General provisions are also covered by the Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to Member States on standards for e-voting (see in particular VIII. Reliability and Security of the System).

Due to the diversity of election systems and election technology in the Member States, it is not feasible to provide universal and comprehensive templates of relevant assets or threats. Therefore, the table above can serve as a starting point as it highlights some examples and is not intended to be all-encompassing.

In this regard, it is important to note that an election process extends over a life cycle consisting of several phases with their respective threats and relevant IT assets. For example, the compilation of electoral rolls and the registration of candidates usually occur at an early phase of the election process and have other security implications than the publication of the final result. As a consequence, the threat scenario is not static. Other tools, methods and procedures are more universal and should be applied to all stages of elections that utilise IT. This chapter highlights the practices that apply across the election life cycle and can be used as a checklist in the development and introduction of technology.

5.1 Development Practices

The development practices to consider in ensuring the cyber security of election technology, regardless of what part of the election process the particular technology is used in, include:

- a unified approach to **data integrity** (and possibly the use of cryptography) across the platforms and solutions used;
    - key parts of code or information can be sealed before the beginning of the election process until its end, as far as practical;
    - alternatively, include integrity checks to safeguard against logic bombs or alterations in the code.
    - back-up all data regularly with increased frequency of back-ups in the run up to an election.
- **compliance with cyber security requirements and standards** as applicable to election technology;
    - reference to standards or technical specifications;
    - the specific protection profile;
    - evaluation criteria and evaluation methods;
    - as well as the intended level of assurance (basic, substantial and/or high);
- documentation and **procedural controls;**
- **secure development, supply chain management and procurement;**
    - support the integrity/confidentiality of votes and the availability of relevant systems in line with relevant national or international standards.
- **ownership model** of the solutions;
- **communication channels and responsible disclosure mechanisms** with different parts of the supply chain should be part of the initial procurement, negotiations and contract;
- **vendor responsibility** including the legal provisions for it should be part of any technology procurement process from the start.

5.1.1 Development and Supply Chain Assurance

Cyber security certification plays an important role in the necessary trust and security of election technology — however it should be understood that certification and accreditation are not security warranties but rather assurance that the solution meets specific criteria in terms of functionality and/or security.

Additionally, while respective approaches can differ, it is necessary to be systematic in applying secure development practices, supply chain management and procurement in order to incorporate feedback fast, almost instantaneously. Securing the supply or development chain is one of the fundamental issues in government technology development and innovation purchasing, with no one "silver bullet" approach. Therefore, those procuring or developing such technology have to consider and find the appropriate balance for their specific situation as a combination of technologies and approaches (often with specific licencing agreements)**.**

Furthermore, in regard to the **ownership model** of the solutions, while election organisers owning the technical proprietary solutions and related intellectual property (even if developed externally) minimises the reliance on commercial products, provides better control and potential security, it also assumes the election organiser's ability to develop technology in a fast-paced environment as threats, errors and vulnerabilities are discovered.

Alternatively, either a licencing agreement or a boxed product provides access to commercial technical expertise, and impact the government's ability to independently develop solutions and increase dependencies, thus lessening control.

Regardless of the model, a multi-stakeholder approach combined with a security buy-in from the election organiser to the cyber security practice (on local, federal state and national level, as appropriate), including clarity of roles and cooperation model, allows for best outcomes.

Case Study: IT-Grundschutz (IT Baseline Protection) in Germany

IT-Grundschutz is a holistic framework that includes standard cyber security recommendations in the areas of organisation, technology, personnel, and infrastructure. It is updated and published on a regular basis by Germany's Federal Office for Information Security (BSI). IT-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.

In terms of IT systems relevant to elections, IT-Grundschutz can be employed to mitigate standard risks and to serve as a foundation for additional and specialised security controls. For instance, the IT-Grundschutz compendium covers security controls in the areas of systems hardening, update/change management, cryptography, access control, and identity management.

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?

5.2 Comprehensive Risk Assessment and Management

As previously mentioned, **cyber-attacks, most likely combined with information operations and other hybrid threats, are a reality of elections and have to be reflected in the planning assumptions and risk management of election technology**; such as in the creation of incident management procedures and during information sharing. Communication during incidents or times of heightened threat is fundamental in providing election security. Comprehensive cross-government risk assessment and incident management is essential to resilience and preparedness.

Proper procedures, security, logs, verification, auditing and other safeguards have to be put in place so election technology is able to detect and call out irregularities – whether network traffic characteristic to a DoS attack or tampering with votes or databases – and therefore prevent or mitigate their potentially devastating impact. This must also cover such attempts by malicious insiders, including election organisers. The risk assessment of election technology can feature risks related to:

- technical risks of the election system, such as;
    - infrastructure communication channels;
    - databases and work processes;
    - critical dependency mapping.
- management and human risks, such as;
    - roles and division of labour;
    - insider threats;
    - the identification and allocation of resources to overcome risks.
- unacceptable external risks and dependencies, such as;
    - vendors;
    - outside systems, etc.
- risks against auxiliary systems and players that can impact the functioning of the elections or cast a shadow over its legitimacy, such as:
    - other government services;
    - parties;
    - candidates;
    - any sort of hybrid attacks integrating information and cyber operations.

While the risks and potential attacks vectors are often specific to elections, most systematic risk assessment, mapping and mitigation approaches can be used. It is advisable for risk assessments to be undertaken by the election organiser or those responsible for election security, as this way it is most likely to also inform and impact planning and resource allocation. Also, approaches that take into account both the likelihood and the potential impact of risks materialising have been proven most useful. Additionally, scenario planning can be a useful tool for dealing with high impact - high probability risks.

Case Study: French Risk Management Approach

The modernisation of the French cyber risk management framework, through a revision of EBIOS, the risk assessment methodology published by the French National Cybersecurity Agency (ANSSI), was necessary to take into account the new realities of the digital age (interconnected systems, threat proliferation, more mature, state of the art, regulation, threat knowledge) and the feedback received on implementing risk assessments.

Feedback showed that the existing risk management methodologies in the shape of fortress-inspired approaches no longer fit for the new security risks of the digital age; due to ecosystems being largely underestimated, a lack of performance management, and a lack of agility at a time of proliferation of cyber-weapons.

The key objectives of the modernised risk management approach are to obtain a shared understanding of cyber risks between decision-makers and IT experts, and for decision-makers to consider cyber risks at the same level as other strategic risks (financial, legal, reputation, and so forth). This shared understanding and shared approach is essential thereafter to the implementation and enforcement of cyber security measures.

The new risk assessment methodology EBIOS is based on three pillars:

1. **A synthesis between compliance and risk scenarios**

The last EBIOS methodology, which dates back from 2010, was focused on compliance with general guidelines and regulations. At present, however, a compliance-based approach is not enough to guarantee a good ability to resist threats. Thus, it needs to be combined with building risks scenarios that need be end to end, and designed from the point of view of attackers, enabling the description of the operational modes of attackers.

2. **Leveraging threat intelligence**

Risk management frameworks need to be better in including threat intelligence. In order to build risk scenarios from the point of view of attackers, in-depth knowledge of threat sources is necessary. Part of the EBIOS method is, therefore, to offer a structure that enables assessing different attackers' profiles, their objectives and motivations.

3. **A better inclusion of ecosystems**

Attackers no longer seek necessarily to reach organisations head-on but rather to target other parties from the same ecosystem, which can be more vulnerable. Usually, attackers are looking for the weakest point to move to their intended target. Therefore, it is vital to take the ecosystem into account in a risk assessment in the present day.

5.3 Planning for Crisis Management, Incident Detection and Response

Planning, routines and cooperation formats for incident response and crisis management should be in place well before elections. **The routines, including the Standard Operational Procedures, should be ready and in place in order to act swiftly when a crisis occurs.** These procedures go hand in hand with table-top or technical exercises where the decision-makers and operators practice reactions to events as well as information exchange, chain of command, etc.

Case Study: Introducing Comprehensive Risk Assessment

"In the past, the risk assessment of the Estonian I-voting systems had focused on the threats under the direct control of the election organizers (including technical risks stemming from the software). Given the changed threat landscape and adversary's hybrid tactics, a more comprehensive risk assessment approach was introduced in 2017 to be able to mitigate risks arising from third parties and world politics as well as the lively digital ecosystem encompassing both Estonian e-governance solutions (including ID-card, population registry etc.) as well as third parties involved in the development and distribution of these solutions.

This is particularly important, as the legitimacy of the elections does not only depend on the technical execution of voting procedures. This approach also accounts for and suggests ways of mitigating risks arising from information/hybrid attacks, dependencies on the ecosystem, management issues, introducing new online voting software, the impact of a large group of first-time voters (for the first time, Estonia invites 16-18-year-olds to the polls) and other factors outside the direct control of the election organizers. The assessment includes dependencies on outside systems and services as well as ways to identify, manage and mitigate them, including approaches to transparent communication.

It is hoped that such a comprehensive approach, particularly as it was introduced early in the planning period, allows prioritization of tasks and resources according to their potential impact. The shared understanding of landscape brings parties involved to the same page in planning and management terms, thus allowing for better responses to eventualities as they arise."

Quoted from Past, Liisa "All Elections are Hackable: Scalable Lessons from Secure I-Voting and Global Election Hacks" from the European Cybersecurity Journal (2017, vol. 3) can be downloaded from https://www.ria.ee/public/RIA/ECJ_Volume3.Issue3_Extract_PAST.PDF.

A multi-stakeholder approach with formalised agreements and procedures includes both detection of irregularities and the procedures for such detections.

5.3.1 Detection and Triage

The process of crisis readiness involves event awareness and the ability to note irregularities:

- **Situational awareness** includes threat intelligence from a variety of government and commercial sources, particularly if the risk assessment reveals high-impact and high-probability cyber-attacks.
- **Incident/log and traffic monitoring** is essential to understanding events, particularly during the election period itself and the tools for it can take time and resources to develop.
- **Traffic and incident monitoring** can be tasked to the respective government body responsible for government networks and managing security incidents, often CSIRT. During

the active phase of elections and as part of the security task force, they can be responsible for detecting anomalies, including possible DoS attacks. Those tasked with monitoring should have access to the appropriate tools, such as visualisation software, log monitoring platforms, etc., that are capable of handling large and unpredictable quantities of machine-created data. These tools are best utilised when constantly improved and developed.

- **Indicators and escalation criteria** are necessary so that those tasked with situational awareness and monitoring know what should be watched for and what the next steps should be in the case of a threat or incident.

Please see Chapter 7 for the specific tools that EU Member States have found useful in protecting their election technology.

5.3.2 Procedures, Cooperation and Chain of Command

Case Study: Procedural Controls and Dispute Resolution in Estonia

"Procedural controls defining the main manual activities and practices that election officials engage in" (Nurse, et al., 2016, pp. 5-6) are a core component of I-voting, and documented in the election manual and security policy available (mostly in Estonian) on the elections website (Author's interviews, 2017) (State Electoral Office, Republic of Estonia). Estonia relies heavily on these procedures focusing on data integrity between parts of the system, access control and mechanisms for dispute resolution and system continuity (Nurse, et al., 2016). Additionally, dispute resolution is designed to be fast, so as not to hinder the election process (Author's interviews, 2017).

Quoted from Past, Liisa "All Elections are Hackable: Scalable Lessons from Secure I-Voting and Global Election Hacks" from the European Cybersecurity Journal (2017, vol. 3) can be downloaded from https://www.ria.ee/public/RIA/ECJ_Volume3.Issue3_Extract_PAST.PDF.

Crisis and incident management relies heavily on procedures, routines, tasking and capability mapping that has been pre-determined and agreed upon:

- **The regular working and information exchange formats in conjunction** with their mandate, resources needed and role descriptions should include all management levels from operational to decision-makers. It is often easiest if the election technology organisational structure follows the structure and cooperation mechanisms of the election management body. Therefore, in addition to different management levels from operators to decision-makers, it might make sense to include thematic streams such as legal, communication, and so on.
- **A clear procedure or policy for incident management** should aim at ensuring information flows and adapted responses in the event of detection of a security incident, specifying:
    - the measures to be taken upon the detection or notification of an incident;
    - a sustainable and reliable organisation for the recording of security incidents and notifying/reporting to relevant stakeholders;
    - risk identification and management;
    - decision-making and crisis management organisation;
    - a communication plan: communication should be part of the crisis management plan as it is essential to maintain the level of trust necessary to the election process;
    - coordination with external stakeholders, regulatory bodies, and other agencies as appropriate.

Case Study: The Value of Cyber Threat Intelligence for Election Security

Operators of systems relying on digital technologies must ensure that they have a good understanding of common attack vectors to be able to defend these systems and the networks that connect them. In this role, structured cyber threat intelligence (CTI) can greatly enhance security controls by providing the real-time deployment of appropriate test mechanisms ranging from indicators and tools as well as techniques and protocols (TTPs) to network defences. This requires an understanding of the threat actor and their motivations as well as their TTPs and associated indicators to detect them. That level of detailed logic is only achievable through a structured CTI approach where operational observations can be linked to a potentially motivated threat actor.

The volume and breadth of data surrounding modern electoral processes cannot be overestimated. Recent cyber-attacks on elections have included information operations seeking to influence the results. To handle the sheer volumes of activity in the information operations arena requires a holistic understanding of the threat landscape. Similarly to electoral systems targeting, these TTPs are not necessarily new but the strategic timing of these can be a force multiplier.

Therefore, in addition to the election technology itself, cyber security incidents that could affect public opinion should also be taken into account. Traditional cyber security incident response procedures, supported by structured CTI, provide governments and political parties a chance to keep pace. This not only requires digital footprint, dark web and social media monitoring for high confidence early warning, but also the means with which to quickly identify incidents with an associated prioritisation (e.g. noted high-confidence motivations of high-threat Intrusion Sets) and the associated courses of action, whether they be technical or political.

Contributed by EclecticIQ Cyber Threat Intelligence

5.3.3 Election Security Task Force

A security or election technology taskforce is useful in both the run-up to an election (as a method for stakeholders to cooperate and coordinate) and during an election as a 24/7 support, coordination and event handling resource. Typically this would include the election management body and the organisation responsible for the information security of the elections, as well as the appropriate governmental and/or national CSIRT teams.

Depending on the election administration and specifics of the government structure, the appropriate law enforcement agencies, representatives of relevant government ministries, intelligence services, and respective other relevant institutions could be invited to be part of the election security task force. It is not uncommon to include the vendors or developers of the technology that elections rely on. Whether part of the task force or simply linked closely, the task force should work in close cooperation with the public communication team and top management / decision-makers.

It is essential that the election organisers and those responsible for the cyber security of elections have a strong link with the organisation responsible for incident handling across the government domain, often CSIRT. These links should be strong and include a 24/7 communication channel and, as back-up, the mobile phone numbers of individuals concerned, including the first responders.

According to each country's specific requirements, the organisation responsible for vote tallying may even create their own CSIRT or a Security Operations Centre.[13]

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

- a single point of contact;
- a ladder of crisis escalation detailing the types and levels of criticality;
- a clear division of roles and responsibilities;
- the means of communication;
- comprehensive documentation;
- flexible resource allocation;
- an adequate training plan.

Case Study: Spanish Incident Response Team

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.

Case Study: Estonian I-voting Task Force

"Functioning of elections cannot be up to only the elections organizers tasked with the technical execution. A multi-stakeholder approach, where all those involved in the electoral process have to be on board, means coordination and integrated (communication) management. In Estonia, for example, I-voting is managed by a task force that brings together the election organizer, the Information System Authority, the service providers I-voting relies on, and the software developer (Estonian National Electoral Committee, 2017). Communication is managed by a team comprising of representatives of the election organizer, the government office and, in the case of I-voting, the Information System Authority."

Quoted from Past, Liisa "All Elections are Hackable: Scalable Lessons from Secure I-Voting and Global Election Hacks" from the European Cybersecurity Journal (2017, vol. 3) can be can be downloaded from https://www.ria.ee/public/RIA/ECJ_Volume3.Issue3_Extract_PAST.PDF.

[13] (2018) Sans.org. Retrieved 14 March 2018, from https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907

5.4 Testing and Auditing

Testing and auditing are the cornerstones of network and information system security, as they are the only methods of gaining a practical assurance of functionality and security. Therefore, testing and auditing need to take a comprehensive and multifaceted approach. The connections, cooperation and overall organisation of elections need to be addressed in addition to individual network and information system elements. It is often advised that the critical systems should be tested by at least two independent (unrelated to each other or the developer/vendor) teams.

This also means that a generic test and audit plan is not sufficient; the specifics of the election process need to be taken into account. The section below lists some of the types of tests and audits to consider.

5.4.1 Testing and Auditing Systems and Software

Systems and software should be audited and tested in many different ways, including security and functionality tests.

5.4.1.1 Functional Tests

The continuous automated testing 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.

Ex-post code review allows other teams within the organisation responsible for development to offer important feedback through internal audit and code review.

Continuous external code quality checks using external testers is good practice, often supported by automated tools.

Functionality testing can take a number of forms and happens at many stages, including unit tests that function on a granular level. 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.

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.

5.4.1.2 Security Tests

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

Case Study: French Organisational and Technical Recommendations Post-Audit

A major contribution from ANSSI to the cyber security of elections was delivered through a critical systems audit, hardening, and additional *ad-hoc* measures meant to improve protection from incidents. In the course of February 2017 at the request of the Ministry of the Interior, a security audit and a hunting campaign on the nation-wide counting information system led ANSSI to recommend a set of organisational and technical measures, including:

- helping to secure the integrity of results through organisational measures (mostly staff assignment) ensuring proper separation between physical ballot counting and the nationwide counting information system;
- performing, in cooperation with the Ministry of the Interior, an *ad-hoc* supervision of the nationwide counting information system.

Additionally, a range of less critical systems were also addressed due to their connection with the elections process. ANSSI specifically recommended 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 journalising (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.

5.4.2 Testing and Auditing of Individuals and Organisational setup

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.

5.4.3 Approaches to Security Testing

Security tests should be tailored to specific cases and are most beneficial if they take a comprehensive overview that tests the entirety of the set-up and routines. Once a system, or part of a system has been earmarked for replacement or updating (of the system, not the product, generally to to a higher standard that was recently made available on the market), it should first be evaluated by qualified security professionals or trusted third parties in the field.

Case Study: Risk Assessment and Penetration Testing in the Czech Republic

In 2017, long before the – arguably most important – elections to the Chamber of Deputies, the Czech National Cyber and Information Security Agency (NCISA) as a central state body responsible for cyber security approached the Czech Statistical Office (CSO) and, together, they began to map the possible risks in the electronic part of the vote tallying process. It took about 3 months to comprehensively understand the CSO work procedures, their ICT infrastructure, and methods of safeguarding the digitalized results.

Based on the thorough analysis, the NCISA decided to perform penetration testing on the two main components of the vote tallying system:

The CSO-owned notebooks used in 500 "hand-over centres", where election results from roughly 14 500 electoral commissions are gathered, processed and then sent via internal network to central CSO database:

- The penetration test of the notebook focused on firewall settings, hard-drive encryption, secure-boot settings, antivirus solution quality, HIPS solution quality, PowerShell settings, examining the system logs that the notebooks gather, (in)existence of bloatware in the notebooks, and much more.
- The penetration testing also focused on the notebook's pre-installed program that is used by CSO employees to enter, verify and send results to the central database. The program was pen-tested for its overall integrity, encryption methods, and examined how users are authenticated, whether they are properly blocked after multiple failed login attempts, etc.
- The final penetration testing report contained over 25 specific recommendations.

The CSO-run website www.volby.cz (in English: www.elections.cz):

- Learning from foreign examples of attacks on election processes, the NCISA focused on the website's ability to withstand a DDoS attack, and explored various paths leading to defacement of the website, etc.
- The CSO also decided to strengthen the anti-DDoS defences and bought a dedicated solution from their ISP. However, when a DDoS attack later really occurred, due to technical shortcomings, the anti-DDoS mechanisms did not work well and the attackers managed to bring the website down for a couple of hours.
- The penetration testing report contained specific recommendations.

The penetration testing was done in parallel with a private company contracted by the CSO. The NCISA pen-test team was aware that there is a parallel effort by a private company, but had no contact with them. Only after the final penetration testing was complete and reports handed over to CSO, were the NCISA team familiarised with other pen-testing team's report and allowed to identify possible weak spots in their own work where applicable, i.e. where reports overlapped. This is a highly recommended procedure, although it is heavily resource-intensive and, in real life, can only be applied to high-profile cases and systems.

Although evaluation methods at this stage are limited to the technical specifications supplied by the manufacturer, the responsible government agency may ask for an onsite demonstration of the product where experts can be given access for penetration and conformity testing, upon prior agreement by all parties.

If the product fulfils expectations and is purchased, the tests have to be rerun once more before its implementation in a live environment. The live environment is where manufacturer guarantees are also conditioned, such as the original manufacturer factory line packaging seals, and code and firmware hashes. To ensure transparency and fair trade conditions, this procedure can be inserted as part of the tender's conformity prerequisite assessments for a winning bid.

5.4.3.1 Penetration Testing

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: Response to Testing 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 each electoral committee counts the votes by hand and determines the votes that have been cast for each list and for each candidate. Voters may attend the manual counting of the votes. Each electoral committee records its result on an official paper report (called *proces-verbaal*). The election committees take the official report to the municipalities.

After receiving the official reports, municipal civil servants add up the results. They can use software named *Ondersteunende Software Verkiezingen* (OSV) of the Electoral Council to add up the votes. The purpose of this work is to determine the result of the vote for the municipality.

The result of this calculation is recorded on a (paper) form that will be taken to the principal electoral committees in person, together with the official reports of the electoral committees of the polling stations. Copies of this form and the official reports of the polling stations are available for inspection at the town hall.

The principal electoral committees of all districts determine the total number of votes cast, the number of votes cast per list, and per candidate. The principal electoral committees announce the total number of votes cast in the electoral district in a public session and will draw up an official report thereof on paper. The principal electoral committees take the official report of their session to the central electoral committee (the Electoral Council) in person. The official reports of the principal electoral committees are published on the internet.

The Electoral Council calculates the seat allocation at party level manually, based on the official reports (paper report of the results) of the principal electoral committees. In addition, the results are worked out at candidate level by means of a calculation tool (Supporting Software for Elections). 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.

In the run-up to the 2017 elections, the Electoral Council of the Netherlands asked Fox-IT to perform a penetration test to examine the security of the (use of) OSV. As a result, a number of vulnerabilities were detected. To mitigate the potential effect of these vulnerabilities, the Minister of the Interior and Kingdom Relations decided to introduce additional measures. First of all the Minister banned the storage of the results on data carriers. At each step (municipality, principal electoral committee and Electoral Council) the data entry in OSV is done manually. Furthermore, additional manual checks were introduced to make sure the results aggregated by the OSV were correct.

More can be read (in Dutch) at https://www.rijksoverheid.nl/ministeries/ministerie-vanbinnenlandse-zaken-en koninkrijksrelaties/documenten/kamerstukken/2017/03/03/kamerbriefover-gebruik-rekenhulpmiddel-voor-berekenen-van-de-uitslag-van-de-komendeverkiezing?_sp=eb51edc9-82fb-45da-b8d5-7c93abb16be6.1529567952525.

5.4.3.2 Public Testing: Security Research, Hackathons and Bug Bounties

Inviting a wide group of experts or the public to examine technology can take many different forms. A **hackathon**, for example, takes place in a relatively controlled setting, in which a select group of people receive a limited amount of time to hack a specific dedicated system. At the other end of the spectrum, a number of organisations invite security researchers to attempt to find problems with the systems that are running and in production. Such invitations are usually open-ended and tied to bug bounty programs where rewards are offered to incentivise disclosure.

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 is able to 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.

More information on a number of transparency measures is also available in a section later in this chapter.

5.4.3.3 Application Code Audit

When multiple vendors are involved, the communication (for example on how various types of data will be exchanged and how data should be verified) between them tends to be a weak point. Thus, effective collaboration amongst vendors needs to be enforced by election organisers.

The “shelf life” of election applications needs to be proportional to the relevant threat landscape; thus, thorough threat modelling should be required at the beginning of every election cycle. With specific attack trees, all scenarios, and risks thoroughly detailed. Again, a federal CSIRT or national Cyber Security Centre can support the continuous improvement of the security of election software is achieved.

Auditing the audit(s) can also sometimes reveal risks that were not correctly assessed at the beginning of the initial audit.

Additionally, open source solutions are not necessarily more secure. Only once the source code is actually reviewed by subject matter experts and revised where needed, can it result in a more secure solution.

5.5 Exercises

While a **fully integrated technical and decision-making exercise** would best allow for the practicing of contingency planning, risk management and incident handling under pressure, such exercises can be prohibitively resource-intensive.

Functionally-focused command post exercise (CPX) can increase proficiency at a lower cost. Alternatively, a **non-technical table-top exercise would allow the testing of routines, procedures and communications** as long as the relevant players participate.

Exercises can have multiple objectives, such as:

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

5.6 Trust and Transparency

Trust in the election process is fundamental in the legitimacy of the outcomes. When dealing with election technology it is crucial, beyond simply doing the right thing, to also be seen doing it through the following measures:

- public oversight of election technology;
  - election observation, including training observers on election technology;
  - publishing documentation and allowing access to technology;
  - visualising and publishing steps in elections in a manner accessible and comprehensible to the public;
  - open risk communication before and during the elections.
- voter education and public trust building;
  - engagement of key opinion leaders;
  - media relations and educating journalists.
- building trust among the expert community to promote discussion, raise awareness, scout for talent and, engage experts in testing.

Case Study: Estonia and Aggressive Openness

Transparency measures have "had a noteworthy impact on building confidence and trust in the I-voting system" (Nurse, et al., 2016, p. 3). This "aggressive openness" (Author's interviews, 2017) means that Estonia:

- Publishes most of the I-voting documentation on the elections website (with the main exception being materials that expose vulnerabilities).
- Publishes the source code of the I-voting software on the open-source coding platform GitHub as of 2013 (I-voting on GitHub) (Internet Voting in Estonia). As a security precaution, the uploaded repository is not used for further development but is the "up-to-date code used in elections" (I-voting on GitHub). The 2017 code is to be published after testing.
- Invites feedback from the technology community and Estonia's volunteer Cyber Defence League (see http://www.kaitseliit.ee/en/cyber-unit) in addition to formalised testing.
- Makes election procedures public and observable and parts of the system audited, all meeting standards similar to voting procedures at a polling station (Author's interviews, 2017).

Quoted from Past, Liisa "All Elections are Hackable: Scalable Lessons from Secure I-Voting and Global Election Hacks" from the European Cybersecurity Journal (2017, vol. 3) can be downloaded from https://www.ria.ee/public/RIA/ECJ_Volume3.Issue3_Extract_PAST.PDF,

6. Specific Technical Measures to Protect Elections

As the electoral systems across states vary greatly in tools, procedures and technologies used, the technical measures follow a "pick and mix" approach and should be deployed as is appropriate to circumstances and needs. However, regardless of the approach, sufficient security controls must be in place to ensure the integrity of the devices used (sourcing, updated firmware), change management of the configuration (traceability), and adequate monitoring of the network traffic. For custom developments, full security tests are recommended.

6.1 Anti-DDoS Protection

Denial-of-service attacks constitute an important segment of all attacks against election technology. With that in mind, several EU Member States have seen successes with anti-DDoS measures in protecting the platforms used to gather election information or publish results.

Different network interfaces for voters, system administrators, and data administrators (the administrator interfaces using VPN, with a filtering of the IP addresses if needed) ensure that operators can access systems even if a DDoS attack is ongoing against the public-facing interface. While there are a number of effective DDoS protection solutions available commercially, monitoring and cooperation with the ISP is essential in the successful mitigation of such attacks.

It should also be noted that while having different network interfaces helps, in many cases the victim system is not responding due to overload of the internal systems. Therefore the system design needs to have measures in place to manage accordingly.

6.2 Access Control

The strong identification of users who have data entry access or change privileges is essential to election security. It is also the basis for tracking questionable actions to their source, if needed, provided that proper logging procedures are in place. Strong authentication uses several of the following: something the user knows (passwords), something the user has (tokens, mobile apps, smart cards) or something the user is (biometrics).

Authentication of the core team of election officials (those who use the systems regularly and for several election cycles) can be easily handled using good, general IT practices. Scalable, cost-effective, easy-to-use but secure authentication methods are required for temporary election workers. Whether they are data entry and verification specialists, polling station officials, or other temporary staff.

In addition to authentication, authorisation is important, and has a number of election-specific details. Access should be granted based on election duties, on the principle of least privilege and while also taking into account the areas that access is required. Time-based access restrictions are also important where there is access to data that is not yet public, especially in the results of the election.

6.3 Data Integrity and Secure Transport

Organisations that are tasked with any part of election technology are also responsible for protecting the data in transit. All data transfers are potential points of compromise. For example, if voter data come from a central registry with transfer to an election system, the data transfer needs to be addressed regardless of the technology used. Even if the voter rolls are printed, transfer from servers to printers needs to be addressed.

As a starting point, checksums and digital signatures are useful tools to ensure data integrity. Many data transfer protocols and storage technologies include checksums, but the use of these need to be verified as appropriate to election technology. If the whole path for data is not trusted, digital signatures should be used in addition to checksums.

Dual-control and independent verification (using separate channels and procedures) for important steps of the election process offers increased security. Where humans are involved, duplicating data entry (by two different people) helps to pinpoint possible errors.

6.4 Network Flow Analysis and Monitoring

In order to provide a real-time analysis of security alerts generated by applications and network hardware, the organisation tasked with the cyber security of election technology can implement a comprehensive security information and event management (SIEM) solution to look for malicious activity using:

- logs from endpoint stations – operating system logs, logs from antivirus instances, web filters, and firewalls;
- logs from infrastructure – routers, switches, firewalls, application servers, and others;
- network data flows – looking for anomalies using network behavioural analysis (NBA);
- external data sources (IP blacklists, reputational databases, and others).

Implementing a SIEM solution requires accounting for the environment necessary for it to function. In particular, the first item to consider before implementing such a solution is to determine the proper log policy on the system. A SIEM without a proper log policy would give a false sense of security as it would not possess the elements required to raise alarms for the operators.

A matured SIEM operator working on a strategic network related to elections might be a member of a 24/7 taskforce, such as one described earlier in the compendium, so that the information route from technician to strategic-level decision-maker is as short as possible. Where applicable, an internal employee should be preferred to an outsourced contractor.

6.5 Network Segmentation

Processes that are not required to be accessible to the public (in particular, the vote gathering and the vote counting) can take place in an isolated environment. System isolation can be achieved through either logical separation (VLAN) or physical separation (air gap). When opting for physical separation, the data carrier (often an encrypted USB device) and the workstation used to record data to the data carrier should be considered inside the security perimeter.

6.6 Back-ups and Recovery Procedures[14]

Sufficient back-up arrangements – in more than two copies and in real time for critical functions – should be in place and permanently available to ensure that elections proceed smoothly. Any back-up system should conform to the same standards and requirements as the original system and secure communication channels should also be duplicated.

During an election or referendum period, a disaster recovery plan should be in place. Central systems should be installed in secure, controlled locations and physical access should be controlled and restricted. An alternative location should be available to enable reacting after a physical

[14] Based on "Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, VIII., 40., i" Last accessed 5 June 2018 on https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726c0b

disaster, with the appropriate equipment pre-reserved. The electoral authorities must define a specific service level before running the system. Risk analysis and scenarios should be based on the desired service level, implying procedures, back-up arrangements, resource reservation, and so on.

7. Security Measures Specific to Stages in Election Life Cycle

The following considerations are related to specific election stages and are considered particularly relevant to the topic. However, the more general best practices and recommendations, as outlined in the previous chapters, have to be taken into consideration and applied universally across the stages of an election life cycle.

7.1 Voter and Candidate Registration and Databases

The process begins with eligibility checks and the identification of individuals participating in the election process (both candidates and voters) relying on a database of those eligible to stand or vote in elections. Therefore, it has to be recognised that the quality of voter rolls and candidate databases as well as the resulting eligibility checks can never be higher than the original database. Whether it takes the form of a central population registry, local property and tenancy records or a solution to which voters register directly.

The importance of voter identification varies through political and electoral systems. The identification becomes especially important as only a small number of illegitimate votes may change the outcome of the elections dramatically depending on the specific voting and counting systems. In decentralised systems, extra emphasis is put on a good security practice being employed at the local level, something that is often difficult due to funding and staff shortages.

Case Study: Electoral Rolls in Germany

In Germany, the electoral rolls are managed by the municipal authorities on the basis of the local civil registers (databases). Polling cards are sent automatically by the respective municipal authority to all citizens entitled to vote. Therefore, there is no central registration process for voters in Germany.

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: Registering to Vote in the UK

In the UK, registering to vote is a physical activity and not an automatic right. Households are required to register any eligible voter resident annually, or at any other time, using an online system called "Register to Vote". During the UK's 2016 EU Referendum, following a TV debate encouraging people to register before the 12 midnight deadline, an unprecedented surge in internet traffic towards "Register to Vote" knocked the site offline and led to some voters being unable to register. As this was a referendum, the sitting Parliament was able to extend the deadline for registration. However, had this happened again in the 2017 General Election – as Parliament would have dissolved – there would have been no scope to do the same. As a result, DDoS protection around "Register to Vote" became a priority piece of work.

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.

Technology has to be deployed with the view that voter identification and reliability of voter rolls must meet similar legal standards, whether electronic or analogue. At this stage, it is of the utmost importance to prove the identity of voters and check their eligibility. If the electoral commission uses computers for this task, security is best provided by centrally distributed and administered workstations that have a high level of security. Fundamentally, all voter and candidate databases are to be safeguarded as any other sensitive database. This approach also highlights the importance of the secure transfer of these databases, regardless of their format.

It should be noted, that even where the electoral commissions do not use computers for identifying voters on Election Day, paper-based systems also – at some point in the process – rely on lists generated on computers. The respective systems are hence also vulnerable to interference and should be considered in the context of cyber security of election technology.

7.2 Digital Tools to Collect and Process Votes

There are a number of approaches to election technology at this stage of elections across the EU. Whatever the model, the entities processing and counting the votes tend to – at least to a degree – rely on ICT systems and, therefore, have to consider cyber security.

If vote counting is centralised and completed electronically, performing the count on a strictly isolated computer network with data access that is strictly limited and under heavily surveillance, both in and out, should be considered.

Vote counting and processing varies greatly across Member States. For example, in Great Britain the votes are counted by public officials on the constituency level, where the local MP is then

proclaimed. The final country-wide election results, however, are communicated not by a government entity, but by independent media, NGOs, and other stakeholders. Therefore, counting of the votes from various constituencies is done in parallel by more entities and does not represent a single point of failure. This is a useful model in a winner-takes-all election system where constituencies have no effect on each other and cannot be replicated in a highly proportionate election system where compensation mandates or vote spill-over is used.

However, in the majority of the Member States the final vote count is centralised and therefore crucial for the final election outcome. The administrators of the involved networks should apply, in full, the cyber security best practice, summed up in various best practice lists. One of the most elaborate and holistic being the German Federal Office for Information Security (BSI) information security standards (IT-Grundschutz),[15] others include a number of EU Member States' recommendations written in their national languages,[16] or outside the EU the Australian Signals Directorate's Strategies to Mitigate Cyber Security Incidents.[17]

One essential recommendation to be singled out in respect to protecting against cyber-attacks or technology failures that could undermine the integrity of an election, would be to ensure the proper separation between physical ballots counting and the nationwide counting information system.

7.3 Systems to Publish or Communicate Election Results

The publication and broadcasting of election result is again greatly varied across states. While some EU Member States rely on a central election information system with a web interface, others depend heavily on mass media. The guidelines will need to be designed to best benefit the election organisers regardless of their particular systems.

Case Study: Sustained DDoS During Czech Elections

In September 2017, the Czech Republic held elections to the Chamber of Deputies. The two websites presenting the results suffered DDoS attacks and were brought down for about two hours. However, because the Czech Statistical Office established a secure parallel data exchange with major media outlets and websites, the results were available elsewhere and the entire incident did not produce any major effects on society and the perception of elections.

[15] *BSI - IT-Grundschutz-Standards*. (2018). *Bsi.bund.de*. Retrieved 4 June 2018, from https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

[16] Radek, H. (2018). *Bezpečnostní doporučení NCKB pro síťové správce, verze 2.0*. *Govcert.cz*. Retrieved 4 June 2018, from https://www.govcert.cz/cs/informacni-servis/doporuceni/2607-bezpecnostni-doporuceni-nckb-pro-sitove-spravce-nova-verze-2-0/

[17] *Strategies to Mitigate Cyber Security Incidents: ASD Australian Signals Directorate. (2018). Asd.gov.au. Retrieved 14 March 2018, from https://www.asd.gov.au/infosec/mitigationstrategies.htm*

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.

Regardless of the specific arrangement, the presentation layer is as important as the correct vote count, and the interface where the citizens and the media learn of the election results (including websites and automated data sharing) should be protected. In Member States with a centralised election process, the organisation tasked with the final counting of the results also presents the results to the wider public.

Consider some of the following measures to protect such interfaces:

- separate the interfaces for media/citizen consultation, data administrator feeding the system, and system administrator;
- regarding the rights of system/application administrators on the system, their access to the system during the election has to be closely monitored and limited to cases where no other option exists;
- the separation between security administrators (ensuring log management, without any right to modify the system) and system/application administrators (in charge of the maintenance but without rights to delete or modify logs) has to be enforced;

- as far as possible system/application administrators should have no access during the election process.

Case Study: Attacks Against the Slovak Local Elections (2014)

On November 2014, Slovakia arranged the processing of the results of Elections to the bodies of communal self-government. The interim results were presented on the website of the Statistical Office, as well as on a parallel contracted secured website.

At the time of processing the election results, Slovakia recorded three waves of hacker DDoS attacks on the presentation of the interim results, which was reflected in the slowing of the page and a long reading of the results. The processing of results had not even been endangered by these attacks.

The slowing of the page and the long reading of the results measured by the monitoring was at a maximum of 12 minutes during the first wave of attacks. The second and third wave of attacks proceeded almost simultaneously and held at 37 minutes. The failures were eliminated in a short time (up to 35 minutes).

However, because a secure parallel data exchange had been established, the interim results were available elsewhere and the entire incident did not produce major effects.

When results are published, users should be able to verify that they are the real results. If the results are published on an official website, HTTPS should be used to protect the integrity of data. Additionally, digital signatures can be included for the results files and keys used to sign these published using other media. This is useful for both websites and delivery of the files for media and other interest groups.

Avoid a single-point-of-failure and create parallel communication channels to the public. For example, when a central electoral body website that presents the election results is down due to a DDoS attack, having direct communication links to various online media continuing to present the underlying data, shall be appreciated. The biggest online media portals could even have an exclusive communication flow using an IP-whitelist and dedicated VPN.

For others, the electoral management body might set up a repository where they can obtain the results (i.e. a pull model instead of a push model) with only a little effort. Diversity in communication models brings resilience and weakens single-point-of-failure risks.

8. Protecting Auxiliary Systems to Mitigate Stakeholder Risks

Recent attacks against elections systems have, more often than not, targeted the connected or auxiliary systems rather than the central functioning of elections. Several Member States have succeeded in working with the owners of these systems, whether they are political parties or government agencies. While not in any way under government control, the national cyber defenders can educate and train the owners of party and candidate IT; as a compromise of these systems could cast a shadow on the legitimacy of the whole election process.

This avenue for attack is something that has been used on a number of occasions in the recent past. With some notable "hack and leak" operations carried out with the intention of undermining confidence in the election process. Taking advantage of poor cyber security, or lapses in secure behaviour by individuals, can lead to hostile actors taking possession of information, which when leaked can influence political opinion and thus the political process. Ensuring this does not happen should be viewed by cyber security agencies in a similar way as they view the protection of government networks and systems.

However, in most nations, political parties fall outside any definition of critical national infrastructure, and if focusing on the networks and systems of central government is something cyber security agencies are comfortable with, engaging with politicians on their own security is traditionally not.

Case Study: UK Changing Mindset

The United Kingdom's "Wilson Doctrine" is a convention that elected politicians' communications should not be intercepted by the police or security services. It is named after former Prime Minister Harold Wilson who announced the policy in 1966, at a time when some members of Parliament were concerned that the security services were tapping their telephones. In practice, the implementation of this Doctrine had led to little to no interaction of any sort between the UK security services (including those charged with information security) and politicians outside of the current government. However, this changed with the opening of the UK's National Cyber Security Centre which was given a remit to engage more broadly with UK society and was turned into action during planning for the 2017 General Election, when political parties were given specific advice on dealing with cyber threats.

8.1 Training and Supporting Parties and Candidates

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, the attacks on parties and candidates have repeatedly demonstrated that their ability to engage in meaningful political discussion can be impacted by cyber-enabled campaigns against them, which, in turn can delegitimise the entire democratic process. Parties and candidates might not directly approach the government for advice on maintaining their cyber security. Therefore, a programme of outreach and direct engagement could be the most effective.

Case Study: UK Prioritising High-Impact Assets

Maintaining political impartiality will be essential, providing an equal amount of support to all parties and not favouring one party over another will also likely be a consideration. However, doing all of this may not always be practical. In some countries, registering a political party is a relatively straightforward process, leading to a vast number of registered parties (in the UK this number is 492).

Additionally, affiliation with an existing registered party is not necessary if you want to stand for election. Any individual who pays the required deposit can stand as an independent candidate. So, in theory, this means that to provide the same amount of support to every candidate taking part in an election, you would have to address a large number of candidates. In the UK's 2017 General Election, the 3 304 candidates who stood for election represented 67 parties, with 183 standing as independent candidates. Engaging with each of these was not deemed possible, or appropriate.

The approach taken by the UK's National Cyber Security Centre was to engage with an entity known as the Parliamentary Parties Panel (PPP), a representative body of all parties who have at least two sitting members of parliament. In 2017, the PPP was made up of 8 parties, ranging from the governing Conservative party with 330 seats, to the Ulster Unionist party with 2 seats.". This provided a manageable number of parties with which to engage and was deemed by the Electoral Commission to be a reasonable way of creating a standard. However, to demonstrate flexibility, one party who traditionally receive a large number of votes but did not have two sitting MPs, were also added to the list of parties with whom they engaged. Additionally, any political party could still reach out to the UK's NCSC for support at their own request.

Given history, any conversation with a political party about its IT security is likely to be the first time they have directly interacted with a government security agency. The resulting exchanges are unlikely to feel like those had with mature partners and there is likely to be a degree of nervousness and reluctance to engage. This makes identifying which part of the party you need to speak to vitally important.

The impact identification process in the UK was thus the following:

1. **Choose WHICH parties/candidates you are going to engage with, and identify a reasonable justification for where you set the bar.**
2. **Identify WHO within those parties to speak to, and HOW to approach them.**
3. **Establish WHAT the parties are likely to need from you, and how much TIME they have to implement it.**

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.

8.1.1 Finding a 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 a number of 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.

Case Study: Reaching Out to Political Parties in the UK

The UK's National Cyber Security Centre held a seminar for the main political parties, as explained above, and invited both IT and party officials. Contributions from the floor during the seminar were limited, but all parties were willing to speak to the NCSC afterwards. The agenda covered an explanation of the scale of cyber threat, likely methods of attack with a focus on phishing, and basic advice on IT security, both for network administrators and end users.

8.1.2 Type of Advice Needed

When party engagement starts, it is likely that each party involved will be on a spectrum of **maturity and experience**. This is likely based on the size of the party, their available resources, understanding of threat (probably linked to whether they have recently been in government), and political outlook. As a result, advice will need to be tailored, and fit the individual or collective requirements of the respective parties.

The amount of time between engagement and election will also affect the depth of advice and guidance the parties are able to digest. If weeks are available, then it is unlikely to go much beyond the absolute basics. If months or even years are available, it is possible – depending on the overall maturity of the parties being spoken to – to go to a much deeper level and treat the parties in a similar manner to providers of critical infrastructure.

Based on the experiences of Member States, the need to reach out is clear, particularly in terms o**f strong technical network security measures and user behaviour.** The cyber security best practices are readily available; however, political parties often lack IT staff and financial resources to maintain a good level of network security. Additionally, as users, their members and candidates often do not have the necessary awareness and do not follow the necessary precautions. In smaller Member States, tailoring the recommendations might be viable, with smaller political parties that have no specialised IT security staff often needing open-source and free-to-use solutions. The most impactful areas of advice, based on experiences of Member States are:

Access control:

- How can the unauthorised access to a candidate's social media accounts, resulting in leaks of private sensitive data (conversations, pictures) or fake announcements resulting in reputational damage be avoided?
    - These can be countered using stronger passwords, two-factor authentication and other tools.
- How can the unauthorised access to a party's website or social media accounts, resulting in defacements and reputational damage be avoided?
    - These, again, can be countered using above mentioned means and penetration testing of the website

DDoS protection:

- Attacks on a party website are not unlikely based on past experiences; they can be mitigated by specialised anti-DDoS services by the party's ISP or a specialised company. For big parties

with big IT departments, a proprietary anti-DDoS solution is feasible. On the other hand, small parties with limited resources may use free but robust cloud services.

Overcoming insider threat:

- Can occur in the form of a disgruntled party candidate or employee, who might leak sensitive party data and documents.
    - This can be countered on a technical level by strong user privilege segregation and network segmentation, and on organisational level.

However difficult that might be for political parties to implement, the first piece of advice is to use dedicated means for campaign communication (avoid personal phones and untrusted communication auxiliary system means like commercial mailboxes etc.). There should be a strict separation between personal usage and professional usage. Additional advice for a relatively inexperienced political party might include the basics of:

- ensure system administrators segregate online work;
- adhere to a good patching regime that works;
- remove anything operating an old operating system;
- regularly back-up any valuable data;
- adhere to a sensible password policy and use two-factor authentication;
- flag external emails as external;
- inspect and manage credentials;
- properly monitor any critical parts of networks;
- use a whitelist of executables;
- turn on encryption for data at rest, and enable firewalls, automatic updates, safe browsing, and ISP filtering;
- apply the same to mobile devices.

8.2 Other Entities Involved in Elections

The resilience of any central government networks that support elections, and the IT security of candidates and their associated parties are the central components of a strong electoral ecosystem. However, from nation to nation, other entities may be involved. These could include:

- other government electronic services that either create a dependency for the election process or may be a reputational risk if compromised during an election period;
- other private sector electronic services (such as online banking) that either create a dependency for the election process or may be a reputational risk if compromised during election period;
- the central electoral commission and their oversight of the overall election process;
- local authorities who may be organising individual elections at the local level, including voter registration, ballot paper dissemination, polling station management and vote counting;
- media that communicates the results.

For each of these, specific advice is needed.

8.3 Other Considerations

As the attacks against elections and campaigns take a comprehensive approach, those defending the election technology against cyber-attacks have to be aware of the wider picture and framework. It is fundamental for the safe adoption of voting technology that a legislative framework is created that

holds digital technologies to the same standards as paper-based elections. Thus, the political decision-makers and courts will need to test the constitutionality of election technology to prove that they meet the legal standards and requirements for free and fair elections.

Given the fundamentality of elections, national governments might wish to set legal and technical standards for election technology. One approach would be through strict compliance with baseline security standards (including appropriate reporting and auditing) or designating elections, voting, or services that elections rely upon and the connection between these elements as essential services. While a national decision, regardless of the approach, these measures are only effective if backed up with resources, including finance and labour.

Annex 1: Examples of Electoral Cyber Incidents

The following table contains examples of electoral cyber incidents and it is by no mean a comprehensive chronological list of electoral incidents. Looking at the examples of electoral cyber incidents worldwide, we can track a pattern of cost-performance rationale on the side of the attackers. The relatively simple DDoS and defacement attacks prevail, with advanced APT-style intrusions being a clear minority.

Country	Year	Method used	Target
Bulgaria	2015	DDoS	Central election commission, ministries
Montenegro	2016	DDoS	media, political parties, mobile network operator
Philippines	2016	defacement, data theft	election commission websites, voters database
France	2017	not published	Socialist party
		supposedly spear phishing	En Marche! Party
Ghana	2016	defacement	National election commission
South Korea	2011	DDoS	National election commission, opposition candidates
Malaysia	2013	DDoS	media and opposition candidates
Nigeria	2015	defacement	election commission
Russian Federation	2011	DDoS	independent media
	2012	DDoS	web cameras in polling station
Taipei	2015	spear phishing, backdoor	media and DPP members
Czech republic	2017	DDoS	Web presentation
Slovakia	2014, 2016	DDoS	web presentation
Tunisia	2014	not published	voters registration system
Ukraine	2014	DDoS	Ukraine election commission
	2014	defacement	Ukraine election commission
US	2015-2016	spear phishing, malware	Democratic party
	2016	spear phishing, malware	suppliers, clerk
	2016	unknown	database of election commission
	2008	unknown	Attempts on Obama, McCain networks
Venezuela	2017	insider	Vote counting

Annex 2: Security Requirements in a Call for Tender for the Creation, Hosting and Updating of a Website for the EP Election Results

The following information is an excerpt of the technical specifications of the Call for Tender published in 2018 for the collection of the 2019 European Elections national results, the consolidation of this data to define the composition of the European Parliament, and the publication of this data. [18]

The service providers are expected to implement a platform for the collection of national election results, consolidation with regards to the composition of the European Parliament and the publication of data ensuring:

- The reliability and resilience of the installations and services that are put in place, not only in terms of performance, failure-resistance, security and peak-load adaptability, but also in relation to the integrity and quality of the information published. Each element of the architecture must be redundant and, at any time, all or part of the system can be switched to the back-up devices.

- A secured communication channel to ensure the transfer of data between the platform for the collection and the consolidation of data and the platform for the publication of consolidated results.

- A back-office system highly secured, only accessible for registered users and using other guarantees in order to avoid the control from third parties (registered IP addresses sets, double identification by email and/or SMS, etc.) It must allow internal users from the European Parliament as well as the contractor´s own team, to do a series of operations (from verifying the data received to its publication on the Internet site, its associated elements and social media). Certain actions will be only run by the contractor´s own team, others will be also accessible for the Parliament´s staff responsible for supervising the dissemination of the election results.

The contractor or a direct subcontractor shall:

- provide hardware and software hosting for the following technical environments:

    - recovery system of data coming from the awarded contractor for the collection and the consolidation of data;
    - back-office infrastructure: accuracy verification of the data received, chain for editing web pages and generating the election results in various formats including for the Internet site;
    - “staging” infrastructure to ensure the publication, verification and then distribution of the results pages in web format;
    - these two production infrastructures cannot, under any circumstance, be hosted on cloud computing servers; they shall be hosted on servers controlled by the contractor or one of his direct subcontractors; the back-up infrastructure could eventually be hosted on a cloud computing server if they are hosted inside the European Union.

[18] Call for tender for the European Parliament elections 2019, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=3334, accessed on 18 June 2018

- use efficient broadband CDN dissemination infrastructure for internet dissemination of the results pages, which shall be capable of withstanding the significant load expected during the election night and the following days;

- ensure proper configuration of CDN proxies and caches so as to prevent obsolete pages from being viewed;

- ensure that the operational services are monitored in real time and that performance data for the entire site is recorded.

Security requirements:

The back-office and dissemination systems must offer a high level of security, based on advanced security architectures and methods, to pre-empt any external or internal attack or intrusion.

Tenderers should describe in detail the measures they shall undertake to ensure this high level of security.

The back-office system must guarantee the protection (with respect to viewing, modification or non-destruction) of confidential or sensitive system data (passwords, information awaiting publication, etc.), and its access must be highly secured.

The dissemination system must guarantee protection of the published data against any attempt to modify or destroy them.

The contractor must comply with the rules currently in force (laws on the protection of privacy and personal data, ISO 27002, etc.)

The installed systems must also have comprehensive anti-DoS (Denial of Service) and DDoS (Distributed Denial of Service) attack protection.

Security audits

During the implementation of the platforms for the collection, the consolidation and the publication of data different security audits will be simultaneously conducted by:

- the contractor providing the services for the collection, consolidation and publication of data;
- the ICT security services of the European Parliament;
- third-party IT security experts independent to the European Parliament and to the contractor providing the services.

The findings of the security audits would be taken into consideration before the rollout of the platforms for production operational management.