Potential Cyber Threats to the National Elections in the Digital Age in Africa

Thuli Mkhwanazi[1,2(✉)], Avuya Shibambu[1,2], Vhuthu Nefale[1,2], Jabu Mtsweni[1,2], Jackie Phahlamohlaka[1,2], Muyowa Mutemwa[1,2], and Norman Nelufule[1,2]

[1] Council for Scientific and Industrial Research (CSIR), Pretoria, Brummeria 0184, Russia
tmkhwanazi@csir.co.za

[2] Defence and SecurityCluster, Information and Cybersecurity Centre (ICSC), Brummeria 0184, Russia

Abstract. This paper is a theoretical review following a systematic literature review aimed at providing insightful information and advisory regarding potential cyber threats to national elections in Africa in the digital age. It therefore, focuses on potential cyber threats to the general elections process in Africa. It highlights the importance of cybersecurity in relation to the digital and traditional electoral process. The paper delves into different types of cyber ills, citing examples from past instances worldwide including Africa, emphasizing the need for robust cybersecurity measures. It also discusses the possible impacts of cyber threats on the electoral process and its stakeholders. This paper offers mitigation techniques to ensure a safe and secure national general election, particularly in the cyberspace.

Keywords: Cybersecurity · Vulnerabilities · Cyber threats · Electoral Process · National Elections

1 Introduction

It is evident across different countries that the cyberspace is now playing an instrumental role in influencing national and local government elections for good or bad, and this is common in low-income, middle-income, and high-income countries. Cyberspace is therefore seen as the equalizer across countries when it comes to elections, and this is irrespective of whether countries have adopted digital applications such as e-voting or not.

Recently, Nigeria experienced over 12 million cyber-attacks during the 2023 Presidential Election [1] and suspicions of cyber spies infiltrating Kenyan networks long before the elections of 2022 were also reported by Reuters in 2023, however the Kenyan officials dismissed the allegations from this report [2, 3]. Regardless of the dismissal of the information by the Kenyana officials, a thesis by [4], corroborated that fake news and disinformation in campaigns has always given negative reflections on the cybersecurity measures of the country hosting elections [4]. In the above-mentioned thesis, it was also mentioned that in Brazil, fake news dominated the Brazilian presidential race including

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 333–350, 2025.
https://doi.org/10.1007/978-3-031-81570-6_22

politicians making claims of the fraudulent nature of the electronic voting system [4]. The false claims of vulnerabilities about the vote counting machines in the United States of America were also made by the presidential candidate in the previous elections and these claims ended up in courts and some cases are still ongoing [5-7].

It is considering the above-mentioned events that this study was conducted. The rest of the paper is structured as follows: Sect. 2 provides a brief description of the research process followed; Sect. 3 provides a high-level overview of current cyber threats and vulnerabilities that may impact on the General Election process; Sect. 4 reviews past cyber incidents that affected the election process in various countries; Sect. 5 presents potential cyber threats in the general election and discusses each; Sect. 6 discusses cyber vulnerabilities in the general election which are different from cyber threats; Sect. 7 delves into the impact of the cyber attacks on the election stakeholders; Sect. 8 discusses mitigation factors as this paper's major offering; and Sect. 9 concludes this paper.

2 Research Approach

The research presented in this paper followed a systematic literature review using popular research databases such as Scopus, Web of Science and Google Scholar. According to [8], a systematic literature review is a research approach that involves a comprehensive and structured analysis of existing academic publications and other relevant sources on a specific topic or research question. The primary goal of a systematic literature review is to provide a thorough and unbiased summary of the current state of knowledge in a particular field or area of study. In this research, we adopted the following steps in reviewing the potential cyber threats in national elections in the digital age focusing mostly on the threats influenced by the cyber space; (1) planning, (2) selection (3) extraction, and (4) execution These steps are demonstrated in the sections that follow.

3 Overview of Cyber Threats, Vulnerabilities and Attacks in General Elections

The proliferation of digital technologies comes with opportunities and benefits to improve electoral processes, such as ease of communication through social media and websites with voters, an increased uptake and awareness of voter registration, the ability for political parties to campaign far and wide with limited resources, casting of votes using electronic machines, digital counting of votes, including the live (instant) dissemination of election results. However, in as much as digital technologies provide benefits, there are increasing malicious actors who take advantage of vulnerable and insecure digital technologies in cyberspace to further their nefarious objectives in the election process.

It is reported by the European Union Agency for Cybersecurity (ENISA) that most countries in the European Union (EU) have "either postponed or discontinued the use of electronic voting, citing high threats and risks". According to the EU Cybersecurity Agency and ENISA, a high-level of cybersecurity is key for safeguarding the whole election lifecycle [9] to ensure:

- Democracy and human rights protection
- Critical assets protection
- Basic security protection
- Election integrity security

There are innumerable cyber threats and vulnerabilities that may affect an electoral process. These vulnerabilities emanate before, during, and after elections, and may be evident in the cyberspace as well as in the physical realm. This is mostly because cyber is cross-cutting. Typical examples of cyber-attacks against elections include that of the Kenyan Election in 2022. It was reported by Reuters that cyber spies infiltrated Kenyan networks in 2019 [2, 3] at least three years before the elections. Another research study highlights the influences of social and mainstream media influences on the 2016 United States (US) Elections [10]. In 2020, it was also reported that a cybersecurity hacker was spotted online selling personal information of over 200 million voters in the US with voter registration data of 186 million [6, 7, 11, 12] and it is suspected that most of this data was sourced through various spear phishing campaigns.

Generally, the election life cycle constitutes several categories of cyber entities that are vulnerable to election threats. The common vulnerabilities and threats to elections can generally be classified under various categories of the election lifecycle (see Fig. 1).

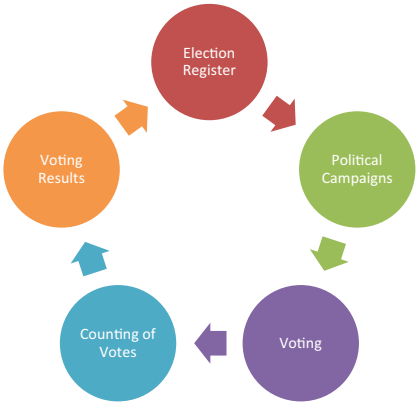

Fig. 1. South African Election Lifecycle

The next sub-sections discuss the Election Lifecycle and its associated cyber-ills in the context of South Africa (SA) (see Fig. 1).

Election register or voters' roll: In SA, elections are conducted by the Independent Electoral Commission (IEC), and eligible voters are SA citizens who are 18 years and older who reside inside or outside SA. According to the IEC, in 2019, a total of 26 million voters were registered with over 17 million casting their votes. Comparing to 1999, the voters registration roll had increased by 8.5 million in 2019. The voters' roll is "gold" to political parties, marketing companies, cyber criminals, and other nation-states. In SA, the voters' roll is online where anyone can check if they or anyone else are registered or not, using an Identity (ID) number. This also technically means the election voters'

roll is susceptible to potential cyber-attacks as well as cyber-criminal activities such as phishing and data breaches.

Political campaigns: According to the IEC, there are over 1500 political parties registered in SA with about 321 parties registered for National Elections [13]. The Western Cape province has the highest number (333) of political parties registered at a Municipal Level. All the political parties compete for 400 seats in Parliament and other seats at Provincial levels. Based on the vast proliferation of political parties in SA, the public political campaigning process is indeed susceptible to cyber interference and manipulation.

Voting: In SA, voting is still manual and no electronic voting is allowed. However, there are digital devices used at the voting stations to confirm the voters' roll and account for those who have voted. A manual register is also used. However, because the voting system is not centralized, possibilities of voting manipulation are a possibility, albeit very minimal with the controls in place. However, disinformation surrounding the voting process should not be ignored.

Counting and Results: In SA, voting results are released as they are confirmed per voting districts and provinces. The results are also released on the IEC website and at the IEC Results Information Centre. The manipulation of the voting results is seen as low risk from a cyber perspective, since the counting of votes is a manual process that involves different stakeholders including political parties. The main cyber threat is the dissemination of fake results and fake news online surrounding the voting results. This has an impact on the integrity of election results.

General Elections present an undeniable opportunity for cybercriminals, political opponents, propagandists, and foreign nation states driven by various motives. While monetary gain remains a primary incentive for cybercrime [14-16], political events like the general elections create a vast cyber threat landscape encompassing power, control, influence, ideology promotion, and even terrorism. As a result, it is imperative for all stakeholders involved in the 2024 General Elections to take proactive and meticulous measures to mitigate cyber threats before, during, and after the elections. Maintaining heightened vigilance and implementing robust cybersecurity measures is crucial in safeguarding the integrity and security of the electoral process.

The next section delves into selected international countries' use cases of past election interference through cyber means.

4 Selected Use Cases of Elections Interference Through Cyber Incidents

The use cases in this section demonstrate that cyber threats and attacks against national elections are no longer something that is discussed by researchers and cyber experts, but it is real and happening across different nations, developed and/or developing. The use cases are presented according to the years that they were reported in.

4.1 United States of America: Democratic Party 2016 Presidential Election Cyber Hacks

On the 2nd of June 2017, the Russian President, Vladimir Putin conceded for the first time that any US presidential election-related hacking attacks may have emanated from Russia [17]. However, he denied the responsibility that the hackers were Russian state-sponsored hackers.

4.2 President Macron and the National Front (France) Targeted by Hackers

On the 25th of April 2017, the security firm Trend Micro published a report stating that the Fancy Bear Russian hacking group was targeting President Macron and his election campaign [18]. According to Trend Micro, they discovered four new fake web domain names that were very similar to the domain names of the Presidential Macron election campaign. The results from the Trend Micro investigations suggested the aim of the hackers was to try to trick careless campaign workers into accidentally compromising their email accounts. In an interview on the 25th of April 2017, President Macron's digital campaign manager, Mounir Mahjoubi confirmed that there were cyber-attacks on the campaign, however they were not successful [18]. On the 5th of May 2017, two days before the elections and during the last hours of the election campaigns, President Macron's election campaign was hacked and about 14.5 gigabytes of emails, personal and business documents were posted to the text-sharing site spanning over 70 thousand files [19, 20]. On close examination of the files leaked, President Macron's election campaign stated that there was a mixture between fake and authentic documents "to create confusion and misinformation".

4.3 SA Local Government Elections (2019)

During the 2019 Local Government Elections in SA, the proliferation of misinformation was observed on social media with the assumed intention to influence and/or interfere with free and fair elections. According to a study by Baldassaro which collected over 400 000 tweets from the political mainstream during the election campaign season and election day [21], it was determined that out of these many tweets, at least about 10 dodgy web domains were disseminating misinformation to over 1 million users, and some of the tweets linked to these domains were also shared by top politicians online.

4.4 Kenya Presidential Election Disinformation and Network Hacks (2022)

During the tightly contested Kenya's Presidential Election in August 2022, disinformation campaigns were widely distributed because of hyped social media engagements in different African countries including SA. Before the election results were officially released, prominent and verified social media users spread false results about who had won the election. As already highlighted in the introduction section, the global news reporter in Reuters released a story in May 2023 claiming that the Chinese-Sponsored Cyber spies called Backdoor Diplomacy [2, 3] infiltrated Kenyan networks from 2019 until 2022 and breached the finance ministry, the president's office intelligence agency

and others, seeking sensitive information on the Kenyan government. These claims, as per Reuters, are based on the analysis of the hacking data and sources who investigated cyber breaches in Kenya [2]. However, Chinese authorities have disputed these claims as "baseless".

4.5 Brazilian Electronic Voting System Questioned in the Presidential Election (2022)

Brazil fully implemented an electronic voting system in the year 2000 and has been seen as a success for many years because it made voting easier for people and prevented fraud. However, from 2018 until the elections in 2023, the system has been called into question. In 2020, the electoral courts' systems in Brazil suffered multiple Distributed Denial of Service (DDoS) attacks with over 5 million access attempts received from overseas countries during the vote counting process and this delayed the release of the results for hours [22].

4.6 Millions of Cyber-Attacks in Presidential Election in Nigeria (2023)

The Nigerian Guardian reported in March 2023 that the over 12.9 million cyber-attacks were recorded during the Presidential Election [1, 23]. The Ministry of Communications and Digital Economy in Nigeria confirmed these cyber-attacks and indicated that they were mostly blocked and originated within and outside Nigeria. The ministry further indicated that there has been a large increase in the cyber threats to the Nigerian cyberspace. It was reported that networks and websites were mostly targeted with over 6 million attacks on the Presidential Election Day, increasing from about 1.5 million attacks on regular days.

By delving into the above historical cyber incidents, this section shed light on the vulnerabilities and risks that electoral processes face in the digital age, emphasizing the importance of strengthening cybersecurity measures to safeguard the democratic process. The next section aims to provide a comprehensive understanding of the specific challenges, threats and vulnerabilities that may impact the 2024 General Elections.

5 Potential Cyber Threats in the General Elections

In conducting a systematic literature review to identify potential cyber threats to general elections, we initially performed comprehensive searches across reputable online databases such as IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar. The search keywords employed included "cyber threats," "election security," "voting systems," "electoral fraud," "phishing attacks," "hacking," "disinformation," and "election interference." We filtered the search results by focusing on peer-reviewed articles, reports, and studies published between 2015 and 2021, giving priority to research specifically related to cyber threats in the context of general elections. After a thorough review, the selected literature provided insights into a range of potential cyber threats, including but not limited to voter registration system breaches, social media manipulation, and election result manipulation. Some of the cyber threats were identified through social media intelligence, previous experience, as well as technical learnings from other elections such as those discussed in Sect. 4.

The threats are grouped into the following four main categories in Fig. 2:

- Political Disinformation Campaigns
- Election Data Breaches
- Phishing Attacks
- Service Disruptions.

The list presented in Fig. 2 is not exhaustive but gives an overview of the most prevalent and common cyber threats in SA and other countries.

Fig. 2. Potential Cyber Threats to General Elections

The following subsections explain the potential cyber threats to general election.

5.1 Disinformation Campaigns

As the cyber threat landscape incessantly advances, it results in a new range of cyber threats that target human weaknesses more than the Information and Communication Technologies (ICT) that humans use. A relevant example of the above-mentioned cyber threats is Information Confrontation, which is a recent and trending type of cyberattack where adversaries make use of Information Weapons to influence politics or gain power [3, 6, 12, 21, 24-26]. As such, Information Confrontation is a cognitive cyber-attack or threat whereby information is purposefully misrepresented and made public by an adversary group or state actor using digital ICT, to sway public opinion on political or social matters. An example of information confrontation is disinformation.

Disinformation campaigns involve deliberate spreading of false information with the intent to deceive and manipulate. Disinformation aims to influence public opinion. In

this instance, disinformation may be used by political opposition actors to manipulate voting or voter turnout.

Similar and related to disinformation is misinformation. These two concepts differ in terms of intent and the spread of false or misleading information. Misinformation may be unintentional, whereas disinformation involves deliberate efforts to deceive or manipulate. Misinformation refers to false or inaccurate information shared unknowingly by individuals who believe the information is true. An example of misinformation would be the public (potential voters) spreading disinformation either through word of mouth or social media platforms, believing it to be true. Misinformation can be the result of misunderstandings, misinterpretations, or the dissemination of outdated or incorrect information.

While the above concepts both encompass various activities, their focus is often on influencing the human mind.

5.2 Data Breaches

Voter registration databases contain the personal information of registered voters. A breach of these systems could result in the theft, manipulation, or deletion of voter data. SA has a Protection of Personal Information Act (POPIA), that is in place, while cybersecurity researchers endeavor on developing tools to assist with POPIA compliance [27].

Data breaches before, during, and after elections can come in myriad ways, including:

- **Election Data Attacks** to voting systems could alter vote counts, modify candidate preferences, steal identities, or manipulate results. Safeguarding the security and integrity of electronic voting systems, including implementing secure transmission protocols and robust auditing mechanisms, is crucial to prevent any manipulation of election results.
- The **Compromise of Voters Data** can come in multiple ways, mainly through third parties such as marketing companies, service providers, political parties, private companies, and government entities. In SA, we have already observed political parties sourcing voters' personal information from marketing companies and using the data to target voters in certain areas via short-messaging-services. Furthermore, hackers may use publicly available data sources to scrap and combine various data points to monetize voters' data such as identity, home addresses, email addresses, phone numbers or voting districts.
- **Hacking Digital Campaigns** for sensitive political information has been observed in local and international elections [4, 5, 14, 19, 20, 28]. With the growing digitalization of campaigns, adversaries have discovered fresh avenues to interfere with, disrupt, and steal vast amounts of information from political opponents. These include email addresses of political party staff members or donors, as well as personal documents obtained from campaign resources such as networks and websites.
- **Insider threats** includes individuals within the electoral process who have authorized access to sensitive systems or information, such as election officials, IT staff, or political party members, may exploit their positions or misuse their privileges for personal gain or to disrupt the electoral process and critical IT systems. These insiders may

engage in data manipulation, unauthorized disclosure of confidential information, or intentional disruption of critical systems.

- **Foreign-sponsored attacks** are prevalent before, during, and after the elections. The conflict between Russia/Ukraine and SA's position provides a threat for nation-sponsored cyber hackers within and outside the country to disrupt the Elections using the cyberspace. Generally, state sponsored attacks focus on stealing classified information from government and intelligence services, as observed in Kenya.

5.3 Phishing Attacks

Phishing attacks or threats in local and international elections refer to a type of cyber-attacks where malicious actors attempt to deceive persons involved in the electoral process, such as voters, political campaign staff, politicians, or election officials to gain unauthorized access to sensitive information or manipulate the election outcome. Phishing attacks are typically carried out through fraudulent emails, text messages, or websites that imitate legitimate sources, such as political organizations, government agencies, or social media platforms. It has been observed in the US that phishing attacks have been prevalent in 2016 and 2018 Presidential Elections [29]. These phishing attacks have been targeting political campaigns as well as candidates online. In 2022, phishing attacks were detected targeting county workers managing elections [29].

Phishing attacks in the 2024 General Elections may come in different ways such as:

- **Spear phishing**, which is more targeted at a specific individual, large groups, politicians, or departments within an organisation using continuous communication over an extended period. Therefore, political parties, candidates, or election officials may be targeted through spear phishing to gain unauthorised access to their accounts or systems or for impersonation of misleading campaign information [29].
- **Smishing attacks** are gaining prominence in the digital age particularly in a country such as SA where mobile phone adoption is over 100%. Smishing can be easily defined as a combination of the words "SMS" and "phishing". It is a form of phishing attack that involves the use of text messages (SMS) to deceive and exploit individuals for various intents including revealing sensitive information.

The consequences of successful phishing attacks in elections can be severe and detrimental to the nation's democracy. They can compromise the integrity of the voting process, erode public trust, and impact the legitimacy of election results.

5.4 Service Disruptions

The threat of service disruption is real on different fronts in Africa. For instance, load-shedding, crime, vandalism, social unrests, and protests are all potential non-cyber threats that are well documented and have been experienced before in the previous elections. Disruptions to Information Technology (IT) systems associated with the elections can never be ignored as a cyber threat. IT service disruptions in elections can have significant consequences, affecting the integrity, efficiency, and trustworthiness of the electoral process. These disruptions can arise from various sources, including technical failures, cyber-attacks, or even deliberate sabotage.

It can be noted from this section that cyber threats against elections are plentiful, and the list provided here is not exhaustive, but provides an indication of what authorities may need to pay attention to for better cyber preparedness before, during and after the general elections.

6 Cyber Vulnerabilities against General Elections

There is a difference between threats and vulnerabilities. Generally, threats come from external and internal sources such as cyber attackers and insiders. It is almost impossible to eliminate cyber threats. On the other hand, vulnerabilities may emanate because of weaknesses in cybersecurity systems, lack of security controls (logical and physical), lack of security awareness in voters, lack of monitoring of social media platforms, and outdated or legacy IT systems.

This section highlights some of the cyber vulnerabilities that may impact General Elections (see Figure 3). The categorized cyber vulnerabilities in Fig. 3 are not exhaustive but cover the most common vulnerabilities based on external information.

Fig. 3. Cyber Vulnerabilities against General Elections

Below, we discuss at high-level some of these vulnerabilities that authorities need to be aware of (see Fig. 3).

Vulnerable Electoral IT Systems: vulnerable IT systems are a common trend across the digital landscape, and systems used in elections for voter registrations are no different. These systems could be vulnerable in the following ways:

- Outdated systems as well as legacy systems can be an easy target for malicious actors.
- Weak access controls without multi-factor authentication, and unaudited access rights can make it easier for cyber hackers to infiltrate IT systems that may lead to data breaches, manipulation of data and system configurations.
- Insecure network infrastructure that has weak or poorly configured security measures could be a vulnerability that may impact electoral IT systems and can expose election systems to data interceptions through attacks such as Man-in-the-Middle attacks.

- Lack of secure coding practices in locally developed systems, such as voter registration portals, could also be a vulnerability that introduces threats that may lead to data breaches impacting on the integrity of the elections.
- Third-party vulnerabilities, in cases where the election authority is relying on external service providers for the development or hosting of their IT systems.

These vulnerabilities may be exploited by insiders and outsiders to undermine the integrity, confidentiality, and availability of electoral IT systems. Vulnerabilities need to be assessed, tracked, and patched where technically feasible or isolated.

Lack of Cybersecurity Assessments: it is best practice to regularly conduct technical and non-technical security assessments and penetration testing against critical IT systems for the elections. An oversight in this regard could expose the IT systems to cyber threats. For such critical IT systems, it is important that technical cybersecurity assessments are done on a regular basis, at least monthly, particularly in the build-up towards elections because vulnerabilities are introduced almost daily for the common IT systems. Non-technical security assessments could be done at least every six months.

Lack of Security Incidents and Events Monitoring: it is a common security maxim that you cannot protect what you do not know or monitor. And it is now well known that African countries such as SA are a "heaven" for cyber criminals[1], and as such lack of security monitoring on critical applications, networks, data leakages, and other events could be a vulnerability that may lead to cyber threats being realized. The Nigerian government made some inroads in this regard by deploying resources before and during the elections to monitor and block cyber-attack attempts, and as reported above, monitored over 12 million events that were all blocked as per the ministry's claim.

Lack of Security Awareness: it has been determined by the Verizon Data Breach Report that 75% of data breaches are caused by human-error, misconfigurations, and social engineering. The lack of security awareness and culture by users, in the context of elections, voters, election officials and politicians, is a serious vulnerability. This vulnerability can realize the cyber threat relating to election data attacks as well as voters personal information leakages. Lack of security awareness raises the threat of phishing, smishing, and vishing attacks, and any breach related to voters' information, election officials, and politicians could have an impact on the elections, even if the leakages and data attacks do not happen directly through the election IT systems and databases.

Lack of Cybersecurity Skills: technical cybersecurity skills are crucial in ensuring a proper cybersecurity posture. The lack of skilled cybersecurity experts could be a vulnerability to General Elections as any potential breaches and incidents may not be reacted upon timeously. The lack of technical skills could lead to risks such as ineffective incident detection and response, limited ability to assess and mitigate systems vulnerabilities, insufficient knowledge of emerging threats, limited ability to incident response and recovery, and too much reliance on third-parties or service providers which could expose the election processes to third-party cyber threats.

Lack of Cybersecurity Response Plans: inadequate cybersecurity response plans and backup procedures and lack of robust disaster recovery plans could result in data loss or prolonged system downtime during elections in the event of a cyber-attack, system

[1] https://www.itweb.co.za/content/KzQenvjyBo2qZd2r.

failure, or natural disaster. This is seen as a critical vulnerability in any IT system and should be mitigated following best practices.

Lack of Incident Response Plans: it is impractical to aim to eliminate all cyber threats and vulnerabilities, and as such, a lack of plans to respond and recover from cyber incident could be more devastating to the election regime. This could lead to issues such as prolonged system down time, increased reputational damage, failure to preserve evidence for cyber investigations, and inability to learn from previous incidents.

The next section explores the significant impact that the discussed cyber threats and vulnerabilities would impose on the various stakeholders involved in the electoral process.

7 Impact of Cyber Attacks on Election Process Stakeholders

The consequences of hackers realizing a cyber threat or exploiting a cyber vulnerability within the election context can have enormous implications. They can compromise the integrity of the voting process, erode public trust, and impact the legitimacy of election results. These threats and vulnerabilities have multi-dimensional impact that covers processes, people, and technology.

Over and above the technical impact imposed by the identified cyber threats and vulnerabilities, the non-technical impacts on the election process are discussed below.

7.1 Psychological

The identified cyber threats to General Elections have the potential to induce significant psychological consequences on both individuals and the broader society [13]. The perceived existence of cyber threats can elicit fear, anxiety, and a pervasive sense of distrust among voters, thereby undermining their confidence in the electoral process. Consequently, these psychological reactions can contribute to voter apathy and reduced voter turnout as individuals may feel disheartened or skeptical about the integrity of the elections. The psychological impact can manifest as heightened political polarization, increased hostility, and a deterioration of social cohesion. Moreover, targeted cyber-attacks directed at political candidates or parties can instill a sense of vulnerability and insecurity, resulting in heightened stress levels and diminished psychological well-being among the affected individuals. Taking proactive measures to address these concerns will safeguard the psychological well-being of individuals, uphold the legitimacy of the electoral process, and preserve the democratic values that underpin a fair and inclusive society.

7.2 Financial Liabilities

Cyber-attacks on the electoral process can result in significant financial liabilities for various stakeholders involved. The financial impact can include costs associated with incident response, investigation, remediation, and restoration of affected systems. Additionally, there may be expenses related to legal actions, fines, and penalties imposed by regulatory authorities. Cyber-attacks can also lead to economic losses due to disrupted

campaign activities, decreased voter trust, reduced donor contributions, and potential lawsuits. Moreover, the need to enhance cybersecurity infrastructure and implement preventive measures further adds to the financial burden.

7.3 Legal Consequences

In the context of SA, the implementation of the (POPI Act which came into effect on the 1st of July 2021, holds significant implications for political parties in SA. If the Information Regulator identifies a political party's failure to adequately protect citizens' or members' personal identifiable information (PII) and neglect of established POPIA minimum security measures, the party may face legal consequences. This could entail initiating legal proceedings against the political party, potentially resulting in penalties, fines, and other punitive measures enforced by the information regulator [27].

7.4 Social Unrest

In July 2021, SA as a nation experienced social unrest known as the July 2021 riots, the Zuma unrest or Zuma riots. The unrests occurred in SA's KwaZulu-Natal and Gauteng provinces from the 9th to the 18th of July 2021 [30]. The cause of these unrests was sparked by the imprisonment of former President Jacob Zuma for contempt of court. It is believed that members of the public or citizens felt the former president was being treated unfairly by his political party.

7.5 Reputational Damage

On February 24, 2023, SA was added to the "grey list" by the Financial Action Task Force (FATF), designating it as a jurisdiction under heightened monitoring due to concerns over compliance with the FATF 40 Recommendations and the effectiveness of its anti-money laundering (AML) and counter-terrorist financing (CTF) system, as highlighted in the 2021 FATF mutual evaluation report. This classification subjects the country to increased financial scrutiny by international bodies. In this context, any instability arising from the national elections could potentially erode the remaining confidence in SA, both domestically and internationally. Furthermore, there is a risk of post-election unrest, which could further exacerbate the negative impact on the country's stability and reputation.

7.6 Divisions Among Different Groups

Division among different groups can be a significant concern. The country's diverse population encompasses various ethnic, political, and social groups, each with their own interests and ideologies. This diversity can create fertile ground for cyber threats, as different factions may attempt to exploit existing divisions and manipulate public opinion through disinformation campaigns, targeted hacking, or social engineering. Divisions based on race, political affiliation, or socioeconomic factors can be weaponized by hacktivists to undermine trust in the electoral process and destabilize democratic institutions, making it crucial to address these divisions and promote unity in safeguarding the electoral system.

7.7 Legislative Paralysis

Legislative paralysis could exacerbate the vulnerabilities and risks faced by the electoral process. Legislative paralysis refers to the inability or delay in passing necessary laws and regulations to address emerging cyber threats effectively. Without comprehensive legislation in place, the country's electoral system might lack the necessary safeguards to protect against cyber-attacks, disinformation campaigns, or manipulation of election results. This paralysis can hinder the implementation of robust cybersecurity measures, leaving the electoral process susceptible to interference and compromising the integrity of the elections. Urgent and proactive action from lawmakers is essential to mitigate potential cyber threats and ensure a fair and secure democratic process.

7.8 Disruption of Election Operations

Ransom attacks can paralyze the IT systems essential for conducting elections. This includes voter registration databases, voting machines, result reporting systems, or communication platforms used by election officials and political campaigns. Such disruptions can hinder voter registration, delay voting processes, or prevent the timely reporting of accurate election results. In some cases, ransomware attacks may involve the manipulation or tampering of election data. Attackers may alter voter registration records, voting tallies, or result reporting systems, leading to inaccuracies, or casting doubt on the integrity of the election outcome. This can undermine public trust and confidence in the electoral process.

While achieving absolute security in the cyber environment is an unattainable goal, there are several cybersecurity controls that can be implemented to enhance protection. The next section provides an in-depth exploration of proactive cybersecurity measures that can be adopted to effectively mitigate potential cyber threats and attacks.

8 Mitigation Techniques Against Cyber Threats and Vulnerabilities

8.1 Mitigation Against Political Disinformation Campaigns

- Regularly monitor, detect and analyse online misinformation and disinformation.
- Develop a rapid response plan in collaboration with tech-companies to deal decisively and close to real-time with false and/or misleading information.
- Develop a clear communication plan that could be used by the election authority and government communication agencies for engagement with political parties on dealing with cyber disinformation, public awareness and education campaigns educating voters about misinformation and potential impact.
- Media to work together with the election authorities to provide guidance on how to identify and verify reliable sources of information.
- Collaborate with the social media platforms to enhance content moderation of election posts including algorithms to detect, flag or remove false information.
- Foster international collaborations and cooperation on information sharing and threat intelligence.
- Establish legal and regulatory frameworks that addresses disinformation campaigns during elections.

8.2 Mitigation Against Election Data Breaches

- Implementing appropriate encryption mechanisms for sensitive data at rest and in transit could help protect the confidentiality and integrity of electoral information.
- Deploy multi-factor authentication (MFA). This will enhances security, protect against password-based attacks, increases accountability, safeguards voter data, deters fraudulent activities, and promotes compliance with security standards.
- Conducting extensive security vetting on insiders and third parties to minimize insider threat attacks as well as third-party breaches such as contractors.
- Implementing backup, restore, and recovery plans which can help ensure data and systems are regularly backed up and can be restored in case of a cyberattack or data loss, thus minimizing the impact and downtime.

8.3 Mitigation Against Phishing Attacks

To mitigate the risk of phishing attacks, it is critical that election officials, campaign staff, and volunteers are trained or made aware about cybersecurity best practices, such as identifying phishing emails, avoiding suspicious downloads, and reporting potential threats that could reduce the risk of successful phishing attacks. It is important for the political parties to appoint a cybersecurity specialist as part of their campaigns to ensure that there is political party members' awareness training. These cybersecurity specialists could work alongside law-enforcers to report, and where possible, take down cybersecurity threat attempts.

8.4 Mitigation Against IT Service Disruptions and Attacks

Preventing and mitigating service disruptions and attacks against IT systems for elections and associated government services requires proactive measures such as:

- Implementing strong cybersecurity measures, including firewalls, encryption, intrusion detection systems, and regular security updates, helps safeguard IT systems from cyber threats.
- Conducting regular maintenance and testing (vulnerability and penetration assessment) of voting machines, registration systems, and other critical IT infrastructure ensures their reliability and identifies potential issues in advance.
- Developing comprehensive contingency plans can help election authorities respond to IT disruptions effectively. This includes backup systems, redundancy measures, and clear protocols for handling technical failures or cyber incidents.
- Engaging IT professionals, cybersecurity experts, and technology vendors can provide valuable insights, assistance, and guidance in identifying and mitigating potential IT service disruptions and security issues. These professionals and experts could be on a retainer basis to avoid delayed procurement process during an incident.
- Developing comprehensive incident response plans enables a swift and coordinated response in the event of targeted attacks or advance persistent threats. For incident response, the NIST Cyber Incident Response Cycle [31] is recommended:

  o Preparation

- o Detection & Analysis
- o Containment, Eradication & Recovery
- o Post-incident Activity

9 Conclusion

Over the years, the cyber space has evolved significantly with the digital transformation changing every sector. With the positive changes that came along with it, negative implications also emerged, including increasing cyber threats and vulnerabilities. This paper gave a highlight of potential cyber threats to the General Elections in the digital era. An introduction of why this is important, and a high-level view of the potential cyber ills was given. The paper went into more detail highlighting different types of cyber threats and vulnerabilities that could impact General Elections in Africa focusing on the South African context, and some examples of instances where cyber-attacks were lodged to disrupt electoral processes in various parts of the world. This sheds some light on the reality of the global cybersecurity challenges and emphasizes the importance of having a strong cybersecurity backbone to safeguard General Elections. The possible impacts of cyber threats to the electoral process and its stakeholders were discussed. This helps with highlighting why the cyber threats identified in this report need to be taken into consideration. Potential mitigation techniques that can be employed by election process stakeholders to try and hinder malicious actors from disrupting the electoral process were outlined. The paper is closed-off by suggesting mitigation techniques that may enhance the security of General Election.

References

1. Opanuga, J.: Nigeria records 12.9 million cyberattacks during presidential election. The Guardian Newspapers, Nigeria, pp. 1–2, 14 March 2023
2. Reuters, "Kenyan Official Dismisses Reuters Report on Chinese Hack as 'Propaganda," US News and World Report, Nairobi, pp. 1–2, 25 May 2023
3. Maweu, J.M.: "'Fake Elections'? Cyber Propaganda, Disinformation and the 2017 General Elections in Kenya," African Journalism Studies, vol. 40, no. 4. Taylor and Francis Inc., pp. 62–76, 2 October 2019. https://doi.org/10.1080/23743670.2020.1719858
4. A. Christiansen, "How are cybersecurity threats, in the form of disinformation campaigns, reflected on the security measures they inspire?," Report, Malmo University, Sweden, 2023
5. Fidler, D.P.: "The U.S. Election Hacks, Cybersecurity, and International Law," In: AJIL Unbound, Cambridge University Press, pp. 337–342 (2016). https://doi.org/10.1017/aju.2017.5
6. Dawood, Y.: Combatting foreign election interference: canada's electoral ecosystem approach to disinformation and cyber threats. Election Law J. Rules Polit. Policy **20**(1), 10–31 (2021). https://doi.org/10.1089/elj.2020.0652
7. Stedmon, N., Security, C., Factors, H.: The impact of cyber security threats on the 2020 US elections. http://maristpoll.marist.edu/wp
8. Okoli, C.: A guide to conducting a standalone systematic literature review. Commun. Assoc. Inf. Syst. **37**, 1–33 (2015). http://aisel.aisnet.org/cais/vol37/iss1/43
9. Ryan, A., Van Geel, O., Pennings, F., Tirtea, R., Follmer, V.: Lection cybersecurity: challenges and opportunities, US, February 2019. https://www.enisa.europa

10. Eady, G., Paskhalis, T., Zilinsky, J., Bonneau, R., Nagler, J., Tucker, J.A.: Exposure to the russian internet research agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior. Nat. Commun. **14**(1) (2023). https://doi.org/10.1038/s41467-022-35576-9
11. Holovkin, B.M., Tavolzhanskyi, O.V., Lysodyed, O.V.: Corruption as a cybersecurity threat in the new world order. Connections **20**(2), 75–87 (2021). https://doi.org/10.11610/Connections.20.2.07
12. Olaniran, B., Williams, I.: Social media effects: hijacking democracy and civility in civic engagement, pp. 77–94 (2020). https://doi.org/10.1007/978-3-030-36525-7_5
13. Love, J., Mamabolo, S.: 2022 IEC annual report, South Africa, June 2022. Accessed 19 August 2023. https://www.elections.org.za/content/
14. Ablon, L.: Data thieves: the motivations of cyber threat actors and their use and monetization of stolen data (2018). www.rand.org
15. Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., van Ruijven, T.: Understanding incentives for cybersecurity investments: development and application of a typology. Digit. Bus. **1**(2) (2021). https://doi.org/10.1016/j.digbus.2021.100014
16. Goldman, Z.K., Mccoy, D.: Economic espionage deterring financially motivated cybercrime (2016). http://cseweb.ucsd.edu/savage/papers/WEIS2012.pdf
17. Higgins, A.: Maybe private Russian hackers meddled in election, Putin says, The New York Times, New York, pp. 1–2, 1 June 2017. Accessed 15 August 2023. https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html
18. CBS, Russia-linked hackers targeting French election, security firm says, 2017 CBS Interactive Inc., Paris, pp. 1–2, 25 April 25 2017, Accessed 19 August 2023. https://www.cbsnews.com/news/russia-hacked-french-election-trend-micro-report-fancy-bear-pawn-storm/
19. Hansen, I., Lim, D.J.: Doxing democracy: influencing elections via cyber voter interference. Contemp. Polit. **25**(2), 150–171 (2019). https://doi.org/10.1080/13569775.2018.1493629
20. Auchard, E.F.B.: French candidate Macron claims massive hack as emails leaked, Reuters, Frankfurt City, Germany, pp. 1–2, 05 May 2017. Accessed 12 August 2023. https://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ
21. Baldassaro, M.: Identifying and tracking disinformation during the May 2019 South Africa Elections, Harvard: Harvard Law School, October 2024
22. Paraguassu, L.: Brazil court to probe Bolsonaro for attacks on voting system, Reuters, Brazil, pp. 1–2, 03 August 2021. Accessed 10 August 2023. https://www.reuters.com/world/americas/attacked-by-bolsonaro-brazils-top-judges-say-electronic-voting-is-free-fraud-2021-08-02/
23. Mohammed, K.H., Mohammed, Y.D., Solanke, A.A.: Cybercrime and digital forensics: bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria. Int. J. Cybersecur. Intell. Cybercrime **2**(1), 56–63 (2019). https://doi.org/10.52306/02010519zjrk2912
24. Fujiwara, T., Müller, K., Schwarz, C.: The effect of social media on elections: evidence from the United States (2023)
25. Baptista, J.P., Gradim, A.: Understanding fake news consumption: a review. Soc. Sci. **9**(10), 1–22 (2020). MDPI AG, https://doi.org/10.3390/socsci9100185
26. Tenove, C., Fellow, P.R.: Digital threats to democratic elections: how foreign actors use digital techniques to undermine democracy (2018)
27. Moabalobelo, T., Ngobeni, S., Molema, B., Phantsi, P., Dlamini, M., Nelufule, N.: Towards a privacy compliance assessment toolkit. In: IEEE IST-Africa Conference Proceedings, Pretoria, South Africa, pp. 1–8. IEEE, May 2023
28. Garnett, H.A., James, T.S.: Cyber elections in the digital age: threats and opportunities of technology for electoral integrity. Election Law J. Rules Polit. Policy **19**(2), 111–126 (2020). https://doi.org/10.1089/elj.2020.0633

29. Suzuki, Y.E., Monroy, S.A.S.: Prevention and mitigation measures against phishing emails: a sequential schema model. Secur. J. **35**(4), 1162–1182 (2022). https://doi.org/10.1057/s41284-021-00318-x
30. Africa, S., Sokupa, S., Gumbi, M.: Report of the expert panel into the July 2021 Civil unrest, Pretoria, November 2021. Accessed 15 Aug 2023.
31. Cichonski, P., Millar, T., Grance, T., Scarfone, K.: Computer security incident handling guide : recommendations of the national institute of standards and technology, Gaithersburg, MD, August 2012. https://doi.org/10.6028/NIST.SP.800-61r2