Handbook for the Observation of Information and Communication Technologies (ICT) in Elections

OSCE
ODIHR

Handbook for the Observation of Information and Communication Technologies (ICT) in Elections

Handbook for the Observation of Information and Communication Technologies (ICT) in Elections

Published by the OSCE Office for Democratic Institutions and Human Rights (ODIHR)

ul. Miodowa 10
00-251 Warsaw
Poland
www.osce.org/odihr

ISBN: 978-92-9271-152-8

Designed by Dejan Kuzmanovski

Foreword

All Organization for Security and Co-operation in Europe (OSCE) participating States have agreed to hold democratic elections in line with the commitments enshrined in the landmark 1990 Copenhagen Document and other relevant OSCE documents. These documents laid down key principles for holding genuinely democratic elections: universal, equal, fair, secret, free, transparent and accountable.

With technology entering every aspect of our lives, the use of Information and Communication Technologies (ICT) in elections has also increased considerably. Today, almost all OSCE participating States use some form of ICT in their electoral processes. These new technological developments inevitably bring certain benefits to states when organizing elections as well as to citizens when expressing their voting rights. Most often the benefits are linked to the greater accuracy or efficacy of some electoral processes, for example, in the counting or transmission of election results, or voter and candidate registration. However, these ICT advances bring new challenges that were not common for the traditional, paper-based electoral and voting processes. Some of these challenges relate to the very specific technical requirements that the ICT systems need to implement in order to respect the key principles for democratic elections. Others relate to concerns over cybersecurity threats, data protection and data privacy abuses. Given the increased potential for abuse or the lack of obvious and understandable transparency safeguards for all stakeholders, for elections that rely on ICT-based solutions further requirements, in addition to the key principles listed above, are needed to protect their integrity and strengthen public confidence.

The OSCE participating States have mandated the Office for Democratic Institutions and Human Rights (ODIHR) to assist them in implementing their human dimension commitments, including those related to elections. This new edition of the Handbook updates the ODIHR methodology for the observation and assessment of technology

used during voting and counting processes and includes new aspects for observation such as electronic registration, verification of voters and candidates, and cyber security issues. The Handbook is mainly for ODIHR and other election observers and international and citizen observers. We hope it will serve as useful guidance material for OSCE participating States in their efforts to introduce and use ICT appropriately during elections. The Handbook offers basic tools for observation and assessment of ICT as used in supporting different electoral processes and it should be read in conjunction with other ODIHR election-related publications, such as the handbooks on the *election administration*, *voter registration* or *campaign finance*.

I wish to thank all the experts and organizations who, through their work and valuable feedback, have helped us create this Handbook together.

Matteo Mecacci
ODIHR Director

List of acronyms

AI — Artificial Intelligence

APT — Advance Persistent Threats

BMD — Ballot Marking Devices

CIS — Commonwealth of Independent States

CISA — Cybersecurity and Infrastructure Security Agency

DDoS — Distributed Denial of Service

DRE — Direct Recording Electronic Voting Machines

E-Voting — Electronic Voting

ECHR — European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms)

EMBs — Election Management Bodies

EU — European Union

EDR — Election Dispute Resolution

EOM — Election Observation Mission

EVRVS — Electronic Voter Registration and Verification System

GDPR — General Data Protection Regulation

ICCPR — International Covenant on Civil and Political Rights

I-Voting — Internet Voting

ICT — Information and Communication Technologies

IFES — International Foundation for Electoral Systems

International IDEA — International Institute for Democracy and Electoral Assistance

IRP — Incident Response Plan

LTOs — Long-term Observers

NAM — Needs Assessment Mission

NFC Reader — Near-Field Communication Reader

NIS Group — Network and Information Systems Cooperation Group

NIST — National Institute of Standards and Technology

NVT — New Voting Technologies

ODIHR — Office for Democratic Institutions and Human Rights

OSCE — Organization for Security and Co-operation in Europe

RLA — Risk-Limiting Audits

RMS — Results Management System

STOs — Short-term Observers

UN — United Nations

USAID —United States Agency for International Development

VVPAT — Voter Verifiable Paper Audit Trail

Contents

Introduction

The use of technology in elections is now drawing strong public attention in most OSCE countries. There have been myriad discussions on the potential benefits as well as the risks of using what is commonly called 'Information and Communications Technologies' (ICT) and 'New Voting Technologies' (NVT).[1] Debate on the benefits has focused chiefly on the potential for greater inclusion of certain categories of voters, reducing human error, the increased speed and accuracy of some election processes, and the opportunities to lower election costs. At the same time, the use of ICT in elections has become a topic of concern, due to a lack of broad public consensus for its introduction or continued use, insufficient legal and procedural frameworks, numerous high-profile attacks on systems, equipment or software failures, and disinformation campaigns that have damaged public confidence. The use of ICT in election processes has therefore become an increasingly important and relevant point of interest for election observation missions (EOMs).[2]

In 2013, ODIHR published its ***Handbook for the Observation of New Voting Technologies,*** which sets out the key principles for assessment of the technology used during voting and counting. This Handbook builds on the methodology of the 2013 Handbook, updating it with the most recent standards in the ICT field and introducing two new aspects for observation and assessment: 1) the various ICT-based election systems and processes related to the registration or identification of voters and the management and publication of election results (so called 'ancillary' election systems and processes), and 2) cybersecurity issues during election periods. Therefore, this Handbook is effectively a new edition of the 2013 Handbook with a new title — *Handbook for the Observation of ICT in Elections*.[3]

1 Electronic or digital technologies for voting and counting in elections have been applied in several OSCE participating States already for a few decades and while there is an academic consensus that these technologies are not 'new' any longer, given their later emergence compared to the paper-based elections, this Handbook refers to them as 'new voting technologies'.

2 Throughout the text, unless otherwise noted, the term 'EOM' also encompasses all types of ODIHR election observation activity formats, including Limited Election Observation Missions, Election Assessment Missions and Election Expert Teams.

3 ODIHR is committed to regularly reviewing and refining its election observation methodology, in line with relevant tasking by the OSCE participating States (Ministerial Council Decision 19/06).

Due to the dynamic nature of ICT development, the complexity of the actors involved in election processes, and with the aim of providing the most up-to-date observation methodology, the Handbook references reports from numerous international organizations and institutions specialized in the fields of elections, ICT and cybersecurity. ODIHR recognizes that the reports and work of institutions referenced in the Handbook constitute only a fragment of the research on this topic and the Office remains open to including other relevant good practice sources and documents in its observation activities in the future. The guidance here is aimed mostly for ODIHR observers. It may also be useful for other international and citizen observers, as well as assisting OSCE participating States in their efforts to introduce or tackle ICT challenges appropriately during electoral processes.

How to use this Handbook

The Handbook deals with the broader application of ICT across different parts of the electoral process and with NVT as a specific aspect of election ICT applied to the casting and counting of votes. The Handbook has been designed as a practical tool for election observers.

- The opening chapter gives an overview of NVT and ICT-based election processes, as well as introducing the concept of cybersecurity and its relevance to election processes.
- Chapter Two outlines the specific OSCE election-related commitments and other international standards and principles relevant to ICT in election processes.
- Chapter Three discusses the roles of different types of OSCE election observation or assessment missions in assessing and observing NVT, ICT and cybersecurity and provides guidance for the ICT (and other) mission analysts on how to assess these topics.
- Chapter Four examines the context in which ICT and NVT are used and identifies issues that should be considered and analysed by EOMs.
- Chapter Five looks at the observation and assessment of NVT, including the role of the election administration and the actions required before voting starts, as well as during voting and counting.
- Chapter Six provides guidance for observation and assessment of 'ancillary' ICT election processes, with specific emphasis on technology used for voter registration and verification and other ICT-based platforms for managing different election processes.
- Chapter Seven discusses the role of the ICT Analyst in assessing the election-related cybersecurity.
- Chapters Eight and Nine identify the aspects of ICT, NVT and cybersecurity that Long-term Observers (LTOs) and Short-term Observers (STOs) should observe to provide the EOM with information on their implementation or impact at regional and local levels.
- The final chapter gives advice for the ICT Analyst during the reporting process and makes suggestions on how to draft practical and implementable recommendations.

Chapter 1

Background to observing NVT and ICT in elections

Technology has been used in elections for several decades already. Initially, the focus was mainly on ballot marking and/or casting votes and results tabulation. These early technological developments were purported to offer greater accessibility and faster processing of election data at lower cost, yet significant challenges emerged. Recently, there has been discussion about introducing Internet voting (i-voting), although very few OSCE countries have implemented such schemes; they come with significant risks associated mostly with concerns over the integrity and secrecy of the vote.

The application of technology in elections has also widened to so-called 'ancillary' systems — those not directly involved in vote casting, but which provide essential support to the process. These include, inter alia, voter registration (digital and/or biometric), web-based voter information services, automated results management systems (RMS), constituency boundary delimitation, candidate registration, political finance reporting and election dispute resolution (EDR). In particular, electronic voter registration and verification systems (EVRVS), sometimes including biometric features, are increasingly used by election management bodies (EMBs) across the OSCE region.[4] These systems bring benefits in terms of providing additional safeguards, but also contain risks in terms of disenfranchisement, secrecy and data privacy violations, and political pressure if data is misused.

Lastly, there is a growing focus on cybersecurity in elections. Elections held during the last decade in particular have highlighted the vulnerability of certain NVT and ICT systems to cyberattacks, be they foreign or domestic. The robustness, resilience and cybersecurity of ICT-based electoral processes and systems is an area for the close attention of election observers.

1.1 Overview of NVT

As noted, NVT refers to the use of ICT applied to the casting and counting of votes, including different types of electronic voting systems (e-voting and i-voting) and devices for casting and counting votes.[5] Different NVT systems and devices are used across the OSCE region and this chapter discusses the key challenges and advantages of their implementation.

1.1.1 Types of NVT

For voting processes, NVT systems are generally either ballot marking devices (BMDs) for electronic voting, or direct recording electronic voting machines (DREs) with or without a 'voter-verifiable paper audit trail' (VVPAT). A VVPAT provides evidence that can be verified by the voter and allows for a manual recount as well as different types of post-election audits (described later in the Handbook).

For counting processes, many OSCE countries use optical scanners and the hand-marked ballot paper is kept as the paper trail. This makes counting easier, while retaining the physical evidence in case of audits or legal challenges. Many countries also rely on an electronic RMS to facilitate the tabulation of results and recently this area has received increased attention over the potential risks and vulnerabilities.

4 Throughout the text, the term 'voter verification' is used interchangeably with the term 'voter identification'. Unless stated differently, these two terms should be understood as synonymous.

5 The term 'electronic voting' (or e-voting) unless otherwise noted, should be considered as synonymous with NVT.

The least used, but potentially most discussed type of NVT in recent years, is remote or Internet voting.[6] While only a few OSCE countries have piloted i-voting, and fewer still currently use it more widely, there are significant potential vulnerabilities along with increased risks of corruption and coercion in remote (non-controlled) voting environments. However, some procedure-based safeguards may alleviate certain risks related to the secrecy and overall integrity of the vote.

The following table gives an overview of the four main categories of NVT currently in use in the OSCE area.

Table 1. Forms of NVT in the OSCE area

Type of NVT	*Features*
Direct recording or ballot marking electronic voting systems	Records or marks a voter's choice in the polling station, usually through touchscreen or push-button devices. BMD and DRE systems are also usually used in controlled environments.
Ballot scanning technology	Uses a ballot paper that is either hand-marked by a voter or with the assistance of a BMD in a polling station. It is then inserted into a scanning device and counted electronically by reading the voter's mark on the ballot. These are usually used in controlled environments (polling stations or counting centres).[7]
I-voting	Allows voters to vote using the Internet from anywhere. Votes are stored and aggregated electronically in a centralized location. In addition to postal voting, the Internet is the voting channel most frequently used in uncontrolled environments.
Hybrid forms of NVT	A combination where the voting and counting processes take place in the controlled environment of the polling station using Internet voting. In such systems, voters must vote on a computer in a polling station and the votes are then transmitted electronically to a central server.

6 Remote voting usually takes place outside the confines of a controlled environment, like that of a polling station, which increases the risks of possible coercion and potential vote-buying.

7 In some instances, ballot scanning technology is also used to count postal ballots that were marked at home and mailed to the electoral authorities.

1.1.2 The principle of 'verifiability' in NVT

When introducing any type of NVT, an important consideration for OSCE participating States is the implementation of two fundamental principles which serve as safeguards for the secrecy of the voters' individual choices and preserve the overall integrity of the election results. These are the principles of ***individual*** and ***universal verifiability.*** The principle of ***individual verifiability*** requires that each voter can verify that their vote was 'cast as intended' and 'recorded as cast'. The corollary principle of ***universal verifiability*** requires that the NVT system can show to all voters that all votes have been 'counted as cast'.[8] There are different verification methods available when using NVT and they are described in the later chapters of the Handbook in the context of counting election results. In all cases, it is imperative that any verification method must adhere to electoral obligations, commitments and standards, and, most importantly in this context, uphold the principle of secrecy of the vote.

Table 2. Verifiability and different types of NVT

Type of NVT systems	*Verifiability*
DRE or BMD systems	DRE and BMD systems which include a VVPAT allow voters to verify the paper record before the vote is cast and allow for corrections if the printed ballot does not correspond to the voter's intention. They also offer the possibility of a manual recount of all votes. In general, these systems allow for individual and universal verification. DRE and BMD technologies that retain a paper record that is not verified by the voter may also allow for a manual recount, but this recount will only tally with what the system has recorded; this may not necessarily be the voters' intended choices. DRE devices that only record votes electronically do not allow for a manual recount. These systems store the record of electronic ballots cast on separate hardware and most keep a log of operations (an audit log). An expert is required to inspect this data and it might not be successful if there are hardware failures or data manipulation.

8 Systems with universal verifiability also allow an independent third party to establish whether the result of an election was reported honestly and without manipulation through either manual or mathematical checks.

Ballot scanning technology	Ballot scanning technology allows for a manual recount. The device's ability to scan the voter's choice depends upon the voter marking their ballot properly and is subject to the devices' margin of error and is reliant on a legal definition of a valid ballot.
I-voting	I-voting systems are usually paperless which does not allow for a manual recount of votes. Some i-voting systems attempt to allow individual voters to verify that their votes have been cast as intended and recorded as cast[9] and can give third parties the opportunity to check by using mathematical proofs that votes have been counted as stored on the server.[10] I-voting systems rely on computer security measures, certification and, ultimately, on a degree of trust in the system programmers and operators. Other systems that use cryptography are also being implemented with the aim of providing end-to-end verifiability.[11]
Hybrid forms of NVT	Some OSCE participating States have introduced electronic voting together with some form of paper trail and ballot scanners or i-voting. Hybrid systems can facilitate a manual recount facility if a VVPAT is included; otherwise, these systems rely on the same mechanisms as i-voting systems to ensure the integrity of the results.

1.1.3 Advantages and challenges of NVT

If universally accessible and implemented appropriately, NVT systems used for casting votes could have the benefit of enfranchising a greater number of citizens. For example, NVT systems could enable persons with disabilities or illiterate voters to vote

9 For example, the Estonian and Swiss systems allow voters to verify the contents of their encrypted vote and provide for some solutions for voters to verify that their votes are stored as cast. In Estonia, this is currently done by using a second device that retrieves the vote cast and stored, which then can be verified by the voter based on a cryptographic solution that it was encrypted with containing their choices. In Switzerland, several computations are conducted between the voter and the voting server on the encrypted vote cast and voters obtain a return code. The return code is then verified by the voter against a pre-printed voting card which associates each return code to a voting option or a candidate. In France, voters can only use a test platform to verify the encryption of test votes, but the actual platform does not provide 'cast as intended' verifiability and voters can only verify that their vote has been received by the server.

10 For example, this can be done by using verifiable mix-nets that break the link between the votes cast and the voter's identity as well as decryption mechanisms that generate zero-knowledge proofs, which can be used by anyone without breaking the secrecy of the vote. In cryptography, a zero-knowledge proof is a method by which one party can prove to another party that a given statement is true without revealing the statement itself.

11 Cryptography is a technique to keep communication (data) secure from any third party. One of these new systems uses blockchain technology which has been recently touted as potentially overcoming the verifiability challenges. However, there are numerous trust-related concerns with this technology, which also does not provide for desired universal verifiability and does not guarantee vote secrecy.

without special assistance, provide greater inclusion for out-of-country voters or those belonging to specific linguistic minorities (if the system has multi-language feature). NVT may also bring some benefits by reducing human error and improving accuracy, especially in complicated processes where a number of different elections are taking place concurrently.

There are still important vulnerabilities to consider however, related to the secrecy of the vote and the integrity of results. Attacks against NVT systems, including cyber-attacks have led some OSCE countries to opt for less technology in their elections. When considering the costs, while short-term costs may initially be lower than those of traditional paper-based elections, the costs of procurement, maintenance, storage, and replacement of NVT equipment can be significantly higher. The potential benefit of increased effectiveness from NVT systems is also in question, as many countries delay implementing them due to legislative challenges or other obstacles.

Ensuring public trust and confidence remains a fundamental challenge for OSCE participating States when introducing or using NVT. Although there may be valid concerns about secrecy of the vote and the lack of fully verifiable systems (which also prevents meaningful and independent observation of election process), effective and well-functioning NVT solutions with proven track records have been publicly questioned and politicized by certain stakeholders.[12] The number of cases going to court for adjudication has risen significantly in recent years. This raises important questions about judicial oversight, expertise and training when introducing NVT.

1.2 'Ancillary' ICT-based election systems and processes

Beyond the application of technology in voting and counting, a large field of 'ancillary' ICT-based election processes has developed and extends to areas such as EVRVS, RMS and other online EMB platforms. These include components for the nomination and training of polling staff, constituency or boundary delimitation, candidate registration, accreditation of observers and political and campaign finance reporting.

1.2.1 Electronic Voter Registration and Verification Systems (EVRVS)

Many OSCE participating States have implemented or are considering upgrading their voter lists management systems using ICT. This Handbook discusses only the technological processes, needs and challenges related to EVRVS and their relationship to international obligations, commitments, and standards for democratic elections. The fundamental principles of equality, universality, and transparency upon which

12 The use of VVPAT has to some extent ameliorated the concerns about verifiability in e-voting systems. However, they are only useful in a context of properly delineated and implemented audit regimes, which is an important area of focus. For i-voting systems, the issue of both individual and universal verifiability is still a work in progress.

voter registration processes should be based and the comprehensive methodology for their observation and assessment are elaborated in the ODIHR *Handbook for the Observation of Voter Registration*.[13]

EVRVS modernization often requires adjustments to the legal, procedural and institutional frameworks. Specific responsibilities must be assigned for the collection of voter's data and for the management and protection (including from cybersecurity threats) of databases, as well as a series of financial, organizational and operational changes related to procurement, setting-up, database migration, equipment testing and staff training.

The transition from a paper-based system or the creation of new digital voter registration databases, which contain different levels of personal data and are stored and transmitted electronically is an extremely expensive, complex and challenging undertaking. The system may also include biometric data, such as fingerprints, facial recognition features or other elements, in an effort to reduce multiple registrations and to assist voter verification. It is underpinned by computer hardware (computers, tablets, scanners, etc.) and software each element of which introduces certain cyber vulnerabilities.[14] Importantly, confidentiality and data protection issues should be considered systematically at different stages of the election process.

In addition to the establishment and maintenance of voter registers, ICT has also been employed in the voter verification stage of the electoral process. Traditional verification methods consist of poll workers visually comparing information provided by a voter (voter card, ID card, invitation, etc.) with that in a physical voting list. In an effort to have better safeguards to prevent impersonation or multiple voting, a number of OSCE countries have introduced some level of technology to this process, a few with a biometric recognition functionality. These types of technology-based verification systems need additional equipment and identity verification devices, bringing with them further hardware and software risks (see Chapter 7 on cybersecurity).

13 Handbook for the Observation of Voter Registration, OSCE/ODIHR, 13 July 2012.

14 See, for example, Briefing Paper on the Cybersecurity of Voter Registration, IFES, 22 May 2023.

Table 3. Most common technologies used for voter verification

Type of EVRVS Device	*Features*
Devices that require the use of ID documents	Devices that require the use of ID cards usually prevent those who are not in possession of the ID cards from voting. Devices that allow the manual entry of ID card numbers can circumvent this safeguard.
Devices with screens that require the use of ID documents	Following an ID document check, these devices show the voter's photo and name on the screen. If a perpetrator has another person's ID card and the face check is not performed correctly by polling staff, or the member of polling staff is colluding with the perpetrator, this safeguard can be circumvented.
Devices with biometric functionality	Biometric checks, such as fingerprint or face recognition, might be conducted at polling stations and matched against previously collected data and stored in databases. If implemented effectively, this system could fully prevent impersonation, since a voter in possession of an ID document would only be allowed to vote if their biometric check matches.
Hybrid Devices (Electronic Poll Books)	These combine several features of the devices above. There are a variety of so-called Electronic Poll Books in use across the OSCE region and they typically provide one or more of the following functions: ✓ Allow voters to sign in electronically; ✓ Read or scan ID documents to check voter's eligibility (thus avoiding data entry errors); ✓ Use a photo to verify a voter's identity; ✓ Provide real-time updates, including on voter turnout; ✓ Devices connected to centralized voter database allow for checking if a voter is registered in a different location or if they have already voted; ✓ Systems that require biometric voter verification will have additional devices that provide this functionality and match the relevant biometric data against previously collected data.

1.2.2 Other ICT-based platforms and processes

In addition to NVT and EVRVS, many EMBs in the OSCE region have also been applying different technological solutions to other aspects of the election process. These include ICT-based platforms and modules for training EMBs and polling staff, constituency boundary delimitation, candidate registration, EDR, voter information campaigns, political and campaign finance reporting, accreditation of observers and other 'ancillary' processes.

One of the most widely used in the OSCE region is an electronic RMS. This is the process by which an election authority tabulates, aggregates and transmits the results of an election.[15] A transparent and efficient RMS can increase the credibility of the overall process. On the other hand, delays in data transfer or in the announcement of the election results or inaccessible EMB results websites caused by, for example, cyberattacks, can severely damage public trust and the credibility of the entire election. Given the critical importance of this process and the growing cyberthreats directed towards these systems, a number of details — trained and professional staff, proper procedures, equipment testing, up-to-date software and public voter information campaigns — must be considered before moving to an ICT-based RMS.

1.3 Cybersecurity

Different ICT-based solutions have already been implemented during elections in the OSCE region, so it is paramount that they are designed and operated in a secure manner. Often, however, they are subject to cybersecurity threats that challenge public confidence in elections. The concept of cybersecurity commonly refers "to how electronically processed information can be secured against disruption, disablement, destruction or malicious control, thereby protecting its confidentiality, integrity, and availability."[16] The most common cybersecurity threats that have occurred during election periods are malware, phishing, ransomware, hacking, social engineering and distributed denial-of-service (DDoS) attacks.[17]

15 Any RMS is comprised of tabulation or aggregation (how and where the results are added together), verification (how the results are checked to ensure their accuracy) and publication of election results. See the Guide on RMS, UNDP, 30 August 2016.

16 Confidentiality means that information is only accessed by designated, authorized users. Integrity means ensuring that information that is accessed is not inappropriately altered. Availability means that information is present and accessible when it is requested. See for example, the United States government NIST Glossary.

17 Hacking is considered to be any illegitimate entry into the system made by anyone external to the management of the process. A distributed denial of service (DDoS) attack involves multiple connected online devices, also known as a botnet, which would be used to overwhelm a target website or service with fake traffic.

Attacks may be targeted at different election stakeholders and processes, compromising voter registration processes, accessing or changing the results of voting, or targeting 'ancillary' systems such as the RMS or entire EMB websites.[18] Known attacks and threat actors have included foreign states or advanced persistent threats (APTs) and their motives may be political — to alter results — financial, or disruptive — to undermine trust.[19] They have also included criminal organizations, sometimes working in concert with domestic actors and disgruntled insiders.[20]

Given the fast development of digital technologies and the associated cyberthreats, full protection of ICT-based electoral systems, processes and equipment is practically impossible. Nevertheless, most of the effective responses to these challenges are based on advance and adequate planning, sufficient and often substantial financial costs, and the creation of cybersecurity strategies that include risk-assessments, testing, maintenance, auditing and certification of equipment, measures for detection and prevention of threats, information sharing, training and public awareness campaigns. Lastly, given the cross-sectional and often transnational nature of cybersecurity issues and threats, the involvement of and cooperation with countries and international organizations, as well as different institutions, such as specialized IT and security agencies, experts, or private entities is a necessary condition for EMBs to ensure comprehensive and effective responses.

The following table summarizes different aspects of the election process and related cyberthreats against these systems observed in the OSCE participating States.[21]

18 The Handbook focuses on cyber-security matters related to NVT and other 'ancillary' ICT-enabled electoral processes. Online media, social networks and other communication tools are outside its scope.

19 APTs are defined as "an adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives". See U.S. NIST Glossary.

20 See Primer: Cybersecurity and Elections, USAID/DAI/IFES, July 2022.

21 See the Compendium on Cyber Security of Election Technology, NIS Cooperation Group, European Commission, 1 July 2018 and Election Infrastructure Security Resource Guide, Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security, May 2019, and U.S. NIST Glossary.

Table 4. Most common types of cyberattack directed at electoral processes

Stage of Election Process	*Types of Cybersecurity Incidents*
Voter registration and verification	→ Data theft and breach of voter privacy → Deleting or tampering with voter data → DDoS or overload of EVRVS
Party and candidate registration	→ Data theft, breach of voters or candidates' privacy → Fabricated signatures and tampering with registrations → DDoS or overload of party/candidate registration
Other EMB platforms (e.g., accreditation of observers and polling staff)	→ Data theft → Hacking or misconfiguration of servers or communication networks → Hacking EMBs' websites, spreading dis- or misinformation on the election process, including about parties/candidates, or results → DDoS or overload of EMBs' websites
NVT (voting and counting)	→ Breaches of voter privacy and issues with vote secrecy → Software bug for altering election results → Tampering with log files → DDoS, or overload of the systems used for casting, counting or aggregating results and communication links used to transfer results
RMS (tabulation and announcement of results)	→ Hacking internal systems used by media → Tampering with election results → Defacement, DDoS or overload of websites or other systems used for results publication

Chapter 2

OSCE commitments and international standards, principles and good practice

Any election process in the OSCE area, including those that are ICT-based, should ensure full respect for all OSCE commitments as well as other international obligations and standards for democratic elections. The OSCE election-related commitments can be summarized in seven **key principles** that also apply when observing and assessing the use of ICT and, specifically, NVT. Additionally, the right to effective remedy and the right to personal data protection are discussed in this chapter as they are of fundamental importance in the context of elections. This chapter also gives an overview of

documents from the Council of Europe and other relevant international organizations. These contain more detailed standards and principles that provide further guidance for states when using ICT in elections.

2.1 OSCE commitments

ICT systems are intended to fulfil the same functions as paper-based elections and must, therefore, meet the same standards. The OSCE commitments define the principles for democratic elections, regardless of the technology used. These principles were agreed by the OSCE participating States in the 1990 Copenhagen Document and in subsequent OSCE commitments.[22] In particular, the voting process requires the exercise of universal, direct, equal and secret suffrage through the casting, counting and tabulation of votes in an honest, transparent and accountable manner.

2.1.1 Secrecy of the vote

Paragraph 7.4 of the 1990 OSCE Copenhagen Document requires participating States to "ensure that votes are cast by secret ballot or by equivalent free voting procedure". This requirement is at the heart of the democratic election process and any voting and counting process that does not meet this commitment cannot be considered democratic.

Secrecy of the vote means that it should not be possible to associate the contents of a vote with a specific voter at any stage of voting. This principle permits the voter to exercise his or her choice freely, without the potential for coercion, intimidation, vote-buying or fear of repercussions. The systems in which NVT are used must be consistent with this requirement. Voters must not be able to prove to anyone how they voted and the system itself must not allow a voter and his or her vote to be identifiable by third parties. When NVT systems give voters receipts or codes to verify that the vote was recorded as cast, supplementary measures should be implemented to safeguard the secrecy of the vote in accordance with OSCE commitments. Likewise, a system that retains an electronic log that could be used to associate a voter with his or her choice would also fail to provide for the secrecy of the vote.

2.1.2 Integrity of results

The integrity of the results — the honest counting of votes and reporting of results as required by paragraph 7.4 of the 1990 OSCE Copenhagen Document — implies a chain of actions. All votes must be cast in a ballot box as the voters marked them; all votes must be counted as cast; and no votes should be illegally added to, or subtracted from the results. There must be no possibility for fraud or error to alter the results.

22 OSCE Human Dimension Commitments, 4th Ed., OSCE/ODIHR, 27 April 2023.

In a paper ballot process, the integrity of this chain can be ensured through observation of each step of the process and verified, if necessary, through the possibility of a manual recount.

Similar to the secrecy of the vote, in order to comply with OSCE commitments on counting and reporting results, NVT systems must provide a guarantee for the integrity of results. There must be the possibility for meaningful verification of votes cast electronically, such as that provided by a manual recount. NVT that rely solely on public trust in the honesty of election officials, vendors, programmers or technicians do not provide an effective means of verifying electoral integrity. The verification mechanism must also fully guarantee the integrity of the results without compromising the secrecy of the vote.

In all cases, verification should be able to be performed by a body independent from that conducting the election and — in conjunction with verifying individual votes — should be able to be performed for the entire number of votes counted. Systems that only allow individual voters to verify that their own votes have been recorded correctly are not necessarily effective in guaranteeing the integrity of the overall results unless verification can also be performed on a broader basis.

2.1.3 Equality of the vote

Paragraph 7.3 of the Copenhagen Document says that participating States will provide "equal suffrage to adult citizens". While this requirement has broader ramifications, one aspect of the principle of equality is that no voter will be able to cast more votes than another, nor will citizens be prevented from participating in voting. This means that NVT systems must prevent any person from casting more votes than is established by law and must prevent any votes from being subtracted from the system.

Some Internet voting systems allow voters to cast their vote more than once, with the condition that only the last cast vote counts. This helps to reduce the risk of voter coercion and vote buying, but it must be possible to verify that no violations of the principle of equality have taken place. If NVT systems are used together with traditional, paper-based voting methods, then all means of voting should be equivalent and voters choosing either should receive equal treatment. Otherwise, the equality of the vote could be endangered.

2.1.4 Universality of the vote

Universal suffrage is enshrined in paragraph 7.3 of the Copenhagen Document. This commitment means that all eligible adult citizens must have the opportunity to participate in an election and effective means for their participation should be provided. If NVT are used in polling stations, they should not be the exclusive method of voting, as less computer-literate voters may have problems operating NVT systems. In such cases, voters should be provided with an alternative way of voting.

Internet voting has the potential to provide easier access and more options for participation in elections, especially for voters facing barriers to accessing polling stations or those living outside their official residence area. As with all forms of remote voting, including postal voting, this comes with a greater risk of voter coercion or vote buying, which require mitigation measures.

2.1.5 Transparency

Transparency is a cornerstone of OSCE election-related commitments, as it is necessary to verify that elections take place in accordance with the law and democratic principles. Election observation is a key aspect of transparency, recognized in paragraph 8 of the 1990 OSCE Copenhagen Document. Political parties, candidates and observers should have the opportunity to observe the work of election authorities at all levels, and especially the voting, counting and tabulation processes.

The observation must be meaningful.[23] The possibility of meaningful observation is particularly important when significant changes, such as NVT and ICT-based solutions are introduced into the election process. In the case of electronic voting and counting technologies, the mere observation of voters and officials operating machines is not likely to be meaningful. Observers need to have additional access (e.g., to critical locations such as maintenance, storage, software and design centres) to be confident that the election is in full accordance with the law and with democratic principles.

Observers should not interfere in the process; however, they should have access to documentation about the system, including auditing, certification and testing reports to allow for meaningful observation and assessment. Observers should not be obliged to sign non-disclosure agreements in order to have access to documentation or to be able to observe processes, as this would jeopardize the ability of the EOM to report on its findings. Legislation and practices that do not allow for sufficient access by observers cannot be assessed as fully meeting OSCE commitments. Transparency also includes the obligation that all election stakeholders, including voters, should be given sufficient means to learn in detail how NVT and ICT systems function.

23 For example, in paper ballot systems counting cannot be considered transparent if observers are present during the counting but are kept at such a distance that they cannot see the content of ballots and cannot verify that votes are being counted honestly.

2.1.6 Accountability

The 2003 Maastricht Ministerial Council Decision No. 5/03 underlined the importance to the electorate of the accountability of those involved in an election process.[24] For NVT, this includes election officials, vendors, certification, verification bodies and others involved in procurement, management and utilization. Election officials must be responsible for the overall conduct of elections, including the oversight of NVT. If NVT involve technology supplied by private vendors, the roles and responsibilities of these vendors must be clearly defined, including crisis management responsibilities. Similarly, certification agencies and other bodies must be held strictly accountable to ensure that they fulfil their responsibilities.

Accountability also means that detailed minutes should be kept, which describe the ways election administrations or other eligible personnel interact with the system, when this is done and who actually performs the work. The procedures described in these minutes should ideally be certified by an independent auditor or by means of separation of duty.[25]

2.1.7 Right to effective remedy

Paragraph 5.10 of the Copenhagen Document provides that "everyone will have an effective means of redress against administrative decisions, so as to guarantee respect for fundamental rights and ensure legal integrity". The right to effective remedy in the context of elections requires that States institute rules and procedures to allow voters, contestants and other electoral stakeholders to challenge violations of their election-related rights through an effective dispute resolution system. The resolution of election disputes can be handled by the election administration, judiciary, law enforcement or any other competent institution in line with their mandate and responsibilities. Disputes may concern any election-related area, such as NVT or broader ICT election-related issues, such as voter and candidate registration, campaigning, conduct of election day procedures or election offences, and can be lodged against any election stakeholder, including EMBs and other relevant authorities, candidates, media regulatory bodies and others. Efficient EDR systems are essential, among other things, for the overall protection of fundamental rights, conflict prevention, electoral integrity, public confidence in the election process and the acceptance of election results.

Legal challenges to ICT and NVT may be raised, for instance, on the (lack of) constitutional or legal basis for using technology in elections, on procurement issues or on various procedural and operational issues related to the use of the ICT-based processes,

24 See OSCE Ministerial Council, Decision No. 5/03, "Elections", Maastricht, 1 and 2 December 2003.

25 Separation of duty means that at least two people are required to operate a system at the same time, thereby providing checks and balances on each other's conduct in an effort to curtail possible malfeasance.

including on matters concerning the counting and verification of election results. The admissibility and way in which complaints are handled, including the mandate, competency and readiness of courts and judges to deal with ICT and NVT-related matters, also has significant impact on overall confidence in the election process.[26]

2.1.8 Data protection and data privacy

Personal data processing lies at the core of running any electoral process; data on voters, candidates, members of the election administration, polling station staff or election observers must be collected and processed. Paragraph 26 of the Copenhagen Document provides for "protection of privacy".[27] The right to privacy and protection of personal data is also spelled out in various other international documents.[28] As a general principle, the processing of personal data should be based on lawful grounds. The regulations should clearly describe who is entitled to access, for what purposes and the limitations on the use of the data.

For ICT-enabled systems associated with voter registration, this principle applies to the processing of voters' personal data, their privacy and measures taken to ensure it is used only for the purposes prescribed by law. In line with this principle, voter lists should not include personal data other than that which is required to establish eligibility to vote (also called data minimization). The law should define the minimum standards of security to protect the voters' register against unauthorized access; it should also define the conditions and limits of access to the data contained in the voters' register. In principle, personal data from the voter register should not be public by default. It should be made clear in law and in relevant guidelines that any personal data from the electoral register which has been made accessible, for example, to political parties and electoral contestants, state institutions or civil society organizations, is still subject to, and protected, by data protection law. Data controllers and data processors should be held accountable for possible misuse of data, for example, for campaign advertising, and the accountability provisions should be clearly set out in the legislation.

26 See Handbook for the Observation of Election Dispute Resolution, OSCE/ODIHR, 17 September 2019.

27 See also Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE (Moscow Document), OSCE, 3 October 1991.Moscow Document, paragraph 24.

28 See for instance Article 8 of the European Convention on Human Rights, European Court of Human Rights, Council of Europe, Rome, 4 November 1950. For a comprehensive overview of data protection issues in the EU area, please refer to the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016. For good practice from the Council of Europe area, please refer to the modernized Convention for the Protection of Individuals with regard to the Processing of Personal Data (CETS No. 108), Council of Europe, Strasbourg, 28 January 1981. Forty-six of the 57 OSCE participating States are also members of the Council of Europe.

2.1.9 Public confidence

Public confidence is an essential element of a democratic election process and has been affirmed in OSCE documents, including in the 2003 Maastricht Ministerial Council Decision No. 5/03, and is always taken into consideration in ODIHR's election observation activities. Public confidence is based, in part, on the extent to which authorities, election officials and courts respect and uphold the key principles. At the same time, public confidence in elections may be reduced by perceptions that elections or even aspects of elections are mismanaged or may not fully reflect the will of the people.

Public confidence is of fundamental importance particularly when NVT are introduced or used. Where a significant level of distrust or dissatisfaction with the election administration exists, the use of NVT or ICT in general may be problematic and may further diminish public trust in elections. An incremental approach to the introduction of ICT and NVT systems, together with thorough testing, verifiability and full transparency, can help develop public confidence. Importantly, working to maintain public confidence is also critical after the introduction of an NVT solution and must be carried on continuously.

2.2 Other international documents

To date, no specialized commitments with regard to ICT or NVT have been developed by the OSCE participating States. However, over the last decade there has been a concerted effort within several international organizations, such as the Council of Europe and the European Union institutions, to develop regional standards for the use of these technologies in democratic and electoral processes. At the global level, the United Nations has developed guiding principles for business and human rights organizations, including for private technology companies, on issues of human rights and political processes. These efforts are supplemented by a number of initiatives led by international organizations such as the International Foundation for Electoral Systems (IFES) or the International Institute for Democracy and Electoral Assistance (IDEA), which have produced a substantial volume of reference documents and reports.[29] At the national level, several OSCE participating States have developed their own ICT or NVT standards and requirements.

2.2.1 Council of Europe recommendation on electronic voting

In 2017, the Council of Europe issued a Recommendation: a comprehensive set of documents that includes recommendations, an explanatory memorandum and guide-

29 See Annexe C Good Practice Documents.

lines for implementation of NVT.[30] This recommendation replaced the 2004 Recommendation on Legal, Operational and Technical Standards for Electronic Voting.[31] The 2017 Recommendation provides a good practice baseline for the implementation and management of digitally enhanced solutions specifically for electronic voting and counting processes. It is important to note that these principles do not constitute a normative framework nor allow for absolute conclusions on the performance of observed electronic voting solutions and do not deal with ICT-related 'ancillary' systems outside the scope of electronic voting and counting. The Recommendation provides 49 e-voting standards which are categorized following a scheme of basic election principles.

Table 5. Council of Europe e-voting standards

Election standards	Electronic voting standards (E-voting systems should…)
Universal suffrage	✓ be easy to understand and use by all voters ✓ enable persons with disabilities to vote independently ✓ be only an additional and optional channel of voting, unless universally accessible ✓ will notify voters if the vote is for a real election or referendum
Equal suffrage	✓ present voting information in an equal way ✓ provide secure and reliable tabulation of all votes, irrespective of the voting method ✓ provide for unique identification of voters ✓ grant a user access only after authenticating eligibility to vote ✓ ensure that votes cast are properly stored and included in the election result

30 See Council of Europe Committee of Ministers to member States Recommendation CM/Rec(2017)5, 14 June 2017, on standards for e-voting and other supporting documents.

31 See Council of Europe Committee of Ministers to member States Recommendation CM/Rec(2004)11, 30 September 2004, on legal, operational and technical standards for e-voting. The Recommendation followed a report by the Council of Europe's European Commission for Democracy through Law (Venice Commission) concerning the compatibility of remote and electronic voting with the requirements of Council of Europe documents. Supplementary documents regarding transparency and certification of electronic voting systems were adopted in 2011.

Free suffrage	✓ not affect a voter's intention ✓ present an authentic ballot and authentic information to the voter ✓ not lead voters to vote precipitately or without confirmation ✓ allow the voter to participate without exercising a preference for any of the options ✓ advise the voter if he or she casts an invalid e-vote ✓ provide voters with verification means that the vote was cast as intended ✓ give confirmation that the vote has been cast successfully ✓ provide evidence that each eligible vote is accurately tabulated ✓ provide independent verification means (universal verification)
Secret suffrage	✓ ensure that the secrecy of the vote is respected at all stages of the voting procedure ✓ process and store only the personal data needed for the conduct of the e-election ✓ guarantee protection of data to prevent misuse, interception and modification ✓ guarantee that voter lists are accessible only to authorized parties ✓ ensure that the voter's proof of cast vote cannot be used by third parties; ✓ not allow the disclosure of the voting results until the closure of voting ✓ ensure the secrecy of previous choices and erase and respect the voter's final vote ✓ ensure that it is not possible to reconstruct a link between the vote and the voter
Regulatory and organizational	✓ be introduced in a gradual and progressive manner and have legal basis ✓ be controlled by the EMB which holds the responsibility as provided by legislation ✓ provide for observation of vote counting

Transparency and observation	✓ provide for transparency in all aspects ✓ inform voters on the steps for election participation, use of technology and timetable ✓ provide for verification and certification ✓ provide for observation of results tabulation ✓ use open standards to enable various technical components or services
Accountability	✓ be based on up-to-date requirements and on relevant legal and democratic principles ✓ be evaluated by independent and competent bodies ✓ be certified, which will include safeguards to prevent modification to the system ✓ auditable in an open and comprehensive manner and with reporting of issues/threats
Reliability and security of the system	✓ be controlled by the EMB, which, in turn, is responsible for the compliance, availability, reliability, usability and security of the e-voting system ✓ provide a clear authorization procedure for access to election infrastructure and data ✓ provide for the EMB to confirm that the system is genuine and operating correctly ✓ provide for regularly installing updates and corrections of software ✓ provide for encryption of votes, if they are managed outside controlled environments ✓ provide that votes and voter information is kept sealed until the counting ✓ provide for the EMB to handle all cryptographic material securely ✓ ensure that the EMB is immediately informed of system integrity incidents ✓ provide for the authenticity and integrity of the voters' and candidates registers ✓ respect provisions on data protection ✓ identify votes that are affected by an irregularity

2.2.2 Council of Europe guidelines on the use of ICT in elections

In addition to these documents specifically addressing electronic voting and counting, in 2022, the Council of Europe published Guidelines on the wider use of ICT in elections.[32] The Guidelines offer an overview of different digital solutions throughout the electoral cycle and cover topics from candidate registration and collection of electronic signatures to election results transmission and publication.

The Guidelines iterate that the use of ICT solutions in elections must: comply with the core principles of democratic elections and referendums as defined by the relevant international documents, including the 2002 Code of Good Practice in Electoral Matters; take into account acceptable trust assumptions; and be balanced against other core considerations such as security and accessibility for users.[33]

2.2.3 Cybersecurity standards

Election-related ICT issues are not directly addressed by the 2001 Budapest Convention on Cybercrime. However, the document, which 47 OSCE participating States are party to, sets out a general framework for cooperation on, and a basis for criminalization of a variety of aspects, such as the misuse of equipment, data and systems interference, and illegal access and interception, including on areas that go beyond the provisions foreseen in the Convention.[34] In the OSCE context, the participating States have agreed on sets of confidence-building measures to increase trust and the security of ICT and which serve as a platform for exchange and cooperation. However, election systems and processes are not specifically addressed in these measures.[35] Similarly, on a global level within the UN, discussions on the adoption of a Convention on Countering the Use of ICT for Criminal Purposes are at the final stage; at the time of writing, the current draft does not explicitly address cybercrimes targeting election.[36]

Specific election-related cybersecurity standards have been developed by several other international organizations, including the EU Compendium on Cyber Security of Election Technology (which provides guidelines and best practices for EMBs), cybersecurity organizations involved in elections, and IFES reference documents and reports.[37] The Commonwealth of Independent States (CIS), all of which are OSCE

32 See Committee of Ministers Guidelines on the use of ICT in electoral processes, Council of Europe, 9 February 2022.

33 See Code of Good Practice in Electoral Matters, Council of Europe Venice Commission, Venice, 5 to 6 July and 18 to 19 October 2002.

34 See Budapest Convention (ETS No. 185) and its Protocols (Budapest Convention on Cybercrime), Council of Europe, Budapest, entry into force 1 July 2004.

35 See the OSCE Cybersecurity dedicated website, last accessed 31 October 2023.

36 See the UN Office on Drugs and Crime website, last accessed 31 October 2023.

37 See the EU Directive on Security of Network and Information Systems (NIS Directive) and the European Commission Compendium on Cyber Security of Election Technology and IFES publications on cybersecurity, last accessed 31 October 2023.

participating States, adopted an agreement in 2018 on cooperation between CIS members in the fight against ICT crimes.[38] At the national level, the majority of OSCE participating States have cybersecurity laws, some specifically addressing electoral processes. At the same time, many OSCE participating States are beginning to define and categorize election processes as 'critical infrastructure'.[39]

2.2.4 The UN Guiding Principles on Business and Human Rights

As many democratic processes often rely on services from the private sector, the UN prepared its Guiding Principles on Business and Human Rights for "business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights".[40] While the principles are not aimed at creating a new international legal framework and do not specifically address ICT-based electoral processes, they are aimed at all States and business enterprises and set standards and good practices on business and human rights.

The 2011 ***UN Guiding Principles on Business and Human Rights*** contain three main pillars — protection, respect and remedy — and actions and activities for governments and private companies to take in order to prevent and, if needed, to remedy any abuse of human rights in their operations. The document notes that "human rights due diligence should be initiated as early as possible in the development of a new activity or relationship, given that human rights risks can be increased or mitigated already at the stage of structuring contracts or other agreements."

During election observation, it is crucial to keep these broader principles in mind when studying the contractual obligations and practices of stakeholders (e.g., ICT solution vendors). For example, observers should analyse the transparency of the procurement and production processes and assess which effective control mechanisms participating States have enacted for any potential infringements of human rights.

38 See the Agreement on cooperation between member states of the Commonwealth of Independent States in the fight against crimes in the field of information technology.

39 'Critical infrastructure' sectors are those that are considered so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health or safety. See for example, the National Institute for Technology (NIST) Cybersecurity Framework, last accessed 31 October 2023, and CISA election cybersecurity website, last accessed 31 October 2023.

40 See the Guiding Principles on Business and Human Rights, UN OHCHR, New York and Geneva, 2011.

Chapter 3

The Role of the NAM and EOM in the observation of ICT and NVT

3.1 Role of the NAM

For the implementation of ICT and NVT, complex and time-intensive preparations are needed that present challenges to national election stakeholders and election observers. Many of the preparations for the use of technology take place before the arrival of a full-scale EOM. This gives Needs Assessment Missions (NAM) — sent to OSCE participating States whenever elections are called to assess the need for ODIHR election-related activities — an important role whenever ICT and NVT is used.

The NAM should inquire about the plans for ICT and NVT-related processes to help assess whether key events will take place before or after the EOM deployment. Such key events could include the production of voter credentials,[41] any public tests, key signing events[42] or data destruction.[43] Based on such information, the NAM may recommend deploying experts ahead of, or after core team deployment dates. Teams of experts may be composed of two or more analysts, such as an ICT Analyst, sometimes together with election, legal or political analysts to follow these key events.

3.2 Role of the EOM

In order to assess effectively the use of ICT and NVT in an election in line with the key principles, each EOM will need to collect and analyse certain information about the technologies in use, including:

- the type of ICT and NVT being used;
- the stated reason for using ICT and NVT and the perceived advantages over existing voting and counting processes;
- the process for choosing, procuring and implementing the ICT and NVT system;
- whether the decision to introduce ICT and NVT was widely agreed upon by political parties, voters and other election stakeholders or, conversely, was controversial;
- the legal regulations in place regarding the use of ICT and NVT, including observer access, as well as any ongoing discussions regarding the introduction or provisions for their use;
- what documentation is publicly available about the ICT and NVT and what is only available to a restricted audience;
- the usability of the ICT and NVT system;[44] and
- the training and voter education efforts for the use of an ICT and NVT system.

41 Voter credentials can be voter identity cards; unique, one-time passwords; smart cards; or other means to unequivocally identify the user as an eligible voter.

42 A key signing event is a meeting (mainly in Internet voting) in which members of the EMB create a secret electronic 'key' that is used to protect the integrity of the electronic voting. This key is often divided into several parts and stored on separate smart cards, which are then kept by individual members of the EMB until after the closing of the election. These members then reconvene to put their parts of the key together, open the electronic ballot box and start the decryption of the electronic votes, similar to the closing and counting process for paper ballots.

43 Data destruction is a method to make data unusable once it is no longer needed in a way that cannot be recovered. This can be done in various ways, most commonly through magnetic, physical or thermal destruction of the storage medium.

44 Usability is defined as an analysis of the ease of use and learnability of a technology.

EOMs with an ICT Analyst will be able to obtain and analyse information in greater depth, considering issues such as the conduct of feasibility studies ahead of decision-making, system selection and procurement, certification and testing, usability, software and hardware security, data protection, transparency, management of the system by election administrators, accountability of vendors and election officials, and verification of the results and audits. However, other EOM analysts will play an important role, especially in situations where an ICT Analyst is not present for the whole mission.

A crucial task for the EOM is to understand whether the ICT, and the NVT specifically, adhere to the principles, as outlined above, including the secrecy of the vote and the guarantee that the results fully reflect voters' choices, or whether there are important gaps that could compromise their fulfilment. Beyond assessing the technology, an EOM should also gather other types of information about ICT and NVT use, based on meetings with state officials, candidates, political party representatives, civil society organizations, vendors, media representatives, judges, academics, specialists in the field and others. The information, conclusions and recommendations of the observation should be included in the EOM's reporting. Later chapters of the Handbook provide more detail on observing and assessing the use of technology in elections.

All EOM core-team members should ensure they are aware of how ICT and NVT issues relate to their specific areas of concern. The ICT Analyst has a leading role in assessing the ICT and NVT issues during an EOM and provides guidance on this for other EOM members, including LTOs and STOs. In addition, the ICT Analyst works closely with the other members of the EOM core team to provide analysis of the context in which the use of election technology takes place, as well as to give input to the drafting of election day observation forms.

3.3 Role of the ICT Analyst

The ICT Analyst plays the leading role in observing and assessing the use of NVT and other ICT applications in an election. Their main task is to understand how the technologies are supposed to function, how they are implemented and to analyse them systematically according to the election standards and principles mentioned above.

At the same time, the ICT Analyst is the primary contact point within the EOM for analysis and assessment of systems that include electronic identification and verification of voters or that use other 'ancillary' ICT-enabled election processes. As the topic of cybersecurity in elections is on the rise and highlights the vulnerability of certain NVT and ICT systems, the ICT Analyst should focus on the integrity, robustness and

resilience of the systems. They should analyse and understand the measures in place to secure the systems and the relationship between, and independence of election commissions and other government agencies tasked with protecting electoral infrastructure.

Therefore, to properly analyse all aspects, the ICT Analyst role requires broad ICT expertise, election systems security experience and a policy background in NVT, as well as advanced reporting skills. In cases where the EOM requires specialist knowledge in technical or policy aspects of ICT and NVT, the EOM may hire more than one ICT Analyst to cover all angles. Specific areas for analysis and guidance for the ICT Analyst in observing and assessing NVT and ICT are given in later chapters.

3.4. Code of Conduct for OSCE/ODIHR election observers

In accordance with the ODIHR *Observer Code of Conduct*, all EOM members must avoid any interference in the election process. In particular, this means that an EOM cannot certify that an ICT and NVT system is working properly; this is the role of national authorities. Non-interference also means that observers must not offer advice or suggestions to election officials or stakeholders (candidates, civil society organizations, etc.), and nor can they express any personal viewpoints on the ICT and NVT used, or not used, in the election. ODIHR observers must never handle ICT and NVT devices or equipment in a way that could be misconstrued as tampering, nor should they conduct unauthorized tests, attempts to hack the system, or otherwise compromise the impartiality and unbiased approach of the EOM. In addition, ODIHR observers should be careful not to violate the secrecy of the vote when trying to obtain information about ICT and NVT.[45]

45 See Code of Conduct for ODIHR Election Observers, OSCE/ODIHR, 14 June 2017

Chapter 4

Assessment of the context for using ICT and NVT

4.1 Decision-making process

As with any change to an election process, ICT and NVT are not introduced and used in a vacuum. EOMs should consider the background and the reasons leading to the implementation of technology in elections. In particular, the EOM should identify the benefits but also the challenges the technology is meant to address. These considerations are equally important after the adoption of any ICT and NVT and in cases where they have already been used in a number of elections.

Many OSCE countries are still only considering the use of technology in their elections. Therefore, the EOM should also look at the decision-making process for implementing ICT or NVT. Significant changes to the election process can affect voter rights, incur substantial costs and can have a far-reaching impact on public confidence in the process. Any changes should be made only after careful study and broad, inclusive public discussion, including within the national legislative bodies. The EOM should look at how public discussion was organized and to what extent this discussion allowed for the input of different views. It is important to note whether political parties, civil society groups and relevant experts were consulted and to what degree their concerns, if any, were taken into consideration. Where observation activities took place and election recommendations on ICT matters were made, the EOM should also assess the status of their implementation.

Another aspect of the decision to use technology is the extent of agreement among political parties. Opposition to the use of ICT or NVT may be an indication of a lack of trust in the technology itself or in the capacity of the election officials to administer it. A decision taken despite the objections of some parties or significant sections of civil society could damage public confidence in the election process as a whole. The decision to implement technology can create challenges for meeting election deadlines. Often, decisions to use technology are made close to calling an election, leaving insufficient time for proper preparation. The gradual introduction of ICT and NVT — through a phase of small, regionally-limited pilot projects that include testing — and gradually extending its use over several elections enables problems to be identified and corrected and may help build public confidence in the technology.

A gradual introduction may be done, for example, through trials in mock elections, in a few municipalities during local elections, or for a limited number of polling stations in national elections. In contrast, introducing ICT and NVT on a wide scale in a single election cycle exposes the election process to increased risks. The EOM should carefully examine the motives for any large-scale introduction and whether this is driven by concrete electoral needs, political interests, vendor interests or other considerations. Decisions to use technology should be made following feasibility studies and should allocate sufficient time for procurement, planning, testing, evaluation, certification, voter education, public confidence building and implementation.

Another important factor is the usability of ICT, along with voters' ICT literacy, the extent of computer ownership and Internet access. Poor ICT literacy could lead to a considerable number of voters requiring assistance, which could impinge upon the secrecy of their vote or on their ability to vote freely. The extent to which the Internet is freely accessible is an important issue. If political information is censored or certain websites are made inaccessible, this may impact the public perception of the use of computer technology in an election process. Another risk is that ICT and NVT could

intimidate certain voters, causing them to abstain from voting. The EOM should also be aware of the overall maturity of the country's digital enablers (i.e., digital identity management, interoperability framework, general government infrastructure and general public access to digital services),[46] in order to assess properly the country's digital ecosystem.

The EOM should also consider the potential impact of the selected ICT and NVT on the electorate as a whole, as well as on specific groups of voters, such as women or representatives of national or language minorities, particularly where media, computer or general literacy is lower among some of these groups. Technology can become an obstacle for all voters when there are technical problems, when security or cost considerations are prioritized over usefulness, or simply when too many voters are assigned to each voting machine. In such cases, the voting process may be complicated, take longer or result in long queues. On the other hand, ICT can bring certain benefits to the election process and possibly expand electoral participation, giving access to persons with disabilities, illiterate voters or those belonging to national minorities.

After considering these issues, the EOM can make an overall assessment of the decision to use ICT and NVT. A determination can be made as to what extent the decision reflects real needs; whether it was based on thorough study and public discussion; whether it was the result of broad agreement or was strongly opposed by some sides; whether ICT are being introduced gradually or hastily; the extent to which voters and election administrators feel comfortable using the technology; and the impact on voting rights. This assessment will be useful in evaluating the effect of the introduction and use of ICT and NVT on public confidence in the election process, as a whole; an issue that the EOM should discuss with all interlocutors.

Possible questions:

- What electoral processes are supported through ICT means?
- What is the timeframe for implementing the ICT solutions in the electoral process?
- Are there sufficient funds in place for effective implementation of the ICT solutions? Which institution is responsible for managing the funds?
- What were the reasons for introducing ICT and NVT? What were the problems or challenges the technology intends to address? Is the use of NVT proportional in regards to adding value to the overall electoral process?

46 See, for example, Digital Government Readiness Assessment (DGRA) Toolkit V.31, Guidelines for Task Teams, World Bank, (Version 3.0), April 2020.

- Was the decision to introduce ICT and NVT taken after conducting a feasibility study? If so, who conducted the study? What issues were covered? Was a cost-benefit analysis made? Were the reports made public?
- What was the extent of public discussion? Were civil society groups, other election stakeholders and academics able to contribute in a meaningful way? What are their positions on the introduction of technology and to what degree have their concerns been taken into consideration?
- Was there broad agreement among political parties or was there substantial opposition? Do all sides feel that their concerns were adequately considered?
- Was technology introduced in a gradual way, such as through pilot projects? If so, how many projects have been conducted? Were they conducted in real and legally binding (not mock) elections? Is information available as to how authentic and realistic the pilot projects or tests were? If ICT and NVT were introduced on a wide scale, what was the reason for doing so? To what extent were the lessons from the pilot integrated into successive uses?
- What is the level of computer and Internet literacy in the country? Are there differences in computer and Internet literacy among certain groups of the population? What is the level of Internet penetration in the country? Do all groups of voters have equal access to Internet?
- To what extent are voters familiar with ICT in general, e.g., automated banking machines, computers and the Internet? Are there studies on information technology literacy among the general public?
- What regulations are in place to ensure against possible conflicts of interests among vendors, certification agencies and election officials? Is there a code of ethics to prevent biased decision-making or the acceptance of anything of financial value between vendors and officials?
- How does the ICT or NVT system affect the voting process for potentially vulnerable groups of voters? What are the views of elderly voters, national minorities, or voters with disabilities? Are they more or less likely to vote as a result of the introduction of ICT and NVT?
- To what extent is there public confidence in the technology? Do the ICT and NVT being introduced command the same level of confidence as the systems they are supplementing or replacing? To what extent are there people (e.g., staff or vendor) to maintain, update and monitor the ICT and NVT on a continuous basis?

4.2 Political parties, civil society and media

The views of political parties on the introduction of technology in elections are an important indicator of public confidence. The EOM should seek to analyse the views of all parties competing in elections. Where this is not possible due to large numbers, the mission should ensure it discusses ICT and NVT issues with the parties represented in parliament or major parties in government and opposition. The reasons behind support for, or opposition to technology will be important for understanding the overall context. Political parties should also be asked what steps, if any, have been taken by the EMB or other authorities to address their concerns. The confidence of political parties in the professional capacity and objectivity of election administration — which may be different from their confidence in the technology — should also be discussed.

Civil society groups are another source of information. Citizen observer groups may be observing the use of technology and may hold public positions in this respect. In some countries, small groups of academics or computer experts may be active on this issue, and the EOM should seek their views. In addition, organizations working with persons with disabilities should be engaged in consultations on ICT and NVT in elections and the EOM should also speak to relevant ICT experts, as this will often be helpful in obtaining insights on the background for introducing the system, the vendors involved and public computer literacy.

The EOM should also assess the extent to which political parties and civil society groups are observing the use of NVT and ICT. The EOM should ask whether parties, citizen observers or others have requested access to any aspect of the process and, if so, what checks they were able to perform and what information they were unable to obtain. The EOM should also find out whether such groups were able to get access to all the requested documentation, including system documentation, certification reports and source codes.[47]

It is also useful to consider whether the use of technology is a campaign issue and to what extent there is public discussion on the topic. The EOM's media monitoring can generate statistical data on coverage of the issue in different media and on the amount of voter education material in the media and its dissemination.

47 Source code is human-readable text written in a specific computer language that can be readily translated into a set of computer instructions, i.e., an executable program.

Possible questions:

- What are the views of political parties regarding the introduction and use of technology? Did any political parties oppose the introduction? If so, do they still maintain that position? What are the reasons cited for any opposition?
- To what extent are political parties and candidates familiar with the technology being considered or implemented?
- What are the views of citizen observer organizations?
- Have political parties, candidates and citizen observer groups observed any aspects?
  - If not, why?
  - If so, what have they found?
  - Were there any aspects of the process or any documentation that they were unable to access?
- What are the views of ICT experts and academics?
- Is the use of technology a campaign issue? What is the extent of public discussion regarding technology issues? To what extent is this discussion present in the media?

4.3 Legal context

While the ICT Analyst leads on assessment of technological matters, for comprehensive analysis of the legal process, cooperation with other EOM members, in particular the Legal Analyst, is necessary. The legal framework should fully ensure that ICT and NVT comply with OSCE commitments and other international good practices for democratic elections, and that the application of any technology is in line with these principles, as well as with national legislation. Thus, the EOM, and in particular the ICT and Legal Analysts, should understand the process leading to the adoption of the legislation and how ICT and NVT are regulated for the election being observed. This requires careful examination of the constitutional requirements, laws and regulations governing elections. It may also require review of other legislation, such as the criminal provisions or that relating to data protection. Previous court challenges to ICT and NVT and the resulting jurisprudence should also be considered.

Detailed regulation may be provided primarily in electoral laws. Alternatively, the legal framework may only establish general rules (at least regulation related to the key electoral principles), leaving the detail to binding regulations issued by the electoral authority. While the latter is advantageous in terms of flexibility, it can give too much scope for election procedures to be adapted to the needs of the technology or the

vendors and circumvent important safeguards. There must also be no significant gaps in the legal framework; for instance, it should be clear what steps are to be taken if the technology partially or completely fails during the electoral process or in one or more polling stations on election day.

The EOM should examine whether the electoral legislation clearly defines at least the principles of secrecy, equality, universality, transparency, accountability and the integrity of the results. The equality and secrecy of the vote are included in the constitutions of many OSCE participating States and, if special provisions are required to ensure that ICT and NVT systems guarantee these principles, these should ideally be set out in the electoral legislation. The EOM should, therefore, confirm that the legal framework requires equality and secrecy of the vote and assess whether the provisions related to ICT and NVT are consistent with these requirements.

The legal provisions should clearly delineate and regulate all stages of the use of technology in the electoral process, including the distribution, set-up, starting, operating, stopping and closing of the system, as well as the storing, counting and tabulation of the votes. As with paper-based voting, the law needs to establish clear criteria for determining the validity of an electronic ballot, especially when an NVT system malfunctions.

The electoral legislation should also address how the NVT system can ensure that votes are counted honestly. This means that, in the event of a legal challenge or an audit of the results, the system should allow meaningful verification of electronically cast ballots. As noted above, the possibility of a manual recount of paper records can be a means of verification when systems are operated in controlled environments. For this to be meaningful, the law should require that the paper record be both verified by the voter and retained by the system (e.g., a VVPAT). The law should determine who may request an audit or recount, under what circumstances and what the effect of the audit or recount will be, particularly where the results after these processes differ. If the law provides for a means of verification of the integrity of the results other than through manual recounts or manual audits of results, the EOM must carefully assess whether the mechanism fully guarantees the integrity of the results without compromising the secrecy of the vote.

For NVT systems with VVPAT, the legal provisions should require a random audit of electronic and paper ballots results in a defined number or statistically relevant sample of polling stations as a further means of verifying results (for example, risk-limiting audits, RLA).[48] These audits should be open to observers. System flaws, printer malfunctions, or intentional malfeasance might result in situations where the electronic

48 Increasingly, risk-limiting audits (RLA) have become and emerging good practice in this field. An RLA is a procedure for manually checking a sample of ballots or voter-verifiable paper records from an electronic voting device.

and paper records do not reconcile and correspond in the event of a manual recount or audit. During a manual recount, where discrepancies do not appear to result from simple human error, the regulations should clearly state how the discrepancy affects the results and whether any portion of the results must be invalidated. The legal framework should address the issue of whether paper or electronic records prevail in the event of legal disputes.[49]

Another important consideration is how the principle of accountability is established in the election legislation and regulations. If private vendors are involved, the legislation should regulate their responsibility and ensure that they cannot usurp responsibilities vested in public authorities. Private contractors or vendors should not replace any functions of the electoral administration, which should remain in full control of the electoral process. Similarly, certification agencies and private auditors must be held strictly accountable for ensuring that they fulfil their responsibilities.

The law should also determine the extent of access for observers, political parties and voters. The EOM should consider whether the law adequately and appropriately provides for observer access to the system in accordance with the principle of transparency. Access can be provided through the possibility to test the technology in an adversarial manner (in which specialists attempt to identify security weaknesses or other flaws in an unscripted manner) and/or to review documentation such as feasibility studies, procurement material, manuals, evaluation and certification reports, electronic logs of the system or source code.

In terms of ICT security, it is important to assess whether and what kind of provisions are foreseen in the criminal code for attacks on ICT and NVT systems. It is also important to understand whether the election administration has been defined as 'critical infrastructure' and what these provisions entail. The specific tasks of the ICT Analyst for observation and assessment of cybersecurity aspects are discussed in the later chapters.

The EOM should also consider data protection issues, particularly where the identity of a voter, candidate or member of the election staff may be recorded in some way. Data protection standards require that every voter is made aware of the existence of automated processing, the type of data collected and the identity of the parties processing personal data. Furthermore, every voter should be made aware that the processing of their personal data has a lawful ground and that, in the case of elections, data is only processed in relation to the respective election and not used for any other purpose. Processing must be limited only to data that is necessary for the conduct of the election, the data must be accurate, and the security and confidentiality of the personal data must be maintained to prevent adverse effects for the subjects of the data. Lastly, the data collector must ensure that the data is only processed in relation

49 In general, preference should be given to the paper record. The focus should be to ensure that both paper and electronic records come up with comparable results. If doubt persists, a repeat of the election could be considered.

to the respective election and not used for any other purpose and that it is not kept for any longer than is necessary (i.e., it is destroyed after the end of the complaint and appeals process). The EOM should assess if the EMBs have specific mechanisms for data subjects to exercise their data protection rights and how the ICT and NVT comply with the specific data protection frameworks.

Possible questions:

- How is the use of ICT and NVT defined and regulated by law? Are the laws and regulations sufficiently detailed so as to provide clear guidance on all technology issues?
- Does the law fully provide for the equality and secrecy of the vote? Are legal provisions relating to ICT and NVT consistent with these principles? For example, does the law give a voter the opportunity to retain any document or data that could enable them to prove the content of the vote if they were coerced, or does the verification process associate voters with their votes?
- Does the legislation require that the NVT system retains a paper record of votes cast?
- Does the legislation provide for full verification that the results represent the authentic choices of the voters?
- What are the provisions for auditing voter-verified paper records? Are these audits conducted automatically or on request? Does the law allow voter verified paper records to be considered in conducting recounts? Which record, electronic or paper, is considered the legally binding ballot?
- Does the legislation adequately define the accountability of EMBs and vendors involved in the procurement, administration and oversight of ICT and NVT systems? To what extent does the legislation require that the actions of the election administration regarding the use of ICT and NVT be documented?
- Do the legal provisions establish what happens if ICT or NVT fail to function properly?
- What are the legal requirements in place for data protection? Do the election procedures respect these requirements, especially in the processing of sensitive data?
- Does the legal framework provide adequate timeframes for key decisions related to ICT and NVT, including procurement and testing?
- Does the legislation provide adequate and enforceable sanctions for attacks on the ICT and NVT systems?

4.4 Acquisition, procurement and the role of the vendors

One issue for the EOM and the ICT Analyst to consider is how the technology was procured or acquired. Although an EOM does not pronounce on what system was chosen, the process by which a particular technology was decided upon and implemented may provide important information for assessment.

OSCE participating States are acquiring their ICT and NVT systems in different ways. In some cases, authorities have developed the technology themselves, often in co-operation with private or public companies. In other cases, they have purchased or leased existing systems from private vendors. No matter the source, the background and experience of the vendor or developer should be considered. If the vendor has little experience with the technologies, or if previous experiences have demonstrated serious flaws with its technology or its application, then there may be cause for concern. Links between a vendor and any political party or public official, or other factors that may cast doubt on the perception of the vendor as a neutral supplier, may also be indicative of a flawed procurement process. It should be considered that the vendors contracted by EMBs might not be the only private actor in the delivery chain, as vendors frequently outsource the development of the parts of ICT or NVT systems to other vendors. The EOM and ICT Analyst should aim to establish all of the actors involved in delivering the ICT and NVT systems.

Another important factor to consider is the transparency of the selection process. The criteria used for selecting a particular type of system should be clearly established before selection and made publicly available. This includes not only the technical but also the procurement criteria. The EOM should try to determine whether there was an open, competitive bidding process based on pre-determined, publicly available criteria. If this was not the case, or if there are indications that the criteria were tailored to a particular vendor, the EOM should take this into account.

It is important that the EOM understands the relationships between the EMB and any vendors. In line with the international standards and good practice, while vendors often have a role in maintaining and updating ICT and NVT, due to their technical knowledge, election officials are responsible for the conduct of elections and should have full authority, oversight and accountability over technicians and the process in general. Where there is a significant degree of reliance on vendors, even on a temporary basis or through intellectual property rights to implemented products and software, observers should inquire further to assess if this reliance has fundamentally altered the ability of the election administration to properly control the implementation of voting processes. Any indication that vendors, rather than election officials, control the process is a cause for concern, as this can compromise the impartiality and independence of the election administration.

The EOM should look into whether essential parts of the electoral process are outsourced to vendors and suppliers and the scope of the vendors' liability and responsibilities. The vendor should have a continuing responsibility to maintain and service the system. This includes addressing design errors, malfunctions or other ICT problems. It should be clear that the role of the vendors and suppliers is limited only to supporting the conduct of democratic elections. The EOM should also establish the vendors' responsibility in the process of the ICT and NVT delivery; in particular, who is responsible for handling incidents on election day, who is legally responsible for non-delivery, accidents or system failure, and what accountability measures are envisaged in the contract between the EMB and the vendor.

Possible questions:

- Who developed and produced the ICT or the NVT?
- Who owns the technology? How long is the contract between the EMB and the vendor? Does the contract contain security or maintenance fees or costs for data storage that result in higher, long-term costs?
- What is the extent of vendor (or other external organizations') involvement in the management and operation of NVT? Does this involvement compromise the impartiality or independence of the election administration? What accountability provisions are in place for vendors?
- Who is responsible for handling incidents on election day; the EMB or the vendor, and who is legally responsible?
- In addition to meeting technical and procurement requirements, does the selected vendor have prior experience with technology systems used in elections?
- Does the vendor or developer have any links to any political parties, candidates, political figures or public officials? If so, have any interlocutors raised concerns about these links?
- When all stages and phases of the tendering process are viewed as a whole, was the process transparent and subject to public scrutiny? What was the duration of the tendering process?
- Was the selection process open so that all vendors had the opportunity to participate or, does it appear that the process was tailored to a particular vendor?
- What legal or contractual provisions are in place regarding the maintenance and update of NVT? What is the contractual relation between the vendors and the EMB? Where are the servers for storing data located?

4.5 Certification

Certification is a process of evaluating whether a given technological system satisfies previously established standards and legal requirements. The certification process may cover hardware and software, but also operating systems, management processes and personnel. It is not the task of an EOM to certify any particular technology. It is the responsibility of the public administration of a country to ensure that the ICT and NVT system has been properly certified before it is used in elections. However, the EOM should assess the certification process. In doing so, the EOM should review relevant certification documentation, establish which components or functions of a given technology and processes have been certified, and understand the views of different parties, citizen observers, the academic community and other technical experts.

Certification requirements or criteria should exist before the technology is introduced, rather than being tailored to match the specific system. While certification is generally a requirement for voting systems, other 'ancillary' election ICT, such as EVRVS or their components, may increasingly become subject to certification procedures. These requirements should be public and in line with relevant national legal provisions and international standards. While, in most cases, the certification process takes place before the deployment of the EOM, the ICT Analyst should try to determine how specific the standards are, and to what extent the certifying body has latitude in assessing compliance with the requirements. Over time, certification requirements may become outdated, and changes in technology may create issues that were not previously addressed by the standards. Potential gaps in certification requirements, including cyber-vulnerability of technology should, therefore, also be identified.

Since the certifying body is part of the certification process itself, information about the certifying body is relevant to the EOM. In order for certification to be meaningful, the certification body should be competent and independent from vendors, suppliers and election administrators. The EOM should make an assessment, determining the experience of the certifying body, whether the certifying body is itself accredited, the source of funding for the certification process and the views of experts, observers, civil society and political parties.

Consideration should also be given as to how the certifying body conducted the certification process and whether the certification was meaningful; the steps taken, the personnel involved and the amount of time devoted to the certification process are all potential indicators. Another indicator is whether the remuneration provided to the body was sufficient to allow a robust certification process. The EOM should also attempt to determine whether the certification body had full access to all information regarding the system, and that no information was withheld on security or proprietary grounds. The EOM should also check whether the certification body required the vendor or manufacturer to modify any hardware or software in order to meet cer-

tification standards and, if there were modifications, whether these changes have been certified. The ICT Analyst should assess the rules regarding de-certification and re-certification, or their absence.

Lastly, the EOM should check if the EMBs bear the ultimate responsibility for any required certification and whether the certification reports are available to academic institutions, citizen observer groups, candidates and political parties, and what their views are.

Possible questions:

- Were certification standards determined before the technology was acquired, or do they appear to have been tailored to an existing system?
- Are the certification requirements publicly available? Do they fully match legal provisions regarding the use of technology and electoral rules? Are the criteria sufficiently specific?
- Are there any significant gaps in the certification requirements?
- To what extent was the certification process meaningful? Were sufficient resources available to the certification body, including time? Did it have full access to documentation? Was the remuneration sufficient to ensure a meaningful certification process?
- To what extent is the certification body truly independent? Is it accredited? How is it funded? How is it perceived by national interlocutors?
- Did the certification body require any modifications to the ICT or NVT in order for it to meet certification criteria? Were any modifications made? If so, were they certified?
- If no formal certification process exists, are there any means available to EMBs, political parties and other national interlocutors to ensure that the NVT system will perform correctly?
- Can observers verify that the system used in the election is the same as the certified system?[50]
- Is complete documentation about the evaluation and certification available to the EOM? Is it available to political parties, civil society, and others? What is their assessment?
- What are the views of electoral administrators, political contenders, civil society groups, academics and other stakeholders about the certification process?

50 For example, this can be done by checking the digital signatures. A digital signature is a mathematical function that allows anyone to verify the authenticity and integrity of a given message, file or software. It proves that it was signed by a known signatory (authenticity) and has not been altered since the point of signature (integrity).

4.6 Accessibility of technology and participation of persons with disabilities

The introduction of ICT and NVT can have numerous benefits and contribute to the independent participation of persons with disabilities on equal grounds as called for by international instruments. At the same time, the introduction of technology in an election process risks further marginalizing persons with disabilities if their needs are not considered when choosing the technology and developing the tools. It is important that the EOM looks closely at how the introduction of technology enhances or detracts from the participation of persons with disabilities whether as voters or candidates.

The EOM should analyse a basic set of data on the use of technology in the election. If ICT or NVT devices are used in polling stations, it is important to know how many polling stations are equipped with the devices, where are they located, how many voters are affected and whether they represent a particular group (e.g., a national minority or persons with disabilities). Specific to NVT, it is also important to know whether voters in selected areas will be provided with alternative voting methods, such as paper ballots. Similar information should be gathered for the EVRVS devices and if i-voting or another remote electronic voting method is used.

One of the expected benefits for introducing ICT-based solutions is that these can enable voters with disabilities to participate in the electoral processes without special assistance. The 2008 UN Convention on the Rights of Persons with Disabilities (CRPD) requires Member States "to promote the availability and use of new technologies, including information and communications technologies, mobility aids, devices and assistive technologies, suitable for persons with disabilities" and, explicitly in relation to the participation in political and public life, to "guarantee to persons with disabilities political rights and the opportunity to enjoy them on an equal basis with others."[51]

51 See the Convention on the Rights of Persons with Disabilities (CRPD), (A/RES/61/106), United Nations, New York, entry into force on 3 May 2008.

CRPD Article 29 — Participation in political and public life[52]

States Parties shall guarantee to persons with disabilities political rights and the opportunity to enjoy them on an equal basis with others, and shall undertake:

a) To ensure that persons with disabilities can effectively and fully participate in political and public life on an equal basis with others, directly or through freely chosen representatives, including the right and opportunity for persons with disabilities to vote and be elected, inter alia, by:

i. Ensuring that voting procedures, facilities and materials are appropriate, accessible and easy to understand and use;

ii. Protecting the right of persons with disabilities to vote by secret ballot in elections and public referendums without intimidation, and to stand for elections, to effectively hold office and perform all public functions at all levels of government, facilitating the use of assistive and new technologies where appropriate;

iii. Guaranteeing the free expression of the will of persons with disabilities as electors and to this end, where necessary, at their request, allowing assistance in voting by a person of their own choice;

b) To promote actively an environment in which persons with disabilities can effectively and fully participate in the conduct of public affairs, without discrimination and on an equal basis with others, and encourage their participation in public affairs, including:

i. Participation in non-governmental organizations and associations concerned with the public and political life of the country, and in the activities and administration of political parties;

ii. Forming and joining organizations of persons with disabilities to represent persons with disabilities at international, national, regional and local levels.

Specific to the voting process, the Convention requires states "to ensure that voting procedures, facilities and materials are appropriate, accessible and easy to understand and use" and to protect "the right of persons with disabilities to vote by secret ballot". The 2017 Council of Europe Recommendation on Electronic Voting, which provides guidance and sets basic standards for the States when introducing ICT solutions in voting and counting process, recommends that "the e-voting system shall

52 CRPD.

be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently."[53]

All ODIHR EOMs should assess the inclusion of persons with disabilities in public and political life and the measures that OSCE participating States are undertaking to enhance their participation. For contexts where new technologies are introduced or already used in electoral processes, the EOM should assess how the international obligations related to the rights of persons with disabilities are implemented, what are the specific legal and practical measures undertaken and, ultimately, what their impact is on these groups of voters. Moreover, the EOM should assess whether the ICT solutions are user-friendly and provide for the broad inclusion in the electoral process of persons with disabilities or if voters with specific disabilities are excluded. Another important aspect for the ICT analyst and the EOM is to assess the level of consultation with organizations working on the participation of persons with disabilities in the decision-making process for the introduction of ICT and NVT and the development of the tools.

When technology is introduced in an election process, it is important that voters and all election stakeholders are educated about the technology and its proper use. Together with the Election Analyst, the ICT Analyst should assess how people with various disabilities are educated about the new technology, looking at whether voter information is available in accessible formats and if there is any targeted voter education programme for them about the technology being used in the election process.

An EOM should also look at the impact of other technology introduced into an election process, for example for EVRVS, campaign finance reporting or submission of election complaints (*see Chapter 6*, *Observation and assessment of 'Ancillary' ICT-based election systems and processes*). ICT tools introduced for these processes can facilitate the participation of candidates with disabilities if accessibility is considered in the development. To increase voter and candidate access to effective remedy, online complaint forms should be available in easy-to-read and understand formats.

53 See Council of Europe Recommendation CM/Rec(2017)5 on standards for e-voting and other supporting documents.

Possible questions:

- What is the scope of ICT and NVT devices used in the election?
- What percentage of polling stations will use NVT and what percentage will use paper voting (or both)? Will voters in polling stations using NVT devices be able to vote by paper ballot if they prefer this method?
- If Internet voting or other remote electronic voting technologies are in use, what percentage of voters will have access to this technology? If such use is limited, what criteria are used by the EMB? Is this use limited to any geographic region or voter group (e.g., a national minority, persons with disabilities or out-of-country voters)? If so, what are the reasons for these limits?
- Are measures for backup and equipment repair guarantees provided?
- Does the technology have special features which can enhance participation and access for persons with disabilities such as audio aides, language support choice, font increase, high contrast, universal plug for a personal assistive device or others? For which aspects of the election process are these tools available (NVT or other 'ancillary' ICT election-related processes?
- To what extent were voter information and education campaigns addressed and tailored to the needs for persons with disabilities? In what formats were the voter education campaign materials made available?
- Were representatives of the organizations representing persons with disabilities included in the legislative consultations and decision-making processes when introducing ICT?
- Were feasibility studies conducted to assess the impact of introducing NVT or ICT in electoral process on persons with disabilities? Does the EMB gathers statistics on the participation of persons with disabilities during elections?

4.7 Observer access, documentation and other transparency measures

An integral part of the assessment of the use of ICT and NVT is the transparency of the system which is also a crucial element for building public confidence. Transparency can be affected by different factors. Where any component or process of the system is secret or protected by law from disclosure, overall transparency decreases. As elections are a public process exercised collectively by and for voters to realize their basic human rights, the technology used should not be kept secret by a private agreement between a vendor and the state authorities. The EOM should, therefore, carefully examine how observers, party representatives and voters can observe all technological elements of an election process (whether voting or 'ancillary' processes), as well as how the EMB and the judiciary fulfil their oversight obligations.

Whilst not all aspects of technology can be directly observed, there are a number of activities that can be assessed, and which should be open to observers. These include the activities of election administrators and vendors in specifying, procuring, deploying, setting up and modifying the system, and the activities of certification, testing and audit authorities. In this respect, the EOM should consider what aspects of the process can be observed and whether observers are given sufficient access to do so.

The EOM should note whether observers use the opportunities available to them. This is important for establishing whether the ICT and NVT are not just verifiable, but actually verified. The reasons given for not observing may be of interest. For example, political parties or civil society groups may state that they do not have the capacity to observe effectively, or they may report that the access provided does not afford meaningful insight into the operation of the system. On the other hand, they may state that they trust the use of the technology with or without proper consideration of the details. All such circumstances should be accounted for in an EOM's assessment.

Consideration should also be given to any efforts made by the election administration or vendors to maximize transparency. An important element of background analysis is to identify what documents are available. The existence of relevant documentation does not conclusively prove the reliability of the technology; however, their absence may be an indication of problems. EOMs should not sign any non-disclosure agreements in order to see documents or to observe processes related to technology, since this could compromise an EOM's ability to report independently and in an unbiased manner.

Other aspects that can contribute to transparency are the opportunity for the observation of testing and review of source codes. This could include offering citizen observers and political parties the opportunity to access or test the technology independently.[54] At a minimum, the results of testing should be made publicly available to these groups. While opportunities for external testing may necessarily be limited due to security, logistical and time constraints, the existence of such testing is an indicator of transparency. With respect to the source code, it is important for the EOM to determine if any meaningful assessment has been made by others and to evaluate their conclusions. Transparency is enhanced if the source code is a matter of public information and the EOM should determine if the source code is available publicly, or at least to registered observers or other relevant groups.

With NVT, a key transparency measure remains — that polling stations and higher EMB levels produce paper protocols of their result, so that political parties, candidates and citizen observers can check the results at lower levels against the centrally-recorded electronic results. If different voting methods are in use, results protocols

54 ODIHR observers should only observe the testing and not test the ICT or NVT equipment themselves.

should provide the results for each voting channel (unless publishing such granular information could result in a breach of the principle of secret suffrage). The EOM should ascertain whether this is a requirement. Some observation methods, especially the review of documentation, may need advance preparation in order to be effective.

Possible questions:

- In what ways does the law provide for observer access to ICT and NVT?
- Are all processes related to the use of the ICT and NVT open to observation by the EOM and by citizen observers? Are there any restrictions?
- Has the EMB made efforts to facilitate observer access? What documentation is available to the EOM and to the public? How can the documentation be accessed (only physically or publicly on the Internet)?
- Are there any reports or other documents that are not available (non-existent or considered secret)? Is there any information or documentation that the election administration itself does not have access to?
- Is the source code for the software publicly available? If so, has it been checked by any group? Is there a mechanism for verifying that the source code is the one actually used on election day?
- Are results protocols available to observers and political parties at each level, including at the polling station level? Are they printed and available online? Do they allow for meaningful verification (e.g., by specifying the election results for different voting methods)?

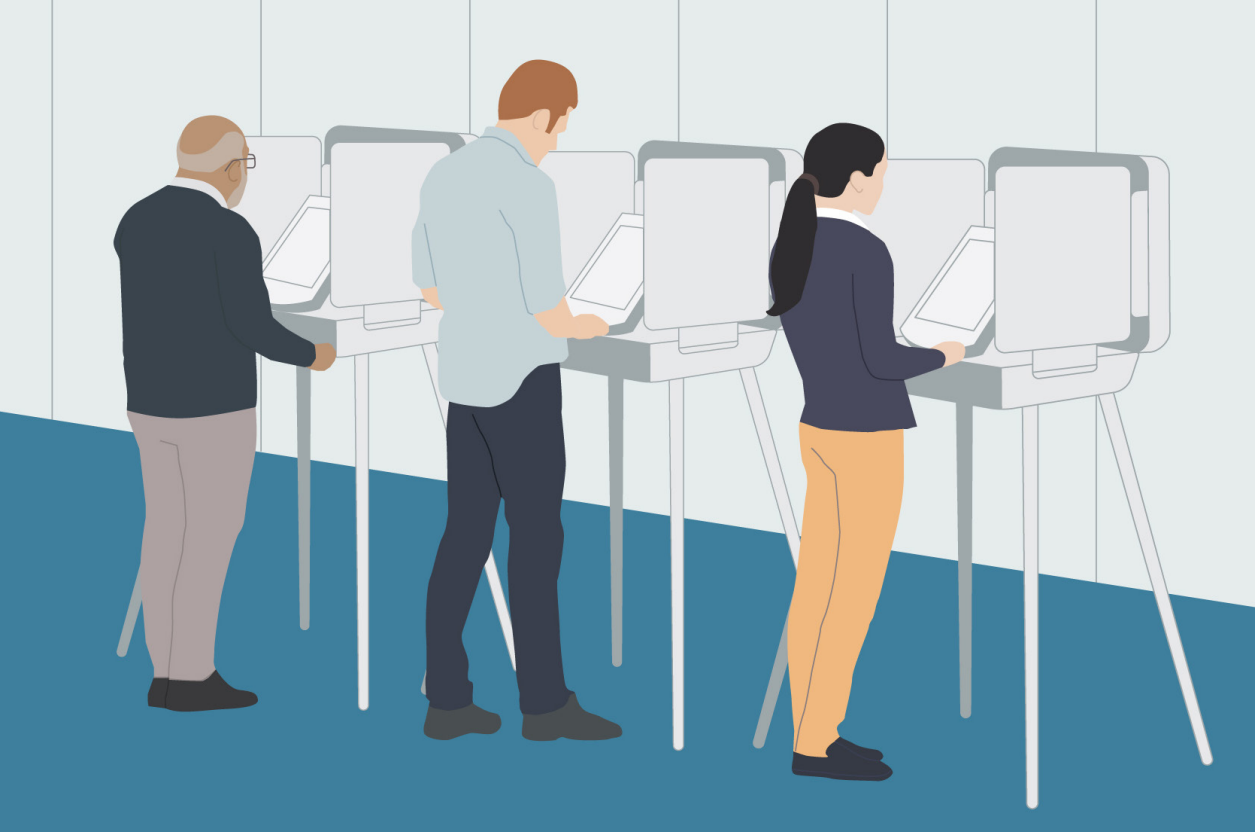
4.8 Election dispute resolution and the role of the judiciary

EOMs should give special attention to the assessment of the legal framework for EDR and to observe the effect of the complaints and appeals process on ICT and NVT issues in practice. Such challenges may be related to the use of the system itself during the voting and counting process, or they may be about other ICT elements. Although technology enables the rapid reporting of results, this should not preclude the possibility to appeal decisions or to challenge results, and the deadlines established by law should reflect appropriately this right. In the event of a successful legal challenge to the results, there should be a legal basis for conducting an audit or recount, and for which body has the authority to order them. A recount may be required if there is a complaint claiming evidence of an anomaly or failure that could have affected the results. The EOM should assess if the EDR deadlines allow for meaningful examination of the ICT and NVT issues and whether complainants have access to relevant documentation and evidence to present a case.

In this emerging field of technology, the oversight role of the judiciary is vital. As the use of ICT in elections becomes more widespread, the number of election challenges on this subject will also increase, which could lead to the overturning of results or re-running of contests. All this shows the fundamental impact the judiciary can have on electoral integrity and public confidence. Several EOM analysts, including the legal, ICT, election and political analysts, as well as the LTOs should be involved in the comprehensive assessment of the effectiveness of the EDR process and the role of the judiciary. To get a proper understanding of these areas, the EOM should evaluate a number of aspects, such as how much knowledge the electoral stakeholders have about the ICT system being proposed/implemented; whether they have the knowledge and skills to lodge properly grounded complaints; whether credible experts can be found to act as expert witnesses in any trial; whether justices are properly trained and supported in this aspect of their role; whether specialized chambers exist for consideration of ICT, NVT or general EDR complaints; and whether all documentation is available to make a sound judgements.

Possible questions:

- Do the legal provisions allow for effective review of technology-related complaints? Who is entitled to file a complaint? What can be considered evidence?
- Has the use of ICT or NVT previously been challenged in court? If so, on what grounds, and how were the cases resolved?
- Do electoral stakeholders have the technical knowledge to bring complaints before the courts about any relevant issues?
- Was any complaint lodged in relation to the procurement of ICT or NVT? Are all levels of documentation fully available to all parties to a complaint?
- How accessible is information for the judges trying the cases, including primary source information and expert witnesses with technical knowledge?
- In case of a dispute, are expert witnesses available in this field of litigation, and are they able to explain the very technical details of the technology used in a way that is understandable by the court?
- Has the judiciary had any previous training or education in this field prior to the electoral process?
- Is there a specialized chamber within the courts to deal with this type of litigation (and, if not, are justices properly supported to independently try such cases)?



Chapter 5

Observation and assessment of NVT

5.1 Role of the election administration in the use of NVT

Analysis of whether the EMB has full control over the implementation and management of the electoral process and the technology used in it is an important consideration for the EOM. In other words, the election administration should see election technology as an integral part of the election process and not as a feature to be delegated to technicians or other institutions. This chapter deals specifically with the role of the election administration in the use of NVT.

The EOM should identify which authorities are responsible for issuing NVT and other technology-related regulations, for programming and operating the systems, and for providing oversight of the electoral process and its integrity. In some countries, all tasks may fall under a single hierarchical system with one primary EMB. In others, these tasks may be decentralized, with one body (for example, a government ministry) responsible for issuing regulations, local authorities responsible for the deployment and operation of the system, and a third body responsible for ensuring that the implementation of NVT takes place in accordance with the law. While this structure may correspond to that used to conduct paper-based elections, there may be important differences that need to be acknowledged when NVT systems are used.

The EOM should also identify the structures within each EMB (departments or units) that have primary responsibility for NVT and establish the scope of their responsibilities. It would be useful to determine whether these structures are dedicated solely to the applied technology or if they also deal with other issues, such as voter lists or the production of voter education materials. If these are not dedicated structures, they may become overstretched when taking on the added role of technology management. For NVT to be implemented successfully in the electoral process, EMBs need to complete a number of formal activities and procedures, some of which would need to take place several years before the election cycle. Some of these activities are described below.

5.1.1 Re-structuring the voting process

Proper, long-term planning is a prerequisite for the successful conduct of an election, especially when using NVT. In addition to defining the technical specifications of the technology, the election administration should adapt the voting process to take explicit account of the use of NVT as an essential element, especially when they are being introduced for the first time. Changes may be required to procedures for advance voting, printing voter material, setting up voting booths and identifying voters, etc. If the management of the voting process is not reviewed and redesigned, this may have unforeseen consequences. For example, insufficient numbers of NVT devices, or voters taking more time than anticipated to vote using the devices may result in long queues. The consolidation of polling stations to accommodate limited numbers of electronic voting devices may cause problems with voter lists or lead to voter confusion about their polling locations. Alternatives to ICT solutions should be foreseen in the regulations and poll staff must be trained and prepared to use them in an emergency.

It is also important to understand that with NVT, new issues may be raised by electoral stakeholders. The EMB should anticipate how they will address these issues and standardize the procedure to ensure consistent implementation. If the EMB makes ad hoc ***decisions***, this may cast doubt on their work and may be perceived as acting arbitrarily, raising concerns about their impartiality or calling into question the integrity of the electoral process.[55]

5.1.2 Multiple voting methods

The voting process may become more complex when NVT are used in parallel to paper-voting systems. The procurement and distribution of electoral materials, management of voter lists, instructions for polling officials, training, voter education and tabulation of results will all be affected to some extent by the use of multiple voting methods or channels.

The EOM will need to check that the availability of multiple channels doesn't disenfranchise voters, nor allows them to vote more than once, nor forces them to use an electronic system against their will. This requires communication between different voting channels. For instance, in systems where paper-ballots may legally cancel and replace a vote cast via the Internet, the EOM should check that the cancelling of electronic votes has been done properly and before the votes are counted. The EOM should also establish whether voters can receive the information of whether one, or all of their votes have been cancelled and whether the process of vote cancelling is subject to public scrutiny. In any case, the systems must prevent multiple voting (casting and counting final ballots by both Internet and paper ballot) and guarantee the secrecy of the vote (the content of the vote is not known until the counting stage, and it cannot be associated with the voter).

One method of voting, in parallel to traditional polling station voting, is out-of-country voting, which adheres to specialized rules and regulations derived from the national context.[56] With the introduction of NVT and other ICT-enhanced solutions (i-voting, voter registration or signature collection abroad etc.) the EOM has to take note of the technology and procedures applied, and which principles are followed in out-of-country voting. It is also important to determine that no potential disenfranchisement of voters occurs due to the additional requirements of an electronic voting system (e.g., the need for additional technological supplies or costs related to personal identification documents) or because the NVT-enhanced solution is the only voting channel available for out-of-country voting. In addition, to ensure the security and transparency of the process, the mode and specifications of the technical connections between the

55 In some cases, the EMB may decide to adopt procedures that are analogous to those already existing for paper-based voting methods. However, NVT and ICT can generate more evidence and traceability and reasoning by analogy may not be sufficient.

56 On alternative voting methods, see Alternative voting methods and arrangements, OSCE/ODIHR, 12 October 2020.

voter list and other components of the voting system have to be evaluated and cyber-security certified (e.g., the security rate of the connections and the types of Internet connection such as landline telephone, wireless connection or dedicated close-circuit network).

Issues related to RMSs are discussed later, however it is important to note that, when assessing the use of multiple voting channels, the EOM must identify the method for transmitting the results in the paper-based system and in the NVT, and how the multiple sets of results will be aggregated. If the data from the NVT and the paper-based process are transmitted by different methods, then there is a need to aggregate the data at some point. The EOM should also establish whether the process of results aggregation is open to public scrutiny. The transparency principle should be respected at all times and the increased complexity — due to multiple systems or any resulting delays in reporting — should not be used as excuses for not providing adequate transparency. Due care should be taken to ensure that the reporting of results on different voting channels does not breach the principle of secret suffrage (e.g., for electoral districts with small number of voters).

5.1.3 Public testing

Public testing is a process for checking the functionality of an NVT system without requiring any knowledge of its inner design or logic. It is an important part of the implementation of NVT. However, the value of testing depends, in part, on the type of testing, who it is done by, and how much access is given to contestants, voters and other interested parties. The technology should be thoroughly tested sufficiently in advance prior to election day, and testing should also be done in a manner that is transparent to voters, election officials and observers.

Since much of the testing happens before an EOM is deployed, the EOM should review the documents or visual material related to any testing that has already been conducted.[57] Another source of information comes from discussions with those involved in the testing. These may include the testing authorities, vendors, certification agencies and election administrators, as well as external groups, such as academic institutions, citizen observer groups, candidates or political parties that were permitted to test the NVT. At a minimum, the EOM should check whether the testing results have been made available to these groups and what are their assessments of the results.

During testing periods, another factor that contributes to the overall trust and transparency of the NVT system is access to the source code. Transparency is enhanced if the source code is a matter of public information. The EOM should determine if the source code for all software used in the NVT (and ICT) system is publicly available, or

57 The EOM should not be involved in testing any systems or devices.

at least available to observers or other relevant groups. Making the source code open may be of limited value unless the public, including political parties, candidates and citizen observers, are able to check this source code is the one actually used in any electronic voting system. It is also possible that parts of the source code are made publicly available. Whatever source code is published, the EOM should check whether the data is well-documented, regularly updated (each release should have a version number), easy to navigate, read and understand, if it has the necessary configuration descriptions, and whether it is available for independent testing without the vendor's or EMB's involvement. Only appropriate conditions such as these, allow for independent scrutiny and meaningful observation and oversight.

The EOM could also check whether the testing of the entire system or its individual components meets design criteria, and whether all parts of the system function together as designed. Such testing is necessary to check the usability and robustness of the system, ballot design and, potentially, the adequacy of training and voter education. Public tests should involve data collection on use, identification of any problems and modification proposals in response to significant issues identified by the testing. Absence of these elements is an indicator that the test event was not a testing in the true sense of the term, but rather a voter education or publicity exercise. This process is known as end-to-end testing of the entire system. The criteria used for testing should be reviewed by the EOM for relevance and completeness. The election administration must also ensure that there is complete documentation establishing that the system has been adequately tested. The use of an NVT system that has not been fully tested, or for which there is insufficient test documentation, risks jeopardizing the election process.

The EOM should consider whether testing satisfies security measures. For instance, while software tests may be conducted in a predetermined manner, software testing can be significantly strengthened by the use of adversarial testing, in which specialists attempt to identify security weaknesses or other flaws in an unscripted manner. Similarly, NVT that rely on the Internet should be subjected to testing involving protection against DDoS attacks (see Chapter 7 on cybersecurity). Testing should always be conducted after the installation of new or upgraded software that is intended for use in upcoming elections and there should be a mechanism for validating that the software has not been modified from the certified or expected version.

In addition, the EOM should consider what plans exist for failed tests and how this is communicated to the public. These plans should include whether a distinction is made between significant and insignificant errors, how and when software is updated, if and when re-testing is foreseen, and whether the testing took place sufficiently ahead of real-time implementation. It should be noted that testing is never a guarantee that the NVT system is fully secure, nor that it will work properly on election day.

5.1.4 Risk management

The election administration should plan for unexpected problems with, or even failure of the NVT system, either for technological or human reasons. EOMs need to assess what contingency planning has been prepared by the election administration for possible system failures. This may include ensuring that electronic data is preserved and recovered in the event of physical failure (e.g., loss of electricity); identifying who is responsible for fixing the problem and the maximum response time; providing a manual to assist polling staff in addressing problems; and providing voters the opportunity to cast their ballots even if the system cannot be returned to working order. Likewise, should major problems be detected during the period for i-voting, it may be stopped several days before election day to give voters the opportunity to vote on paper. The EMBs should develop risk-mitigation strategies that will include protection measures and alternative plans in case of physical dangers (floods, loss of electricity, etc.), or technical and other cybersecurity threats, or non-delivery of the system by vendors.

The risk-mitigation strategies should standardize the actions to be taken when a risk materializes and the main criteria on which the risk-mitigation strategies are based should enjoy broad consensus. The procedures for addressing different risks should be discussed and enacted well in advance.[58] The consequences of miscommunicating the impact of a risk or a vulnerability of an NVT system may be worse than the very risk itself, so the EMB should also develop an effective communication and public relations plans for these types of situations.

5.1.5 Training EMBs and polling officials

As with paper-based systems, it is critical to train election officials in how to use NVT in a manner consistent with legal and democratic principles. Given the complexities and challenges of using NVT, extended training for polling officials is likely to be necessary. Commissioners and other polling staff must have a basic understanding of how the NVT work, so they can respond to minor and major technical problems, explain the technology and answer questions about it, inform voters and, last but not least, help build confidence in the system.

The EOM should assess the overall effectiveness of training, to the extent possible. Training plans should reflect the timelines and budgets necessary for extended training, and the methodology should focus not only on legal requirements and procedures, but also on what to do in case of problems. The EOM should observe the training of polling officials and review training materials. This may provide a better understanding of the electronic voting process and could be particularly valuable for the

58 For example, if there is a shortage of bandwidth or, due to a DDoS attack, voters could be left without the possibility to cast their vote, there should be clear procedures on extending the voting period; if the secrecy of the votes is compromised adequate procedures for dealing and deletion of the compromised votes should be in place, which might involve alternative voting methods.

STO briefing. Observation of training sessions and review of training materials could also reveal shortcomings in training that might lead to potential election day problems about which observers should be aware.

5.1.6 Voter education

Voters should generally be able to make their choices and cast ballots without assistance and therefore voter education is critical for the implementation and use of NVT. The EOM should assess the extent to which information about the system has been made available to voters and the completeness of this information, particularly when a new system is being implemented or where significant modifications have been made to an existing system. In addition, voter education should give a balanced overview of the benefits and challenges of voting by electronic means or, where both voting methods are available, by paper ballots. Special attention should be paid to whether the voter education material is also available in minority languages and accessible to voters with special needs.

Detailed information on voting procedures should be made publicly available before the election period and at polling stations on election day. In addition to being informed on how to use the NVT, voters should be informed about how the system works in general, how the secrecy of the vote is ensured and how the results can be meaningfully verified. As voters themselves will often be the first to notice any problems with a given voting machine or other application, voter education materials should include information on how to deal with potential problems (normally, the appropriate course of action is to inform a polling official or use the communication channels provided by the EMB).

Ideally, election day should not be the first occasion when a voter uses the electronic voting system. Apart from a gradual approach to introducing NVT, hands-on testing by the public prior to election day or mock elections can be an effective method of voter education.

Possible questions:

- Do the EMBs have full managerial control and oversight of the NVT process? How is the management of NVT structured within the election administration? Are the roles and responsibilities clearly defined? Are there departments or units in the election administration dedicated to NVT? How does the management of NVT function in practice?
- What level of understanding do election officials have of NVT, both in practice and in general? To what degree are they involved in oversight of the use of NVT? Do they have any concerns about the use of NVT in the election?
- How thorough is the election administration's planning for the introduction and use of NVT? Have election officials received information, materials, and financial resources sufficiently in advance to enable them to manage the system appropriately? Have contingency plans been made for potential breakdowns of the technology or for problems in the deployment and use of NVT?
- If multiple voting methods are used, has the election administration taken into account the different requirements of these methods for distribution of materials, instructions for polling officials and electoral deadlines?
- Are measures in place to prevent voters from multiple voting by using different voting methods?
- How will results from paper ballots and electronic ballots be tabulated? Do political parties, candidates and observers have access to the results at each stage of the counting and tabulation process? Is the publication of results detailed and complete?
- What measures are in place to ensure secrecy of the vote (both in NVT and traditional voting)?
- How do NVT address the situation when a candidate is de-registered or pulls out of an election?
- Are ICT solutions used as the primary voting method for out-of-country voting? In cases of Internet voting, how may out-of-country voters participate (including registration, receipt of voting credentials, etc.)? Are the training and information policies similar to in-country voting?
- Has the election administration ensured that the NVT system has been completely tested and reviewed before use? Has end-to-end testing been conducted, including transfer of data between multiple information systems, or have only the individual components been tested?
- Is complete documentation about testing available to the EOM? Is it available to political parties, civil society and others? What is their assessment?

- How rigorous does the testing appear to have been? Has software gone through adversarial testing? Was testing done after new or upgraded system components were installed?
- Was official testing observed by outside groups? Did any external group have the opportunity to conduct their own tests? If so, under what conditions?
- Were tests conducted in mock elections or in binding elections? Were any problems identified in the testing? If so, how were they addressed?
- Has the source code used for the NVT (or ICT) been made publicly available? Was it reviewed by the expert community or other interested stakeholders? If vulnerabilities or errors were disclosed during the review of the source code, how have they been handled?
- Does the training ensure that election officials are able to manage polling procedures? Does training on the operation of NVT cover their interaction with other parts of the process?
- How are voters being educated on NVT? Do educational materials go through each step of the voting process? Is hands-on testing available to the public? If so, how well did voters appear to understand the voting process? Were any problems observed? In case ICT is used in other processes where the voter is directly involved (i.e., signatures or biometric data for voter identification and list population in the polling station), is the voter information sufficient?
- To what extent are voter education materials presented in the media? Are they available from multiple sources and throughout the country? Are the materials adjusted for the needs of different categories of voters, including for different vulnerable groups?
- Does the EMB have procedures for handling voters who claim not to have voted but the system shows that their vote is already cast? What is the EMB procedure for voters that claim that their voting receipt is not included amongst those registered by the NVT system?
- Are there procedures in place for voters who claim that the NVT system shows a different choice than the one they have made? What happens if it is not possible to verify the universal recorded-as-cast proofs generated by the NVT system?
- How will the EMB deal with votes that cannot be decrypted due to a malfunction with the encryption method (e.g., digital certificates, software versions, etc.)?

5.2 Voter access, usability, ballot design and reliability

Voters should be presented with clear choices, and the universality of suffrage should be maximized. At the same time, essential safeguards should be in place to protect electoral integrity. The EOM should carefully consider the extent to which NVT systems are accessible, understandable and usable by voters. The main aspects that should be assessed in this respect are the user-friendliness of the technology, ballot design, the ability of the NVT to accommodate all voters and the robustness of the system in terms of malfunction or voter error. In order to assess these aspects, the EOM should attend public and closed pre-election tests, analyse voter education materials and election statistics and conduct interviews with relevant stakeholders.

5.2.1 Accessibility

One of the advantages of NVT is that they can increase access for voters, especially those with special needs. NVT systems should be designed to allow all voters, including those with disabilities, to cast their ballots, to the extent possible, without assistance. Consideration should also be given to whether a voter can use NVT in a minority language. Where it is possible to vote in a minority language, the EOM should verify that the minority-language ballot contains the same information and is in the same format as the majority-language ballot. Any special modalities, such as audio ballots for the visually impaired and illiterate or the use of ballots in a minority language, should not have the potential to compromise the secrecy of the vote. This means that the content of the vote should be electronically recorded independently of the method used to mark the electronic ballot.

Particular attention should be given by the EOM to cases of eligibility for voting and accessibility of other specific groups (e.g., illiterate voters, marginalized groups and vulnerable communities, migrant workers, etc.). The EOM should determine if there are rules concerning possible access restrictions to polling, such as for instance any additional costs or cumbersome procedures of identification or registration for electronic means of voting (e.g., need for special ID documentation or special permits for electronic voting). The regulation should follow similar principles as stipulated for traditional voting methods.

5.2.2 Usability

NVT systems should be created in such a way that they are simple to use and facilitate the voting process. The usability of NVT will generally be correlated to overall computer literacy in a country, the scope of voter education efforts and the opportunity for public testing of devices before elections. The NVT system should not allow voters to switch off the device or application, nor to undertake any action that would prevent

them from casting their ballots. To facilitate voting, the size of the screen, brightness and legibility of the display should all be considered. If touch screens are used, the ease with which selections can be made should also be considered, as well as any potential over-sensitivity of the system that could result erroneous choices being recorded.

Just as important as physical design, the EOM should consider if the NVT system provides voters with feedback when the electronic ballot is about to be cast and confirmation that the vote has, indeed, been cast and when the voting process is finished. The system should inform the voter if they are going to cast an invalid ballot (e.g., if they have made more selections than they are entitled to, also known as over-voting). Ideally, the system will also notify the voter of an 'under-vote', 'over-vote' or any other unintentional mistakes and provide the opportunity to change their previous choice before finalizing the voting process. The usability of the NVT should also take into account how much time it takes for a voter to complete the process, together with the overall number of voters in the polling station. There should be sufficient devices available so that voters do not face unreasonable waiting times.

5.2.3 Ballot design

As with paper ballots, ballot design is often of crucial importance in NVT as design problems can cause voter confusion or bias in favour of certain parties or candidates. In general, the same principles that apply to the design of paper ballots apply to the design of electronic ballots. Ballot design is determined, in part, by the electoral system, type of elections or registration of candidates, which may not be concluded until shortly before an election. The EOM should consider whether candidates or parties are presented equitably on the ballot and whether all information required by law is presented. All candidates or parties contesting the election should be given an equal amount of space on the electronic ballot and it should be possible to see all the available choices at the same time before the ballot is cast.

After the election administration has determined the electronic ballot format, the EOM should assess whether voters may experience any difficulties in voting due to the ballot format. Ballots that exceed the size of the screen, thus requiring the voter to scroll or change screens to see the entire range of choices, can confuse voters and favour contestants that are displayed first. Therefore, the need to scroll or switch the screen must be clearly indicated and well communicated to the voter.

For instance, for parliamentary elections, a nationwide, proportional system with closed lists may require only one type of ballot, used by all voters. A preferential list system allows voters to choose one or more candidates within a list, or even across multiple lists. A constituency-based system, whether multi-mandate or single-man-

date, will require different ballots for each constituency. Multiple elections conducted simultaneously, such as local and regional elections, will require ballots for each constituency. All of these impact the ease with which NVT can be implemented.

Regardless of the relative complexity of the electoral system, it is important that every voter in a given constituency receives the correct ballot. Uploading the ballot can be done by different technical means and can happen centrally or at a lower level. An important consideration is that uploading data entails certain cybersecurity risks and should be done according to a pre-determined protocol available to observers. In contrast to paper ballots, which are not always restricted by size, the size of computer screens limits the number of options that can be shown at one time.

As for paper ballots, the regulations for last-minute changes to the candidate list (e.g., death or withdrawal of a candidate) should be inspected, especially as to how these regulations are implemented in practice at the device level (e.g., would re-programming be needed for ballot changes).

5.2.4 Reliability

NVT devices must be able to function for the entire duration of the voting process. The EOM should observe whether there are situations where extensive malfunctions, power outages, lengthy set-up times or other technical problems prevent voters from casting their vote, discourage them from doing so, or cause votes already cast to be lost. The EOM should, therefore, consider how the voting device is protected against foreseeable malfunction, whether basic problems can be repaired easily by election officials and whether officials have been adequately trained to deal with problems that may arise.

For Internet voting, in which server failures or other system unavailability could prevent large numbers of voters from casting their ballots, the EOM should determine what measures are in place to ensure the availability of the system.

Possible questions:

- How are the NVT protected against physical damage or other problems, such as loss of electricity?
- Can basic problems be addressed by election officials? If so, how is that arranged? Have officials been adequately trained to deal with problems?
- What kinds of ICT systems are used by the election administration? How compatible are the different kinds of software being used to manage the election process and to run the NVT? Have tests been conducted to ensure that data is transferred smoothly across interfaces between different software?

5.3 Voting process — casting, security and secrecy of the vote

5.3.1 Casting votes

As indicated above, voters should receive clear feedback while interacting with the technology and should be made aware of when the electronic ballot is about to be cast. Voters should then receive confirmation that the vote has, indeed, been cast and that the voting process is finished. The EOM should check that the NVT system clearly indicates what choice a voter has made before the ballot is cast and that it allows the voter to correct mistakes. If the recording or transmission of the vote takes time to complete, the NVT should inform the voter of this, so that they do not inadvertently terminate the process.

The EOM should assess how NVT advises the voter if they have cast an invalid e-vote. For example, they should check how the systems deal with unintentional mistakes or 'under-votes' —, i.e., when the voter does not make a choice in a particular race or makes fewer than the permitted number of choices. The system should be designed to notify the voter of an 'under-vote' or 'over-vote' or to give the opportunity to change their choice. The voter may also intentionally choose not to vote in a specific race.

In some systems, the possibility of a 'blank vote' is explicitly provided for. If not, the refusal to make a choice for a given race should not prevent the voter from completing the voting process. However, the NVT system should inform voters in case of 'over-voting' — i.e., making too many choices and thereby invalidating the ballot — and it should do so in a way that allows the voter to understand and correct the error. The EOM may also assess whether intentional spoiled electronic ballots are provided for in the law and how the NVT system deals with these votes.

A relatively frequent occurrence, especially when NVT are first introduced, is that voters may terminate the process before finally casting their electronic ballot. This may occur unintentionally, because the voter mistakenly believes that the vote has already been cast, or intentionally, often because the voter does not understand the system and is reluctant to request assistance. The EOM should check the NVT features for these situations and whether the device properly indicates the end of the voting process, resets after a certain amount of time, or whether an election official must intervene. If the intervention of an election official is required, the rules should be clearly defined in advance, including how the intervening official is selected. In any case, any intervention by an official should respect the secrecy of the vote. The EOM can note how often this occurs during observations and attempt to identify how often the voting process is terminated during the election by asking the polling staff, although such data may not be known to election officials.

5.3.2 Secrecy of the vote

Special attention needs to be given to protecting the secrecy of the vote when introducing NVT. When digital technologies are used to cast the vote, even the recording of metadata (e.g., about when a vote has been cast) could be used to link the contents of a vote to the voter who has cast it. For this reason, it is of utmost importance to adopt technological and procedural measures that will ensure the confidentiality and anonymity of the vote. In the case of i-voting, asymmetric encryption at the application level can be used to render the votes cast unintelligible, thus ensuring confidentiality. Before the votes are decrypted, anonymization measures can be used (e.g., mix-nets, which shuffle the votes and break the correlation between the votes received by the voting server and the mixed ones, or homomorphic encryption, which allows votes to be counted while still encrypted).[59] These measures may be supplemented by additional guarantees, such as conducting the decryption offline and in different machines, and by splitting the decryption key between different members of an electoral board.

Furthermore, in the case of i-voting, the EMB may decide to adopt additional measures to mitigate the risks associated with casting votes from uncontrolled environments (e.g., coercion, intimidation, and vote-buying). Voters can be given the option to cast several votes using the i-voting system, or even to cancel any i-vote by voting on paper in polling stations before the voting period is concluded. The EOM should analyse whether concerns about voting from uncontrolled environments have been taken into account and if these alternatives have been considered.

5.3.3 Security and integrity of the vote

While comprehensive guidance for assessing broader ICT-related cybersecurity threats is given in chapter 7 of the Handbook, it should be noted that, specifically for the voting and counting processes, the EOM should check that the NVT system includes robust security measures against potential threats and that the legal framework regulates measures to be taken against such attacks. Even when the basic architecture of the system is appropriately designed to safeguard the secrecy and integrity of the results, NVT will still be subject to a number of potential security threats. These threats may be external to the system, such as hacking, or may come from within, such as manipulation by election officials, vendor, or other technicians. While security threats also exist in traditional paper voting processes, a key difference is that, in order to be detected or observed, attacks on NVT may require technical skills and significant resources not possessed by the typical voter.

59 Since in i-voting, encrypted votes tend also to be digitally signed to ensure voter eligibility, it is of utmost importance that these processes are conducted before the decryption or the counting. Otherwise, an internal attacker could have enough information to breach the anonymity of the ballots, for example, by looking at the order in which the votes have been cast.

Safeguarding the secrecy of the vote and ensuring the integrity of the results in a verifiable manner must be part of the design of the NVT system. These principles can be adversely affected by technological or design flaws. The integrity of the process is violated when the system does not properly record or count the choice made by the voter. Software bugs that cause errors in vote counting or tabulation for any candidate would damage the integrity of the results. Some of the measures described above, such as VVPAT or individual verifiability mechanisms for i-voting, would help voters identify some of these irregularities.

If the NVT system is responsible for ascertaining the identity of the voter, special attention should be paid to preventing attempts of voter impersonation. This issue is a key concern when voters are given the option to cast their vote from unsupervised or uncontrolled environments.[60] The EMB needs to balance the need for accurate voter authentication with issues of accessibility and usability, since the most advanced voter authentication mechanisms may disenfranchise voters if they are asked to provide advanced or specific technologies for voter authentication or if they need to receive voting credentials at the time of voting. In the case of i-voting, it is also advisable to check the eligibility of the voter twice: once when voters access the voting platform and again before the counting stage, for example, by verifying the signatures of the votes cast and stored in the digital ballot box. EVRVS are discussed in later chapters of the Handbook.

Possible questions:

- Does the NVT system indicate when the vote is about to be cast and confirm that it has been cast? Does it show which choice was selected and give the voter the opportunity to make changes?
- Are measures in place to allow voters to avoid undue influence, such as the ability to re-cast a ballot electronically or cancel an electronic vote by casting a paper ballot? Are these measures effective?
- How do the NVT deal with 'under-votes', 'over-votes' and termination of the voting process? Do they allow for blank or invalid ballots?
- Do the NVT ensure the secrecy of the vote?
- Does the NVT system allow a voter to be identified with their vote, or allow for a voter to be directly intimidated or influenced in their choice?
- What safeguards are in place to prevent hacking? If NVT are used in polling stations, are these transported and stored in a secure manner? Is there a protocol for handling the devices? Is there any documentation regarding who has had access to the devices since their last use? When were the last updates made to the software and by whom?

60 There are different mechanisms that EMBs use to verify the identity of the voter in these cases. They may rely on existing infrastructure for citizen authentication, or they may decide to introduce ad hoc authentication mechanisms (such as voter credentials) which may be sent to the voter using different means (by post, by email, by SMS, etc.).

- Who or what institution is responsible for providing cybersecurity and intrusion resilience?
- Do the devices have any readily-accessible interfaces, such as USB ports? If so, how are these secured? What capacity do the devices have for receiving data from external sources? Can they be accessed by Internet, or wireless means? If so, what protection measures are in place to ensure data integrity?

5.4 Counting process and verification methods

A crucial aspect of NVT systems is the ability to verify that the technology has performed as envisaged. In particular, it should be possible to verify that the results are the honest tabulation of all voter choices. While it is not the role of an EOM to conduct verification, it should be able to assess whether full and meaningful verification is possible and to observe the verification process. Meaningful verification in the context of the use of NVT means that the votes are cast as intended (individual verification) and counted as recorded (universal verification).

As described at the beginning of the Handbook, there are different ways of conducting verification, and these may be performed in various combinations, depending on the technology in use. Observers should be aware of the limits of verification methods, and the EOM should carefully consider how verification is done and whether there are any gaps in the verification process that could allow malfeasance or errors to remain undetected. Voting and counting procedures that rely solely on trust in the honesty of election officials and vendors cannot be assessed as meeting OSCE commitments for democratic elections.

5.4.1 Election results audits

While aspects of the functioning of the technology are often subject to audit and verification, counting audits, which guarantee the accuracy and integrity of election results (e.g., risk-limiting audits), are increasingly used across the OSCE region and can contribute to building public confidence in the elections. The EOM should determine what audits are required by law or other regulations, whether these audits are conducted by independent bodies and when the post-election audits are required, i.e., before or after the certification of the election results. The EOM should observe the conduct of audits wherever possible.

The EOM should check whether audit criteria and mechanisms provide relevant information for the NVT system, from the specific voting device to the tabulation of results. Audit mechanisms should preserve the secrecy of the ballot but should also reveal whether any violations of secrecy of the ballot have taken place. Additionally, in case

of complex post-election audits, attention should be paid to any reports of incorrect use of the foreseen method. The EOM should consider whether representatives of political parties, candidates, citizen observers and other interested parties are allowed to be present during audits or can send their own auditors.

Should an audit reveal any discrepancies, another consideration for the EOM is whether additional action is required by law and what effect, if any, this has on the results. An audit is of little value if it does not require some form of corrective action in case of discrepancies.

5.4.2 Voter-Verified Paper Audit Trails (VVPAT)

When DRE devices are used, verifiability can, in principle, be achieved through the use of a VVPAT: the paper record for any or all devices can be compared with the electronic results through partial or full recounts. Although the use of a VVPAT ensures that a crosscheck is available for electronic results, it must be implemented properly to achieve the goals of transparency and to ensure public confidence.

If the NVT system produces a paper record, the EOM should consider a number of aspects. First, the EOM should check whether the paper record can be verified by the voter before the electronic ballot is actually cast. The voter's choice should be clearly indicated and easily visible for the voter and should not be in the form of a machine-readable code or other marks that the voter cannot interpret. The EOM should consider if mechanisms are provided for visually-impaired or illiterate voters to verify their ballot. Voters should be able to cancel the vote and revote if the paper record does not match what the voter believes they have chosen. The EOM should also assess whether the voters have been informed about the functionality of the VVPAT and, therefore, know what they should verify.

A second aspect that is important to observe is the way in which the VVPAT ensures the secrecy of the vote. For instance, paper records that are maintained in a continuous scroll could allow votes to be associated with individual voters.

Third, technical issues, such as the type of paper, printing, cutting and depositing the paper in the ballot box, can significantly impact the effectiveness of the VVPAT. For example, printers can malfunction or run out of ink and paper. If problems are not detected and corrected quickly, the utility of the VVPAT is limited. A paper record must also be of sufficient quality to permit a recount.

Fourth, some NVT systems print VVPAT records and then the voters have to take them and put them into a physical ballot box. Sometimes voters accidently or intentionally take these VVPAT records with them. The EOM should establish what proce-

dures are in place for preventing this and assess how that may impact the subsequent management of the receipts and the accuracy of the recount.

A fifth important consideration for VVPAT records is whether they are used in post-election recounts in practice. The EOM should observe any post-election audits or recounts to assess whether the process meets legal requirements. For audits, it is likely that only a certain percentage of paper records will be checked. The selection of paper records to be audited should be determined randomly based on regulated criteria. The percentage to be checked should be sufficient to provide a statistically valid sample.

5.4.3 Scanned ballots

Ballot scanning can also provide universal verifiability if implemented appropriately. In this case, there are also technical aspects that should be evaluated by the EOM. The ballot paper used should be readily understandable for the voter and it should be straightforward to mark. Nevertheless, some OSCE countries use devices where the ballot paper is printed with only a QR or barcode or legible text with an additional code that is read by the scanner. This makes it more difficult for the voter to verify the correctness of the ballot.

When ballots are scanned in polling stations, voters should be able to insert the ballot into the scanning device themselves, without assistance and without the secrecy of their vote being violated. In some elections, voters are provided with special privacy sleeves, which they can use to prevent anyone, including a person assisting the voter, from seeing the content of their ballots while inserting the ballot into the scanner. If the ballot is not marked in a valid manner or any other technical error occurs, the device should clearly indicate this to the voter, and the voter should have the opportunity to cast a correct ballot.

Since scanners can be subject to human or other errors, it is important that at least a statistically representative sample of ballots are counted manually through audits and, if required, recounts are conducted. Audits of the paper record should be random and on a statistically relevant scale. The law should prescribe the means for a recount that are independent of the vote counting hardware and software and based on a randomly selected and statistically meaningful percentage of votes or number of polling stations. The EOM should also establish the overall margin of error of the scanning devices and whether there is any provision in the regulation for ‘zero report’ verification before the start of the voting procedure (before the first ballot is cast) and automatic recounts if the margin between two electoral contestants falls within this margin of error.

5.4.4 Verification and Internet voting

For i-voting systems, universal verifiability is difficult to provide without jeopardizing the secrecy of the vote, especially in cases where ballots are complex. The EOM should carefully examine verification processes, the technical and logical proofs and regulated procedures that purport to provide universal verifiability for Internet voting.

In some i-voting systems, mechanisms are provided for individual verifiability. In principle this means that the voter is able to check — combining several pieces of information — whether the vote cast was recorded correctly according to their intention. Any single piece of information should not reveal the content of the vote, as this would violate the secrecy of the vote if it gave the voter a way to prove to third parties how they had voted. Where such mechanisms are used, the legislation should always provide for verification to be undertaken to determine whether or not any falsification has occurred and what sanctions should be taken in the event that it has.

Possibly the most extended mechanisms for ascertaining that all ballots have been counted-as-recorded are cryptographic zero-knowledge proofs. In some cases, eligibility checks are also conducted (e.g., by means of verifying voters' digital signatures in encrypted ballots as received by the server, and before they are anonymized and decrypted) to ensure that there has been no ballot box stuffing. However, there is widespread consensus among the expert community and election practitioners that, in general, the infrastructure needed for i-voting is probably one of the most difficult for EMBs to implement.[61] Furthermore, important challenges inherent to Internet voting remain, even with these cryptographic measures and with blockchain technology, including those related to the secrecy and verifiability of the vote and lack of transparency and possibility for observers to have full access to the system.[62]

61 See USAID/DAI/IFES Primer: Cybersecurity and Elections.

62 Regarding the blockchain, there is academic consensus that also concludes that this technology makes solutions only more convoluted rather than more transparent. See Annexe C for additional reading on this topic.

Possible questions:

- What verification methods are used to prove the integrity of the results? Do they result in the end-to-end verification of the results, or are there gaps in the verification process?
- How thoroughly do the voters conduct the verification process in practice?
- Do observer groups, political party representatives and other stakeholders have full access to the observation of the verification process? Have any such individuals or groups observed the verification process? If not, what are their reasons for not observing the result?
- What audits are undertaken and by whom? What happens when an audit reveals errors or discrepancies? Have any manual recounts been requested and conducted?
- If DRE voting systems are used, do these devices provide a paper record? If so, can it be verified by the voter before casting their ballot?
- Is the voter given any data during the voting process for verification purposes that could potentially violate the secrecy of the vote? Does the VVPAT preserve the secrecy of the vote?
- Does the VVPAT serve as a reasonable verification method, or do technical or design weaknesses reduce its value? Were any problems identified with the VVPAT itself (printing, storage)?
- Are random audits of the VVPAT conducted? Were any discrepancies or problems identified as a result of partial or full recounts of the VVPAT? If so, how were these addressed?
- If ballot scanning devices are deployed, does their use preserve the secrecy of the vote? Are the scanned paper ballots audited or manually recounted to verify the electronic results? Does verification take place before or after results are announced? How are discrepancies addressed?
- If Internet voting is used, how do the verification methods ensure end-to-end verification?
- What types of verification method does the NVT system provide ('cast as intended', 'recorded as cast', 'counted as recorded')?
- Regardless of the verification method used, how do political parties, candidates and citizen observers assess the verification process?
- If the tabulation process relies on transmission of data by Internet, what measures are in place to prevent or detect external hacking to either retrieve or alter data? What measures are in place to prevent illegitimate internal manipulation of the system? Are these likely to be effective?

Chapter 6

Observation and assessment of 'ancillary' ICT-based election systems and processes

6.1 Electronic Voter Registration and Verification Systems (EVRVS)

Election observation and assessment of electronic voter registration and verification processes is another aspect of fundamental importance.[63] As noted earlier, this Handbook provides guidance only on the use of ICT voter registration and verification pro-

63 According to many international organizations specialized in the fields of electoral observation and assistance, this is an area with 'high impact' on electoral processes and 'has high exploitation potential' by malicious actors. See for example, USAID/DAI/IFES Primer: Cybersecurity and Elections or Introducing Biometric Technology in Elections, International IDEA, Stockholm, 2017. See also IFES Briefing Paper on the Cybersecurity of Voter Registration.

cesses. ODIHR's methodology for the comprehensive assessment of voter registration is elaborated in the *Handbook for the Observation of Voter Registration*, which is mostly used by Legal and Election Analysts within the core team. Thus, there are many elements of these processes that will require cooperation between various core-team analysts on an EOM, including the ICT Analysts.

6.1.1 Considerations for introducing EVRVS

The voter registration process normally begins significantly earlier than the official start of the electoral period and before the deployment of an EOM. The starting point for analysis and inquiry by the EOM should be an assessment of the process leading to the adoption of the ICT. The key aspects that should be looked at are whether the process was transparent and inclusive, whether it was based on perceived societal needs and whether feasibility studies, pilots and testing of functionality and cybersecurity were conducted. These can be assessed, to a certain degree, through legal and regulatory analysis of the existing documents and information received from credible electoral stakeholders about how the process was conducted and its level of transparency during deployment.

Also important is voters' understanding of the ICT in place so that it does not negatively impinge upon their fundamental rights. In this regard, an extensive information campaign by the EMB is often necessary to inform the public of these important changes to ensure that they properly understand the process and have the proper identification document.

In addition to the timeline and public information campaign, the EOM should assess the estimated and allocated funding for introducing the EVRVS. While it is in the public interest that the costs related to introducing ICT are reasonable, sufficient funds for effective implementation need to be allocated. Moreover, the cost may depend significantly on the functionality of the chosen solution and on whether it is purchased or supplied by vendors. For example, buying inexpensive equipment might be the most economical solution, but it might not effectively address the needs of the EMB. On the other hand, introducing sophisticated equipment for biometric checks, securely connected to a central server for instant voter eligibility checks with high fidelity, might be prohibitively expensive. Lastly, the EOM should consider if the estimated funds include costs related to polling staff training and servicing, updating and protecting the equipment from cybersecurity threats (which should include protection, detection and recovery).

Before the official use of the new technology and to prevent or mitigate the risks from different unforeseen situations the EMB should run tests and pilots. Extensive testing of any new component of the system is essential for uncovering potential issues such

as malfunctioning hardware or software. These tests could also be conducted during small-scale real elections (for example, local level by-elections) or a mock election. Testing in binding elections is often equated to piloting, as the election authorities may try out certain features that might not necessarily be used for the first time in country-wide elections. Given that some of these processes will take place before deployment, the EOM should analyse the reports and other related documents from these tests.

6.1.2 Operating EVRVS during election periods

Several important elements related to the functioning of the EVRVS should be observed during an EOM. In addition to analysing the legal and procedural framework to ascertain whether it covers all of the necessary aspects for introduction of the EVRVS, the EOM should also assess the institutional capacity of the EMB to manage the system.

Once the decision is made to introduce the EVRVS and the necessary legislative amendments are adopted, the EMB should develop a comprehensive plan for implementation and continuous monitoring and allocate the necessary resources.[64] For example, the EMB might need to employ additional staff specialized in IT processes or cybersecurity, conduct training for polling staff on the EVRVS, including on data protection, and develop a timetable with implementation stages and decide which solutions will be implemented by the lower-level commissions or vendors and the level of supervision. An important aspect of assessing the EOM is the existence of contingency plans in case of problems with the newly introduced EVRVS. The legal framework should clearly define under which conditions the EMB can invoke the contingency plans.

EOMs should assess the infrastructure, features and functionality of the EVRVS. Solid ICT infrastructure is necessary for the flawless functioning of any EVRVS and the EOMs should assess the maturity of the infrastructure and its cybersecurity resilience. This should include an understanding and evaluation of what measures are in place for when the system is not in use (i.e., system and data integrity checks).

Special attention should also be paid to the effect that the new system has on voters in terms of inclusiveness, opportunity to vote in different locations and time needed for identification at the polling station, as well as the workload it creates for the EMBs. Many OSCE participating States have centralized voter lists and, in these contexts and where BMD or DRE are used, some EVRVS can give voters the opportunity to vote in a different polling station to the one assigned by their residence.[65] The EOM

64 If the EVRVS is used solely for elections, it is good practice to take the system offline completely until it is needed for the next election. However, protective and detective measures should still be in place, as there is always the risk of an insider threat.

65 This possibility can be limited if voters want to vote outside their constituency and due to the type of electoral systems and the need for different ballots.

should assess if there are sufficient safeguards against multiple voting and also if the system provides guarantees that votes cast from different locations are included in the final results.

When introducing EVRVS, one of the principal decisions that the EMBs need to make is how the electronic voter list will be used. Some OSCE participating States have introduced electronic voter lists to check whether or where the voter is registered and the paper voter lists remain the only official documents. Others have parallel use of electronic and paper voter lists or use electronic devices with the option of printing the voter list on demand in case of contingency. Where electronic voter lists are used, whether online of offline, there are several possibilities that might interrupt the voting process, including interruption to the electricity supply, or problems with network or cable connectivity, or a device malfunctioning. One contingency measure is to have voter lists printed and to have pre-established and practiced procedures for using them.

One benefit of the EVRVS is that, if implemented effectively, these systems can prevent or reduce possible election violations such as impersonation and multiple voting.[66] To tackle the issue of multiple voting, a number of the OSCE participating States have introduced electronic voter verification devices with biometric features.[67] For these types of devices to be deployed in elections, there needs to be a centralized voter registration database with biometric characteristics. Therefore, the EOM should assess the inclusivity, quality and accuracy of the voter registration database as well as the general confidence in the voter registration system. While the stated benefits of these devices are obvious, this type of technology usually has high costs for procurement and maintenance and carries certain risks related to equipment malfunction or low-quality databases which can lead to disenfranchisement and possible misuse of voters' private data.

The protection of voters' data is a crucial topic in any EVRVS system. Any EVRVS is based on voters' personal data which should be collected and used in line with international standards, election legislation and the national data protection laws.[68] For this reason, EMBs introducing EVRVS should ensure that they have the legal grounds for processing personal data, including in some cases sensitive categories of personal data (such as health data or biometrics). This may require specific legislation to be passed or existing legislation to be amended. Furthermore, only information neces-

66 Additionally, providing features for machine reading the ID document data (such as magnet-strip-, bar-code- or near-field communication ((NFC) readers) could be used to enhance the identification of voters in the polling station and minimize human errors in the process.

67 The most commonly captured biometric features in elections are fingerprint identification systems, facial recognition systems or scanned signatures. See International IDEA, Introducing Biometric Technology in Elections.

68 See Technology, Data and Elections: A 'Checklist' on the Election Cycle, Privacy International, June 2019.

sary for identifying a voter as eligible for a particular election should be processed.[69]

International standards for the protection of personal data provide for special safeguards when data is processed or stored, including the secure processing of personal data (e.g., by the use of pseudonyms, encryption, etc.). These security measures must be evaluated on a continuous basis and the EMB may even be required to conduct Data Protection Impact Assessments (DPIA) of their EVRVS. In case organizations other than the EMB can access or process personal data from the EVRVS, it may be necessary to conduct agreements or legal contracts with these third parties, clearly setting how they are expected to process the personal data. Information about voters shall be accurate, up-to-date and not excessive in relation to the purposes for which it is stored. Lastly, personal data should not be kept for longer than is necessary, and the EVRVS data should be securely deleted within the legally established deadlines.

Some EVRVS produce paper slips containing different voter personal data (e.g., a voter's name, address, photograph, biographical data, ID number, etc.). EMBs should have clear procedures and publicly disclose how voters' data is used throughout an election cycle, what measures are put in place to protect voters' data and report on fraudulent data misuse. The use of EVRVS provide for having highly systematized and centralized voter information which could be misused for various purposes. Therefore, EMBs must ensure protection of data from unauthorized access, ensure the protection of the data against cyberattacks and have clear procedures for data destruction after the legally prescribed period.

Lastly, the EOM should assess the integrity of the EVRVS; namely who has access to the system, the management of user roles and authentication of users. Comprehensive management of user access helps to protect the system from physical and cyber-intrusion. The EOM should observe the method used for accessing the system and the EMBs should have a user-managing protocol explaining the different roles of those with access to the system and prescribing the creation, distribution and use of all their credentials in the system.

69 For example, an EVRVS may include health data if certain alternative voting methods are restricted to voters with disabilities, ill or hospitalized voters.

Possible questions:

- Were there transparent and inclusive discussions held and feasibility studies conducted before introducing EVRVS? Was a comprehensive implementation plan later developed by the EMB? Were any concerns raised regarding this process by stakeholders?
- Are proper regulations in place to delineate roles and responsibilities over the technical aspects of the voter registration process, including access to the data?
- Is there a proper delineation of roles and responsibilities between the different agencies that may be involved in the implementation of a voter registration database (e.g., the Ministry of Interior, the Office of Statistics, etc.)? Do these regulations ensure the independence of the EMB and its overall control on the conduct of election process?
- Has the EMB chosen an in-house solution or have they contracted external vendors to provide the system? If the latter, are the roles and responsibilities appropriately delineated, recognizing that the EMB holds primary responsibility?
- Are there proper resources spent on addressing the issues of technology in the voter registration process, both human and financial?
- Has vulnerability mapping been conducted and a proper risk-mitigation strategy (including on cybersecurity) implemented?
- Is there a system of access rights and controls in place to ensure that data is only available to those authorized and under specific conditions? Can this access be logged and tracked for future reference?
- Is a chain of custody documentation in place to ensure the integrity of data during any transfers?
- Are there measures in place to ensure that data is only changed under specific conditions and inappropriate changes can be identified and attributed?
- Has there been proper training of the EMB staff authorized to use the EVRVS on the risks or vulnerabilities that may exist and on their role in mitigating these risks? Have training materials (handbooks, leaflets, videos, etc.) been developed and distributed?
- Has there been sufficient transparency and outreach by the EMB to inform voters of the EVRVS so that they understand how the system works and the need to have proper identification documents?
- Have proper risk assessments been undertaken, has extensive testing taken place to identify any issues prior to implementation of the system, and are measures in place to ensure that data is available and protected in case of attack, system failure, power outages and the like?
- Is the EVRVS functioning properly throughout all stages of the electoral process and especially on election day? Is the system having any impact on the flow of voters and their ability to vote?

6.2 Other ICT-based platforms and processes

A number of EMBs have been developing ICT modules for various elements of their operations. These include the ICT-based platforms and modules for RMSs, training and allocation of EMB staff, technical solutions for constituencies' boundary delimitation, candidate registration process, EDR components, voter information campaigns, political finance reporting and other 'ancillary' processes. While the ICT Analyst will observe and analyse the type and integrity of technologies used for administering these ICT-based platforms and modules, the content analysis and assessment of these specific election-related processes or aspects will be the subject of different analysts within the core team. For instance, the ICT Analyst will need to work with the Election Analyst when assessing issues related to the RMS, training and allocation of EMB staff, or with the Legal Analyst for assessment of EDR or other legal issues.

6.2.1 Results Management Systems (RMSs)

One of the most widely implemented ICT modules in electoral processes has been RMSs, used for tabulation, verification and publication of results. Each of these elements is necessary for building public trust and ensuring the overall integrity of elections and, as such, should be observed and assessed by EOMs. The tabulation and verification of the election results were discussed earlier in the Handbook in the context of accurate counting and aggregation of votes as well as the need for respect of the NVT principles of verifiability. This section deals with the ICT aspect of RMSs related to the publication of election results.

The use of technology in an RMS has enabled the EMBs to conduct more accurate processes for aggregating data and publishing results more quickly. At the same time, the technology has created new challenges for EMBs, such as recruiting staff with IT skills, additional costs for creating adequate infrastructure, equipment supply and software development, and intricacies related to the custody chain in the management of results, as well various issues with in-house development or contracting external suppliers for the RMS. The EOM should assess if election stakeholders have trust in the RMS technology and whether it provides the necessary elements for verifying the accuracy of the election results.

Irrespective of the technology used for tabulation, ICT or paper-based, election results should be disaggregated at the polling station level; this can help electoral stakeholders to verify they have been accurately aggregated and published. Several elements should be included such as: the identification number of the polling station, the total number of registered voters and the number that voted (the number of signatures on the voter list, the number of ballot papers received, used and unused), the number of

votes for each contestant and the credentials of the people authorized to count the votes.

Within the OSCE region, the most commonly used RMS technique is manually completed paper protocols for official results and ICT for electronic publishing of preliminary results.[70] However, some OSCE participating States have RMSs that exclusively use ICT and include data entry at polling stations, scanning results protocols at polling stations, or that have ballot scanners and transmit protocols directly from polling stations to a centralized results database.

The EOM should assess: if the staff operating the system possess the necessary skills; how smooth the process is; whether it contains sufficient safeguards and provides for verification and accuracy of the transmitted and published results. Due consideration should also be given to data protection issues in case the RMS processes personal data about individual candidates, other personal data that may be included in results protocols (e.g., the members of the polling station committee who complete and sign the protocols), or even personal data about the users of the RMS.

Direct entry at polling stations may require significantly higher human, financial and infrastructural resources than a centralized RMS. Polling stations are usually provided with computers or additional equipment (if protocol scanning is required) and are connected to the central database. The EOM and especially the LTOs and STOs should assess the conditions and the equipment in the polling stations, and the capabilities and roles for data entry of the polling staff.

It is recommended that the networks operating the RMS are not connected to the Internet or that a Virtual Private Network (VPN) is set up and, if a website is used for publishing election results, it should be tested. The testing of the entire RMS, including the website and the source code of the software operating the system, should be done well in advance of the elections and under realistic conditions, with the participation of interested stakeholders and the results of the testing should be made publicly available. It is the role of the EOM to assess the results of the testing and, during election day, to observe how the system functions and if there are any failures that might impact the integrity of results and the election process. To increase trust in the RMS, it is good practice for electoral contestants and sometimes media or citizens observers to be granted privileged access to the system.

Given its importance, the RMS is an area that also presents the greatest vulnerabilities in terms of external exposure, attack surface and attractiveness to foreign and

70 RMSs can be categorized into three general models depending on the incorporation of technology: paper-based manual; fully automated (aggregate, verify and transmit results without human interaction) and hybrid (include both manual and automated elements). See the UNDP Guide on RMS.

domestic threat actors.[71] As many OSCE countries have been moving from a manual system to either hybrid or fully technology-based applications for counting, tabulation, transmission and publication of election results, the potential for these types of threats increases. While cybersecurity issues are discussed later, it should be noted that contingency plans should be in place well in advance of election day and these should be assessed by the EOM.

Possible questions:

- How is the RMS structured?
- Who is responsible for data entry? Who is responsible for supervision and oversight?
- Do the polling staff have the necessary skills for data entry and overall management of the system? Have they received training?
- Who is authorized to make changes to the protocols and election results databases? How are users authenticated?
- Are there audit logs that maintain records of when databases were accessed and are there written procedures to monitor them?
- Was the RMS tested and reviewed before deployment? Who has tested the system? What are the views of election stakeholders on the integrity of the RMS?
- Are polling stations or tabulation centres adequately equipped? What is the condition of the equipment?
- What is the level of connectivity? Are there any issues with the electricity supply or network connectivity?
- Are there risk-mitigation strategies and plans in place in case of equipment or software failure? Are the members of the EMB and polling staff aware of these plans?
- Do the electronically published results and protocols contain the necessary data for verifying the accuracy of the election results? Are the results audited?
- Are political parties or other election stakeholders granted privileged access to the RMS? What are their views?

6.2.2 Online Training of Election Officials

EMBs often conduct online training of election officials and, therefore, the EOM has to look into the execution of the ICT-related training courses and should aim to understand how well the EMBs are prepared to use their technological solutions.

71 In cyber-security, an 'attack surface' is defined as a set of points on the boundary of a system, a system element or an environment where an attacker can try to enter, cause an effect on or extract data from that system, system element or environment. See NIST Glossary.

Specific attention should be paid to the clarity of the rules around irregularities or ***force majeure*** incidents and the practical application of the curricula (e.g., when implementing new ICT solutions, how well officials are able to instruct the voters). Another facet of the training process to be looked at should be the overall number of trained staff: if there are sufficient staff for the efficient conduct of the election, the way in which substitutions and replacement procedures are regulated, any differences between local and regional reserves of trained staff and whether there is sufficient regulation for handling extraordinary circumstances. Lastly, since the ICT-related training programmes require the processing of the personal data of trained officials (amongst other data subjects), data protection issues should also be taken into account.

Possible questions:

- Is online training incorporated into the EMBs overall technology and cybersecurity strategy?
- Is there clarity about the procedures and formal rules in place in case of ICT equipment or software failures? How are replacements of staff dealt with? Are there any regional or local differences?
- Are access rights to the system properly delineated and understood at all levels of the EMB? How many staff have been trained and is this number adequate to needs?

6.2.3 Platforms for electronic registration of candidates

Democratic elections can only take place within a pluralistic environment in which a range of political views and interests are represented. Responsibility for the registration of election contestants often lies with the EMBs, either at the central or local level. The process of registering election contestants must ensure respect for freedom of association and the right to stand for elections. Candidate nomination and registration rules are largely shaped by the electoral system for a given election.

An increasing number of OSCE participating States are using digital solutions for the nomination and registration of candidates (e.g., for the collection of signatures in support of a candidate) by parties or other nominating bodies. In such cases, the technology and regulations for signature collection have to be scrutinized by the EOM, which should also consider the available solutions and if they are universally accepted (for instance, if the digital signatures are widely accepted, if there are electronic ID cards or specially generated tokens, whether the signature collection is organized by the state or by electoral contestants). Emphasis should be put on hybrid signature

collection systems (paper-based and through ICT), the type of technology used and the procedure for merging the signatures collected via ICT and paper-based means.

As in the case of the above-mentioned technologies, electronic registration of candidates and signature collection entails the processing of personal data. It is important that this processing has proper legal grounds and that the principles of data protection regulations are satisfied. Furthermore, and since supporting a specific candidate may reveal political opinions or ethnic origins (which are considered sensitive data), special attention should be paid to lawfully and securely processing the personal data of all signatories.

Possible questions:

- Is the system in place for collecting candidate signatures adequate and do contestants fully understand the process?
- Is the ICT solution properly regulated from a legal point of view, protecting all fundamental rights, including personal data protection?
- Are the available solutions universally accepted by electoral stakeholders?
- Is the signature collection environment maintained by the public sector or by electoral contestants?

Chapter 7

Cybersecurity of elections

When EOMs observe and analyse the electoral framework and process, cybersecurity in elections must be considered. This analysis should be done holistically, throughout the electoral infrastructure, to take account not only of elements relating to voting, but also of 'ancillary' systems being used. The EOM needs to look across the whole process of electronic information and data storage, processing, transmission, confidentiality, integrity and availability.[72]

72 A properly delineated and executed Incident Response Plan (IRP) is crucial to any holistic cyber-security strategy. An IRP is a formal document that clarifies roles and responsibilities and provides guidance on key phases and resources (including human) during a crisis.

Any cybersecurity analysis and response should be achieved through a triad of policies, education and technology. Different stages of possible cyberattacks should also be analysed, so that appropriate measures can be taken at each stage of the process.

The assessment should start at the NAM phase, with an analysis of the various elements of the electoral process that use ICT. NAMs should inquire of relevant interlocutors about the EMBs attack surface, which comprises both physical and digital threats, their potential impact, risk evaluation and mitigation measures. Given the complexity of the issue, multiple state agencies are often responsible for technology security. It is crucial for the NAM, and later for the EOM, to properly map and assess the delineation of roles and responsibilities of different agencies involved in the electoral process.

The ICT Analyst needs to explore how the technology is supplied, implemented and secured through a holistic cyber-risk mitigation framework. Aside from the general cybersecurity aspects, other elements that should be explored are specific measures relevant to NVT and EVRVS, as well as other web-based portals used by the EMB. Electronic registration of observers, parties and candidates are also elements that require scrutiny. It is important for the EOM to evaluate whether the EMB properly understands the risks in implementing such technologies and whether they have sufficient funds and appropriate measures in place to mitigate potential risks, such as contingency planning and extensive hardware and software testing prior to deployment.

The table below provides a non-exhaustive list of recommendations that an EMB could consider when devising a cybersecurity strategy.

Table 7. Cybersecurity recommendations for EMBs

	Recommendations
1	Increase the level of EMB awareness, understanding of the associated cybersecurity risks, potential threats and vulnerabilities of the devices through various activities. E.g., through testing equipment, assessment and feasibility studies, workshops, etc.
2	Include cybersecurity resilience as an integral part of any terms of reference for acquiring new equipment. E.g., the terms must reference, on a technical level, cryptography and certification methods and protocols that will be used for transferring data between devices, which levels of authorizations will be required, and whether multi-factor authentication will be required and at which stages of the process, etc.

3	The EMB should be able to determine whether it has the capacity to provide adequate cybersecurity resilience, or if it needs to rely on external providers. E.g., assistance can be from another state institution or private vendor. In these cases, and when using the assistance of the vendor, the EMB must ensure that the entire election process is ultimately the EMB's responsibility.
4	The EMB should understand how certain functionalities, if introduced, may negatively impact its cyber-resilience. E.g., if there is an online solution, or the system uses wireless connectivity, this could introduce a whole range of threats that otherwise might not be present.
5	The EMB should keep equipment and software up-to-date. Similarly, all input-output devices or ports should be considered separately, in terms of vulnerability to unwanted access.

7.1 Cybersecurity of NVT

Voting machines (DRE or BMD), ballot scanners and any i-voting systems should all be properly evaluated for their cyber-resilience. Adequate safeguards must be in place to prevent physical tampering with ICT equipment (e.g., USB ports or other external connections should not be easily accessible). Additionally, storage and transport of NVT devices should be done in a secure manner under defined protocols and access to the devices should be observed when they are not in use, with appropriate records kept. The EOM should check whether NVT devices have the capacity for remote access and, if so, what measures are in place to prevent illegitimate access, especially during the voting procedure.

Special protection measures for NVT systems that rely on the use of the Internet for the transmission of data is especially important to avoid significant failures, such as the loss of even a small number of votes or a period of downtime. Ideally, these protection measures would include mirrored operation in several access-controlled data centres with physical separation from any other information system operated in the same location.

In addition, the EOM should assess how the system and procedures detect and, if possible, prevent illegitimate or unauthorized access (including by internal or associated employees), and should assess the potential effectiveness of these measures. In i-voting systems, the EOM must consider how the system verifies the voter's identity and what potential threats that could create (e.g., loss of secrecy of the vote). In addition, the overall protection of the information systems from unauthorized external access, through the use of dedicated transmission lines, firewalls and overall security concepts, should be analysed.

7.2 Cybersecurity of EVRVS

States' efforts to make voter registration databases accessible online for voters to register or check their status significantly increases the risk of cyberattacks. Threat actors have leveraged weaknesses in these 'ancillary' processes and attacks have breached databases but have attacked also hardware and software to access voter information to either attempt to change it or sell it.[73] Thus, this area should be assessed by the EOM and the ICT Analyst.

Since voters' data is often collected at the local level, the proliferation of devices used in such a system also magnifies the risks. Many EMBs have also used external-facing technological applications like online and mobile phone access to voter registers to increase accuracy and transparency; but this has also increased exposure and potential risks. To mitigate these risks, cryptography should be used when transferring voter registration data. If hardware, such as storage devices, is being used to transfer data, that must also be secured against cyber-vulnerabilities such as malware that can alter the data. In any case, integrity checks should be built into any registry system in order to ensure that the collected data matches the data transferred. Where multiple entries are flagged, human verification is generally considered a good practice before they are removed.

Given the resources and skillsets required to manage voter registries, some countries have turned to external vendors and increasingly to 'cloud-based' data storage, sometimes based outside of their jurisdiction. This raises another set of potential risks and vulnerabilities, including issues related to data segmentation, access rights, additional configuration requirements, compliance with data protection regulations and incorporation of these added elements into a holistic cybersecurity response plan. Many OSCE countries choose to keep paper records in case of system failure as this might also be required for evidentiary purposes and especially for post-electoral EDR.

73 See USAID/DAI/IFES, Primer: Cybersecurity and Elections: "direct manipulation of voter registration data – for example, adding or deleting voters – also cannot be ruled out as a possibility if voter registration database security is compromised."

EVRVS needs to be examined holistically by several EOM analysts. For instance, the issue of the collection, processing and storage of personal (biometric) data is something that will be part of the responsibilities of the legal, electoral and ICT analysts. All aspects should be evaluated according to the electoral cycle approach discussed above — from initial discussions and feasibility studies to introduction and implementation in the election process.

7.3 Cybersecurity of other ICT-based platforms and processes

RMSs have several areas that may have cybersecurity issues and need to be examined by the EOM and the ICT Analyst. In the first place, it is crucial that proper risk management and security control frameworks have been put in place by the EMB in order to mitigate any potential threats. For EMBs that choose to outsource and use external providers for RMS management, it is important for the EOM to understand whether the tender phase took place in a transparent manner and whether potential bidders were cybersecurity vetted. As previously noted, the EMB has the ultimate responsibility for infrastructure, data, processes, and communications and should ensure that selected vendors have clear security requirements, and protocols and certifications for the systems that are to be used in the RMS process.

Risk assessment and contingency planning is crucial for an ICT-based RMS to succeed, and this often relies upon other state agencies that may be necessary to secure systems in the event of a possible attack. The potential risks should be identified in advance and appropriate protocols developed prior to any implementation. The EOM should examine whether all election staff have been properly trained on the potential risks and cyber-hygiene responses to enable them to respond properly.

Possible questions:

- What legal and administrative cybersecurity provisions pertain for elections and what bodies are responsible? Has the provision of cybersecurity been done holistically, according to an electoral cycle approach?
- Has the EMB introduced a formalized, well-defined cybersecurity risk management framework to deal with possible vulnerabilities? Is cybersecurity high up the agenda of the EMB and do they understand the potential ramifications on electoral integrity if not properly handled?
- Have cybersecurity frameworks and risk-management strategies been tested well in advance of election day? Has a strategic review been conducted and what are its findings?
- Have there been any previous cyberattacks and of what nature? Are there concerns of possible cyber threats in these elections? How large is the potential attack surface? Is it centralized or localized?
- Are EMB staff at all levels properly trained on their role within this framework and do they have a solid understanding of cyber-hygiene and its importance?
- Has inter-agency collaboration been established, including on general cyber-incident management (e.g., with Computer Emergency Response Teams), and are roles and responsibilities properly delineated?
- Has the election administration been classified as 'critical infrastructure'? If so, for what reasons and are the comparative benefits/risks understood?
- Has the EMB provided selected vendors with clear security requirements and protocols? In the event of vendor selection, is it clear that the EMB is ultimately responsible for infrastructure, data, processes and communications, in line with international good practice?
- Are there appropriate paper backups in the event of system failure and have appropriate contingency plans been made and rehearsed?
- What bodies are responsible for conducting security assessments and preventing cyberattacks on election-related infrastructure? Do laws and regulations provide for cooperation among these bodies?
- How is the security of systems monitored throughout the election and what communication mechanisms are in place in case of any security issues?
- What long-term privacy mechanisms are in place to ensure that sensitive data is duly destroyed after elections to avoid any privacy risks?

Chapter 8

The role of Long-term Observers

When a full or limited EOM is deployed to a State using ICT in an election process, the contributions of LTOs, as well as STOs, will be important in assessing the preparations for, and the conduct of electronic voting, counting, tabulation and EVRVS. Their tasks will vary according to the type of technology, the extent and form of ICT, whether ICT are used throughout the country or being piloted or tested in certain areas, and the way in which ICT are integrated into the overall election process.

The core team of the EOM should adequately prepare LTOs for their tasks by providing them with clear and concise information about the ICT used and by defining precisely the information and data to be collected. LTOs should not be expected to be experts on ICT issues. The ICT Analyst should remain mindful that observation of the use of ICT and NVT will be one of a number of tasks for LTOs and that observers should not focus on one aspect of the election process to the detriment of others.

LTOs will generally focus on several key aspects of the use of ICT: the technical and operational preparations by regional or local EMBs, training of election officials, voter education campaigns and the views of political parties, candidates and civil society organizations at the local level. Additionally, institutions responsible for voter registration or identification solutions with an ICT element have to be considered. LTOs will also be able to inform the core team about the questions and concerns of local election officials and voters.

Where ICT or NVT are used in polling stations, LTOs should observe how the devices (e.g., devices for voter identification or voting) have been distributed and by whom, how they are stored prior to being set up, who has access to them, and what security measures are in place to prevent unauthorized access. LTOs should ask whether the devices have been delivered fully prepared for election day or whether software updates are needed, including to 'ancillary' or NVT systems. If ballots or voter lists are uploaded locally, the LTOs should observe how this is done, who is responsible for performing the work and what security measures are in place. LTO observations should also include potential testing of the ICT and NVT if conducted at the local level before official use.

Where different kinds of ICT are used or where ICT are supplied by different vendors, LTOs should identify the kind of ICT that are to be used in their respective area of observation and communicate this to the core team.

LTOs should discuss ICT with local and regional election officials. This will give the EOM a better understanding of how these officials view their role in administering ICT and to what extent they feel adequately prepared for their responsibilities and for any problems or faults that may appear. LTOs should also determine what role external technicians have in electronic voter lists or voting preparations and to what extent election officials are able to provide oversight of their work. LTOs should attend training sessions for polling station officials.

With the help of local staff, LTOs should observe the existence and potential effectiveness of voter education and information campaigns in local media. LTOs should also ask about and observe any tests of the technology conducted with the public. Ob-

serving such tests may indicate not only how comfortable voters are with the devices, but also any potential issues with the usability or robustness of the devices.

In the course of their regular meetings with local political party and civil society representatives, LTOs can inquire about the ICT. Importantly, in these meetings LTOs should ask stakeholders about their trust in the ICT or NVT systems and their confidence in the integrity of the systems. In particular, they should find out how parties and observers plan to observe the ICT and whether they are doing so in advance or only on election day. LTOs should ask about the access parties and citizen observers have to the ICT or NVT systems, if there is any documentation that they have been unable to obtain and whether they have had the opportunity to test the devices. In case of EVRVS, LTOs should be able to follow the preparatory procedures similar to other ICT solutions, with attention on database formation, training, data protection and maintenance issues.

In case of remote i- voting, the role of LTOs will be more limited. Nevertheless, they will still need to gather information about voter education, testing and early procedures as well as any interaction of the NVT with the traditional voting process; for example, the implementation of the system to prevent voters from casting multiple valid votes through different methods.

Possible questions:

- To what extent are election officials familiar and comfortable with their role in organizing or providing oversight of the use of NVT and other electoral technologies?
- What are the plans for training lower-level election officials? How useful does such training appear to be in practice? How much is technology integrated in the training process?
- How will technical expertise or assistance be provided on election day, especially in the event of problems?
- Have a sufficient number of ICT/NVT devices been received, and were they received and set up in a timely manner?
- How is electronic voting or voter identification equipment stored? What security measures are in place to prevent tampering? Who has access to the ICT devices and is access recorded in a protocol?
- Are the ICT systems connected to the Internet? If so, what security measures are in place to guard against possible hacking?
- Are voter education materials available? How widespread are voter education activities by the EMBs or in local media?
- Are any tests or trials with voters planned before election day? If so, what are the reactions of voters to the devices? Have any problems been identified as a result?
- What are the views and levels of trust of local political party representatives and citizen observers regarding the use of ICT in their area? Have they had the opportunity to test devices or review documentation about the process? If parties or observer groups do not observe the use of ICT or NVT systems, why not?

Chapter 9

The role of Short-term Observers

STOs play a crucial role in gathering a statistically valid sample of data about voter registration and identification, electronic voting, counting and tabulation. Although the general task of the STOs in observing ICT-related aspects and, specifically, electronic voting should not be different from observing paper-based voting, the information that the STO should be seeking will vary depending on the technology used in the particular country and the extent of its implementation.

In this respect, the ICT Analyst should brief the STOs on the main elements of the ICT and provide specific guidelines on how to assess the performance, security and usability of the system. Sufficient attention should be given in the briefing to ICT characteristics, ballot design and other elements of voter or election management interaction with the technology, in addition to necessary descriptions of the ICT system itself.

STOs, much like LTOs, cannot be expected or required to have an ICT background. Their training should be focused on how to observe correct and secure operation of the ICT systems on election day so that they are able to identify any differences in practice in the polling stations during the voting procedure or during counting and tabulation.

A special section on election technology should be included in the STO briefing package. This will help STOs assess how well-prepared polling station officials are to use the equipment, as well as the level of voter confidence and understanding of the procedures. Questions about the performance of election technology should be included in observation forms to be completed by STOs.

As STOs may be unfamiliar with ICT in general, the observation forms must be carefully and clearly designed so as to obtain relevant and usable information and to avoid any potential bias. Where ICT and NVT are used in conjunction with traditional paper voting, the core team and the LTOs should be careful to ensure that STOs are trained and deployed in such a way that they do not give disproportionate attention to electronic voting issues.

There are a number of aspects of ICT that STOs can be asked to observe during the voting process. The key set of issues includes the secrecy of the vote, the storage of ICT devices, the usability of ICT devices, security, the adherence of polling station officials to procedures and how officials deal with any problems that arise.

The set-up of polling stations will be one of the first processes STOs observe (although this may be done by LTOs if ICT devices are set up in polling stations before election day). STOs should report on whether the set-up process follows pre-established protocols, including what steps are taken to ensure that the electronic memory does not contain any votes before the start of voting (so called zero reports). STOs should also observe any tests that take place during set-up, either of voting equipment or transmission of data to a central server.

STOs should observe where in the polling station the devices are stored, repaired and maintained. They should also observe how voters are identified and registered and if they mark their ballots in secret. Potential problems can include unattended storage of equipment, lack of polling booths or other secrecy dividers. Another important factor

is how election officials assist voters and whether such assistance potentially violates the secrecy of the vote.

STOs should assess how comfortable voters appear to be using the machines and should observe if a significant number of voters need assistance from election officials or other voters, and if voters are taking an unusually long time to cast their ballots. The usability and functioning of NVT with VVPAT functionality should also be considered, if applicable. STOs may wish to have brief interviews with voters outside polling stations to hear about their experiences and views on the use of EVRVS and NVT in the voting process. The accessibility of the NVT for persons with disabilities, the elderly, illiterate voters or speakers of minority languages is another important aspect of the usability of the system.

The physical security of the NVT devices in the polling station is another issue. This includes who has access to voting equipment and other components of the system in the polling station and whether any vendor service personnel access the machines without the presence of an election official. STOs should also observe whether any security measures that should be in place, such as the seals with unique numbering placed over external interfaces, are in fact utilized. Additionally, STOs should verify (using serial numbers or other unique identifying criteria) that the NVT devices in the polling stations are actually the ones supposed to be deployed there (where this information is available).

Regarding the conduct of the voting process, STOs should observe whether election officials adhere to established procedures or whether they deviate from them, which could jeopardize the integrity of the process. This includes situations where NVT are used as an alternative voting method, requiring special attention to the voter list in order to avoid multiple voting. STOs should also attempt to assess polling officials' understanding of NVT. They should inquire about the extent of training polling officials have received and observe whether manuals related to the NVT are present in the polling station and whether they are called upon by polling officials. STOs should ask any citizen observers or political party representatives about their views of the process in the polling station and to what extent they are able to observe the use of NVT in the process.

If the implementation of electronic voting allows voters in a polling station to choose between voting electronically and voting by paper, STOs should look at how this process is administered, including whether voters can choose their voting method freely or if election officials or other individuals recommend any specific voting method. It is also important to note whether voters are marked according to the method of voting

in the voter lists and whether the number of voters using each method is reconciled during the closing process.

STOs should observe, if applicable, how officials deal with any problems that arise with the system. They should note what the problem appears to be, how long it takes to remedy and whether this remedy seems effective and according to regulations. This includes delays in opening polling stations due to longer than expected set-up times. In case of EVRVS, STOs should assess the impact on the voting process in the observed polling station; if the electronic system is not working, for example, are voters marked by using paper voter lists? Or, for an incident with a voting solution, are voters given the opportunity to vote by paper ballot or are they turned away? If the system fails, functions abnormally, or if procedures regarding the operation of the system are not followed properly, STOs should observe whether the incident is written down in the polling station protocol that is to be submitted to the higher-level EMBs and whether this transfer actually takes place.

STOs should observe the closing of the polling station and whether this is done in accordance with procedures. These procedures should include proper documentation of proceedings, storage of gathered data (e.g., in case of biometric data), termination of the voting process, the start of counting, implementation of any testing and verification mechanisms and checks or safeguards of the integrity of results. STOs should observe whether a final voting result protocol is printed and made publicly available. STOs should observe how results are transmitted to higher-level election commissions and whether this is done by electronic communication of results or by delivery of hardware elements (such as memory sticks or disks).

If there is an immediate audit of turnout or paper records to verify results, the STOs should observe and report on any verification mechanism and audit procedures of paper records produced during the use of ICT. The observation of this is crucial to the assessment of the ICT's integrity and should include whether manual recounts of paper records are conducted in a transparent and accountable way. STOs should also observe if any discrepancies in the results of the electronic counting and tabulation processes are detected. They should also report what is done in such cases and what explanation is provided by the authorities for inconsistencies.

Possible questions:

- Do any problems arise during the set-up of ICT devices in polling stations? If so, are election officials able to resolve them? Are polling stations able to open on time?
- What steps are taken to ensure that the devices' electronic memories do not contain any voters' data or votes prior to the start of voting? Is this verifiable?
- Does the set-up of the ICT devices in the polling station protect the secrecy of the vote? Do election officials ensure that voters cast their ballots in secret, even if voters need assistance in using the devices?
- Do voters appear to understand how the ICT devices function? How many voters require assistance in order to complete the voting process? Do any voters terminate the process after initiating it, but before casting a ballot?
- Do voters approach NVT devices alone? Do election officials prevent two or more voters from using the NVT devices at the same time? Where assistance is given to voters, who is providing this assistance and are measures taken to safeguard against any influence on the voters?
- Is there overcrowding? How long do voters have to wait in order to vote? Are there a sufficient number of devices to keep waiting times reasonable?
- Are disabled and elderly voters able to use the devices without assistance? If minority languages are used in the voting process, can these be accessed on the device without difficulty?
- If any external ports or other elements of the ICT devices are supposed to be sealed during the course of voting, can STOs verify that the seals are in place and that the seals' unique numbering is recorded?
- Do officials adhere to established procedures, or do they deviate from the procedures? For what reasons?
- How well do polling officials appear to understand the process? Are they able to address problems if necessary? If not, are there technicians present who are responsible for fixing problems and are they commissioned by the election administration or by the vendor? If there are problems with devices while STOs are present, are these recorded in an official logbook or protocol and then duly transmitted?
- If the ICT equipment is unavailable, do voters register by paper voter lists and cast paper ballots, or do they have to wait for a replacement device? In the case of ballot scanners, are votes deposited in a temporary ballot box? Do any voters leave without voting?
- What are the views of observers, political party or candidate representatives on the use of ICT and NVT in the voting process in the polling station?

- Are closing procedures adhered to? Is a paper copy of the results per device and polling station printed and made available for observers and political party representatives? Are copies also posted for public display?
- How are the polling station results transmitted to higher levels of the election administration? Are they supported by ICT? Are the procedures for this transmission followed? If not, why not?
- Are any immediate audits of the results conducted at the polling station?
- Do voters have a choice between voting electronically or on paper? Are they instructed to use either option?

Chapter 10

Reporting: making ssessments and recommendations

It is vital that EOM reporting on all aspects of an election process is factual, accurate and balanced. Where election technology is used, assessments of the use of these technologies should contribute to the overall assessment of an electoral process. This assessment should also form the basis for any recommendations that the EOM may make in this area to assist OSCE participating States with improving their electoral processes in line with their commitments and standards for democratic elections.

The aim of this chapter is to explain how to provide an assessment of the functions of the ICT system and other election technology use-cases. Where an election includes the use of technology for voting and other processes, EOM reports may have a section dedicated to this aspect of the election. This may deal with cybersecurity issues in the electoral process and may have a broader emphasis on ICT solutions. Reporting should be as concise as possible and understandable for a non-technical audience, yet in-depth enough to present a nuanced understanding. While it may be necessary to include some technical details about the system, these should generally be put in footnotes or annexes. The EOM's reporting on the use of election technology should identify positive elements of the process as well as any weaknesses of the system. The EOM should bear in mind that the use of technology cannot be seen in isolation but as part of a broader electoral process. In making assessments, consideration should be given to how the implementation of technology affects other aspects of the election process.

Many of the assessments that must be made about the use of technology cut across the roles of the various core-team members. The Legal Analyst should work with the ICT Analyst to assess whether the legal framework adequately regulates the use of ICT solutions and whether there have been any complaints and appeals related to, or impacting upon the use of ICT or NVT. Together with the Political and Media Analysts, the ICT Analyst will assess the political and public discourse that surrounds the use of NVT and other election technologies.

Together with the LTOs, the ICT Analyst will assess any regional disparities in the use of ICT, as well as any usability and testing issues. At the same time, the Political Analyst and LTOs, together with the ICT Analyst, will evaluate the opinions of political parties, contestants and other electoral stakeholders about the system, and the Election Analyst will assess the feedback of the election administration on ICT and NVT.

The OSCE commitments and international standards are the basis for making assessments and recommendations about technology. Where appropriate, relevant international good practice should also be considered, especially as it relates to detailed aspects of the use of the technology. The assessments should also include applicable national legislation.

The commitments and standards are summarized in the principles discussed in Chapter 2 of this Handbook. The EOM's assessments, conclusions, and recommendations about the use of ICT and NVT in a given election should relate to these principles. All of these should be taken into consideration in the mission's assessment of the degree to which the use of NVT and other ICT is consistent with OSCE commitments, and the principles described above.

The EOM should make relevant recommendations on how the use of ICT in electoral processes can be improved, through modifications to the system, changes in its management or implementation, or with amendments to legislation. The recommendations should provide sufficient guidance for the stakeholders on how to implement or change certain ICT solutions in line with the international obligations and standards and good practice.

It is crucial that recommendations are concise, not overly prescriptive and drafted in line with the principles mentioned above. The electoral recommendations of the final report are the guiding benchmarks for follow-up activities before the next elections.[74]

While it is important for recommendations to be sound and implementable, it is also crucial that recommendations about technology are understandable to non-specialists. Recommendations should be backed up by concrete findings of shortcomings and possibilities for improving current practices to bring them more in line with standards and good practice. It is also important that recommendations are coherent and do not contradict one another.

Of any set of recommendations, some may be priority recommendations, to address essential changes of greater urgency or importance. A balanced evaluation needs to be made about whether a given recommendation on technology qualifies as a priority recommendation.

When shortcomings are more serious and the verifiability of results is not possible, or when the continued use of technology appears to undermine public confidence in the electoral process, the EOM may decide to recommend that the use of NVT or any other technological solution be reconsidered until such issues can be overcome.

74 See Handbook on the Follow-up of Electoral Recommendations, OSCE/ODIHR, 6 June 2016.

Annexe A

Master Checklists

ASSESSMENT OF THE CONTEXT FOR NVT OR ICT IN ELECTIONS

- Which electoral processes are supported by ICT? What are the reasons for introducing ICT in elections?

- What was the extent of public discussion for introducing or using ICT in elections? Were the views of political parties, civil society organizations and experts taken into account? What is the level of overall public confidence in the election process, the election administration and the technology?

- How does the ICT affect potentially vulnerable groups of voters and what are their views?

- How is the use of ICT and NVT defined and regulated in the legislation? Is the regulation governing the use of ICT and NVT sufficiently detailed to provide clear guidance on all technology issues, including in cases of ICT failures?

- Does the legal framework adequately define the role of the EMB as the main institution with overall responsibility and oversight for the conduct of the election process? Are different phases of the ICT and NVT processes, (such as procurement, testing, certification, audit of equipment and software) and the roles and responsibilities of other actors, such as private vendors or other state agencies, clearly defined in the legislation?

- What is the extent of vendor involvement in the management and operation of ICT or NVT systems? Does such involvement guarantee the independence or impartiality of the EMB? What are the contractual arrangements between the EMB and the vendor and what accountability provisions are in place?

- Were certification standards determined before the acquisition of the technology or do they appear to have been tailored to an already existing system? Were the standards and certification reports made publicly available? To what extent was the certification process meaningful?

- What percentage of polling stations will use NVT or other ICT-based devices? Will voters in polling stations with NVT devices be able to vote by paper if they prefer this method? Are there any noticeable regional differences across the country? How are specific groups of voters affected, such as persons with disabilities, illiterate voters, the elderly or voters belonging to national minorities?

- Do observers have access to meaningful observation of the NVT and ICT in elections? Are there any parts of the process to which observers do not have access? Are all reports related to the introduction and use of ICT and NVT in elections publicly available?

- Do legal provisions allow for effective review of ICT and NVT based complaints? Who can file complaints and what is considered evidence? Were complaints lodged before on ICT or NVT-related matters?

OBSERVATION AND ASSESSMENT OF NVT

- *EMB Management:* Does the EMB have full managerial control and oversight of the NVT process? Are there departments or units in the election administration dedicated to NVT? Are the roles and responsibilities clearly defined? What level of understanding do EMB officials have of NVT and have they received necessary training? Have officials received information, materials and financial resources sufficiently in advance to enable them to manage the system appropriately?

- *Secrecy Measures:* What measures are in place to ensure the secrecy of the vote (both in NVT and traditional voting method)? Have interlocutors raised any doubts about the effectiveness of these measures? Does the NVT system allow a voter to be identified with their vote, or permit a voter to be directly intimidated or influenced in their choice?

- *Testing:* Has the election administration ensured that the NVT system has been completely tested before use? Is complete documentation about testing available to the EOM and/or other election stakeholders such as political parties, citizen observers, etc.? Was official testing observed by electoral stakeholders? Could they conduct their own test?

- *Voter Education:* How are voters informed about the introduction of NVT? Are there public information campaigns organized on universal terms (for voters with disabilities, in minority languages etc.)?

- *User Experience and Accessibility*: How easy is the system to use and how easy is it for the voters to learn to use? Have usability tests been run and what were the results? What functions have been included to increase access for voters with disabilities?

- *Ballot Equality*: Are all contestants presented equally on the ballot and is scrolling needed to access the full list of candidates? Is all information required by law presented on the ballot?

- *Contingency Plans***:** Is there an alternative plan in case the NVT system is not functional? How are the NVT protected against physical malfunctions and other incidents (e.g., loss of electricity) and are polling officials trained to deal with the problems? How are basic issues with the NVT mitigated, by election officials or other specialists?

- *Data Compatibility*: Are the different kinds of software used to manage the election process and to run NVT compatible and have there been tests to verify this?

- *Voting Process*: Does the NVT system indicate when the vote is about to be cast and confirm that it has been cast? Does it show which choice was selected and give the voter the opportunity to make changes?

- *Coercion Resistance*: In an uncontrolled environment for voting, are measures in place to provide voters to avoid undue influence (e.g., the ability to re-cast a ballot electronically or cancel an electronic vote by casting a paper ballot)?

- *Security Measures*: What safeguards are in place to prevent hacking? (e.g., is there a protocol for handling the devices and other centrally used systems?) Who/what institution is responsible for providing cybersecurity and intrusion resilience? Do the devices have any readily accessible interfaces, such as USB ports? If so, how are these secured? Can they be accessed by Internet, or wireless means? If so, what protection measures are in place to ensure data integrity?

- *Verifiability*: What verification methods are used to prove the integrity of the results? Do observer groups, political party representatives and other stakeholders have full access to the observation of the verification process?

- *Post-Election Audits*: What audits are undertaken and by whom? What happens if an audit reveals errors or discrepancies? Have any manual recounts been requested and conducted?

- *Tabulation and Results Publication*: If the tabulation and results publication process relies on transmission of data by Internet, what measures are in place to prevent or detect external hacking to either retrieve or alter data? What measures are in place to prevent illegitimate internal manipulation of the system?

OBSERVATION AND ASSESSMENT OF 'ANCILLARY' PROCESSES AND SYSTEMS

- *EVRVS Responsibilities:* Is there proper delineation of roles and responsibilities between the different agencies involved in the implementation of a voter registration database (e.g., the Ministry of Interior, the Office of Statistics, etc.)? Do these regulations ensure the independence of the EMB and its overall control on the conduct of election process?

- *EVRVS Resources:* Has the EMB chosen an in-house solution or have they contracted external vendors to provide the system? If the latter, are the roles and responsibilities appropriately delineated, recognizing that the EMB holds primary responsibility? Are there proper resources available to address the issues of technology in the voter registration process, both human and financial?

- *EVRVS Data Access:* Is there a system of access rights and controls in place to ensure that data is only available to those authorized and under specific conditions? Can this access be logged and tracked for future reference?

- *EVRVS Integrity Measures and Training:* Is chain of custody documentation in place to ensure the integrity of data during any transfers? Are there measures in place to ensure that data is only changed under specific conditions and that inappropriate changes can be identified and attributed? Has there been proper training for the EMB staff authorized to use the EVRVS on the risks or vulnerabilities that may exist and their role in mitigating these risks? Have training materials (handbooks, leaflets, videos, etc.) been developed and distributed to this end?

- *EVRVS Outreach:* Has there been sufficient transparency and outreach by the EMB to inform voters about the EVRVS so that they understand how the system works and have proper identification documents?

- *EVRVS Security:* Have proper risk assessments been undertaken, has extensive testing taken place to identify any issues prior to implementation of the system and are measures in place to ensure that data is available and protected in case of attack, system failure, power outages and the like?

- *EVRVS Functioning:* Does the EVRVS function properly throughout all stages of the electoral process and especially on election day? Is the system having any impact on the flow of voters and their ability to vote?

- *RMS Responsibilities:* How is the RMS structured? Who is responsible for data entry? Who is responsible for supervision and oversight? Do the polling staff have the necessary skills for data entry and overall management of the system? Have they received training?

- *RMS Data Access:* Who is authorized to make changes in the protocols and elections results databases? How are users authenticated? Are there audit logs that maintain records of when databases were accessed, and are there written procedures to monitor them? Are political parties or other election stakeholders granted privileged access to the RMS? What are their views?

- *RMS Testing:* Was the RMS tested and reviewed before deployment? Who has tested the system? What are the views of the election stakeholders on the integrity of the RMS?

- *RMS Functioning:* Are polling stations or tabulation centres equipped adequately? What is the condition of the equipment? What is the level of connectivity? Are there any issues with the supply of electricity or network connectivity? Do the electronically published results and protocols contain the necessary data for verifying the accuracy of the election results? Are the results audited?

- *RMS Integrity Measures:* Are there risk-mitigation strategies and plans in place in case of equipment or software failure? Are the members of the EMB and polling staff aware of these plans? Is there clarity about the procedures and formal rules in place in case of ICT equipment or software failures? How are staff replacements dealt with? Are there any regional or local differences?

- *Candidate Registration:* Is the system for collecting candidate signatures in place adequate and do contestants fully understand the process? Is the ICT solution properly regulated from a legal point of view, protecting all fundamental rights, including personal data protection? Is the signature collection environment maintained by the public sector or by electoral contestants?

ASSESSMENT OF CYBERSECURITY MEASURES

- What legal and administrative cybersecurity provisions pertain to elections and what bodies are responsible? Has the provision of cybersecurity been done holistically, according to an electoral cycle approach?

- Has the EMB introduced a formalized, well-defined cybersecurity risk management framework to deal with possible vulnerabilities? Is cybersecurity high up the agenda of the EMB and do they understand the potential ramifications for electoral integrity if not properly handled?

- Have cybersecurity frameworks and risk-management strategies been tested well in advance of election day? Has a strategic review been conducted and what are its findings?

- Have there been any previous cyberattacks and of what nature? Are there concerns about possible cyber-threats in these elections? How large is the potential attack surface? Is it centralized or localized?

- Are EMB staff at all levels properly trained on their role within this framework and do they have a solid understanding of cyber-hygiene and its importance?

- Has inter-agency collaboration been established, including on general cyber-incident management (e.g., with Computer Emergency Response Teams) and are roles and responsibilities properly delineated?

- Has the election administration been classified as 'critical infrastructure'? If so, for what reasons and are the comparative benefits/risks understood?

- Has the EMB provided selected vendors with clear security requirements and protocols? In the event of vendor selection, is it clear that the EMB is ultimately responsible for infrastructure, data, processes and communications, in line with international good practice?

- Are there appropriate paper backups in the event of system failure and have appropriate contingency plans been planned and rehearsed? For which systems there are paper backups?

- Which bodies are responsible for conducting security assessments and preventing cyberattacks on election-related infrastructure? Do laws and regulations provide for cooperation among these bodies?

- How is the security of systems monitored throughout the election and what communication mechanisms are in place in case of any security issues?

- What long-term privacy mechanisms are in place to ensure that sensitive data is duly destroyed after elections to avoid any privacy risks?

LONG- AND SHORT-TERM OBSERVERS

- *EMBs Preparations*: To what extent are election officials familiar and comfortable with their role in organizing or providing oversight of the use of NVT and other electoral technologies? How will technical expertise or assistance be provided on election day, especially in the event of problems?

- *Training:* What are the plans for training lower-level election officials? How useful does such training appear to be in practice? How much is technology integrated into the training process?

- *Equipment and Functioning*: Have a sufficient number of ICT and NVT devices been received, and were they received and set up in a timely manner? How is electronic voting or voter identification equipment stored? Do any problems arise during the set-up of the devices in polling stations? If so, are election officials able to resolve them? Do voters appear to understand how the devices function? How many voters require assistance with completing the voting process? Do any voters terminate the process after initiating it but before casting a ballot?

- *Security Measures:* What security measures are in place to prevent tampering? Who has access to the ICT devices and is this access recorded in a protocol? Are the ICT systems connected to the Internet? If so, what security measures are in place to guard against possible hacking? If any external ports or other elements of the ICT device are supposed to be sealed during the course of voting, can STOs verify that the seals are in place and that the seals' unique numbering is recorded?

- *Outreach:* What are the reactions of voters, party representatives and citizen observers to the technology? Have they had the opportunity to test devices or review documentation about the process? Will they observe the process? Are voter education materials available? How widespread are voter education activities through the EMBs or in local media?

- *Secrecy:* What steps are taken to ensure that the devices' electronic memories do not contain any voters' data or votes before the start of voting? Is this verifiable? Does the set-up of the ICT devices in the polling station protect the secrecy of the vote? Do election officials ensure that voters cast their ballots in secret, even if voters need assistance with using the devices? Do voters approach NVT devices alone?

- *Accessibility:* Are disabled and elderly voters able to use the devices without assistance? If minority languages are used in the voting process, can these be accessed easily on the device?

- *Polling Boards:* How well do polling officials appear to understand the process? Do they adhere to established procedures, or do they deviate from the procedures and for what reasons? Are they able to address problems if necessary? If not, are there technicians present who are responsible for fixing problems and are they commissioned by the election administration or by the vendor? If there are problems with devices, are these recorded in an official logbook or protocol and then duly transmitted?

- *Voting Procedures:* Do voters have a choice between voting electronically or on paper? Are they instructed to use either option? Do voters register by paper voter lists and cast paper ballots, or do they have to wait for a replacement device, if the ICT equipment is unavailable? Do any voters leave without voting? What are the views of observers, political party or candidate representatives on the voting process in the polling station?

- *Counting Procedures:* Are counting procedures adhered to? Is a paper copy of the results per device and polling station printed and made available for observers and political party representatives? Are these copies also posted for public display?

- *Tabulation Procedures:* How are the election results transmitted to higher levels of the election administration? Are they supported by ICT? Are the procedures for transmission followed? If not, why not? Are any immediate audits of the results conducted at the polling station?

Annexe B

Selected OSCE election-related commitments

1990 OSCE Copenhagen Document

(6) The participating States declare that the will of the people, freely and fairly expressed through periodic and genuine elections, is the basis of the authority and legitimacy of all government. The participating States will accordingly respect the right of their citizens to take part in the governing of their country, either directly or through representatives freely chosen by them through fair electoral processes. They recognize their responsibility to defend and protect in accordance with their laws, their international human rights obligations and international commitments, the democratic order freely established through the will of the people against the activities of persons, groups or organizations that engage in or refuse to renounce terrorism or violence aimed at the overthrow of that order or of that of another participating State.

(7) To ensure that the will of the people serves as the basis of the authority of government, that participating States will

(7.1) hold free elections at reasonable intervals, as established by law;

(7.2) permit all seats in at least one chamber of the national legislature to be freely contested in a popular vote;

(7.3) guarantee universal and equal suffrage to adult citizens;

(7.4) ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public;

(7.5) respect the right of citizens to seek political or public office, individually or as representatives of political parties or organizations, without discrimination;

(7.6) respect the right of individuals and groups to establish, in full freedom, their own political parties or other political organizations and provide such political parties

and organizations with the necessary legal guarantees to enable them to compete with each other on a basis of equal treatment before the law and by the authorities;

(7.7) ensure that law and public policy work to permit political campaigning to be conducted in a fair and free atmosphere in which neither administrative action, violence nor intimidation bars the parties and the candidates from freely presenting their views and qualifications, or prevents the voters from learning and discussing them or from casting their vote free of fear of retribution;

(7.8) provide that no legal or administrative obstacle stands in the way of unimpeded access to the media on a non-discriminatory basis for all political groupings and individuals wishing to participate in the electoral process;

(7.9) ensure that candidates who obtain the necessary number of votes required by law are duly installed in office and are permitted to remain in office until their term expires or is otherwise brought to an end in a manner that is regulated by law in conformity with democratic parliamentary and constitutional procedures.

(8) The participating States consider that the presence of observers, both foreign and domestic, can enhance the electoral process for States in which elections are taking place. They therefore invite observers from any other CSCE participating States and any appropriate private institutions and organizations who may wish to do so to observe the course of their national election proceedings, to the extent permitted by law. They will also endeavour to facilitate similar access for election proceedings held below the national level. Such observers will undertake not to interfere in the electoral proceedings.

1991 OSCE Moscow Document

(24) The participating States reconfirm the right to the protection of private and family life, domicile, correspondence and electronic communications. In order to avoid any improper or arbitrary intrusion by the State in the realm of the individual, which would be harmful to any democratic society, the exercise of this right will be subject only to such restrictions as are prescribed by law and are consistent with internationally recognized human rights standards. In particular, the participating States will ensure that searches and seizures of persons and private premises and property will take place only in accordance with standards that are judicially enforceable.

Annexe C

—

Good practice documents, relevant court cases and additional reading

Good practice documents, guidelines, reports and other reference materials

- Council of Europe Committee of Ministers to member states Recommendation CM/Rec(2017)5 on standards for e-voting.

  https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f

- Council of Europe Committee of Ministers Guidelines on the use of ICT in electoral processes.

  https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9

- Council of Europe Handbook on Digital Technologies in Elections (2020) (overview of recommendations and explanations on regulation and implementation of digital solutions).

  https://rm.coe.int/publication-digital-technologies-regulations-en/16809e803f

- Understanding Cybersecurity Throughout the Electoral Process: A Reference Document by IFES (2022) (report on the many facets of cybersecurity in elections).

  https://www.ifes.org/document/understanding-cybersecurity-throughout-electoral-process-reference-document-overview-cyber

- Primer: Cybersecurity and Elections, USAID/DAI/IFES (2022) (Introduction to the key risks, their mitigation strategies and industry-standard frameworks in the topic of cybersecurity and elections).

  https://pdf.usaid.gov/pdf_docs/PA00ZK5K.pdf

- Cybersecurity of Voter Registration by IFES (2023).

  https://www.usaid.gov/democracy/document/may-22-2023-briefing-paper-cybersecurity-voter-registration

- Compendium on Cyber Security of Election Technology by NIS Cooperation Group (ENISA, EU) (2018) (compendium of the topic of securing election technology).

  https://www.govcert.cz/download/akce-a-udalosti/Election_security_compendium_July_5_2018.pdf

- Certification of ICTs in elections by International IDEA (2015) (a good practice overview of the certification of technology used in elections).

  https://www.idea.int/sites/default/files/publications/certification-of-icts-in-elections.pdf

- Electoral management handbook by International IDEA (2014) (a good practice compendium on electoral management, with a comprehensive chapter on election technology).

  https://www.idea.int/publications/catalogue/electoral-management-design-revised-edition

Relevant court cases

- Austria: Constitutional Court, Judgment of 13 December 2011 regarding the 2009 Federal Students' Elections (V 85-96/11-15).

  https://www.vfgh.gv.at/downloads/VfGH_V_85-96-11_e-voting.pdf - in German

- Estonia: Constitutional Review Chamber, Judgment of 1 September 2005, regarding Petition of the President of the Republic (3-4-1-13-05).

  https://www.riigikohus.ee/en/constitutional-judgment-3-4-1-13-05 - in English

- Finland: Supreme Administrative Court, Judgment of 4 September 2009, regarding Finnish Municipal Elections 2008 (687/1/09).

  https://www.finlex.fi/fi/oikeus/kho/vuosikirjat/2009/200900899 - in Finnish

- Germany: Federal Constitutional Court, Judgment of 3 March 2009 regarding the 2005 Federal Bundestag elections (2 BvC 3/07, 2 BvC 4/07).

  https://www.bverfg.de/e/cs20090303_2bvc000307en.html - in English

Additional academic reading

- Mark Lindeman and Philip B. Stark, "Gentle Introduction to Risk-limiting Audits", *IEEE Security and Privacy*, Special Issue on Electronic Voting, Vol. 10, Issue 5, 2012.

  https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

- Dirk Helbing et al., "Will Democracy Survive Big Data and Artificial Intelligence", *Scientific American*, 25 February 2017.

  https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/

- Jesse Dunietz, "Are Blockchains the Answer for Secure Elections? Probably Not", *Scientific American*, 16 August 2018.

  https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/

- Lucas Mearian, "The top 8 problems with Blockchain", Computerworld.com, 8 July 2019.

  https://www.computerworld.com/article/3236480/top-8-problems-with-blockchain.html

- Bernard Marr, "The 5 Big Problems With Blockchain Everyone Should Be Aware Of", Forbes.com, 19 February 2018.

  https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/

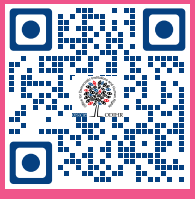
- Colleen M. Newbill, "Defining Critical Infrastructure for a Global Application", *Indiana Journal of Global Legal Studies*, Vol. 26, Issue 2, Summer, 1 August 2019.

  https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1717&context=ijgls

- Brian E. Humphreys, "Critical Infrastructure: Emerging Trends and Policy Considerations for Congress", Congressional Research Service, 8 July 2019.

  https://www.everycrsreport.com/files/20190708_R45809_54416d7b2f43d41696e8e971832aea5fe96a9919.pdf

Almost all OSCE participating States use some form of Information and Communication Technologies (ICT) in their electoral processes. These technological developments inevitably bring certain benefits but also numerous challenges that were not common for traditional, paper-based elections. This new edition of the Handbook updates the ODIHR methodology for the observation and assessment of ICT used during voting and counting processes and includes new aspects such as electronic registration, verification of voters and candidates, and cybersecurity issues. While the Handbook is mainly for election observers, we hope that it will provide useful guidance for OSCE participating States in their efforts to introduce and use ICT-based election solutions.



Office for Democratic Institutions and Human Rights
OSCE ODIHR