Scientia Militaria
2025, VOL. 53, NO. 1, 1-26
DOI 10.5787/53-1-1493

Cyber Hygiene: The Case of the SANDF

Kyle John Bester[1]
University of South Africa

Abstract

The landscape of cyberspace is growing at an incredibly fast pace, and it has penetrated deep into every aspect of society. In order to address this issue, the current study took a unique approach of focusing on cyber-hygiene practices among senior South African military officers, which is a largely understudied subject in the South African armed forces domain. The study was guided by the securitisation theory, which emphasises that the military plays a key role in orchestrating a "security move". The South African National Defence College was selected as the site of importance where senior military officers undergo educational training. The military is considered a unique population, and is therefore often overlooked. The aim of the study was to explore how military officers in particular conceptualise cyber hygiene and how cybersecurity behaviour is practised in the context of the South African National Defence Force. The study utilised a qualitative approach, and conducted ten semi-structured interviews. It was found that cybersecurity awareness was key in the formation of cyber hygiene and locating potential cyber threats. These factors play a role in the development of security behaviour that is able to identify vulnerabilities in the system and within their own behaviour. Cultivating cybersecurity in the organisation was found to be challenged by knowledge and experience relating to cyberspace usage. The study also found that senior military officers practise cyber hygiene by taking appropriate security procedures to protect themselves and the organisation; however, organisational challenges prevent the full application of this practice.

Keywords: Cyber Hygiene, Information Security, Cybersecurity Awareness, South Africa, Behaviour, Security Practices

Introduction

Bester suggests that cyber threats are pervasive in society and have the potential to affect various sectors, such as the finance, defence, transport, and maritime sectors, as well as critical infrastructure.[2] In addition, the surge in cyber threats locally and internationally is a consequence of the expanding nature of cyberspace and the move towards a digitally connected society.[3,4] In a connected society, users increasingly use the Internet to undertake their daily activities, which might be intensifying due to remote working conditions where access to the Internet is emphasised.[5] Adding to this, since the inception of the COVID-19 pandemic, there has been a transition towards online or remote working conditions. This may not necessarily be true for the military context, where South African National Defence Force (SANDF) members were domestically deployed to maintain order during

the pandemic. Remote working conditions did not apply to all military members during the period 2020–2022.[6] The COVID-19 pandemic saw an increase in cyber threats in the South African context. This is largely due to infective security behaviours employed by users when working remotely and having limited cybersecurity awareness. Several significant factors affect the cybersecurity landscape in South Africa. These include limited investment in cybersecurity measures, slow progress in developing regulations and laws related to cybersecurity, and a general lack of awareness regarding cyber threats and security protocols.[7] Additionally, the widespread use of digital devices has contributed to the complexity of the cyber threat landscape in South Africa.[8] Moreover, the country has been identified as a prime target for cyber attackers, which makes it even especially susceptible to security breaches.[9] Taking the above into consideration, from a securitisation theory (ST) perspective, cyber threats pose a significant concern for nation-states. This necessitates responses that may include prolonged emergency measures or swift actions. When discussing cyber hygiene, a term often used interchangeably with cybersecurity awareness, the emphasis is however on individual behaviours that prioritise security. The focus of ST in this study was therefore, on individual measures rather than on a broad state-centred perspective.

From a large societal perspective, South Africa has experienced increased ransomware and phishing attacks.[10] The increase in cyberattacks points towards the overall cybersecurity maturity of the nation-state, and highlights the deprioritisation of defence spending in favour of social demands.[11] In addition, the maturation of cyber capabilities also comes into question since the SANDF was suspected of being the victim of a data breach in 2023.[12] From a perspective where the military member is the focus, it is unclear how SANDF members were affected by the surge of ransomware attacks and suspected data breaches in 2023, since recent research on cybersecurity on South African military officers only points out aspects related to:

- Cybersecurity awareness;
- Knowledge of specific threats in an organisational context; and
- Security behaviour in cyberspace.[13,14,15]

This article reflects the research findings of the study conducted by Bester on cybersecurity awareness among South African military officers.[16]

What is Cyber Hygiene?

In terms of cybersecurity behaviour, the researcher used the lens of cyber hygiene to highlight the increasing threat faced by users who are experiencing online security threats. The exploration of cyber hygiene among military officers has not been engaged with in the South African context, although aspects related to awareness and training have been extensively examined.[17,18,19] The term "cyber hygiene" has not been used frequently in the South African context, and contributes to Bester's argument that cybersecurity research that emphasises the human element, is emerging.[20] The definition of cyber hygiene lends itself to 'a set of practices aiming to protect from negative impact to the assets from cyber

security related risks'.[21] This definition fails to consider the essential component of the human element, whereby risk and threats are thwarted by applying security behaviour and following security procedures to mitigate potential attacks. The research on which this article is based focused on the individual level of cyber hygiene by referring to the security practices and behaviour of military officers in the SANDF. It is argued that engagement with cyber-hygiene practices may enhance the cyber resiliency of potential targets, thereby reducing the vulnerability towards cybercrime.[22] In this instance, the exploration of behavioural practices associated with cyber hygiene may therefore contribute to this emerging concept in the South African armed forces context.

The idea of hygiene practices refers to cleansing one's hands. In a similar fashion, cyber hygiene refers to the conscious effort to ensure the system well-being of the user online.[23] Advancing the description on cyber hygiene, one needs to highlight the idea of digital well-being and practical steps to ensure online safety. Cyber hygiene is the practical steps that users take to advance their online security and safeguard their system health, which may come in the form of computers or devices.[24] In addition, when referring to the concept of cyber hygiene, the element of adaptability must be present, as a security-oriented approach needs to be considered by users to avoid potential threats. A security-oriented approach is essential for individuals to cultivate a proactive mind-set aimed at identifying and mitigating potential threats. It demands that users in organisations consistently adhere to best practices, monitor for threats, and maintain a strong awareness of risks as they navigate the Internet.[25] To achieve cyber hygiene within an organisation, the following practices must be applied:

- Ensure that adequate training is provided to all members of the organisation to identify and report suspected threats;
- All organisational devices need to receive updated software;
- Ensure that there is strong system access management and that multi-factor authentication is applied; and
- The organisation should invest in systems that enable clear access to the network infrastructure of the organisation.[26]

The dynamics between cybersecurity awareness and cyber hygiene can be linked in two ways:

- In order to practise cyber hygiene, there needs to be a concerted effort to apply guidelines and best practices;[27] and
- The human element executes security behaviour by applying knowledge at the network, individual, and device levels.[28]

McMahon argues that the human element is an important facet in the cybersecurity chain.[29] The connection between cyber hygiene and cybersecurity awareness is based on the practice of implementing security measures. Individual cyber hygiene requires training and education on cybersecurity. This is true, as most cyberattacks occur due to a lack of user awareness.[30] The practice of cyber hygiene results in safe internet browsing by users, and improves cyber health.[31] In this case, "cyber health" refers to the notion of mechanisms to protect a user's online security and data through a series of procedures.[32]

Cybersecurity Awareness

The researcher raised the question from a philosophical perspective: 'The chicken or the egg?' This question underpins the process that, in order to practise cyber hygiene (cybersecurity practices), there must be some level of awareness and knowledge of threats. Cybersecurity is fundamentally influenced by the convergence of outcome of laws, best practices and individual security behaviour. It is therefore necessary to shift the focus to cybersecurity awareness as the basis of cyber hygiene. The researcher considers the human element as an important component in the cybersecurity chain. For this article, the researcher used Bester's proposed definition as a reference point:

> Cybersecurity is a flexible security process through which individuals are constantly interacting with a technical environment in the social context. Cybersecurity is also the immersive process through which the human factor utilises security software tools in tandem with education, training, guidelines, technical knowledge, and best practices such as awareness training, technical skills, and risk assessment. Cybersecurity also requires the notion of applying knowledge to risk perception and precautionary behaviour, while being fully aware of vulnerabilities in both the physical and cyberspace domain.[33]

Bester's definition highlights the essence of human behaviour within the cybersecurity chain and the multitude of activities users need to undertake when confronted with ensuring security in an online space.[34] The definition raises the idea of considerable cybersecurity practices and the application of security mechanisms. The definition however, attempts to incorporate too many elements that may not necessarily be contextually applicable to everyday functioning. This contextual limitation is dependent on two aspects, namely time and space. In terms of time, users often do not have the luxury to acquire advanced knowledge and skills to enhance their own cybersecurity awareness. The same may apply to organisations that are experiencing budgetary constraints, and are thus unable to offer cybersecurity training and education for all members.[35] In terms of space, the researcher is of the opinion that each context demands a tailored response and risk management plan to mitigate cyber threats and attacks. Moreover, the exchange of information in the armed forces context is contingent upon the functionality of technological systems. This functionality may, however, be subject to certain contextual impediments, such as financial limitations.[36]

Dagada asserts that the increasing number of cyberattacks in South Africa is a serious concern that demands immediate action.[37] The recognition of these threats has prompted the South African government to develop legislation and frameworks to address these contemporary threats and safeguard the nation against potential harm. The National Cybersecurity Policy Framework was introduced in 2015 to provide a comprehensive view of key stakeholders responsible for mitigating cyberattacks and threats.[38] The classification of threats in terms of complexity is not linked explicitly to the measures of action, however, but rather to the allocation of duties and responsibilities among the South African security cluster. Furthermore, ensuring protection against cyber threats is considered a top priority for the SANDF. To maintain and ensure the best possible

form of defence, the SANDF has the responsibility of co-ordinating, implementing, and taking accountability for all cyber-defence issues.[39,40] Adding to the importance of the SANDF, militaries across the globe are increasingly becoming reliant on information technology (IT), and the risks have become more severe as cyber threats and attacks are increasing. The SANDF approach to reducing threats and taking a more offensive stance on maintaining cybersecurity is to advance its cyber command.[41] While this is an important factor in advancing capacity, it may not necessarily address the issue of awareness and consideration of cyber hygiene by the SANDF. Furthermore, the role of cyber hygiene cannot be underplayed in organisational contexts, such as the SANDF, where information can be critical to operations. It has been found that the implementation of basic cyber-hygiene practices and the sharing of best practices can result in averting up to 90 per cent of cyberattacks.[42] The implementation of online security behaviour and information-sharing practices in organisational contexts may therefore contribute to the mitigation strategies of addressing cyber threats and protecting both individual and organisational data from being compromised. In the current digital landscape, the human component remains a crucial factor in ensuring robust cybersecurity measures. As individuals move between the digital and physical worlds, their actions can significantly affect the security of digital systems. Humans are however susceptible to committing security-related errors and can become vulnerable to various threats that can compromise the security of these systems.[43] It is important to note that many users may lack the required awareness of the nature and diversity of cybersecurity threats. Educating and training individuals on the various types of threats in this domain are therefore critical in reducing the risk of security breaches and safeguarding digital systems against harm.[44] Such measures should include continuous awareness programmes and training sessions to raise the level of understanding among users and to promote best practices in cybersecurity.[45] By doing so, businesses and organisations can create a culture of cybersecurity that is essential for protecting sensitive data and ensuring the continuity of operations.

The Effect of Cyber Threats on the SANDF

The emergence of cyber threats and cyberattacks has had a significant effect on the economic and social sectors of South Africa. The increasing reliance on information and communications technology (ICT) has rendered civil society and the armed forces vulnerable to cyber threats.[46,47] As a result, the role of the military in safeguarding national interests has become increasingly crucial.[48] The SANDF however faces a significant challenge in mitigating the risks associated with cyber threats. The Department of Defence confirms that, while the threat of cyberattacks is on the rise, the tools available to the SANDF are outdated.[49] Furthermore, the SANDF faces resource constraints due to insufficient funding, as noted in a report by the former Minister of Defence.[50] This lack of resources may impede the ability of the SANDF to integrate ICT capabilities fully and to enhance technology for mitigating cyberspace threats. Dlamini and Modise argue that organisations that embrace ICT capabilities tend to operate more efficiently than those that avoid technological incorporation.[51] Embracing ICT capabilities however also requires accepting the notion of security in this domain. In addition, the increasing rate of cyber threats and cyberattacks has emerged as a significant concern for the economic and social sectors of South Africa, resulting in questions being posed regarding the current state of

national security and the way the security cluster is advancing cybersecurity efforts from a multi-disciplinary and collaborative perspective.

Vulnerability of Force Members

The security of software and hardware used in personal computer devices at home is a growing concern due to the increasing incidence of cyberattacks. This is compounded by the scrutiny under which SANDF senior officers have come due to the practice of sharing information on unofficial social media networks.[52] Martin highlights that the organisation is cognisant of the use of social media and that its organisational data might be vulnerable to other militaries and non-state actors in terms of obtaining intelligence.[53] The notion of maturity also comes into question when relating the idea to mobile device use. It has been identified that the younger generation of military members are more inclined to use social media on their mobile devices than senior military members.[54] This dynamic of use is confirmed by Bester, who asserts that maturity levels have an influence on how social media are used and how information is shared among different age groups.[55] It was identified that senior military officers are more apprehensive to share information than junior military members. Department of Defence spokesperson, Siphiwe Dlamini, noted in 2023 that unauthorised access to and sharing of classified organisational information are prohibited and that there are guiding principles and policies to guide members' functioning.[56] Bester and Arendse argue that limited information on the risk of threat information in the organisation is conveyed to military members.[57] This adds to military members' cyber-hygiene vulnerability and overall cybersecurity awareness of possible threats and security protocols.[58] It is however noted that, while the dissemination of policies and directives is not equally received throughout the organisation, directives geared towards the processes and procedures on information and communications systems of security in the Department of Defence exist.[59] Singh *et al*. suggest that all users must have some sense of accountability when applying best practices when navigating the Internet.[60] A lack of information on these best practices may also lead to the ineffective application of cyber hygiene in organisational contexts. The onus is therefore not only on organisational management to enforce guidelines and best practices but also on personal accountability.[61] In addition, it has been shown that employees will exhibit better cyber-hygiene behaviour in organisations that have invested significantly in cybersecurity measures.

Ncubukezi and Mwansa indicate that effective and clear communication strategies and policies should be the priority of all organisations.[62] The effective practice of these strategies has however not been executed comprehensively in the SANDF, as Bailie notes that the organisation has experienced substantial challenges related to internal and external communication.[63] Ncubukezi and Mwansa draw attention to several factors that may cause poor cyber hygiene in organisational contexts:

- Limited cybersecurity awareness of threats and safety precautions;
- Cybersecurity policies and guidelines that are ineffective in addressing emerging threats; and

- Limited knowledge of the technical component of cybersecurity.[64]

The authors indicate that there must be a connection between the technical features of cybersecurity and behavioural elements. When making the link to SANDF members, Bester draws parallels, and suggests that cybersecurity should be flexible and approached from a multi-disciplinary perspective where there is a blend of technical and human factors.[65]

Organisations that experience budgetary constraints may find it challenging to acquire new technological tools for their personnel to use. Sharing information quickly is however crucial in the digital age, and limiting technology in organisations may hinder the psychological need to share information rapidly. In an organisation, such as the SANDF, sharing information digitally might be critical for operations and instructions to be executed rapidly.[66]

As noted, the rise of cyber threats may result in significant security challenges at the individual level, but may also pose security challenges to organisations, multiple sectors, and national security.[67] The significant increase in cyber threats has led to the SANDF being more resolute in enhancing its cyber resilience and digital capacity.[68] Bester and Arendse assert that the SANDF acknowledges the importance of cyber threats and attacks and the vulnerability of its members.[69] It is thus necessary to explore online security practices and behaviour from a multi-disciplinary perspective.[70] This multi-disciplinary view is echoed in cybersecurity awareness research that highlights technological advancement, psychosocial factors, and the development of cybersecurity awareness and education.

The Link Between Cyber Hygiene and Cybersecurity Awareness

Hygiene encompasses the conscientious practice of upholding bodily cleanliness to support both mental and physical well-being.[71] This brief reiteration of hygiene can be linked to cyber hygiene, which highlights the efforts made by users to ensure online safety through appropriate mechanisms that ensure system health and online security. The implementation of efficient cyber-hygiene practices among users has been identified as an important factor in addressing cyber threats and risks.[72] This also points towards the facets of knowledge and routine practice of security protocols. Van't Wout refers to the idea that cybersecurity training should be provided on a regular basis in order to build knowledgeable security personnel that can manage risks effectively.[73] Bester adds that a one-size-fits-all approach cannot be the only solution for an organisation the size of the SANDF, as specific needs must be addressed.[74] Furthermore, cyber threats are unique in their own right and may affect strategic parts of cyber well-being and functioning.[i] Bester therefore recommends that threats need to be mitigated by using uniquely tailored training programmes and behavioural mechanisms that are well positioned to deal with

[i] The researcher refers to "cyber well-being" as a term that encompasses both the technical and the psychological well-being of the user functioning in cyberspace and making use of it.

the technical features and psychological attributes that seek to exploit user vulnerability.[75]

Cyber hygiene is a concept that needs more attention in the organisational context as it aligns with the development of cybersecurity awareness. Introducing cyber hygiene to personnel in organisational contexts may enable the efficient behaviour of managing risks.[76] In organisational contexts, the practice of cyber hygiene is recommended to be the responsibility of every employee. Therefore, the successful practice of cyber hygiene implies that responsibility for maintaining security behaviour rests not only with the organisation, but also with the individual.

Securitisation Theory

Securitisation theory originates from the fields of international relations and political science. There is, however, an ongoing debate about the necessity of expanding this theory to encompass aspects related to human and climate security. The foundation of securitisation theory in the context of cyber hygiene is based on the idea that security is a performative act, where language plays a crucial role in influencing the execution of authority. While securitisation theory is primarily utilised to illustrate conceptualisations of security within the political landscape, the current study applied the theory to examine how cyber-hygiene practices among military officers are shaped by the perceived importance of and threats posed by cyber threats and attacks. Philipsen argues that, to engage in security, one must also articulate matters of security, in other words, one should implement security practices, such as maintaining strong password management or ensuring the use of secure networks. Individuals must therefore be aware of and participate in a discourse about security.[77] Such discourse functions as a speech act that communicates the nature and extent of the threat. Bester however points out that, even if the speech act is initiated, it does not necessarily indicate a complete awareness or understanding of the threat involved.[78]

Method

The study on which this article is based, adopted an interpretivist approach, mainly to explore cyber hygiene within the SANDF context. A cross-sectional design was utilised as the research was not focused on the long-term impact of cyber hygiene practices and behavioural implications, but on the short-term impact. Moreover, participants were recruited using a non-probability sampling method. Homogenous purposive sampling, a non-probability method, was used as the technique to obtain information from the participants.[79]

Connection to the Larger Study

The current study formed part of a larger study that focused on cybersecurity awareness among the South African armed forces. The larger study comprised two methodological phases. Phase 1 focused on the qualitative exploration of cybersecurity awareness by targeting participant perceptions and views. Phase 2 consisted of a quantitative investigation that employed the Cybersecurity Orientation Questionnaire.[80] The larger study made use of a sequential design, which is a phased approach typically used in mixed-methods studies.[81] The current study explored the findings of Phase 1 of the larger study by providing a detailed account of three dominant themes related to cyber-hygiene practices in the SANDF, namely:

- Theme 1: Training and knowledge development of cybersecurity awareness;
- Theme 2: Lack of trust in organisational devices and services; and
- Theme 3: Practical experience with cyber-hygiene practices

Research Aims and Objectives

The current study explored cyber-hygiene practices among South African military officers. The focus on cyber hygiene emphasises the role of cybersecurity awareness in the SANDF context, and contributes to the existing narrative that the human element is central to the formation of online security behaviour. In recent times, cybersecurity research in the South African context has received much attention in terms of elements related to awareness, security management, and training.[82] Bester however asserts that more research needs to be conducted on cybersecurity awareness behaviour within the SANDF.[83] While there might be limited research on cybersecurity awareness in the SANDF, a wealth of research in this regard exists outside the SANDF context. In the context of the SANDF, limited research exists that focused on cyber hygiene and cybersecurity awareness. For this reason, it was necessary to explore the following dimensions:

- Information-sharing culture;
- Security orientation;
- Cybersecurity posture; and
- Cybersecurity practices.[84]

These four dimensions were developed to emphasise the importance of the human element within the cybersecurity process. Consequently, the purpose of the study was to explore the cyber-hygiene behavioural practices of a South African military sample. This was the first time that research has been conducted on the cyber-hygiene behavioural practices in a military context, and it is trusted that it will promote further research into refining the measurement of cybersecurity awareness within the military context.

The research question for this study was whether South African military officers practise cyber hygiene in the organisational context. The aims of the study were to explore the cyber hygiene of South Africa military members, and to explore how cyber-hygiene practices are conducted by military members.

Participants

The researcher enlisted participants from the South African National Defence College (SANDC), a distinguished military institution that provides comprehensive education, training, and development programmes.[85] The study deliberately omitted age and gender as criteria for selecting participants, as these factors were deemed irrelevant in terms of the research aims. Despite his best attempts, the researcher could only enlist ten senior military officers, as other potential participants were unavailable owing to academic commitments.

Data Collection

The participants completed semi-structured interviews about their perceptions of cybersecurity awareness and online security behaviour executed within the organisation. Semi-structured face-to-face interviews were conducted during January 2020 and lasted between 35 and 50 minutes each.

Data-Collection Tool

The study employed an interview guide encompassing four dimensions pertinent to cybersecurity awareness, namely:

- Information-sharing culture;
- Security orientation;
- Cybersecurity posture; and
- Cybersecurity practices.

While the primary purpose of the interview guide was not to concentrate on cyber-hygiene practices, the analysis phase of the broader study highlighted the significance of security behaviours and practices in understanding cybersecurity awareness. Furthermore, it is essential to recognise that behaviour and security practices are integral to comprehending the concept of cyber hygiene. Consequently, the positionality of this study justified the need to investigate this emerging topic further.

Participant number	Gender	Location	Rank	Race	Arm of service
P1	Male	Western Cape	General	Coloured	Air Force
P2	Female	Gauteng	Colonel	White	Air Force
P3	Male	Gauteng	Colonel	White	SA Army
P4	Female	Gauteng	Colonel	Indian	SA Army
P5	Male	Gauteng	Colonel	White	SAMHS*
P6	Male	Limpopo	Captain	Black	SA Navy
P7	Female	Gauteng	Colonel	Black	SAMHS
P8	Female	Gauteng	Colonel	White	Air Force
P9	Male	Gauteng	Colonel	Black	SA Army
P10	Male	Gauteng	Colonel	Coloured	SA Army

*South African Military Health Service (SAMHS)

Table 1: Participant Profile

Ethical Considerations

Upholding ethical considerations throughout the study was important. The study was conducted in alignment with established ethical best practices to ensure the integrity of the study and the protection of the participants' rights. All ten senior military officers provided written informed consent to participate in the interview process. All ethical standards were rigorously maintained throughout the duration of the interviews and the research. The information presented during the semi-structured interviews was of a sensitive nature; the researcher therefore utilised participant numbering to ensure anonymity. In addition, access to the data was restricted to the principal researcher. Safeguarding of data in this study was important, as it not only focused on military knowledge, but also on the confidential information of military officers. Given the sensitive context of cybersecurity within the SANDF, the researcher exercised caution to avoid inducing anxiety among the participants regarding the subject matter. When posed with challenging questions, the participants were afforded the opportunity to reflect to ensure their composure and to allow them the flexibility to respond in a manner that aligned with their comfort level.[86] The researcher adopted a non-judgemental approach, and established rapport in order for the participants to provide rich and detailed information.[87] Ethical clearance for this study was secured from Stellenbosch University, South Africa. The data supporting the findings of this study can be requested directly from the corresponding researcher; however, please note that the data are not publicly available because of confidentiality restrictions.

Data Analysis

The study used a qualitative content analysis approach to identify patterns in the themes derived from the data source.[88] This method helped in recognising commonalities and the frequency of occurrence of these patterns. Qualitative inquiry is believed to provide a deep understanding of events and phenomena in the social world.[89] In the context of

the SANDF, exploring cyber hygiene necessitated a method that allowed participants to share their experiences, which the researcher could then analyse.[90] Additionally, since the study aimed to investigate the cyber-hygiene practices of South African military officers, a qualitative approach was appropriate for this research. Qualitative content analysis involves systematic and transparent procedures for processing data and substantiating trustworthy interpretations in the social science domain.[91] The study followed an eight-step process:

- Preparing the data after the interview data had been collected;
- Defining the unit of analysis, expressed in a singular theme or paragraph;
- Developing categories and a coding scheme;
- Testing the coding scheme through the text from the obtained narratives;
- Coding the text;
- Evaluating the code consistency by checking and rechecking for duplication and irregularities;
- Drawing inferences from the coded data; and
- Highlighting the findings and methodology used in the research process.

Three main themes emerged from the content analysis. The first theme focused on the crucial development of training and knowledge in the field of cybersecurity awareness, which highlighted the need for continuous learning and skill development to combat evolving security threats. The second theme pertained to the prevailing lack of trust in emerging technology, which underscored the challenges and mistrust surrounding the adoption of new technological innovations and their potential cybersecurity implications. The third theme emphasised the practical implications of executing security behaviour that contributes to cyber hygiene in the organisation. The theme titles and descriptions are presented in Table 2.

Theme	Description
Theme 1: Training and knowledge development of cybersecurity awareness	This theme focused on the notion that training and development processes are important for the advancement of cybersecurity awareness.
Theme 2: Lack of trust in organisational devices and services	This theme focused on the trust that military members have in the ability of the organisation to implement its policies and directives. The notion of trust also included the military officers' ease and confidence using digital devices, such as laptops and stationary computers at their respective units.
Theme 3: Practical experience with cyber-hygiene practices	This theme addressed how exposure to security behaviour and knowledge may assist with cyber-hygiene practices.

Table 2: Themes

Results

This section discusses the three themes derived from the interviews conducted with military members.

Theme 1: Training and Knowledge Development of Cybersecurity Awareness

The interviewed senior military officers agreed that cybersecurity training and education were crucial for advancing security in their organisational context, and they highlighted the importance of teaching and learning within the military context. Training and knowledge production regarding cyber threats and security behaviour are essential in the advancement of cyber-hygiene practices and ensuring that rational decisions are made when encountering threats.[92] These findings echo the need for training as eight out of ten participants indicated that, at the time, training was required to advance their security behaviour and daily practices in the workplace. Two participants indicated some training on cyber threats at the time and highlighted that it was largely the responsibility of the military member to seek external training on cybersecurity. Eight participants emphasised the importance of staying up to date with the latest cybersecurity trends to ensure that they were prepared for potential threats. The participants also suggested that regular information sessions would help to force members to adopt better security behaviour and remain vigilant in their daily data-sharing tasks. Although the senior military officers were aware of potential threats, they acknowledged that not all members of the organisation received critical information on potential attacks. They therefore recommended that cybersecurity and risk information training should be available to all levels of the organisation, without any exclusionary factors. Relating this to cyber hygiene, training on cybersecurity is key in raising the awareness levels of personnel in organisational contexts and reducing the notion of risk. Howell *et al*. however argue that training and providing threat information may not necessarily improve security behaviour or advance cyber-hygiene practices; instead, it may only improve decision-making on how to mitigate threats and address previous or existing security behaviour.[93] Some participants also indicated that, at the time of the research, there was some level of awareness of cyber threats and they revealed that, while very limited training on information security and overall cybersecurity behaviour was provided to all members of the organisation, the acquisition of knowledge could be performed in a private capacity. This could indicate the willingness and resourceful nature of force members to educate themselves and to be contextually aware of threats that may have an influence on their personal and organisational data. In this regard, some participants mentioned the following (please note that all quotations are reproduced verbatim and unedited):

> If someone was really aware of the dangers of cyber threats and attacks they would take the proper measures and log out, because what will happen when someone imports something through your Internet account or email address, then it spreads at work and on our computers and when they investigate the issue, then you are the source without you being aware. (P3)

> Cybersecurity training should be intervention-based where training is offered on a monthly basis so that we're able to adapt to technology that is moving quickly. (P2)

> All military members should be trained in the Department of Defence, and information should not only belong to specific group of people such as specialists or Defence Intelligence. The organisation must empower people so that we can go beyond the current measures put in place to solve our challenges with cybersecurity. (P3)

The above excerpts indicate that training on cyber hygiene should be a continuous exercise. Organisations that offer regular cybersecurity training from a technical and behavioural standpoint may benefit from an employee base that is aware of threats and that may exhibit practical cyber-hygiene traits. Van't Wout indicates that routine cybersecurity awareness training is an effective approach to increasing the digital security of an organisation.[94] Bester recommends that routine cybersecurity awareness training is beneficial for practising cyber hygiene among employees in organisations.[95] The participants' narratives suggested that regular cybersecurity training is required to reduce the threat to organisations and members of organisations.

Theme 2: Lack of Trust in Organisational Devices and Services

This theme focused on the digital trust that participants should have in cyberspace, and the technology required to access this space. Six of the ten participants considered there to be mistrust regarding the use of organisational devices, such as laptops, as well as the implementation of policies related to the use of these devices. Four of the ten participants considered there to be trust among military members; however, it was noted that senior management should discipline those who violate procedures. The element of digital trust in Theme 2 was an important factor for the participants, as this trait allowed for peace of mind when gaining access to devices and navigating the Internet and organisational networks. The implementation of effective cyber-hygiene practices empowers employees to navigate the Internet and organisational systems with confidence.[96] Furthermore, fostering digital trust within organisations is likely to enhance employees' cyber-hygiene practices, thereby contributing to a secure operating environment.[97] This theme also raised another important aspect, which was that the participants did not trust the technological devices supplied by the organisation to access cyberspace without the risk of malware being present. The participants shared the opinion that trust was an important factor in achieving effective communication in the organisation. Expanding on the point made by the participants, it is noted that effective, transparent communication strategies form a good foundation to establish trusting relationships, especially since cybersecurity requires collaboration among stakeholders. The narratives of the military officers in this regard were as follows:

> I would personally make cybersecurity more visible in the organisation. There are military members who violate certain security procedures, and this is usually kept quiet. I believe the organisation should expose those that are violating trust and existing security measures. (P2)

> I must admit, there is an absence of clear communication in the Department of Defence. There are certain systems in place, but these have been adjusted as times goes on, you understand. Unfortunately, I am not aware whether we have an official network that will allow us to engage in rapid information sharing of threats. (P2)
>
> [A]t this stage, if you look at Lotus Notes, we are looking at meetings, performance plans, and that sort of stuff. I don't think the network is secure enough, and I don't think any secret or top-secret information should be shared on this platform; it should be in a central place where you look at the information and go away. (P8)
>
> [W]e not actually securing the information in the organisation, so if I lose my laptop in the organisation, I lose everything. I do have a password, but that's about it. (P5)

These narratives show that, at the time of the research, there was a level of mistrust among military officers concerning the network security and the devices provided to military members. The narratives provided insight into the complex relationship that participating military officers had with the resources supplied by the SANDF at the time. The precautions implemented to address security challenges related to theft were also raised, where Participant 5 (P5) indicated that setting a password is sufficient to secure a device that is subject to theft. This raises the argument that physical security needs to be taken as seriously as the enforcement of online security behaviour in the workplace. This particular stance on a lack of trust may extend to Participant 3's view, which was that, at the time, the organisation did not trust its employees with the official allocated laptop devices and therefore applied strict security policies to monitor this. The awareness related to the existing network security also came into question, where Participants 2 and 8 remarked that they were neither aware of its existence, nor were they confident in the capability of its implementation. The researcher argues that existing security procedures come in the form of best practices and guidelines. Moreover, existing procedures detailing the security steps in cybersecurity should also be made more accessible for military members in the organisation, as pointed out by Participant 5. Participant 2 indicated that there were gaps in the communication strategies to deploy risk information on cyber threats.

Theme 3: Practical Experience with Cyber-Hygiene Practices

Nine out of ten participants indicated that they actively engaged in setting new passwords and storing their data in secure locations. Enhancing cyber-hygiene practices may facilitate a cost-effective way to address cybersecurity in the workplace as the focus is on an individual level.[98] Practising cybersecurity awareness and information security has been shown to depend on individual factors related to age and gender.[99] These factors as variables are both considered to be present when security behaviour is practised in organisational and personal contexts. This also shows that there is a limited gap between the two contexts and the practice of security behaviour.[100] Moreover, it was evident from the narratives that the practical experience of cyber hygiene was not dependent on years of experience in

the organisation or the period in which an individual is exposed to the Internet. Instead, the narratives alluded to the knowledge and experience gained by observing the security protocols executed in the organisation. In this discussion, information-sharing activities play an important role in the formation of perceptions of cyber-hygiene practices. The narratives showed a lack of guidance when interpreting cyber threats, as well as when exercising cybersecurity behaviour. The theme showed that the participants practised cyber hygiene by regularly changing their passwords and securing organisational data by refraining from storing sensitive information on their personal memory sticks or flash drives, and avoiding connecting to public Wi-Fi access points. The narratives indicated that certain steps were taken by military officers in the SANDF to ensure cyber hygiene; however, not all practices were ideal. Skorenkyy *et al.* suggest that technical training is required to enhance the expertise of employees in organisations.[101] These training programmes however often fail to include policy and regulatory frameworks. Based on the participants' narratives, it was evident that, when storing information, the boundaries are not always transparent. This may lead to misunderstandings, and may also affect the execution of behaviour. Excerpts from the participants' narratives are presented below.

> Ever since the computer generation in terms of putting documentation on the hard drive, it becomes […] a risk because you are sometimes requested to work at home. Although sometimes it's easier said than done and this is where […] you sometimes blur the line when saving official information on your personal hard drive. And sometime vice versa as sometimes you are not in possession of your Defence hard drive, and sometimes you transfer that information to a personal hard drive, which could be problematic. (P1)

> Yes, I have a MacBook and I store all my work information on my personal device. And then I save all work-related information on a flash disk which I received from Air Force HQ [headquarters]. Tomorrow I will bring it back to work and then work in such a way again. (P2)

> I don't secure my passwords regularly. I'm not so fussy about it. For example, right now we know it's supposed to happen, but there's not much going into it. (P7)

> Government information should not really be stored on a personal flash drive and they can store it on a hard drive, but it must be controlled. (P6)

> I would say one way to limit breaches to systems and computers and stuff is to make sure you are in your office working and not leaving your work on the database. You need to avoid leaving your information on memory sticks that should not be done what I think. (P5)

> [A]s an officer you should know what is right or wrong. And to be ethical, to save your official information on your personal hard drive is not right. But […] sometimes you are forced to do things that are not supposed to be done in that manner. (P1)

> I don't believe military members are aware of how they should behave in cyberspace and how they should treat information. For example, the in thing as of late is, when you get a signal, you take a photo and send it to your colleague via WhatsApp, though WhatsApp is encrypted. (P9)

Participant 9's narrative showed that procedures concerning the information shared in terms of cybersecurity were unclear. In addition, Participant 9 noted that secure information-sharing practices were limited and that sensitive information was shared on social communication platforms, such as WhatsApp. Participant 1's words showed that behaviour was adapted based on risk. The researcher concluded that behaviour is influenced by risk perception, which entails that users adapt their security behaviour based on how much risk they are willing to take. This risk was also demonstrated in Participant 2's words. The narratives indicated that the participants were able to implement some cyber-hygiene practices in the organisation by changing passwords on their personal and organisational devices, refraining from storing sensitive data on flash drives, and making use of a controlled and secure space to store organisational data.

Discussion

The participants reported experiencing various challenges in acquiring cybersecurity awareness training, in their personal and in their professional capacity. This resulted in feelings of frustration with the senior management of the organisation. According to Van't Wout, training should be tailored and customised to the needs of the organisation.[102] Bester advances this idea by pointing out that cybersecurity training should not only be reserved for those with technical abilities and those in specialised roles; instead, it must form part of a structured training programme that is accessible to all members of an organisation.[103] Ncubukezi and Mwansa argue that all employees (management included) should be involved in establishing cyber hygiene.[104]

The impact of the digital culture has been substantial in promoting the incorporation of technology into professional roles. Culture plays a vital role in organisational settings and signifies the readiness of an organisation to embrace a digital culture that is marked by cybersecurity awareness and compliance with established best practices and guidelines.[105] Trevors and Wallen highlight the importance of organisations establishing a well-defined framework and action plan to manage cyber threats and potential incidents effectively.[106] Their findings revealed that the organisation acknowledges the significance of cyberattacks to national and individual security. Tabrizi *et al*. argue that, while organisations embrace digital transformation, the efforts of these attempts may not necessarily yield effective outcomes.[107] Mvubu and Naudé attribute the lack of digital transformation in organisational contexts to risk taking, innovation, and collaborative efforts.[108] The current findings indicated indicate that some senior military officers are applying cyber-hygiene practices in the organisation; however, the underlying feeling was that there is a growing digital culture that demands attention. It is worth noting that organisational culture plays a significant role in the acceptance of digital technologies.[109] In the case of the SANDF, increasing budgetary constraints may however complicate the advancement of a digital

culture. This may also affect the overall securitisation process where security moves may not occur fully. A reflection of these budgetary constraints can be found in the Department of Defence Annual Report 2023–2024.[110]

Theme 2 showed that the majority of the participants had mistrust in the use of organisationally sanctioned devices for performing their day-to-day tasks. Access to devices (laptops and computers) that were safe within the organisation was revealed to be problematic. The findings showed that most members did not trust the devices in their respective units. Instead, they relied on their own laptops and mobile devices to conduct their duties. This shows that, at the time, there was mistrust among participating military members of their allocated organisational devices. The bring-your-own-device (BYOD) scenario in the workplace signifies a level of risk, but may also be an indication of the limited execution of policy that dictates the use of personal devices in organisational settings, such as the SANDF.[111] Moreover, from a contextual standpoint, it can be argued that budgetary limitations may neither consistently enable the facilitation of comprehensive training throughout the entire organisation nor ensure the accessibility of devices equipped with sophisticated security software essential for enhancing cybersecurity. When examining the potential impact of financial limitations on the cyber-defence capabilities of the SANDF, it is important to emphasise four strategic objectives, namely:

- The development of capabilities;
- The implementation of awareness initiatives on cybersecurity;
- The facilitation of research and training; and
- Co-ordination and engagement with national and international stakeholders.[112]

Consequently, budgetary constraints could hinder the successful implementation of these strategic goals, particularly in the domain of training, which is essential for fostering awareness and understanding of cybersecurity.[113]

The Department of Defence Instruction DODI/CMI/00008/2001 refers to the auditing of personal and organisational devices in order to safeguard against threats and attacks.[114] Although the directive exists, the participants noted that, at the time of the research, there was a lack of seriousness among members in the organisation regarding the use of personal devices and the storage of sensitive organisational information on unsanctioned devices. Akter *et al.* argue that cyber threats and attacks are becoming increasingly prominent in society and are targeting employees in organisational contexts. Akter *et al*. suggest that employees with limited cybersecurity awareness and knowledge may be susceptible to threats.[115] Practical skills and knowledge are therefore recommended for enhanced capacity to mitigate potential cyber threats. The participants showed an acceptable level of awareness of potential cyber threats; however, some participants were not able to recognise that their own behaviour increased their vulnerability to potential attacks, and might act as a gateway for organisational data to be at risk. The human factor is therefore not only the weakest link, but also the most significant component in the cybersecurity chain.

Theme 3 revealed that some participants had been exposed to online security practices that assisted with their cyber hygiene in the organisation; however, their exposure to

cyber-hygiene practices was not as a result of age or gender. There is therefore a need for self-development and staying secure in a digital environment. Additionally, participants who practised cyber hygiene recognised that cyber threats require attention and must be addressed through behavioural strategies. This acknowledgment of the threat aligns with existing literature on securitisation theory, which states that recognising a threat is essential for implementing any emergency measures.[116] Moreover, the Department of Defence Instruction DODI/CMI/00008/2001 indicates online security practices must be adhered to, as the storage of restricted information on officially registered organisational storage devices as well as on laptops must be approved by the designated ICT specialist at the unit level.[117] This was however not the case for all participants, as some indicated that there was limited exposure to training on cybersecurity awareness and policies that deal with online security in the organisation. The level of experience gained when practising cyber-hygiene may also point to the idea that age and gender differences might be predictors of security behaviour.[118] Humaidi and Shahrom argue that work experience might be considered a strong predictor of security practices, such as connecting to open-source Wi-Fi access points.[119] The current findings showed that the majority of the participants did not connect to open-source Wi-Fi, and applied security behaviour in their personal and professional contexts. Moreover, in terms of experience, the participants also did not have high expectations of how cybersecurity was executed in the organisation at the time. The participants' perception of this limited execution was therefore based on their experience with unclear guidelines and directives, as well as a lack of seriousness in considering cybersecurity as an outcome. In addition, effective cyber hygiene demands acknowledgement by senior management in organisational contexts and, in the case of the SANDF, the findings showed that threat acknowledgement has not fully occurred, which means that, from a theoretical view, the securitisation of cyber threats has not yet reached a point where emergency measures are introduced.

Limitations and Recommendations

The current study was limited to a specific subset of participants due to limitations in accessing and recruiting military officers to participate in the study. As a result, the findings of this study may not be broadly applicable to the entire SANDF. he findings revealed that senior officers were aware of the current directives in the SANDF related to cybersecurity or information security; however, abiding by the directives was not considered important. To enhance the development of a more cohesive policy in the SANDF, it is recommended that future contributions should be more explicit and incentive-based. This method could potentially promote adherence to policies and persuade military personnel to view policy and directives as advantageous. The findings also underscored that awareness of specific threats could influence the implementation of online security measures. Better alignment between the directives of the organisation and the level of awareness required from military members at the unit level is therefore required.

In the context of bolstering cybersecurity protocols within military ranks, it is imperative to explore the adoption of gamification as a methodological approach to training programmes. This approach focuses on raising awareness of information security threats

and the vulnerabilities that arise from human behaviour. Gamification is especially suitable for employees who prefer a more relaxed and engaging way to undergo cybersecurity training. Additionally, integrating the Cybersecurity Orientation Questionnaire developed by Bester[120] with the 16 Personal Factor Questionnaire could help to measure how different personality types might be susceptible to various cyber threats and how users should approach risk in the SANDF. This recommendation is crucial because psychological practitioners in the SANDF conduct assessments for selection purposes. Improving psychological measurements could therefore contribute to the overall goal of understanding and focusing on human psychology within the cybersecurity domain.

Conclusion

This article focused on the cyber-hygiene practices employed by military members in their everyday functioning within the organisational context. The findings showed that some military members practised cyber hygiene by engaging in safe data practices and storing sensitive information, although there were a few military members that indicated that, at the time, data-safety practices were challenging to adhere to since organisational demands superseded these indicated security practices. Additionally, the majority of the military members highlighted that additional training and clear guidelines should be implemented to avoid a mismatch between security practices and expectations. Furthermore, the lack of confidence in the technical capability of the organisation was hampering the advancement of a digital culture in the organisation framed around security and technological integration. The ability to practise cyber hygiene shows that military members feel more secure about their organisational and personal data when using their own devices, rather than the allocated organisational devices.

The insights produced by this study offer a humanistic view on the cyber-hygiene practices employed by senior South African military officers. This study may act as a starting point to view the human element as one of the strong links in the cybersecurity chain. Practising cyber hygiene is by no means a once-off procedure, but requires investment through resources and leadership to convey the importance of mitigating malware infections and data corruption as well as data loss. Ultimately, the promotion of cyber hygiene in organisational contexts may lead to a healthy cyber environment, which in turn may advance the security behaviour of users and their understanding and awareness of cybersecurity.

Acknowledgements

This article was based on research supported by the National Institute for the Humanities and Social Sciences (NIHSS)Disclaimer

The views expressed in this article are the researcher's own and do not reflect the official position of any institution.

Endnotes

[1] Dr Kyle Bester is a registered Research Psychologist and senior psychology lecturer at the University of South Africa. He holds a master's degree in research psychology from the University of the Western Cape. He supervises postgraduate students who have taken up research related to cybersecurity, online security behaviour, artificial intelligence and digital culture. He specialises in research focused on cybersecurity awareness in the South African armed forces context. He has a PhD in Military Science from Stellenbosch University. He serves as an executive committee member in the Division for Research and Methodology (DRM) at the Psychological Society of South Africa (PsySSA). Dr Bester is an emerging researcher, and his research interests include military science, data-colonialism, cybersecurity awareness, securitisation of cyberspace and online security behaviour.

[2] KJ Bester, *Exploring the Perceptions and Views on Cybersecurity Among South African Military Officers* (PhD dissertation, Stellenbosch University, Stellenbosch, 2023).

[3] H Pieterse, 'The Cyber Threat Landscape in South Africa: A 10-year Review', *African Journal of Information and Communication*, 28 (2021), 1–21.

[4] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 53.

[5] J Cilliers, *Challenges and Opportunities: The Future of Africa* (Cham: Palgrave Macmillan, 2021).

[6] Parliamentary Monitoring Group, 'SANDF Deployment to Prevent & Combat Crime: Update on Security Situation in the Country; with Minister: Joint Standing Committee on Defence', 18 July 2021. <https://pmg.org.za/committee-meeting/33303/> [Accessed on 23 September 2024].

[7] B van Niekerk, 'An Analysis of Cyber-incidents in South Africa', *The African Journal of Information and Communication*, 20 (2017), 113–132.

[8] KJ Bester, 'Cybersecurity Awareness from the Perspective of the South African National Defence Force Military Officer', in E Jakaza, H Mangeya & I Mhute (eds.), *The Palgrave Handbook of Language and Crisis Communication in Sub-Saharan Africa* (Cham: Palgrave Macmillan, 2024), 273–294.

[9] Pieterse, 'The Cyber Threat Landscape', 5.

[10] J Devanny & R Buchan, 'South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority', Carnegie Endowment for International Peace, 12 January 2024. <https://carnegieendowment.org/research/2024/01/south-africas-cyber-strategy-under-ramaphosa-limited-progress-low-priority?lang=en> [Accessed on 30 August 2024].

[11] Devanny & Buchan, 'South Africa's Cyber Strategy'.

[12] *Daily Maverick*, 'SNATCHed – SANDF Data Leaked in Cyberattack Appears to be Authentic, Say Cybersecurity Analysts', 6 September 2023. <https://www.dailymaverick.co.za/article/2023-09-06-snatched-sandf-data-leaked-in-cyberattack-appears-to-be-authentic-say-cybersecurity-analysts/> [Accessed on 6 September 2023].

[13] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 80.

[14] KJ Bester & D Arendse, 'Measuring Cybersecurity Awareness: Exploring the Reliability and Factor Structure of the Cyber Security Questionnaire in a South African Military Sample', *Scientia Militaria: South African Journal of Military Studies*, 52, 1 (2024), 5–33.

[15] Bester, 'Cybersecurity Awareness', 291.

[16] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 42

17 Bester, *Exploring the Perceptions and Views on Cybersecurity*, 79.

18 Bester, 'Cybersecurity Awareness', 288.

19 C van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture'. Paper presented at the *Fourteenth International Conference on Cyber Warfare and Security*, Stellenbosch, 28 February to 1 March 2019. <http://hdl.handle.net/10204/11345> [Accessed on 25 September 2024].

20 Bester, *Exploring the Perceptions and Views on Cybersecurity.*

21 K Maennel, S Mäses & O Maennel, *Cyber Hygiene: The Big Picture* (Cham: Springer, 2018), 291–305.

22 Maennel *et al*., *Cyber Hygiene*, 1.

23 V Babić & A Bratić, *Guidebook on Staying Safe Online: Cyber Hygiene for Public Institutions and SMEs* (Geneva: Geneva Centre for Security and Governance, 2022), 1–18.

24 Babić & Bratić, *Guidebook on Staying Safe Online*, 2.

25 J Nowicka, Z Ciekanowski, J Kudins & P Dąbrowski, 'Managing Organizational Security in the Era of Digital Transformation', *European Research Studies Journal*, 27, 3 (2024), 460–471.

26 Babić & Bratić, *Guidebook on Staying Safe Online*, 4.

27 T Ncubukezi & L Mwansa, 'Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid19 Pandemic', *Journal of Internet Technology and Secured Transactions*, 9, 1 (2021), 714–721.

28 Ncubukezi & Mwansa, 'Best Practices', 715.

29 C McMahon, 'In Defence of the Human Factor', *Frontiers in Psychology*, 11 (2020), 1–4.

30 K Khando, S Gao, SM Islam & A Salman, 'Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review', *Computers & Security*, 106 (2021), 1–22.

31 S Gupta & S Furnell, 'From Cybersecurity Hygiene to Cyber Well-being', in A Moallem (ed.), *HCI for Cybersecurity, Privacy and Trust (HCII 2022): Lecture Notes in Computer Science, vol. 13* (Cham: Springer, 2020), 124–134.

32 T Karayel & A Akbıyık, 'Managing Cyber Security Risks and Cyber Hygiene in Organizations: Improving Cyber Resilience', in M Albakri (ed.), *Digital Transformation and Innovation in Emerging Markets* (Hershey: IGI Global Scientific Publishing, 2025), 205–226.

33 Bester, *Exploring the Perceptions and Views on Cybersecurity*, 33.

34 Bester, *Exploring the Perceptions and Views on Cybersecurity*, 58.

35 Teceze, 'Overcoming Poor Cyber Hygiene and Budget Constraints', 5 January 2024. <https://teceze.com/strengthening-cybersecurity-resilience-overcoming-poor-cyber-hygiene-and-budget-constraints> [Accessed on 23 September 2024].

36 Bester & Arendse, 'Measuring Cybersecurity Awareness', 10.

37 R Dagada 'The Advancement of 4IR Technologies and Increasing Cyberattacks in South Africa', *Southern African Journal of Security*, 2, (2024), 1–27.

38 Republic of South Africa, 'The National Cybersecurity Policy Framework (NCPF)', *Government Gazette*, 39475, 4 December 2015. <https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf> [Accessed on 26 February 2025].

39 Parliamentary Monitoring Group, 'Cyber Warfare Policy: Department of Defence Briefing', 11 March 2020. <https://pmg.org.za/committee-meeting/30014/> [Accessed on 18 March 2024].

40 Department of Defence, 'South African Defence Review 2015', Parliamentary Monitoring Group, 2015. <https://static.pmg.org.za/170512review.pdf> [Accessed on 12 March 2023].

41 Parliamentary Monitoring Group, 'Cyber Warfare Policy'.

42 United States Government Accountability Office, 'Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene', 13 April 2020. <https://www.gao.gov/products/gao-20-241> [Accessed on 13 September 2020].

43 A Georgiadou, S Mouzakitis & D Askounis, 'Detecting Insider Threat via a Cyber-security Culture Framework', *Journal of Computer Information Systems*, 62, 4 (2021), 706–716.

44 Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 463.

45 Bester, 'Cybersecurity Awareness', 279.

46 N van der Waag-Cowling, 'South Africa and the Cyber Warfare Threat: A Strategic Overview', in B Wells (ed.), *Civil-military Cooperation and International Collaboration in Cyber Operations* (Georgia: University of North Georgia Press, 2018), 22–51.

47 MJ Aschmann, L Leenen & JC Jansen van Vuuren, 'The Utilisation of the Deep Web for Military Counter-terrorist Operations'. Paper presented at the International Conference on Cyber Warfare and Security, Dayton, OH, 2–3 March 2017, 1–8.

48 S Nielsen, 'The Role of the U.S. Military in Cyberspace', *Journal of Information Warfare*, 15, 2 (2017), 27–38.

49 Department of Defence, '2020/21 Department of Defence Annual Report', 2021. <https://www.gov.za/sites/default/files/gcis_document/202110/defenceannualreport202021.pdf> [Accessed on 25 September 2024].

50 Department of Defence, '2020/21 Department of Defence Annual Report'.

51 Z Dlamini & M Modise, 'Cyber Security Awareness Initiatives in South Africa: A Synergy Approach'. Presentation at the Seventh International Conference on Information Warfare and Security, University of Washington, Seattle, WA, 22–23 March 2012, 1–10.

52 G Martin, 'Uncontrolled Use of Social Networks: A Security Risk for the SANDF', *Defence Web*, 12 March 2020. <https://www.defenceweb.co.za/sa-defence/sa-defence-sa-defence/uncontrolled-use-of-social-networks-a-security-risk-for-the-sandf/> [Accessed on 23 September 2024].

53 Martin, 'Uncontrolled Use of Social Networks'.

54 Bester, *Exploring the Perceptions and Views on Cybersecurity*, 156.

55 Bester, *Exploring the Perceptions and Views on Cybersecurity*, 156.

56 S Mavuso, 'Department of Defence Says it Thwarted an Attempt to Hack its Network, All State Secrets are Safe', *IOL*, 3 September 2023. <https://www.iol.co.za/news/politics/department-of-defence-says-it-thwarted-an-attempt-to-hack-its-network-all-state-secrets-are-safe-26b9f67d-ff22-464e-84a7-b89514de7e3c#google_vignette> [Accessed on 2 September 2024].

57 Bester & Arendse, 'Measuring Cybersecurity Awareness', 20.

58 Bester, 'Cybersecurity Awareness', 288.

59 Department of Defence, *Policy, Process and Procedures on Information and Communications: Instruction DODI/CMI/00008/2001* (Pretoria, 2011).

60 D Singh, NP Mohanty, S Swagatika & S Kumar, 'Cyber-hygiene: The Key Concept for Cyber Security in Cyberspace', *Test Engineering and Management*, 9, 1 (2020), 8145–8152.

61 T Karayel, B Aktas & A Akbıyık, 'Human Factors in Remote Work: Examining Cyber Hygiene Practices', *Information & Computer Security*, 33, 1 (2025), 96–116.

[62] Ncubukezi & Mwansa, 'Best Practices', 718.

[63] C Bailie, 'The SANDF's Ingrained Culture of Secrecy and Non-communication is Counter-productive and Anti-democratic', *Daily Maverick*, 24 August 2021. <https://www.dailymaverick.co.za/article/2021-08-24-the-sandfs-ingrained-culture-of-secrecy-and-non-communication-is-counter-productive-and-anti-democratic/> [Accessed on 24 August 2021].

[64] Ncubukezi & Mwansa, 'Best Practices', 720.

[65] Bester, 'Cybersecurity Awareness', 284.

[66] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 200.

[67] S Akter, MR Uddin, S Sajib, WJT Lee, K Michael & MA Hossain, 'Reconceptualising Cybersecurity Awareness Capability in the Data-driven Digital Economy', *Annals of Operations Research*, (2022), 1–26.

[68] South African Government, 'Minister Thandi Modise: Defence and Military Veterans Dept Budget Vote 2023/24', 23 May 2023. <https://www.gov.za/news/speeches/minister-thandi-modise-defence-and-military-veterans-dept-budget-vote-202324-23-may> [Accessed on 25 September 2024].

[69] Bester & Arendse, 'Measuring Cybersecurity Awareness', 25.

[70] T Ramluckan, B van Niekerk & L Leenen, 'Cybersecurity and Information Warfare Research in South Africa: Challenges and Proposed Solutions', *Journal of Information Warfare*, 19, 1 (2017), 80–95.

[71] H Ames, 'Why is Personal Hygiene Important?', *Medical News Today*, 20 May 2020. <https://www.medicalnewstoday.com/articles/personal-hygiene> [Accessed on 25 September 2024].

[72] Ames, 'Why is Personal Hygiene Important?'

[73] Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 457.

[74] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 125.

[75] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 127.

[76] M Trevors & C Wallen, 'Cyber Hygiene: A Baseline Set of Practices', Carnegie Mellon University, 2017. <https://insights.sei.cmu.edu/documents/4146/2017_017_001_508771.pdf> [Accessed on 25 September 2024].

[77] L Philipsen, 'Performative Securitization: From Conditions of Success to Conditions of Possibility', *Journal of International Relations and Development*, 23 (2018), 139–163.

[78] Bester, 'Cybersecurity Awareness'.

[79] JW Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Thousand Oaks, CA: Sage, 2009).

[80] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 149.

[81] R Roomaney & B Coetzee, 'Introduction to and Application of Mixed Methods Research Designs', in S Kramer, S Laher, A Fynn & HH Jansen van Vuuren (eds.), *Online Readings in Research Methods* (Johannesburg: Psychological Society of South Africa, 2018), 1–24.

[82] ML Ngoma, M Keevy & P Rama, 'Cyber-security Awareness of South African State-mandated Public Sector Organisations', *Southern African Journal of Accountability and Auditing Research*, 23, 1 (2021), 1–17.

[83] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 110; Bester, 'Cybersecurity Awareness', 289; Bester & Arendse, 'Measuring Cybersecurity Awareness', 25

[84] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 60.

[85] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 89.

86 H Westland, S Vervoort, M Kars & T Jaarsma, 'Interviewing People on Sensitive Topics: Challenges and Strategies', *European Journal of Cardiovascular Nursing*, 24, 3 (2024), 488–493.

87 I Holloway & K Galvin, *Qualitative Research in Nursing and Healthcare* (West-Sussex: Wiley Blackwell, 2017).

88 S Elo, M Kääriäinen, O Kanste, T Pölkki, K Utriainen & H Kyngäs, 'Qualitative Content Analysis: A Focus on Trustworthiness', *Sage Open*, 4, 1 (2014), 1–10.

89 CE Hill, BJ Thompson & EN Williams, 'A Guide to Conducting Consensual Qualitative Research', *The Counselling Psychologist*, 25, 4, (1997), 517–572.

90 G Goldkuhl, 'The Generation of Qualitative Data in Information Systems Research: The Diversity of Empirical Research Methods', *Communications of the Association for Information Systems*, 44, (2019), 572–599.

91 Y Zhang & BM Wildemuth, 'Qualitative Analysis of Content', *Human Brain Mapping*, 30, 7 (2005), 2197–2206.

92 C Howell, D Maimon, C Muniz, E Kamar & T Berenblum, 'Engaging in Cyber Hygiene: The Role of Thoughtful Decision-making and Informational Interventions', *Frontiers in Psychology*, 15 (2024), art. 1372681.

93 Howell *et al*., 'Engaging in Cyber Hygiene'.

94 Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 466.

95 Bester, 'Cybersecurity Awareness', 274–275.

96 DE Marcial, JCL Palama, FP Bucog, BJL Seraspe & MA Launer, 'Digital Trust and Social Interactions Among Employees in the Workplace', in J Paliszkiewicz, K Chen & M Mendel (eds.), *Trust in Social and Business Relations* (New York, NY: Routledge, 2024), 97–108.

97 DA Williamson, 'User Trust in Social Platforms is Falling, According to Our New Study', *Emarketer*, 19 September 2022. <https://www.emarketer.com/content/user-trust-social-platforms-falling-according-our-new-study> [Accessed on 3 February 2025].

98 RMA El-Maksoud, 'Exploring the Role of Cybersecurity in Enhancing Digital Trust of Egyptian Travel Agencies', *Journal of Association of Arab Universities for Tourism and Hospitality*, 26, 1 (2024), 185–204.

99 T Pósa & J Grossklags, 'Work Experience as a Factor in Cyber-security Risk Awareness: A Survey Study with University Students', *Journal of Cybersecurity and Privacy*, 2, 3 (2022), 490–515.

100 Pósa & Grossklags, 'Work Experience as a Factor in Cyber-security Risk Awareness', 495.

101 Y Skorenkyy, R Kozak, N Zagorodna, O Kramar & I Baran, 'Use of Augmented Reality-enabled Prototyping of Cyber-physical Systems for Improving Cyber-security Education', *Journal of Physics: Conference Series*, 1840, 1 (2021), 1–9.

102 Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 464.

103 Bester, *Exploring the Perceptions and Views on Cybersecurity*, 90.

104 Ncubukezi & Mwansa, 'Best Practices', 721.

105 A Cardoso, MS Pereira, JC Sá, DJ Powell, S Faria & M Magalhães, 'Digital Culture, Knowledge, and Commitment to Digital Transformation and Its Impact on the Competitiveness of Portuguese Organizations', *Administrative Sciences*, 14, 1 (2023), 8.

106 Trevors & C Wallen, 'Cyber Hygiene'.

[107] B Tabrizi, E Lam, K Girard & V Irvin, 'Digital Transformation is not About Technology', *Harvard Business Review*, 13 March 2020. <https://hbr.org/2019/03/digital-transformation-is-not-about-technology> [Accessed on 23 September 2024].

[108] M Mvubu & MJ Naudé, 'Digital Transformation at Third-party Logistics Providers: Challenges and Best Practices', *Journal of Transport and Supply Chain Management*, 18 (2024), art. 1023.

[109] S Kocak & J Pawlowski, 'Digital Organizational Culture: A Qualitative Study on the Identification and Impact of the Characteristics of a Digital Culture in the Craft Sector', *SN Computer Science*, 4 (2023), 819.

[110] Department of Defence, 'Department of Defence Annual Report 2023/24', 2024. <https://nationalgovernment.co.za/department_annual/502/2024-department-of-defence-(dod)-annual-report.pdf> [Accessed on 12 February 2025].

[111] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 128.

[112] Mvubu & Naudé, 'Digital Transformation at Third-party Logistics Providers'.

[113] S Lesedi, 'Funding Mars SANDF Cyber Command', *Military Africa*, 13 January 2023. <https://www.military.africa/2023/01/funding-mars-sandf-cyber-command/> [Accessed on 30 November 2023].

[114] Department of Defence, *Policy, Process and Procedures.*

[115] Akter *et al*., 'Reconceptualising Cybersecurity Awareness', 3.

[116] T Balzacq (ed.), *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2011).

[117] Department of Defence, *Policy, Process and Procedures.*

[118] Pósa & Grossklags, 'Work Experience as a Factor in Cyber-security Risk Awareness', 494.

[119] N Humaidi & M, 'Shahrom Assessing Employees' Cybersecurity Attitude Based on Working and Cybersecurity Threat Experience', The African Journal of Information Systems, 15, 3, (2023), 207-221

[120] Bester, *Exploring the Perceptions and Views on Cybersecurity*, 129.