Report of the State Comptroller of Israel | March 2022

Cyber Security Safety

Information Systems and Cyber Security in the Elections to the 21st, 22nd, and 23rd Knesset

Information Systems and Cyber Security in the Elections to the 21st, 22nd, and 23rd Knesset

Background

The Knesset elections lie at the foundation of the democratic nature of Israel's political regime and the right to vote and be elected was recognized as one of the fundamental rights in Israel.

The Israeli Central Elections Committee is in charge of preparations for the Knesset elections and their proper management, including organizing the elections, supervising them, and summarizing their results. Operating under the Central Elections Committee is a regular administrative staff (the Elections Committee) of 30 employees, preparing for the elections and organizing, managing, and executing them.

The Elections Committee is an independent statutory body established under the Knesset Elections Law (Consolidated Version) 1969; hence, it is not subordinate to the decisions of the executive authority nor its instructions, in light of the need for its independence from the government.

Upon the declaration of elections and approximately 90 days before them (the elections period), the Elections Committee establishes regional committees across the country in charge of the management, organization, and execution of the elections in the constituencies entrusted to them. In the years 2019 and 2020, 19 regional committees were appointed.

The Elections Committee manages the data systems and infrastructure operated in the elections procedure and their cyber security aspects.

The voting process in Israel is mainly manual; a computer network performs only the stages of summing up and publishing the election results. However, many data systems are operated to support the many processes associated with preparations for the elections, managing them, and supervising their purity. Harm to the reliability, availability, and confidentiality of the data in the system could undermine public trust in the election process and its results.

For the first time in Israel's history, three consecutive election campaigns were held within less than a year, from 9.4.19 to 2.3.20. In light of this, since December 2018, the Elections Committee has been in election periods. This report was submitted to the election committee several weeks before the election campaign for the 24th Knesset. This report includes a review of the three election campaigns regarding the data systems and cyber security, the deficiencies that repeated themselves in the three election campaigns and deficiencies that were rectified between the campaigns. This audit examined the preparations and workflows of the Elections Committee, according to the guiding professional infrastructure formed over the years by the regulatory bodies of the state to regulate the activity of bodies with sensitive computer infrastructures.

Key figures

NIS 1 billion

execution of the Elections Committee[1] budget in the three election campaigns examined

NIS 139 million

execution of the computerization budget in the three election campaigns examined

10 data systems

the number of systems reviewed in the audit, including System 1, the main system serving the Committee, and System 2

19 year has passed

since winning the tender (2002) for development and maintenance of System 1, the main data system serving the Elections Committee until the end of the audit in August 2020

1,855 polling stations (17%)

the number of polling stations out of 10,631 polling stations controlled, regarding election purity, in the elections to the 23rd Knesset

middle of 2017

the Elections Committee began to increase the level of cyber protection of its data systems. The Committee had not previously seen any threat to the elections from the cyber aspect

333,603

the number of voters through double envelopes[2] in the 23rd Knesset elections – growth of 37% in less than a year (between the elections to the 21st and 23rd Knesset). The total growth rate in the number of voters in the stated period was approx. 6.3%

nearly a quarter

23% of the double envelopes either disqualified or not counted in the elections to the 23rd Knesset were those of the polling stations committees members or their secretaries, in charge, among other things, of protecting the purity of the election process

[1] Execution of the budget including all of its changes, not including required surpluses.

[2] The official name is external envelopes.

Audit actions

From January 2019 to August 2020, the State Comptroller's office examined, intermittently, the preparedness of the Election Committee for the election campaigns of the 21st, 22nd, and 23rd Knesset on the following issues: the Committee's data systems, their cyber protection, and functioning in the three election campaigns. The audit was conducted in the Elections Committee and the regional committees. Completion examinations were conducted at the national superintendent of the elections in the Ministry of Interior, at the Privacy Protection Authority in the Ministry of Justice, at the office of Cyber and Digital Matters – in the e-government unit in the Government (information and communication) ICT Authority, and the Prime Minister's Office in the National Cyber Directorate.

On election night of each of the three elections and in the following days, 30 State Comptroller's office auditors conducted an audit at the Elections Committee in the Knesset and 10 of 19 regional committees. 18 of 19 regional committees were examined in all of the election campaigns.

After each of the two first election campaigns, the State Comptroller's office submitted a list of topics in which it found gaps in the auditing process undertaken on the previous election campaign that could be rectified quickly; for example, by a change of instructions. After each of the first two election campaigns, the Elections Committee rectified some of the gaps noted by the State Comptroller's office.

As part of the audit, the State Comptroller's auditing team performed statistical analysis for the election campaigns of the 22nd and 23rd Knesset, performed shortly after the elections based on election results files published by the Elections Committee every few hours after the closing of the Election Day. In each statistical analysis, the results of the elections published were examined (results that were still unofficial at that time) as opposed to the official results of the previous elections to pinpoint polling stations with irregular activity.

The statistical analysis performed by the State Comptroller's office encompassed 150 polling stations consisting of irregular activity. This information was submitted to the Committee as part of the election purification operation. The election committee examined all polling stations delivered to it by the State Comptroller's team, including 26 new polling stations it had not previously reviewed as part of the election purification operation. Furthermore, in three polling stations, the voting results were changed following the Committee's examination.

By the authority given to the State Comptroller's Office under Section 17(c) of the State Comptroller Law 1958 [Consolidated Version], considering the government's arguments, consulting with the bodies protecting of national security data, coordination with the Chairman of the Knesset, and as the subcommittee of the Knesset's State Control Committee failed to convene; it was decided to publish this report while imposing confidentiality on sections of it. These sections shall not be submitted to the Knesset, nor shall they be published.

Section 1 – Cyber security

Background

In Government Decision 2444 in 2015, cyber security is defined as the set of actions designed to prevent, neutralize, investigate and contend with cyber threats and cyber incidents and reduce impact and damage caused by them, before, during, or after their occurrence.

Key findings

- **Cyber security policy** – the Committee's work regarding the cyber field should be based on a defined procedure and work plans for routine between elections and during election campaigns. Gaps were found regarding policy formation.

- **The steering committee for cyber security** – the steering committee on cyber security was established in November 2018 but did not convene until the end of the audit in August 2020, while the Elections Committee was busy conducting three election campaigns.

- **Advancement of cyber security** – the government's preparedness for handling cyber security began over a decade ago, with decisions made in the years 2011 and 2015 designed to regulate this field. It was found that until 2017, the Elections Committee had not advanced the cyber security field.

- **A cyber audit during the election periods in the years 2019–2020** – the National Cyber Directorate and the Cyber Protection Unit (YAHAV) conducted cyber audits during the three elections periods examined. Conducting the audits during the election periods in which the systems are operated affected the content of the audits; thus, there was no way of conducting comprehensive, complex examinations that included all required aspects of cyber security doctrine: organizational application, network, and infrastructure. The gaps discovered in the audits were only partially rectified due to time constraints and the risks involved in making changes to the system just before the elections. In these circumstances, the Elections Committee circumscribed some gaps found in the audits with alternative means.

- **The information system and the interrelations between them** – the Elections Committee did not have a complete, updated picture of the data systems and infrastructure used by them (updated inventory) and the interrelations between the systems (architecture document).

- **Management of functional continuity** – the Elections Committee, worked without a functional continuity management document defining the systems and processes vital to the continued activity of the Committee during the election period and their recovery time.

- **The appropriate level of logical security for protecting the data** – the Elections Committee did not define the proper level of logical security for protecting the data in its systems, especially the sensitive data. In addition, gaps were found in various aspects of the logical security level.

- **Physical data security** – in the three election campaigns examined, gaps were found in this field.

- **The use made of electoral rolls by parties and factions** – in the supervision performed by the Privacy Protection Authority toward the elections to the 23rd Knesset, considerable gaps were found in how 19 parties examined implement the Privacy Protection Law and the regulations deriving from it. Examples of these gaps are as follows: the parties keep susceptible databases that include, among other things, information on people's political views. Most of the parties examined purchase information to improve their data or conduct polls without verifying whether the sources of information obtained are legal.

- **Election processes in Israel and around the world** – in Israel, a computer performs only the stages of summing up the results and publishing them. According to an international survey conducted in 2016–2019 in 182 countries, including the USA (about 160 countries responded), it was found that in 26% of them, voter identification at the polling station is performed by computer; in 20%, voting and counting procedures are computerized, and in 60% counting and publishing the results are performed by computer.

- **Voting with double envelopes** – between the 21st Knesset and 23rd Knesset election campaigns, there was a growth of 37% in the number of voting by double envelopes. Their number in the 23rd Knesset was 333,603, costing NIS 8 million[3] (twice the cost in the elections to the 21st Knesset and approximately 2% of the entire election budget).

- **Computerization of the voter identification process** – in 2007, the Elections Committee began computerizing the voter identification process; however, no further

[3] As part of the deployment for the elections to the 23rd Knesset, procurement processes were performed in order to serve future election campaigns as well, and from the elections to the 22nd Knesset on, the wages of the counting committees were updated.

progress was made. Computerization of the process is expected to make the voting with double envelopes redundant. In addition, no use was made of the smart ID card to identify voters at the polling station.

Formulating a security concept for the elections period – at the end of 2018 and toward the elections to the 21st Knesset, the Elections Committee formed a security concept deriving from two main threats. The Elections Committee operated the three election campaigns examined according to its concept.

Increasing the level of systems' security in the years 2019‒2020 – over these years, the Elections Committee increased the security level of its main data systems and performed by the Cyber Directorate and YAHAV, ten audits, and penetration tests, rectified a significant part of the gaps raised in these audits or circumscribe them.

Use of a magnetometer to detect voting materials in the regional committees – in some of the regional committees in the 23rd Knesset elections, detectors to locate sensitive materials were used, including double envelopes, in real-time, to prevent their transfer to the logistical, operational center of the Elections Committee.

Key recommendations

- It is recommended that the Elections Committee convene the cyber security steering committee and form policy procedures for the Committee's work during the elections period and routine times (between election campaigns) regarding all aspects described in the YAHAV instructions. It is recommended that the Elections Committee manage, on an ongoing basis, the cyber risks on both the organizational level and that of the main systems, according to the commonly accepted standards. It is further recommended that the Committee monitor the treatment of gaps through recurring audits.

- Due to the high risk to democracy from cyberattacks that might sway election results, the Elections Committee should adopt (as mandatory professional norms with the necessary changes for the Committee) the guidelines of the Cyber Directorate and YAHAV for cyber security or other stringent rules according to international standards. Similarly, it is recommended that the Elections Committee consider the possibility of ongoing cooperation with the Cyber Directorate in both routine times and elections. The Cyber Directorate will thus accompany the Elections Committee and guide it through all of the main processes.

- It is recommended that the Elections Committee define the level of logical security appropriate for protecting the data and the sensitive business processes it manages. It is also recommended that the Committee adopt the YAHAV guidelines to implement security mechanisms.

- It is recommended that the national elections supervision unit, in collaboration with all the relevant bodies: the Population and Immigration Authority, the Elections Committee, and the Privacy Protection Authority, change the method of making electoral rolls accessible to parties and factions and thus enable tighter data security as well as monitoring and documenting the data used by the parties and factions and their suppliers.

- It is recommended that the Elections Committee reconsider computerizing the electoral rolls and the process of voter identification at the polling stations, considering the implications of the change and its suitability for voting procedures in Israel. Computerization of the process is expected to redundant the double envelopes and indirectly enhance the purity of elections in Israel.

- It is recommended that the Elections Committee and Ministry of Interior reactivate the public Committee for computerization examination of the elections to the Knesset and local authorities. Accordingly, advise computerization of voter identification at the polling stations and subsequently the entire voting process, including in comparison with progress in this field in the rest of the world.

The main actions of the Elections Committee and Cyber Directorate in cyber security in the years 2019–2020

Issue	Description of action
Forming an outline of the activity	• Arrangement of all work processes between the Election Committee and the Cyber Directorate considering the Committee's unique status • The outline of the activity was presented before the Attorney General of Israel
Forming a protective "shell" for the main IT and communications system	• The Cyber Directorate formed a protective "shell" for three election campaigns. • The Elections Committee approved the "shell" Reference threats have been defined

Issue	Description of action
	• The Committee's critical systems have been defined • Writing an operation command for each election campaign • Drawing conclusions and validation of the protective "shell" with linkage to a future election campaign
Audits and resilience tests in three election campaigns	• The Cyber Directorate – on some of the main data system components • YAHAV – on components of System 2
Forming of work procedures for the investigation of cyber incidents	• Division of areas of responsibility between the Cyber Directorate and the Elections Committee
Raising awareness of cyber attacks	• Development of educational software to increase awareness of cyberattacks among Committee employees and faction representatives
Immediate response to cyber incidents and irregular behavior	• Setting up a alertness room for the Cyber Directorate with representatives of various bodies attending • Representatives of the Cyber Directorate attending the main management sites of the IT systems
Reliability test	• The tests were performed for Elections Committee employees and its service providers by the General Security Service • The Committee has installed regulations on the matter
Reference threats and reference scenarios	• The Elections Committee has created a document for routine and as well as election periods
Forming and application of a security concept in the three election campaigns	• The Committee's security concept is derived from two main threats • The Committee implemented the security concept

Section 2 – Data analysis as an assistance tool for control of election purity

Background

Data analysis is used intensively around the world as an assistance tool for making decisions and exhausting the business value of the data. Data analysis is performed, among other things, with artificial intelligence (AI) technologies and machine learning, in which the computer studies the existing data in the database and uses mathematical models to perform segmentation of the data, identify irregularities, identify trends, and present predictive models.

Key findings

- **Consolidated database –** no consolidated database was managed in which all incidents occurring in polling stations over several election campaigns were documented. Creating a consolidated database and using AI technology to analyze data could help the Committee in the decision-making process. For example, quick identifying polling stations where irregularities occurred over several election campaigns and predicting the Committee's actions to prevent recurring.

- **Control of the data completeness in systems operated in the election purity operation** – in the elections to the 22nd and 23rd Knesset, data systems were performed to receive complaints regarding suspicious polling stations compromising election purity (source systems). None of the source systems documented data on the status of complaint closure (if decided to transfer for handling in system five or terminate handling). Without documentation, it is impossible to control the process as a whole and verify that all complaints the Committee decided to transfer for handing in system five were treated.

- **Authority separation for the handling of complaints on election purity** – it was found that the Elections Committee handled a sensitive process such as a complaint on election purity by one official examining and deciding and no additional control (not even sampled) to prevent human error, as required by the YAHAV instruction.

- **Voting on behalf of deceased voters –** in the 23rd Knesset elections, it was found, based on a comparison between Form 1000 and the resident registration that about 260 "deceased" people had voted. The Elections Committee performed an in-depth examination of 65 cases, and it found that 20 voters had indeed voted on behalf of the deceased. Thus, about 80 votes were on behalf of deceased persons in the elections to the 23rd Knesset[4].

- **Voting by citizens who, according to border control data, were abroad on Election Day –** an examination conducted by the State Comptroller's office based on Form 1000 found that approximately 9,000 people allegedly voted in the 23rd Knesset elections on behalf of citizens who were abroad. A random sampling of 5% of such voters in the elections to the 23rd Knesset indicated that 79 voters voted on behalf of people who were abroad (approximately 18% of voters in the sampling). Regarding 64 others (about 14%), the Elections Committee did not find the alphabetical index of the polling stations at which they voted. In addition, it was found that around 1,600 voters (about 18% of approximately 9,000 voters allegedly) voted on behalf of people who were abroad on Election Day (approximately 0.035% of actual voters).

Establishing a data system for managing an election purity operation since the elections to the 22nd Knesset – managing an election purity operation through a computerized data system enables control over thousands of polling stations examined as part of the operation and analyze the data of the examination processes and the treatment given.

Key recommendations

- In cooperation with the Population and Immigration Authority, it is recommended that the Elections Committee consider means to eradicate the phenomenon of people voting with the ID of deceased persons or abroad on Election Day. Computerizing the voter identification stage at the polling stations and comparing voter identity with the resident registration could prevent this.

- It is recommended to create a consolidated computerized database under the provisions of the law to assist decision-making while preparing for the next elections and in the process of identifying polling stations with irregular data over several election campaigns.

[4] Approximately 0.002% of voters in practice.

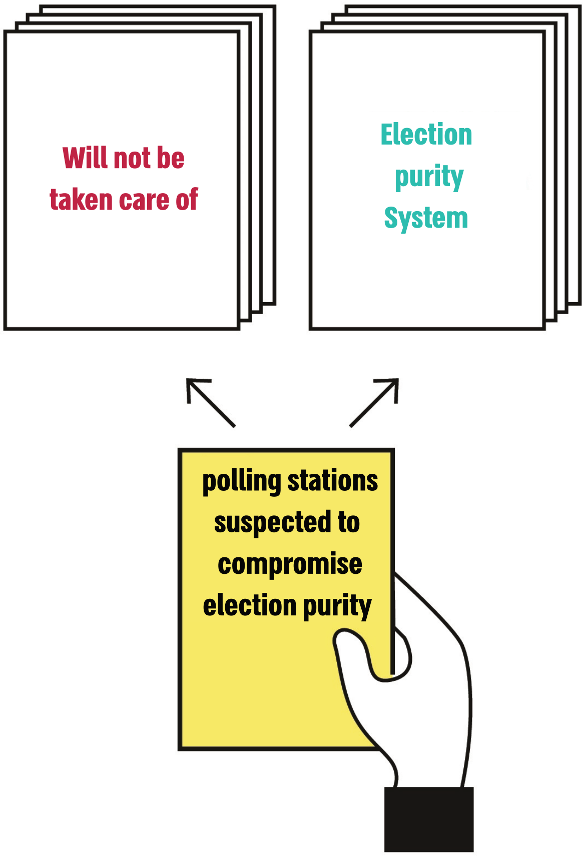
- As part of the computerized controls applied by the Committee, it is recommended to include statistical analysis, similar to that performed by the State Comptroller's office, to locate polling stations with irregular activity compared to election results published for the same polling station in previous elections. Accordingly, it is recommended that the Committee try to reduce the changes in the electoral rolls and polling station numbers.

- It is recommended to document the data of each campaign regarding complaints about election integrity compromise, assist the Committee in control over the integrity of the process, and verify that all complaints were handled to the end by the election purity system. In addition, the Committee will be able to analyze the overall data of complaints to identify trends and draw conclusions in preparedness for the next elections.

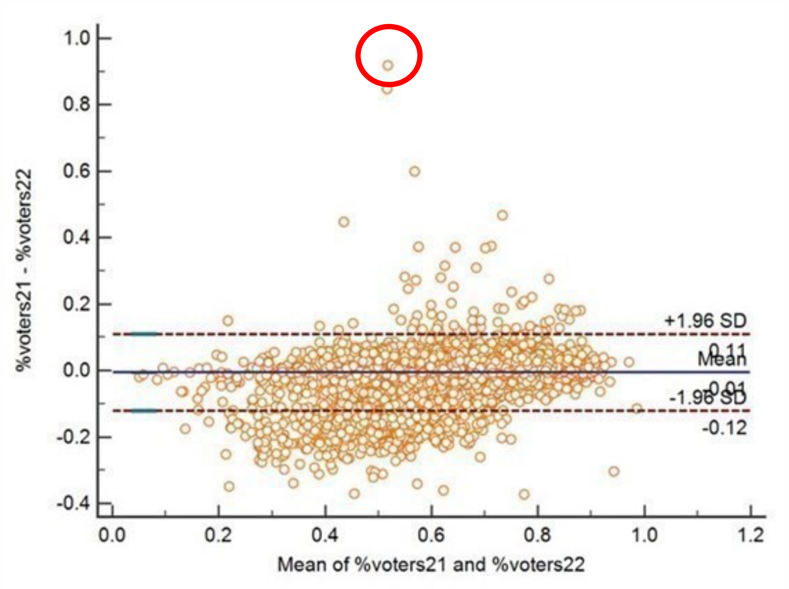
- It is appropriate to implement the separation of authority principle[5] regarding sensitive processes such as handling polling stations suspected of compromising election purity. Thus, one person will not be able to complete the whole process on his own and thereby avoid human error. In addition, it is appropriate to compare the data sample entered in the data system to the data in manual test forms scanned into the data system. Thus, controlling the handling of the complaint and verifying that it was performed as written in the forms.

[5] Separation of authority is to diminish data damage by one person with malicious or unintentional intent. According to the framework directive published by Yahav (11.11) in sensitive processes, a separation of powers must be implemented and one person will not be able to carry out a full process.

One person handling a complaint regarding election purity compromising


Will not be taken care of
Election purity System
polling stations suspected to compromise election purity

An example of statistical analysis performed by the auditing team in locating polling stations with irregular difference – 92% of the voting rate – between the 21st and the 22nd elections



Explanation: after the elections to the 22nd and 23rd Knesset, the State Comptroller's office submitted details of the 150 polling stations where statistical irregularities arose to the Elections Committee. After the elections to the 23rd Knesset, the Elections Committee announced that it had examined all 150 polling stations, including 26 that it had not previously reviewed as part of the election purity operation. Because of the examination performed by the Committee, the results of three polling stations were changed. In the Committee's response, detailed explanations were given for the irregular changes in voting rate observed at some polling stations.

Section 3 – Data system auditing

Background

The IT Department of the Elections Committee manages over ten different IT projects at various stages of initiative, establishment, and maintenance – the cost of which in the election periods of the three elections examined totaled approximately NIS 139 million. The IT Department is in charge of maintaining the data systems and their infrastructure, thus enabling them to support the management of the election campaigns. Maintenance of the systems includes developing the systems to support the requirements and new processes, handling the expected workloads, updating software versions, and data security updates.

Key findings

- **Engagement periods for development and maintenance of the Elections Committee's IT system** – the Committee has engaged with all IT firms to develop and maintain its data systems for an extended time – eight to 21 years. At the end of the audit date, in August 2020, 19 years had passed since the last tender was held (in 2002) for the development and maintenance of the main IT system serving the Committee – System 1.

- **Strategy and policy for ICT and the annual work plans of the IT Department** – no ICT strategy or policy has been formed yet. Furthermore, the IT Department does not manage yearly and multi-annual work plans for computerization activity in the department.

- **Management of work plans for the data systems** – the IT Department does not manage annual work plans for its data systems in various maintenance stages. However, the scope of payments to the five companies developing and maintaining these systems stood in 2019 at approximately NIS 50 million.

- **Steering committee** – the Elections Committee managed a steering committee for its main data systems – System 1 and System 2. No protocols of steering committee discussions were found, except for two protocols produced: one of a discussion on System 1 from December 1, 2012, and the other of a discussion on System 2 from August 2017. In addition, the Elections Committee did not conduct a steering committee for other data systems of financial scope greater than NIS 2.5 million, including System 3 and System 8.

- 👎 **System 2** – in the three election campaigns examined, malfunctions were found in the system, including incompatibility between the data of System 1 and System 2, which undermined the confidence of some of the Committee's Heads in the system's data due to operating the interface once a day, unavailability of the system and inability to contend with the workload and slowness.

- 👎 **System 3** – in the three election campaigns examined, malfunctions were found in the system, including communications problems, the inadequate skill of the scanners of voting materials, and partial scanning of voting materials, with some scanned at poor quality.

- 👎 **Preparedness for the replacement and updating of IT systems** – most engagements for the Elections Committee's IT system maintenance, including System 1, end within five years. The Elections Committee has not adequately prepared during the routine period to replace and substantially update the data systems to support new requirements and processes.

- 👎 **Documents of the conclusions drawn after each election campaign** – the Elections Committee did not require receiving documents from its main IT systems suppliers – of the conclusions drawn following each election campaign, not even regarding systems operated for the first time.

👍

Rectifications of the deficiencies noted in the elections to the 21st and 22nd Knesset – Following are examples of deficiencies rectified: the Elections Committee stopped the configuration of its information systems a month before election day; documented malfunctions and irregular events that occurred in the general rehearsal and on election night; checked the computerization plans before their operation; and applied control processes to the election results before they were published.

Development of a business intelligence (**BI**) **system** – to present activity status in the regional committees.

A general rehearsal was held, including all of the processes – exercises simulating reality vis-a-vis all bodies involved to simulate the entire election procedure.

Key recommendations

- All engagements regarding the Elections Committee's IT systems, except for System 2, are supposed to be terminated in the next five years (until 2025), including System 1, which the Committee has begun to prepare for its replacement. In light of the complexity of replacing IT systems, the Committee is advised to prepare in advance for their replacement.

- It is recommended that the Elections Committee form work plans and budgets of the IT Department as well as of each department separately and supervise execution vs. planning, adopt the Government ICT Authority's guideline regarding the lifecycle of ICT systems and establish a steering committee for projects defined by ICT Authority's as medium-sized projects and up or complex projects.

- It is recommended that the Elections Committee substantially change its IT systems during routine times. To test their impact on all involved bodies without compromising their systems, some of which have been operated since the election period beginning.

- It is recommended that the Elections Committee receive feedback and reports with conclusions from its main IT suppliers employed in the elections by no later than the end of their employment.

Summary

The Knesset elections are part of the foundation of the democratic nature of Israel's political regime. Therefore, it is essential that the election process is transparent and its results reflect the will of the voters. Compromising the reliability, availability, and confidentiality of the data stored in the IT systems used in the election process could undermine public trust in the election process.

The government's preparedness for dealing with cyber security began over a decade ago, with decisions made in 2011 and 2015 to regulate this field. Government activity in cyber security over the years was supposed to lead to the deployment of the Committee in earlier stages, including the establishment of a steering committee for cyber security and implementation of its decisions. Earlier preparations could have been an appropriate response to this sensitive issue if done between election campaigns.

The threat of cyberattacks on Israel's elections was identified only in the middle of 2017 in the wake of possible interventions in the US elections. Since then, the Elections Committee has begun mapping the threats with the Cyber Directorate. At the end of 2018, the Committee formed a security concept for handling the critical risks. It then started work on protecting essential systems and processes according to the newly developed concept.

Nevertheless, the audit raised some gaps concerning cyber security, data analysis as an assisting tool for controlling election purity, and auditing of data systems. In addition, gaps arose concerning the forming policy on cyber security and ICT.

The Elections Committee is recommended to convene the cyber security steering committee to form the policy procedures for the Committee's work during election period and in routine times, periods quite different in nature. It is also recommended to adopt (with the necessary changes for the Committee) the guidelines of the ICT Authority and the Cyber Directorate – bodies in charge of guiding the ministries in these fields – or other stringent rules according to international standards, in addition to the special-purpose tools designed to deal with complex attacks on organizations.

It is better not to engage in development work or measures designed to close gaps during the election period since this could jeopardize the system's operation and cause malfunctions. Therefore, it is recommended that the Committee increase the level of security of its systems, including management of cyber risks on an ongoing basis while closing gaps in this field. It is also recommended that the Committee convene steering committees to verify the development and maintenance of the systems according to the planning.

Regarding control of election purity, it is recommended that the Committee make sure that sensitive processes such as handling polling stations suspected of compromising election purity decisions be made by more than one person, so not one person can perform an entire process independently. In addition, it is appropriate to compare a data sample entered in the

data system to the data in manual forms. It is recommended that the Committee increase data analysis as an assisting tool for decision-making and concluding incidents that occurred in previous election campaigns to improve preparedness for the next elections.

It is commended that the Election Committee has met the challenge of conducting three election campaigns within just one year. Furthermore, the audit raised improvement in aspects examined from one election to another, and it is recommended to preserve them.

In light of technological development and increased use of voting with double envelopes and the high costs involved, it is recommended that the Elections Committee conduct an in-depth examination of the computerization of electoral rolls and voter identification process at the polling stations, and consider enhancing voter identification through the use of smart ID cards. The Committee should consider the implications of the change and whether it suites Israel's election procedures. Computerization of the process is expected to make the double envelopes redundant and indirectly enhance the purity of elections in Israel. It is also recommended that the Elections Committee and Ministry of Interior reactivate the public Committee for examining the computerization of the elections to the Knesset and the local authorities and advise requirements for the computerization of voter identification at the polling stations and, ultimately, the entire voting process, following the technological development and experience gained in this field in the rest of the world.

The Elections Committee and the rest of the audited bodies should rectify the deficiencies found and consider the recommendations.