


Measuring Cybersecurity Awareness in a South African Military Sample

Kyle Bester¹ 

*Department of Psychology, University of South Africa,
Pretoria, South Africa*

Danille Elize Arendse² 

*The Centre for the Study of the Afterlife of Violence and the Reparative
Quest (AVReQ), Stellenbosch University,
Stellenbosch, South Africa*

Abstract

Cyberspace has been identified as a new domain of warfare; awareness of cyber threats is therefore crucial for members of the military because it allows for greater insight into potential cyber threats and attacks. Furthermore, developing cybersecurity awareness may assist in the detection of cyber threats in the workplace, and may further assist members of the military to be cognisant of their own vulnerability in cyberspace. In South Africa, cybersecurity is a topic of interest, and the South African National Defence Force has highlighted the need to enhance its cybersecurity capacity. The Cybersecurity Orientation Questionnaire was developed for members of the South African military with the fundamental objective of assessing their cybersecurity awareness as part of a larger study. The purpose of the study on which this article is based, was to explore the initial validation of the Questionnaire using a South African military sample. The study design was quantitative, and the reliability and factor structure of the Questionnaire were analysed by means of the Statistical Package for the Social Sciences. The sample size consisted of 182 military participants who were based at two military educational institutions. The Questionnaire showed acceptable reliability for research purposes ($r = .79$; $p = .000$) and the prominent three-factor structure was in line with the theorised factors envisioned during the development of the Questionnaire. Initial validation of the Questionnaire showed promising results for assessing cybersecurity awareness in the South African military sample. This study therefore emphasises the importance of developing instruments specifically for the South African military context.

Keywords: cybersecurity, South Africa, cyber awareness, reliability, factor structure, Cybersecurity Orientation Questionnaire

Introduction

Cyberspace is considered a new domain of conflict; therefore it is critical for members of the armed forces to be cognisant of cyber threats as it may enable greater insight into potential vulnerabilities within their own security behaviour, but also the risks in

the virtual reality sphere. While the emphasis is mostly on the technical features, in more recent times, the focus has shifted to the human element as a key component of ensuring cybersecurity.^{3,4} Individual cybersecurity awareness is crucial in understanding how people practise cybersecurity behaviour in organisations. It is therefore essential to highlight users' knowledge, behaviour, and perceptions, as humans are the weakest link in the security chain.⁵ For the purpose of this study, the researcher utilised the definition created by Bester as the foundation for terms of reference:

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.⁶

In South Africa, the seriousness of cyber threats and attacks has compelled the South African (SA) government to consider the development of legislation and frameworks in order to address these contemporary threats in cyberspace.⁷ The rise of cyber threats not only signifies significant security challenges at individual level, but may also pose security challenges to organisations, various sectors, and national security.⁸ The significant increase in cyber threats has led to the South African National Defence Force (SANDF) becoming increasingly resolute in enhancing its cyber resilience and digital capacity.⁹ The SANDF also recognises the importance of exploring cybersecurity from a multi-disciplinary perspective.¹⁰ This multi-disciplinary view is echoed in cybersecurity research focusing on technological advancement and on social as well as psychological development of awareness education on cybersecurity.^{11,12,13,14,15,16} Cyberspace and technology are expanding at a rapid pace. This includes extending their reach to growing numbers of individuals, governments, and other sectors.¹⁷

The rapid upsurge in malicious threats to mobile devices increases the possibility of digital exploitation of users.¹⁸ Mobile internet technology, such as mobile devices, has made it affordable for people to communicate and access information.¹⁹ Digital and technological development may have an influence on the economic and social situation in nation-states.²⁰ The development of technology has seen acceleration during and after the COVID-19 pandemic. The advancement of technologies has allowed nation-states to facilitate the innovation of new services. This enables strengthening of communications for modern economies.^{21,22} Economic and technological transformation, which advances with the use of the Internet, opens users up to being increasingly vulnerable to potential attacks.^{23,24} The roles played by cyberspace, cybersecurity, and cybersecurity awareness are key to how users approach the practice of digital security and information sharing. As noted earlier, due to the rapid surge in malicious threats and evolving technological advancements, it has become increasingly important to ensure that users are equipped with the necessary skills to mitigate cyber threats.²⁵

The human element remains the cornerstone of all matters of a cyber nature as humans need to move continuously between the digital space and the physical space.²⁶ In this kind of security, the human element is susceptible to committing security-related errors and is left vulnerable to potential threats.²⁷ It should be noted that many users possibly still lack the required awareness of the nature and variety of threats in this domain. According to Zwilling *et al.*, users of cyberspace may fall victim not only to cyber threats but also to knowledge gaps, which expose them to cyber-related hazards. Moreover, these users often fail to acquire the minimum amount of knowledge necessary to protect their computing devices.²⁸ Zwilling *et al.* emphasise that in more severe cases, individuals suffer from a total lack of awareness of cyber hazards.²⁹ Not possessing sufficient awareness of cyberspace and its potential threats may put users at risk.³⁰

So far, scholarly efforts have been directed largely towards the exploration of students' perceptions of cybersecurity awareness and practices in various contexts outside the defence environment.^{31,32} Research concerning cybersecurity and online behaviour has gained some momentum in recent years, as there is an increasing need to understand the notion that the use or overuse of cyberspace may alter human behaviour.³³ The topic of cybersecurity awareness has received significant interest in the race to obtain an understanding of vulnerabilities, as pointed out by Bester.³⁴ The surge in research relating to cybersecurity awareness points to the apparent lack of education in this area among users, which is vital when noting the high level of risk associated with cyber threats.³⁵ Cybersecurity awareness has received some attention in the SA context where the following aspects have been addressed: perceptions of cybersecurity,³⁶ information warfare,³⁷ the review and development of cybersecurity policy frameworks,^{38,39} and exploring the cyber threat landscape.⁴⁰

The Role of Cyberspace

Cyberspace is described as a physical and non-physical territory, which consists of 'computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users'.⁴¹ Furthermore, cyberspace introduces new challenges to governments, and therefore demands enhanced capacity of cybersecurity and the need to address national security threats in cyberspace.⁴² Cyberspace is an invisible domain that allows users to be anonymous.⁴³ The consequences of this invisibility present a security challenge, where a hybrid (physical and digital) form of warfare may emerge as either offensive or defensive. This domain may therefore be perceived as both a potential challenge and a benefit for governments.⁴⁴ Cyberspace is considered a borderless platform that enables more sophisticated threats, such as cybercrime, cyber terrorism, cyber war, and cyber espionage.⁴⁵ On the other hand, the Internet is described as a global network of computers that enables worldwide communication and information exchange.⁴⁶

The Impact of Cyber Threats on Users and Society

As technology advances and becomes more affordable, so too does the complexity of cyber threats and attacks.⁴⁷ The importance of cybersecurity awareness becomes integral with the human element being placed in a vulnerable position.⁴⁸ Furthermore, the low levels

of cybersecurity awareness are believed to contribute to the cyber threats that African nation-states are encountering.⁴⁹ Low levels of cybersecurity awareness may also have an influence on securing cyberspace.⁵⁰ What makes matters worse is that Africa is viewed as an attractive haven for cyber criminals who operate illegally on this continent.⁵¹ Many African nation-states recognise the importance of improving their approach to developing their respective cybersecurity capacity and strategies.⁵² Some challenges related to the slow adoption of technology and the slow-paced development of cybersecurity strategies and frameworks however still prevail.⁵³ In addition, the importance of cybersecurity is underemphasised even though cyber threats have the ability to cause economic and political damage.⁵⁴

With cyberspace extending its reach into multiple sectors, the vulnerability of individual users and organisations increases as well. Cyber threats are pervasive, and are threatening to cause havoc.⁵⁵ Obtaining the necessary cybersecurity knowledge and awareness is vital when navigating the Internet while maintaining information security at the same time. Bester suggests that cybersecurity awareness is a flexible and continuous process during which the individual is cognisant of threats and his or her own vulnerability. Moreover, Bester argues that the application of knowledge, precautionary behaviour, and risk perceptions are elements required by the human element to counteract cyber threats.⁵⁶ Additionally, being aware of the limitations of certain security software may also assist an individual in being cautious when navigating cyberspace.^{57,58} If users are not properly trained in or do not have sufficient cybersecurity awareness, it may leave them vulnerable, and their technological devices might remain unsecured.⁵⁹ From a wider perspective, users who may not possess the necessary cybersecurity awareness knowledge and who have unsecured technological devices might be especially vulnerable to cyber threats and possible attacks.

The mobile Internet penetration rate increased from 51.51% in 2019 to 82.2% in 2023.⁶⁰ This growth in the mobile Internet penetration rate shows that there is a dramatic increase in the information and communications technology (ICT) capability, mainly because mobile devices have become cheaper and more accessible.⁶¹ With mobile devices becoming more affordable and cyber threats being on the rise, the human element might be vulnerable. This vulnerability might result in debilitating consequences for users. Shifting the discussion on cyber threats to the SA context, Ndlovu reports that in 2021, 220 million email threats were detected in South Africa, and that Post Bank was a victim of cybercrime where 100 000 fraudulent emails imitated the entity, causing it to suffer a loss of R18 million.⁶² When considering security incidents, based on severity in the SA context, the following issues were highlighted in the State of Cybersecurity in South Africa Report during the period 2022 to 2023: business emails compromised (37%), ransomware (18%), disinformation campaigns (17%), insider threats (15%), cloud breaches (12%), and supply chain attacks (12%).⁶³ Moreover, during the COVID-19 pandemic in 2020, there was increased dependency on ICT.⁶⁴ Due to the increased dependency of users on ICT, their risk to cyber threats becomes greater. This potential risk faced by users of ICT is elevated when they are unaware of the potential threats they face, such as phishing, pretexting, and baiting, which are all forms of social engineering attacks that rely on deception.⁶⁵

Along with the significant increase in the use of accessible technology and cyberspace, it has been observed that individuals from various sectors in society (government, industrial, and social) have become dependent on mobile devices and the Internet.⁶⁶ The increase in the use of digital devices and the processing of personal data have resulted in an increase in cyberattacks in South Africa.⁶⁷ Regrettably, several SA government departments, state-owned entities, and citizens have recently fallen prey to cyberattacks.⁶⁸ These cyberattacks might have significant consequences for South African national security data and citizens' personal data. Furthermore, the SANDF was also a victim of an alleged cyberattack when its network system was breached.⁶⁹ Along with an increase in the use of digital technology, the armed forces in most countries are increasingly relying on emerging technologies and cyberspace to enhance their reach in relation to national security issues. Consequently, cybersecurity and the use of technology are important force multipliers for advancing defence and economic factors in a nation-state.⁷⁰ Furthermore, if the cyberspace domain is effectively integrated and maintained as an operational element, it can be considered a force multiplier.⁷¹ This additional component may help the military to gain an advantage in cyberspace operations.⁷²

The Human Element in Cybersecurity

The human element is a key component in cyberspace as it continuously alternates between the digital space and the physical space. An individual connects to cyberspace through the means provided by physical infrastructure; one cannot function without the other. The human element in the cybersecurity chain is susceptible to committing security errors and therefore becomes vulnerable to potential data breaches, malware, and cyberattacks.⁷³ The increase in the use of Internet-connected devices is linked to advancements in the ICT sector.^{74,75} It is therefore important to acknowledge that many users still lack the required awareness of the nature and variety of cyber threats. According to Zwilling *et al.*, users often fall victim to both cyber threats and knowledge gaps that expose them to cyber hazards. In fact, these users often fail to ensure that they obtain the minimum required knowledge to protect their computing devices.⁷⁶ Zwilling *et al.* confirm that, in more severe cases, individuals suffer from a total lack of cyber hazard awareness.⁷⁷ If users do not have sufficient awareness of cyberspace and its potential threats, they and their respective countries may be at risk. Moreover, when considering the response to cybersecurity incidents, the human element has an important role in identifying security management tools for responding to threats. In addition, the human element, regardless of the technology utilised, should still possess some awareness of potential cyber threats and the vulnerabilities from a technical and human standpoint.⁷⁸

In terms of positioning the human element in an organisational context, Akter *et al.* argue that cyber threats and attacks are becoming increasingly prominent in society and have targeted employees in organisational contexts. Akter *et al.* suggest that employees with limited cybersecurity awareness and knowledge may be especially susceptible to threats; practical skills and knowledge are therefore recommended for enhanced capacity.⁷⁹ In addition, flexible working conditions have been identified as a risk factor due to employees not being able to interact physically with their secured network system; their own devices might thus be susceptible to phishing. Moreover, the internal operational conditions of

an organisation may also link to the confidence in how cybersecurity is practised, which alludes to how well guidelines and secure network systems are implemented. As previously noted, the human element is the weakest link in the security chain; individual cybersecurity awareness should thus be emphasised by gauging users' knowledge, behaviour, and perceptions.⁸⁰ The practical application of knowledge transfer and simulations are components in addressing awareness.⁸¹ At individual level, the focus on cybersecurity awareness is essential for understanding how individuals practise cybersecurity behaviour in organisations.⁸² It should be noted that employees of large organisations develop higher levels of cybersecurity awareness due to the greater financial resources available to put security systems in place, and the possibility of having policy frameworks that are strictly enforced.⁸³ When linking cybersecurity awareness to an organisation that is as large as the SANDF, it is vital for security systems and policies to be in place as the military is responsible for guaranteeing national security. Emphasising cybersecurity awareness in organisations therefore remains essential when aiming to reduce cyber threats.⁸⁴ Moreover, educating and training members in an organisation may also reduce the likelihood that they will fall victim to threats, and increase the chances of a threat being reported.⁸⁵

Expanding on the latter, exploring cybersecurity awareness among people in general may have an understanding of how awareness, knowledge, and cybersecurity behaviour might be perceived differently as an outcome. Bester proposes that, to enhance cybersecurity awareness among individuals, attention should be paid to four main facets, namely malware and mitigating factors; physical security, which implies that users need to secure their devices; navigating cyberspace securely; and social aspects regarding how to communicate in cyberspace.⁸⁶

Van't Wout and Murire *et al.* suggest that organisations are able to provide training to their employees at low cost to equip them with the necessary skills to fulfil existing expectations.^{87,88} Lehto and Raju *et al.* indicate that training material and education on cybersecurity awareness might be valueless if there is not appropriate engagement in and understanding of cybersecurity risks and the effective application of security behaviour.^{89,90} Abawajy suggests that cybersecurity awareness may not necessarily be enough to ensure that users are completely secure, as it may not be sufficient to have appropriate knowledge of cybersecurity protection to decrease cyber threats.⁹¹ Training in cybersecurity awareness knowledge relating to security tools is required if individuals are to mitigate risks effectively, instead of only acquiring theoretical knowledge.⁹² An alternative training method, which focuses on enhancing users' practical understanding of cybersecurity, is the phishing simulator. Phishing simulation offers members of an organisation the opportunity to advance their knowledge and skills on cybersecurity by routinely exposing them to emails that may contain suspicious URLs and spelling mistakes.^{93,94,95} By incorporating phishing simulation into cybersecurity awareness training, the individual can acquire knowledge and practical skills that may enable him or her to distinguish effectively between legitimate emails and phishing emails. When adding these approaches to the training arsenal of users in organisations, it should be emphasised that both technical and social approaches are necessary for approaching cybersecurity training holistically.⁹⁶

Theoretical Background of the Cybersecurity Orientation Questionnaire (COQ)

The Internet plays a significant role in how people go about performing activities in both the digital and physical domains. The COQ was therefore developed for members of the SA military with the fundamental objective of establishing their cybersecurity awareness, and to take into consideration the hybrid nature of cyberspace, as the consequences of cyber threats and potential attacks may be significant in the physical domain in which individuals function as they carry out their daily activities. The COQ was designed as a tool to explore how members of the military respond to cybersecurity threats, as well as to consider the practices and behaviour adopted for securing their information. The COQ comprises four key dimensions that emphasise various aspects relating to cybersecurity awareness, namely:

- Information-Sharing Culture;
- Security Orientation;
- View on Cybersecurity; and
- Cybersecurity Behaviour.

These dimensions were informed by literature that focuses on cybersecurity awareness in organisations and the behavioural practices associated with information security.

It is important to note that the current article is based on a larger research study by Bester.⁹⁷ The article focuses on one aspect of the larger study, namely the development of the COQ, and emphasises the exploration of the factor structure and reliability of the COQ. The four dimensions were derived from findings of the qualitative phase in the larger study. The findings of Phase 1 of the larger study reflected qualitative themes, which assisted in the development of the COQ dimensions in Phase 2 of the larger study.

The first dimension focuses on the **information-sharing culture** in the organisation. This dimension of the COQ focuses on the available resources and the culture of sharing practices in an organisational setting. Information-sharing culture also deals with the exchange of information between individuals to facilitate decision-making.⁹⁸ According to Zwilling *et al.*, awareness plays a crucial role in the practice of information security.⁹⁹ The questions developed for this specific dimension of the COQ therefore emphasise users' awareness relating to security tools and cybersecurity threats. Awareness can only develop if there is understanding in relation to what is being learned.¹⁰⁰ The dimension of information sharing culture therefore also focuses on the dissemination of best practices and guidelines to members of the organisation.

The second dimension refers to **security orientation** among military officers which include the candidate officers. Security orientation denotes how members of the military use the precautionary mechanisms that dictate how they secure themselves and their organisational data based on the knowledge they have obtained from previous experience with security.

The third dimension refers to the **view on cybersecurity**. This dimension highlights how military members view the efforts of the organisation to address cybersecurity and the measures employed to mitigate cyber threats. This dimension was drawn from the research conducted by Al-Mohannadi *et al.*, who argue that awareness, monitoring, and prevention are essential for understanding the possible challenge that cyber threats may pose to employees and the organisation.¹⁰¹ Owing to this, insufficient training in the application of risk assessment relating to cyber threats may result in data loss. It is therefore important that users assess and continuously monitor their own vulnerability, as well as that of the information systems they use.¹⁰²

The fourth dimension of the COQ focuses on **cybersecurity behaviour**. This dimension relate to the practical activities of addressing security behaviour in the workplace.¹⁰³ Duman argues that, when users have been exposed to cybersecurity training, it may advance their knowledge and behaviour in terms of security risks; thus, increasing the user's cybersecurity awareness and reducing cyber risks.¹⁰⁴ Furthermore, the short questions in the COQ were used as the basis for exploring the deeper meanings of the scale items. Nine questions were included in the COQ, each asking the participant to provide a short description of the way they view information sharing, their view of their online behaviour, and the way cybersecurity is managed in their organisation.

The findings of the larger study allowed the researcher to establish a foundation for determining which areas in cybersecurity awareness need to be focused on in the military context. The main findings of the larger study highlighted three main themes. The first theme was **knowledge production and training**, which concentrated on cybersecurity awareness. The second theme was **challenges relating to trust** between technology and members of the military. The final theme focused on the way members of the military related to **security in the physical world**, and applied the measures attached to security using the Internet. Apart from using these main themes as the basis for the construction of the questionnaire, it is worth noting that the findings from the literature, which related to the security behaviour of students,¹⁰⁵ contributed to the development of some of the items in the questionnaire.

The study assumed that cyber threats could come in various forms as they might relate to spam and phishing,¹⁰⁶ ransomware,¹⁰⁷ spear phishing,¹⁰⁸ social engineering,¹⁰⁹ threats, and man-in-the-middle attacks.¹¹⁰ Dimension 2 of the questionnaire, "security orientation", utilised and adapted some of the focus areas identified by Du Toit *et al.*, which relate to online behaviour in schools.¹¹¹ Although the context and sample population in the current study differed from the educational setting in which Du Toit *et al.* conducted their study, the premise was the promotion of security behaviour and perceptions in cyberspace. Dimensions 1, 3, and 4 of the COQ were based on the qualitative themes that emerged from the findings derived from the larger study.

Research Aims and Objectives

The COQ was specifically developed to explore cybersecurity awareness among members of the SANDF. Recent cybersecurity research in the SA context focused especially on elements related to awareness, security management, and training.¹¹² Bester asserts that

limited research exists concerning the development of cybersecurity awareness screening tools in the SANDF.¹¹³ Bester however notes that, while there might be limited research on cybersecurity awareness in the SANDF, there are screening tools outside the SANDF context.¹¹⁴ In the context of the SANDF, limited research has so far focused on developing a cybersecurity awareness-screening tool. For this reason, it was necessary to explore the dimensions of the COQ in the SANDF context, and to emphasise the importance of the human element in maintaining cybersecurity. Consequently, the purpose of the study reported on here was to explore the preliminary validity and reliability of the COQ in South Africa using an SA military sample. This is the first time that research has been conducted on the applicability of the COQ in terms of a military sample, and the researchers believe this will promote further research on refining the measuring of cybersecurity awareness within the military context.

The research question of this study was whether the COQ was applicable in terms of the SA military context. The two objectives of the study were the following:

To explore the factor structure of the COQ for an SA military sample; and

To explore the reliability of the COQ for an SA military sample.

Method

The study used a quantitative cross-sectional design. The quantitative data analysis method chosen for this study was exploratory factor analysis (EFA) and reliability. The factor structure and reliability of the COQ were analysed by means of the Statistical Package for the Social Sciences (SPSS). These data analysis methods were essential for establishing the initial validation of the COQ, as no previous research has been conducted in terms of the questionnaire.^{115,116,117}

Participants

The cluster sampling technique was used in the study, as the research required two samples, which were obtained from two senior military educational institutions in South Africa. *The* military sample for the COQ comprised 182 military participants. Table 1 indicates the participant demographics. The majority of the military sample was aged between 20 and 54 years, with an average age of 35. This South African military sample included candidate officers (COs) based at the Military Academy. Most of the participants in the study were 25 (6%) or 27 (6%) years old. Based on the distribution of ages as reflected in Table 2, most of the participants were young enough to have been exposed to technology in their careers compared to the older participants. In addition, many of the participants were males, and in the SA Army.

Table 1: Participant demographics for the COQ military sample

Gender	Percentage	Age distribution	Arm of service	Percentage
Male	62	20–54 years	SA Army	59
Female	34		SA Navy	17
Missing	4		SA Air Force	15
			South African Military Health Service	6

Table 2: Distribution of ages for COQ military sample

Age	Frequency	Percentage
20	2	1.1
21	5	2.7
22	7	3.8
23	6	3.3
24	8	4.4
25	10	5.5
26	6	3.3
27	10	5.5
28	2	1.1
29	5	2.7
30	8	4.4
31	5	2.7
32	6	3.3
33	6	3.3
34	6	3.3
35	7	3.8
36	5	2.7
38	6	3.3
39	2	1.1
40	1	.5

Age	Frequency	Percentage
41	4	2.2
42	3	1.6
43	5	2.7
44	5	2.7
45	7	3.8
46	5	2.7
47	4	2.2
48	7	3.8
49	3	1.6
50	5	2.7
51	1	.5
52	5	2.7
53	1	.5
54	3	1.6
Total	171	94.0

Instrument

The COQ is a measurement tool that was designed to assess the cybersecurity awareness of military members in an SA context. The COQ has four dimensions, which comprise multiple-choice questions and short questions after each dimension. The short questions were inserted in the questionnaire to ascertain a deeper perspective from participants. The multiple-choice questions in the COQ have four answer options, namely “strongly disagree”, “disagree”, “agree”, and “strongly agree”. Although the COQ is still in development, it was administered to the South African military members to assess its potential as a measurement tool. The COQ was thus only used for research purposes. The initial version (version 1.1) was used in the larger study as a tool to ensure triangulation of the qualitative themes that emerged from Phase 1 of the larger study.

The COQ does not focus on factors such as age or rank in the military. Instead, the questions were constructed in such a way that all members of a military organisation would be able to evaluate their level of cybersecurity awareness. The purpose of the COQ is to encourage military members to engage actively in advancing their knowledge of cybersecurity awareness. The COQ highlights elements related to their security behaviour and their views on cybersecurity threats in the organisation. The COQ has been designed as a self-assessment tool for military members to obtain information about their behaviour and perspectives, which will ultimately promote interest in cybersecurity awareness and facilitating learning.

The COQ version 1.1 has 44 multiple-choice items, and takes 25 to 35 minutes to complete. When the COQ was administered to the participants, no time limit was imposed. Table 3 shows an example of the structure and question style of the items used for the COQ.

Table 3: Example of questions in the COQ

Statements	Strongly disagree	Disagree	Agree	Strongly agree
I feel that it is safe to share information on social media.				
I feel that using a storage device (USB) is the best way to store information.				
I change my passwords on my laptops, cell phone, and computer on a regular basis.				

Data-Collection Procedure

Of the 182 officers (including candidate officers), 80 officers were located at the South African National War College (Pretoria), and 102 (which included the candidate officers) were located at the South African Military Academy (Saldanha). All the respondents were military officers (and candidate officers) who had been exposed to cyberspace in their daily functioning in their organisations. Before the administration of the COQ commenced, the participants completed an informed consent document. The respondents were informed of the purpose and nature of the COQ, and were asked whether they would agree to take part in the research voluntarily. Once the administration of the COQ had been completed, the respondents were provided with the researcher’s contact details if they had additional questions about cybersecurity in organisational settings.

Ethical Considerations

Applying and maintaining ethical considerations in the study were considered imperative. The lead author ensured that the anonymity and confidentiality of the participants were maintained throughout the study. All personal information regarding the respondents was stored safely in an area where strictly access-controlled measures were in place. This significantly increased securing the confidential data. The safeguarding of data in this study was considered important, as it not only reflected military knowledge, but also confidential information of military officers. The participants in the study were informed of their right to withdraw at any point during the study without penalty, and emphasis was placed on their participation being voluntary. It should be highlighted that the data that were collected for this study may only be accessed by the lead author of this study. Access to the data was therefore limited strictly to registered professionals. Ethical clearance for

this study was obtained from Stellenbosch University, South Africa. The data that support the findings of this study are available on request from the lead author of the article. The data are not publicly available due to the confidentiality attached to it.

Data Analysis

The factors included in the COQ were analysed by conducting EFA and using principal axis factoring in SPSS. Missing data were handled through the deletion of pairs in SPSS. As the factors in the COQ were theorised to be related, the Promax oblique rotation method was followed.^{118,119} The suitability of the COQ data for EFA was evaluated with the following indices: correlation matrixes, Kaiser–Meyer–Olkin (KMO), and Bartlett’s test of sphericity.¹²⁰ The KMO value was .725, which indicated that the sample was adequate for factor analysis. Bartlett’s test for sphericity was significant ($p = .000$), which indicated that the data were suitable for factor analysis.^{121,122,123} The suitability of the data was important since the sample size was quite small.

Cronbach’s alpha was used as the reliability coefficient, and was calculated in SPSS.^{124,125} This measure was selected to assess the internal consistency of the COQ and to provide information about the intercorrelation between the items in the COQ.^{126,127,128,129} Cronbach’s alpha applies a scale that ranges from 0 to 1, with values closer to 1 indicating that the COQ was reliable and that the items in the COQ were consistently measuring the intended construct.^{130,131,132}

Results

The next section of the paper indicates the results of the Exploratory Factor Analysis (EFA) performed on the COQ. It is important to note that the factors derived from the EFA analysis are not the same as the four dimensions stemming from the creation of the COQ. Although some of the factors may share similar labels to the dimensions of the COQ, they are different due to the items loaded within the factors. To avoid any confusion, factors refer to the EFA generated COQ scales and dimensions refers to the initial theorised scales that led to the creation of the COQ.

Exploratory Factor Analysis (EFA)

The choice regarding the assessment of factors for the EFA was done by consulting the scree plot (indicated in Figure 1), which pointed towards three factors. Consequently, the EFA was rerun, and a three-factor solution was selected. The total variance explained by these three factors was 32%.

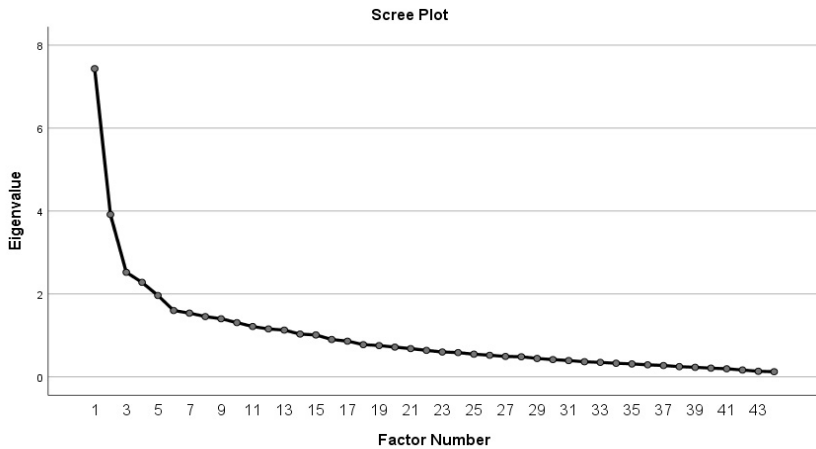


Figure 1: Scree plot for the COQ

The pattern matrix was evaluated to assess how the different items loaded on the factors of the COQ. Based on the loadings of the items, the factors were labelled as follows in Table 4: Cybersecurity Awareness factor, Security Orientation factor, and Information-Sharing factor. These three factors accounted for 38 items in the COQ. The Cybersecurity awareness factor had a loading of the most items (16 items), while the Information-Sharing factor had a loading of the least items (eight items). This similarly mimics the scree plot of the factors.

Table 4: Pattern matrix of the COQ

Questions	Cybersecurity Awareness factor	Security Orientation factor	Information-Sharing factor
Q50	0.873	-0.104	
Q51	0.853		
Q49	0.797		
Q34	0.675		
Q32	0.618		
Q48	0.600		
Q35	0.565		
Q44	0.549		
Q36	0.451		
Q10	0.441	0.113	-0.172
Q39	0.441	0.202	

Questions	Cybersecurity Awareness factor	Security Orientation factor	Information-Sharing factor
Q46	0.409		-0.145
Q47	0.401		
Q33	0.395		
Q43	-0.312		0.166
Q19	0.303	0.204	-0.101
Q20	0.276		
Q2	0.202	0.177	-0.178
Q41		0.622	
Q24	0.134	0.585	
Q40		0.572	0.377
Q23		0.559	
Q37		0.515	0.456
Q22	-0.102	0.503	
Q13		0.489	
Q31		0.488	
Q30	-0.118	0.471	
Q42		0.442	-0.153
Q18	0.142	0.410	-0.278
Q5		0.357	
Q25		0.343	
Q11		0.325	0.166
Q45		0.270	-0.142
Q1			0.559
Q6		-0.147	0.489
Q8	0.175	-0.201	0.464
Q9		-0.258	0.435
Q29		0.149	0.403
Q38		0.295	0.393
Q12	0.256		-0.324
Q4			0.305
Q3		0.107	0.272
Q7	-0.111	-0.223	0.247
Q21			0.187

*Promax rotation converged in four iterations.

Two items (Q37 and Q40) were cross-loaded on the Security Orientation and Information-Sharing factors. These items however loaded slightly more on the Security Orientation factor. The items nevertheless measured both constructs. There were only two negative loadings – one (Q43) on the Cybersecurity Awareness factor and one (Q12) on the Information-Sharing factor. The six remaining items of the COQ that did not load on any of the three factors had below acceptable loadings.

Table 5 shows that the three factors are correlated with one another. There was a moderate yet negative relationship between the Cybersecurity Awareness factor and the Information-Sharing factor (-.366). This indicates that the participants' responses to these factors were opposites; thus, when participants agreed with items relating to the Cybersecurity Awareness factor, they disagreed with the items of the Information-Sharing factor. The Cybersecurity Awareness and Security Orientation factors had a small relationship, which indicates some similarity between these factors. The Security Orientation and Information-Sharing factors appear to have a negligible relationship, which indicates that these factors are not related.

Table 5: Factor correlation matrix for factors of the COQ

Factors	Security Orientation factor	Information-Sharing factor
Cybersecurity factor	.281	-.366
Security Orientation factor	1	-.095

Reliability

Table 6 indicates that the full-scale reliability of the COQ was .79, which is acceptable for research purposes. If the COQ is to be used with greater confidence, the reliability would need to be improved. The revised reliability of the COQ was .867, which is very good reliability, and indicates that there is good internal consistency in the COQ. The revised reliability, however, required the removal of 12 items, thereby settling on a scale of 32 items.

Table 6: Reliability statistics for the COQ

Instrument	Cronbach's alpha	Total items
Full-scale COQ	.787	44
Revised COQ	.867	32

Table 7 indicates the 12 items that had been removed along with their associated Cronbach's alpha values. Based on the removed items, most of the items were from the theorised and observed Information-Sharing factor.

Table 7: Items removed from the COQ

Removed items	Cronbach's alpha
Q7	.799
Q6	.808
Q9	.818
Q43	.828
Q21	.834
Q1	.841
Q3	.847
Q8	.854
Q4	.859
Q29	.864
Q38	.866
Q45	.867

Four dimensions were theorised as part of the COQ in the composition of the questionnaire. Since these four dimensions were theoretically envisioned as factors in the COQ, their reliability was evaluated. As shown in Table 8, the Cybersecurity Behaviour factor had the least number of items but was the only dimension acceptable for research purposes. The Information-Sharing Culture dimension had the lowest reliability, with the second most items in the COQ. When assessing the performance of the theorised dimensions in the COQ, it became clear that the arrangement of these dimensions did not produce consistency among these groupings of items.

Table 8: Reliability statistics for the four dimensions of the COQ

Dimensions	Cronbach's alpha	Total items
Information-Sharing Culture	.417	13
Security Orientation	.578	8
View on Cybersecurity	.647	16
Cybersecurity Behaviour	.765	7

Since the EFA identified three factors, the reliability of these factors was important for further development and refinement of the COQ. As Table 9 shows, the reliability of the three different factors was indicated. The Cybersecurity Awareness (.847) and Security Orientation (.807) factors presented with very good reliability, which indicates that the items for these factors consistently measured the construct. The Information-Sharing factor presented with very low reliability, which similarly mimicked the low reliability of the theorised Information-Sharing factor. This could possibly be an indication that the items in the Information-Sharing factor did not consistently measure this construct.

Table 9: Reliability statistics for the three factors of the COQ

Factors	Cronbach's alpha	Total items
Cybersecurity Awareness factor	.847	16
Security Orientation factor	.807	14
Information-Sharing factor	.495	8

Discussion

The EFA indicated three factors that accounted for most of the items in the COQ. There were two strong factors, namely Cybersecurity Awareness and Security Orientation. Based on the strength of the factor loadings, it should be highlighted that, theoretically, these two linked very strongly with each other as they fundamentally dealt with cybersecurity awareness threats and knowledge pertaining to cyberspace, and the precautionary measures to mitigate cyber threats.¹³³ The Security Orientation factor referred to the information security practices that users applied in cyberspace, whereas the Cybersecurity Awareness factor highlighted the overall knowledge that users might possess concerning cyber threats in the workplace. The literature shows that there is a consistent link between online behaviour and user knowledge of cyber threats.¹³⁴ Furthermore, while there might be emphasis on knowledge and online security behaviour, it is recommended that routine awareness training and the implementation of skills are necessary to be proficient in practising cybersecurity.¹³⁵ Kovačević et al. argue that individuals who have prior experience of threats will adhere to stronger security practices.¹³⁶ It may thus also be suggested that in this study, the link between the Cybersecurity Awareness and Security Orientation factors, both having higher factor loadings, was apparent. The aspect of knowledge and that of the presence of cybersecurity awareness are required to advance a user's approach to mitigate cyber threats; however, these two aspects are insufficient to change online security behaviour.¹³⁷ This view is strengthened by the idea that, even when users are aware of certain risks in cyberspace, it does not deter them from engaging in risky online activities.¹³⁸ Adding to this, users navigating cyberspace may also interpret risk-related information differently, which is due to the perceived emotional state of the individual. This implies that, when individuals have a positive attitude when they share information online, they may be less likely to be aware of the security risks and thus less likely to adhere to security-ensuring behaviour. Zwilling et al. suggest that a risk factor in establishing information security is the level of cybersecurity awareness displayed by an individual.¹³⁹ Behaviour that is attributed to a low level of awareness includes generally not paying attention to security practices, such as accessing an open-source Wi-Fi service when using a personal Internet-enabled device. On the other hand, a high level of awareness is associated with knowledge of cyber threats and the required skills to mitigate these threats effectively.¹⁴⁰

The Information-Sharing factor had the smallest loadings and negative and negligible relationships with both the Cybersecurity Awareness and Security Orientation factors. In addition, two items cross-loaded on the Security Orientation and Information-Sharing

factors. On inspection of these two items (Q37 and Q40), the content suggested that there might be an overlap between these two constructs. It must however be highlighted that cybersecurity behavioural practices and the knowledge of cyber threats might go together. This view may lend itself to the stance that the acquisition of knowledge and awareness regarding cybersecurity is an important component for users to safeguard themselves against cyber threats.¹⁴¹ It is however worth noting that this alone is insufficient to elicit a change in security behaviour. Moreover, it is essential to note that the effectiveness of these strategies is enhanced when combined with other influencing factors. The Information-Sharing factor emphasises how military members engage in the electronic exchange of information in their organisations. Moreover, the Information-Sharing factor focuses on military members' views of how well security information is promoted across the organisation.¹⁴² In addition, the efficacy of information sharing was argued to have a direct link with online security behaviour and vice versa. Furthermore, the reason for the low score of the Information-Sharing factor could be the lack of awareness relating to cybersecurity practices. Contextually, a shift in attention to information-sharing practices is essential in government institutions, such as military organisations, which are notorious for having top-down structures. When connecting to the individual in the organisational setting, it is necessary to note that the procedures that govern the sharing of information may provide a member of an organisation with the necessary peace of mind when engaging in virtual information sharing.¹⁴³ It is worth noting that, when there is a high level of information sharing between members of an organisation, operations and participation may increase. The level of privacy attached to the information may however also be a reason for why information does not reach all levels of an organisation.¹⁴⁴ In terms of the findings related to the Information-Sharing factor, this appears to be a cause for concern as it may not contribute to the overall construct of the COQ.¹⁴⁵ In addition, understanding the questions that are related to Information-Sharing Culture as a dimension could possibly have been a challenge for the participants. Furthermore, it is important to note that the scale items were informed by the qualitative themes extracted from Phase 1 of the larger study. It is also important to note that a major portion of the development of the questionnaire relied on literature that fell outside the African domain.

The removal of 12 items to obtain improved reliability for the COQ provided insight into the problematic items that had lowered the internal consistency of the COQ. When evaluating the items that lowered the reliability, it became apparent that they belonged to the Information-Sharing factor. All the questions that lowered the reliability focused on the security practice of sharing information in a public or secure space. This may also be linked with the knowledge of how information should be shared in settings where strict adherence to security measures applies.¹⁴⁶ Furthermore, the practice of sharing information in the military context depends on the available technology systems. This availability may however be affected to a certain degree by contextual challenges, such as budgetary constraints.¹⁴⁷ In terms of the impact that financial constraints may have on the cyber defence capacity of the SANDF, one needs to focus on four strategic objectives, namely developing capabilities, creating awareness initiatives regarding cybersecurity, conducting research and training, and coordinating and participating with both national and international stakeholders.¹⁴⁸ The SANDF may find that budgetary constraints have

an influence on the execution of these strategic goals, especially on the objective that focuses on training, as this connects with the development of cybersecurity awareness and knowledge.

The Information-Sharing factor, however, showed poor reliability, which was consistent with the theorised scale of the COQ. The Information-Sharing Culture dimension of the COQ therefore appears to be problematic, and might have hindered the measurement of the intended construct. The act of sharing information can be defined as the transfer of information between a sender and a receiver.¹⁴⁹ In the context of cybersecurity, information sharing plays a crucial role in establishing trust in an organisation. Trust and information sharing are indeed closely connected.¹⁵⁰ Information sharing is therefore a fundamental element in promoting a secure environment for organisations and their employees alike. Information-sharing practices also refer to best practices, policies, and guidelines relating to cybersecurity in the SANDF context. While the sharing of pertinent information is central to organisational settings, it may be a discouraging aspect of their jobs for members of the military to share information electronically. The hesitancy of information-sharing practices executed electronically in the SANDF context may explain why the dissemination of information did not load very high in the COQ. Mohammed *et al.* argue that attitudes towards technology could potentially be an indicator of how information sharing is conducted by individuals in organisations.¹⁵¹ Furthermore, the military is a unique context in which certain pieces of information can be identified as sensitive. Sharing information on digital platforms can therefore be considered a risk, and the respondents might be less likely to share information online.¹⁵² This was evident from the questions removed from the COQ, as indicated in Table 7, namely Questions 1, 3, 4, 6, 7, 8, and 9.

When the theorised dimensions of the COQ were evaluated, the Cybersecurity Behaviour scale was the only scale that showed acceptable reliability. The factors indicated by the EFA, however, presented with good internal consistency, particularly the Cybersecurity Awareness and Security Orientation factors. It is therefore no surprise that these factors had good internal consistency, as the literature indicates that the security measures and practical steps utilised by users have a strong link with awareness of cyber threats and attacks, as well as knowledge of cyberspace.¹⁵³ Precautionary online security mechanisms and education are highly significant in the context of the armed forces, and it is essential for members of the military to be aware of cyber threats and possible risks. The Cybersecurity Awareness factor highlighted the elements of cybersecurity views and knowledge. Zwilling *et al.* argue that, in order to advance knowledge on the subject of cybersecurity awareness, attention must be paid to training programmes in order to mitigate the risks.¹⁵⁴ It is therefore of the greatest importance to emphasise that these two factors had a level internal consistency owing to the fundamental connection between precautionary mechanisms and awareness.¹⁵⁵ In addition, individual cybersecurity awareness may be influenced by top management in organisational structures.¹⁵⁶ Given the current findings, it should be highlighted that contextual factors, such as attitudes and possible managerial support, might influence how cybersecurity awareness is approached in organisational contexts.

Based on the EFA and reliability results, it is clear that the COQ is a very promising measurement instrument. The full-scale COQ showed acceptable reliability, and once the problematic items had been removed, the COQ showed very good reliability, which indicated that it consistently measured the intended constructs. The EFA and reliability indicated that the COQ had two strong factors with very good internal consistency. Furthermore, the EFA and the reliability results highlighted an important issue relating to the Information-Sharing factor that was present in both analyses. The Information-Sharing factor presented negligible reliability and appeared to have contradictory relationships with the two stronger factors in the COQ, namely the Cybersecurity Awareness and Security Orientation factors. When considering the above findings, it is argued that the COQ may be a useful screening tool for military units, as it shows good potential.

Limitations and recommendations

This study was limited to a select sample only, mainly for the reasons relating to accessibility and availability of military officers. A restriction on range prevailed; the findings derived from this study therefore cannot be generalised to the entire SANDF. Due to the nature of the recruitment for the larger study, the sample size of this study was small, and follow-up studies on the COQ will thus require a much larger sample. Although age and rank are regarded as potential factors that could affect cybersecurity awareness, these were not evaluated in this initial exploration of the COQ due to a predominately young sample and limited number of each rank category present. Rank and age were, however, noted as potential factors that may have affected the results.

The findings also suggest the necessity for further investigation of the items relating to the different factors and possibly the elimination or revision of ill-fitting items. As a result, the statements in the COQ will be revised as part of the further development and refinement of the questionnaire. The authors recommend follow-up research in terms of the COQ be done and that a pre-knowledge survey of cybersecurity awareness be conducted. The focus on pre-knowledge will group the data based on a three-cluster classification, namely as a high level of pre-knowledge, a medium level of pre-knowledge, and limited pre-knowledge or a lack of such knowledge.

The development of the COQ is ongoing and flexible to accommodate new technological trends and expected security behaviours that may emerge. Furthermore, the COQ may be used as a valuable component in contributing to the development of a curriculum that focuses on cybersecurity awareness in the SA military context. This curriculum could target the cyber education of members of the military at all levels. The COQ provides a foundation through which military officers could evaluate their level of awareness of cybersecurity. In addition, the COQ may also be used before and after cybersecurity education to determine whether members acquired knowledge. Furthermore, future research could explore the complexities of a digital culture in the SANDF, as this may serve as a contextual view on technological integration. Further exploration and development of the COQ scale items are therefore necessary. Moreover, while psychology was not the focus of this article, a recommendation for future research on cybersecurity awareness is to investigate how psychologists in the SA armed forces context may explore the behavioural aspects of cybersecurity awareness.

Conclusion

The COQ showed acceptable reliability for research purposes ($r = .79$; $p = .000$). The prominent three-factor structure was in line with the theorised factors envisioned during the development of the COQ. The initial validation of the COQ delivered promising results for assessing cybersecurity awareness in an SA military sample. The findings of this study indicate that the COQ may provide valuable information on cybersecurity awareness among military members, and it is thus considered a promising screening tool to be used for military units.

In summary, this article emphasises the importance of developing measuring instruments specifically for the SA military context. Cybersecurity will continue to be a pressing issue that gives cause for concern in the context of the SA armed forces. It is therefore important to develop future military officers who have a comprehensive skill set inclusive of cyber-related aspects, such as cybersecurity awareness and education.

Acknowledgements

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

Disclaimer

The views expressed in this article are the authors' own and are not the official position of any institution.

Endnotes

- ¹ Kyle John Bester is a registered Research Psychologist and cybersecurity awareness specialist. He obtained a M.A Psychology (Masters in Research Psychology) degree from the University of the Western Cape in 2017. He functions as a psychology lecturer at the University of South Africa (Unisa) and specialises in cybersecurity awareness in the South African armed forces context. He completed his PhD in Military Science at Stellenbosch University in 2023. His research interests include military science; data-colonialism; cybersecurity awareness; securitisation of cyberspace and cyber-psychology. He has published and presented papers both locally and internationally.
- ² Danille Elize Arendse obtained a BA (psychology), BA Honours degree (Psychology) and MA (Research Psychology) degree from the University of the Western Cape. She joined the SANDF in 2011 as a uniformed member and became employed as a Research Psychologist at the Military Psychological Institute (MPI). She completed her PhD in Psychology at the University of Pretoria in 2018. She holds a Major rank and was the Research Psychology Intern Supervisor and Coordinator at MPI. She is also a Research Associate for the Department of Psychology at the University of Pretoria and an Accredited Conflict Dynamics Mediator. In 2022, she was awarded the Diverse Black Africa research grant and travel grant that is affiliated with Michigan State University. She is currently a postdoctoral fellow at the Centre for the Study of the Afterlife of Violence and the Reparative Quest (AVReQ) at Stellenbosch University and funded under the NIHSS/SU prestigious postdoctoral fellowship. She has presented and published papers both locally and internationally. Her research interests include 'Coloured' identity, mentoring, psychometric assessments, cognitive psychology, psycholinguistics, military, wellbeing, gender and sexuality and decolonial research.
- ³ KJ Bester, *Exploring the Views and Perceptions of Cybersecurity among South African Military Officers* (PhD dissertation, Stellenbosch University, 2023).
- ⁴ T Lejaka, *A Framework for Cyber Security Awareness in Small, Medium and Micro Enterprises (SMMEs) in South Africa* (Master's dissertation, University of South Africa, 2022).
- ⁵ M Zwilling, G Klien, D Lesjak, L Wiechetek, F Cetin & H Nejat Basim, 'Cybersecurity Awareness, Knowledge and Behavior: A Comparative Study', *Journal of Computer Information Systems*, 62, 1 (2020), 82–97.
- ⁶ Bester, *Exploring the Views and Perceptions of Cybersecurity*.
- ⁷ State Security Agency, 'National Cybersecurity Policy Framework for South Africa', *Government Gazette*, 609, 39475 (4 December 2015), 1–30.
- ⁸ 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), August, 1–26.
- ⁹ South African Government, *Defence and Military Veterans Department Budget Vote 2023/24* (Pretoria: Government Printer, 2023).
- ¹⁰ 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.
- ¹¹ Bester, *Exploring the Views and Perceptions of Cybersecurity*.
- ¹² R du Toit, PN Hadebe & M Mphatheni, 'Public Perceptions of Cybersecurity: A South African Context', *Acta Criminologica: Southern African Journal of Criminology*, 31, 3 (2018), 111–131.

- ¹³ J Griffiths, *Cyber Security as an Emerging Challenge to South African National Security* (Master's thesis, University of Pretoria, 2017).
- ¹⁴ T Lejaka, *A Framework for Cyber Security Awareness*.
- ¹⁵ H Pieterse, 'The Cyber Threat Landscape in South Africa: A 10-year Review', *African Journal of Information and Communication*, 28 (2021), 1–21.
- ¹⁶ C van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', in the *14th International Conference on Cyber Warfare and Security (ICCWS 2019)* (New York: Curran, 2019), 457–466.
- ¹⁷ E Sutherland, 'Governance of Cybersecurity: The Case of South Africa', *The African Journal of Information and Communication*, 20 (2017), 83–112.
- ¹⁸ Interpol, 'African Cyberthreat Assessment Report: Interpol's Key Insight into Cybercrime in Africa', 2021. <https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf> [Accessed on 4 April 2022].
- ¹⁹ J Cilliers, *Challenges and Opportunities: The Future of Africa* (Cham: Palgrave Macmillan, 2021).
- ²⁰ S Zhao, Y Zhang, H Iftikhar, A Ullah, J Mao & T Wang, 'Dynamic Influence of Digital and Technological Advancement on Sustainable Economic Growth in Belt and Road Initiative (BRI) Countries', *Sustainability*, 14 (2022), 1-16.
- ²¹ F Kolini & L Janczewski, 'Cyber Defence Capability Model: A Foundation Taxonomy', in *CONF-IRM 2015 Proceedings*, 2015, 32. <<https://aisel.aisnet.org/confirm2015/32>> [Accessed on 22 November 2021].
- ²² Cilliers, *Challenges and Opportunities*.
- ²³ J Cilliers, *Africa First: Igniting a Growth Revolution* (Cape Town: Jonathan Ball, 2020).
- ²⁴ H Mukiibi, 'Cybersecurity in Africa: The Boring Technology Story that Matters', *XRDS: Crossroads, The ACM Magazine for Students*, 26, 2 (2019), 56–59.
- ²⁵ K Aaltola, H Ruoslahti & J Heinonen, 'Desired Cybersecurity Skills and Skills Acquisition Methods in the Organizations', in *Proceedings of the 21st European Conference on Cyber Warfare and Security* (University of Chester: Academic Conferences International Limited, (2022), 1–9.
- ²⁶ Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 457–466.
- ²⁷ Ramluckan *et al.*, 'Cybersecurity and Information Warfare Research in South Africa', 80–95.
- ²⁸ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ²⁹ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ³⁰ F Al Dawod & B Stefanska, *The Importance of Risk Awareness in Cybersecurity among Companies* (Master's thesis, Linköping University, 2021).
- ³¹ Du Toit *et al.*, 'Public Perceptions of Cybersecurity', 111–131.
- ³² K Lingelbach, 'Student Perceptions of a Cybersecurity Service-Learning Project', *Issues in Information Systems*, 22, 3 (2021), 307–311.
- ³³ Bester, *Exploring the Views and Perceptions of Cybersecurity*.
- ³⁴ Bester, *Exploring the Views and Perceptions of Cybersecurity*.
- ³⁵ R Chandarman & B van Niekerk, 'Students' Cybersecurity Awareness at a Private Tertiary Educational Institution', *African Journal of Information and Communication*, 20 (2017), 133–155.
- ³⁶ Bester, *Exploring the Views and Perceptions of Cybersecurity*.

- 37 Ramluckan *et al.*, 'Cybersecurity and Information Warfare Research in South Africa', 80–95.
- 38 SSK Mtuze & M Musoni, 'An Overview of Cybercrime Law in South Africa', *International Cybersecurity Law Review*, 4 (2023), 299–323.
- 39 Sutherland, 'Governance of Cybersecurity', 83–112.
- 40 Pieterse, 'The Cyber Threat Landscape in South Africa', 1–21.
- 41 State Security Agency, 'National Cybersecurity Policy Framework for South Africa', 1–30.
- 42 State Security Agency, 'National Cybersecurity Policy Framework for South Africa', 1–30.
- 43 G Noel & M Reith, 'Cyber Warfare Evolution and Role in Modern Conflict', *Journal of Information Warfare*, 20, 4 (2021), 30–44.
- 44 E Haber & L Topor, 'Sovereignty, Cyberspace, and the Emergence of Internet Bubbles', *Journal of Advanced Military Studies*, 14, 1 (2023), 144–165.
- 45 State Security Agency, 'National Cybersecurity Policy Framework for South Africa', 1–30.
- 46 Tech Target, 'Definition of the Internet', 2023. <<https://www.techtarget.com/whatis/definition/Internet#:~:text=The%20internet%2C%20sometimes%20simply%20called,an%20established%20set%20of%20protocols.>> [Accessed on 12 June 2024].
- 47 C Stevens, 'Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet', *Contemporary Security Policy*, 41 (2020), 129–152.
- 48 Bestor, *Exploring the Views and Perceptions of Cybersecurity*.
- 49 Africa Center for Strategic Studies, 'Cyberspace and Security Sector Governance in Africa', 2022. <https://africacenter.org/wp-content/uploads/2022/09/Cyberspace-and-Security-Sector-Governance-in-Africa-ES_FINAL_EN.pdf> [Accessed on 24 November 2023].
- 50 Accenture, 'Insight into the Cyber Threat Landscape in South Africa', 2019. <https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf> [Accessed on 12 January 2022].
- 51 N Kshetri, 'Cybercrime and Cybersecurity in Africa', *Journal of Global Information Technology Management*, 22, 2 (2019), 77–81.
- 52 Africa Center for Strategic Studies, 'Cyberspace and Security Sector Governance in Africa'.
- 53 Africa Center for Strategic Studies, 'Cyberspace and Security Sector Governance in Africa'.
- 54 Kshetri, 'Cybercrime and Cybersecurity in Africa', 77–81.
- 55 Kshetri, 'Cybercrime and Cybersecurity in Africa', 77–81.
- 56 Bestor, *Exploring the Views and Perceptions of Cybersecurity*.
- 57 Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 457–466.
- 58 J Jansen van Vuuren & L Leenen, 'Cybersecurity Capability and Capacity Building for South Africa'. Paper presented at the IFIP International Conference on Human Choice and Computers, Posnan, 19–20 September 2018.
- 59 Kshetri, 'Cybercrime and Cybersecurity in Africa', 77–81.
- 60 Statista, 'Mobile Internet User Penetration in South Africa from 2019 to 2028', 17 October 2023. <<https://www.statista.com/statistics/972866/south-africa-mobile-internet-penetration/>> [Accessed on 21 November 2023].
- 61 Cilliers, *Africa First*.
- 62 M Ndlovu, 'Spyware Attacks in South Africa Increase by 18.8%', *Mail & Guardian*, 19 May 2023. <<https://mg.co.za/article/2023-05-19-spyware-attacks-in-south-africa-increase-by-18-8/>> [Accessed on 22 November 2023].

- 63 Arctic Wolf, 'The State of Cybersecurity in South Africa Report 2023', 2023. <http://arcticwolf.com/resource/_pfcnd/assets/10926/contents/520015/5265a603-64cd-42ea-a8bf-7eab9c602ed7.pdf> [Accessed on 2 November 2023].
- 64 Arctic Wolf, 'The State of Cybersecurity in South Africa Report 2023'.
- 65 N Veerasamy, 'Cyber Threats Focusing on Covid-19 Outbreak'. Paper presented at the International Conference on Cyber Warfare and Security, Tennessee, 25–26 February 2021.
- 66 S Mei, J Chai, S Shi-Bin Wang, C Ng, G Ungvari & Y Yu-Tao Xiang, 'Mobile Phone Dependence, Social Support and Impulsivity in Chinese University Students', *International Journal of Environmental Research and Public Health*, 15 (2018), 504.
- 67 Mtuze & Musoni, 'An Overview of Cybercrime Law in South Africa', 299–323.
- 68 A Moyo, 'Hackers Demand R1.1bn Ransom from TransUnion, Experian', *IT Web*, 23 November 2023. <<https://www.itweb.co.za/content/DZQ58MV8ymzvzXy2>> [Accessed on 23 November 2023].
- 69 *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].
- 70 Parliamentary Monitoring Group, 'Cyber Warfare Policy: Department of Defence Briefing', 11 March 2020. <<https://pmg.org.za/committee-meeting/30014/>> [Accessed on 23 November 2023].
- 71 Supreme Headquarters Allied Powers Europe, 'Nato Cyber Defensive Capability as a Spearhead and Force Multiplier', 16 December 2020. <<https://shape.nato.int/news-archive/2020/nato-cyber-defensive-capability-as-a-spearhead-and-force-multiplier>> [Accessed on 24 November 2023].
- 72 Supreme Headquarters Allied Powers Europe, 'Nato Cyber Defensive Capability'.
- 73 N Majumda & V Ramteke, 'Human Elements Impacting Risky Habits in Cybersecurity', in *AIP Conference Proceedings*, 2519, 1 (2022), 1–12.
- 74 Cilliers, *Challenges and Opportunities*.
- 75 PB Maurseth, 'The Effect of the Internet on Economic Growth: Counter-evidence from Cross-country Panel Data', *Economics Letters*, 172 (2018), 74–77.
- 76 Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- 77 Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- 78 Al Dawod & Stefanska, *The Importance of Risk Awareness*.
- 79 Akter *et al.*, 'Reconceptualising Cybersecurity Awareness Capability', 1–26.
- 80 Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- 81 S Chatchalermpun & T Daengsi, 'Improving Cybersecurity Awareness Using Phishing Attack Simulation', IOP Conference Series: Materials Science and Engineering, Volume 1088, Annual Conference on Computer Science and Engineering Technology (AC2SET), Medan, 23 September 2021.
- 82 LJ Hadlington, 'Employees' Attitudes towards Cybersecurity and Risky Online Behaviours: An Empirical Assessment in the United Kingdom', *International Journal of Cyber Criminology*, 12 (2018), 269–281.
- 83 Hadlington, 'Employees' Attitudes Towards Cybersecurity', 269–281.
- 84 Chatchalermpun & Daengsi, 'Improving Cybersecurity Awareness'.
- 85 Chatchalermpun & Daengsi, 'Improving Cybersecurity Awareness'.

- ⁸⁶ Bester, *Exploring the Views and Perceptions of Cybersecurity*.
- ⁸⁷ Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 457–466.
- ⁸⁸ OT Murire, S Flowerday, K Strydom & CJ Fourie, 'Narrative Review: Social Media Use by Employees and the Risk to Institutional and Personal Information Security Compliance in South Africa', *Journal of Transdisciplinary Research Southern Africa*, 17, 1 (2021), a909.
- ⁸⁹ M Lehto, 'Phenomena in the Cyber World', in M Lehto & P Neittaanmäki (eds.), *Cybersecurity: Analytics, Technology and Automation. Vol. 78: Intelligent Systems, Control and Automation: Science and Engineering* (Cham: Springer, 2015), 3–29.
- ⁹⁰ R Raju, NHA Rahman & A Ahmad, 'Cyber Security Awareness in Using Digital Platforms among Students in a Higher Learning Institution', *Asian Journal of University Education*, 18, 3 (2022), 757-766
- ⁹¹ J Abawajy, 'User Preference of Cybersecurity Awareness Delivery Methods', *Behaviour Information Technology*, 33, 3 (2014), 237–248.
- ⁹² Abawajy, 'User Preference of Cybersecurity Awareness Delivery Methods', 237–248.
- ⁹³ Chatchalermpun & Daengsi, 'Improving Cybersecurity Awareness'.
- ⁹⁴ A Baillon, J de Bruin, A Emirmahmutoglu, E van de Veer & B van Dijk, 'Informing, Simulating Experience, or Both: A Field Experiment on Phishing Risks,' *PLOS ONE*, 14, 12 (2019), 1–15.
- ⁹⁵ N Beu, A Jayatilaka, M Zahedi, M Ali Babar, L Hartley, W Lewinsmith & I Baetu, 'Falling for Phishing Attempts: An Investigation of Individual Differences that are Associated with Behavior in a Naturalistic Phishing Simulation', *Computers & Security*, 131 (2023), 103-313.
- ⁹⁶ Van't Wout, 'Develop and Maintain a Cybersecurity Organisational Culture', 457–466.
- ⁹⁷ Bester, *Exploring the Views and Perceptions of Cybersecurity*.
- ⁹⁸ M Mohammed, E Maroof, A Thamer & I Huda, 'What are the Electronic Information Sharing Factors that Influence the Participation Behavior in the Higher Education Sector?', *Procedia Computer Science*, 72 (2015), 49–58.
- ⁹⁹ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ¹⁰⁰ Lehto, 'Phenomena in the Cyber World', 3–29.
- ¹⁰¹ H Al-Mohannadi, I Awan, J Al-Hamar, Y Al-Hamar, M Shah & A Musa, 'Understanding Awareness of Cybersecurity Threat among IT Employees', in *Sixth International Conference on Future Internet of Things and Cloud Workshops* (Barcelona: FiCloudW, 2018), 188–192.
- ¹⁰² Al-Mohannadi *et al.*, 'Understanding Awareness of Cybersecurity Threat among IT Employees', 188–192.
- ¹⁰³ FK Duman, 'Determining Cyber Security-related Behaviors of Internet Users: Example of the Faculty of Sport Sciences Students', *European Journal of Education*, 5 (2022), 114–131.
- ¹⁰⁴ Duman, 'Determining Cyber Security-Related Behaviors of Internet Users', 114–131.
- ¹⁰⁵ Du Toit *et al.*, 'Public Perceptions of Cybersecurity', 111–131.
- ¹⁰⁶ D Lain, K Kostianen & S Capkun, 'Phishing in Organizations: Findings from a Large-scale and Long-term Study', in *IEEE Symposium on Security and Privacy* (San Francisco: IEEE, 2022), 842–859.
- ¹⁰⁷ A Minnaar & FJW Herbig, 'Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services during the COVID-19 Pandemic', *Acta Criminologica: African Journal of Criminology & Victimology*, 34, 3 (2021), 154–185.
- ¹⁰⁸ AJ Burns, ME Johnson & DD Caputo, 'Spear Phishing in a Barrel: Insights from a Targeted Phishing Campaign', *Journal of Organizational Computing and Electronic Commerce*, 29, 1 (2019), 24–39.

- 109 K Aaltola *et al.*, 'Desired Cybersecurity Skills', 1–9.
- 110 E Yllia & J Fejzaj, 'Man in the Middle: Attack and Protection', in *Proceedings of RTA-CSIT 2021* (Tirana: CEUR-WS, 2021), 109-134
- 111 Du Toit *et al.*, 'Public Perceptions of Cybersecurity', 111–131.
- 112 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), 53-64.
- 113 Bester, *Exploring the Views and Perceptions of Cybersecurity*.
- 114 K Parsons, D Calic, M Pattinson, M Butavicius, A McCormac & T Zwaans, 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies', *Computers & Security*, 66, (2017), 40–51.
- 115 DE Arendse, 'The Impact of Different Time Limits and Test Versions on Reliability in South Africa', *African Journal of Psychological Assessment*, 2, 14 (2020), 1–10.
- 116 DE Arendse & D Maree, 'Exploring the Factor Structure of the English Comprehension Test', *South African Journal of Psychology*, 49, 3 (2019), 376–390.
- 117 B Williams, A Onsman & T Brown, 'Exploratory Factor Analysis: A Five-step Guide for Novices', *Journal of Emergency Primary Health Care*, 8, 3 (2010), 1–13.
- 118 Arendse & Maree, 'Exploring the Factor Structure of the English Comprehension Test', 376–390.
- 119 BG Tabachnick & LS Fidell, *Using Multivariate Statistics* (Boston: Pearson Education, 2013).
- 120 Arendse & Maree, 'Exploring the Factor Structure of the English Comprehension Test', 376–390.
- 121 Arendse & Maree, 'Exploring the Factor Structure of the English Comprehension Test', 376–390.
- 122 AC Yong & S Pearce, 'A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis', *Tutorials in Quantitative Methods for Psychology*, 9, 2 (2013), 79–94.
- 123 Williams *et al.*, 'Exploratory Factor Analysis', 1–13.
- 124 Arendse, 'The Impact of Different Time Limits', 1–10.
- 125 LJ Cronbach, 'Coefficient Alpha and the Internal Structure of Tests', *Psychometrika*, 16 (1951), 297–334.
- 126 Arendse, 'The Impact of Different Time Limits', 1–10.
- 127 C Hedge, G Powell & P Sumner, 'The Reliability Paradox: Why Robust Cognitive Tasks Do Not Produce Reliable Individual Differences', *Behaviour Research*, 50 (2018), 1166–1186.
- 128 KS Taber, 'The Use of Cronbach's Alpha when Developing and Reporting Research Instruments in Science Education', *Research Science Education*, 48 (2018), 1273–1296.
- 129 Cronbach, 'Coefficient Alpha and the Internal Structure of Tests', 297–334.
- 130 Arendse, 'The Impact of Different Time Limits', 1–10.
- 131 Taber, 'The Use of Cronbach's Alpha', 1273–1296.
- 132 M Tavakol & R Dennick, 'Making Sense of Cronbach's Alpha', *International Journal of Medical Education*, 2 (2011), 53–55.
- 133 Raju *et al.*, 'Cyber Security Awareness in Using Digital Platforms among Students in a Higher Learning Institution', 237–248
- 134 Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.

- ¹³⁵ P Limna, T Kraiwant & S Siripipattanukul, 'The Relationship between Cyber Security Awareness, Knowledge, and Behavioural Choice Protection among Mobile Banking Users in Thailand', *International Journal of Computing Sciences Research*, 6 (2022), 1–19.
- ¹³⁶ A Kovačević, N Putnik & O Tošković, 'Factors Related to Cybersecurity Behaviour', *IEE Access Journal*, 8 (2020), 125140–125148.
- ¹³⁷ Limna *et al.*, 'The Relationship Between Cyber Security Awareness', 1–19.
- ¹³⁸ P van Schaik, D Jeske, J Onibokun, L Coventry, J Jansen & P Kusev, 'Risk Perceptions of Cyber-security and Precautionary Behaviour', *Computers in Human Behavior*, 57 (2017), 547–559.
- ¹³⁹ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ¹⁴⁰ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ¹⁴¹ Limna *et al.*, 'The Relationship Between Cyber Security Awareness', 1–19.
- ¹⁴² Mohammed *et al.*, 'What are the Electronic Information Sharing Factors', 49–58.
- ¹⁴³ Mohammed *et al.*, 'What Are the Electronic Information Sharing Factors', 49–58.
- ¹⁴⁴ R Omar, T Ramayah, MC Lo, TY Sang & R Siron, 'Information Sharing, Information Quality and Usage of Information Technology (IT) Tools in Malaysian Organizations', *Global Journal of Business Management*, 14, 2 (2020), 1–14.
- ¹⁴⁵ Bester, *Exploring the Perceptions and Views on Cybersecurity*.
- ¹⁴⁶ South African Department of Defence, 'South African Defence Review 2015', 2015. <<https://static.pmg.org.za/170512review.pdf>> [Accessed on 20 March 2021].
- ¹⁴⁷ J Gerber, 'While Internal SANDF Deployments Increase, the Defence's Budget Decreases', News24, 24 May 2023. <<https://www.news24.com/news24/politics/parliament/while-internal-sandf-deployments-increase-the-defences-budget-decreases-20230524>> [Accessed on 30 November 2023].
- ¹⁴⁸ 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].
- ¹⁴⁹ A Pala & J Zhuang, 'Information Sharing in Cybersecurity', *Decision Analysis*, 16 (3), 2019, 157–237.
- ¹⁵⁰ F Ahmad & I Huvila, 'Organizational Changes, Trust and Information Sharing: An Empirical Study', *Aslib Journal of Information Management*, 71 5 (2019), 677–692.
- ¹⁵¹ Mohammed *et al.*, 'What Are the Electronic Information Sharing Factors', 49–58.
- ¹⁵² Mohammed *et al.*, 'What Are the Electronic Information Sharing Factors', 49–58.
- ¹⁵³ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ¹⁵⁴ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ¹⁵⁵ Zwilling *et al.*, 'Cybersecurity Awareness, Knowledge and Behavior', 82–97.
- ¹⁵⁶ S Mogoane & S Kabanda, 'Challenges in Information and Cybersecurity Program Offering at Higher Education Institutions', in *Proceedings of Fourth International Conference on the Internet, Cybersecurity and Information Systems 2019: Kalpa Publications in Computing*, 12 (2019), 202–212.