Chapter Eleven

Applying Securitisation Theory to Understand Cybersecurity within the South African Armed Forces Context

Kyle Bester
Department of Psychology
University of South Africa
Pretoria, South Africa

Abstract

The pervasive nature of cyber threats poses a significant security challenge to governments, organisations and individual users. Cybersecurity in the context of South African armed forces has received minimal attention as an emerging threat in the 21st century. In terms of Agenda 2063, the South African National Defence Force has yet to place cybersecurity at the centre of its plan to advance itself as an African cyber army. The chapter aims to explore the views and perceptions of military officers, which requires a qualitative approach. A non-probability purposive sampling technique was used to select 13 participants enrolled in a senior officer's course at a South African site where professional military education is offered. The views and perceptions of the South African military officers were analysed within a securitisation framework. Under the guise of Securitisation Theory's (ST) security process of transforming an ordinary threat into the realm of politics, rests the central tenant of the speech act. This study locates itself within the widened view of ST, which suggests that the military officer is a key role player in orchestrating a security move through the speech act. Two main findings emerged from the individual views on cybersecurity. First, not all threats require an emergency response in the context

of South African armed forces, alluding to the value placed on cyber threats. Second, cyber securitisation is a continuous process and does not necessarily take on existential features that require an emergency response. The findings showed that cybersecurity is an emerging issue in the South African threat landscape. The theoretical value placed on ST highlights the various dimensions, threat actors and the mechanisms through which the speech act is executed. The chapter contributes to the existing body of knowledge concerning securitisation theory by (1) expanding the contextual boundaries through which security threats are viewed, (2) positioning the military officer as a key player in the securitisation process, and (3) understanding the process of threat elevation in the context of the South African National Defence Force (SANDF).

Introduction

Cyber threats have become an international concern for many nation-states, and this is due to the transnational nature of the consequences emanating from extremely complex, malicious software (Bester, 2023). With the ever-changing nature of threats and attacks originating from cyberspace, the importance has shifted to cybersecurity and its capabilities by nation-states due to four reasons: (1) Nation-states are increasing their cybersecurity capability to compete with their adversaries and nefarious actors (Letho & Henselmann, 2020; Gazula, 2017). (2) Cyber threats and attacks have distressing consequences for the socio-economic capacity of a country; therefore, whatever measures are taken should ensure civil society and national security interests are taken into account (Hlase, 2018). (3) Nation states advance their cybersecurity capabilities to maintain their approach to a modern armed force and also for defensive measures to secure their interests from cybersecurity threats (Mulazzani & Sarcia, 2011). It is important to define cybersecurity at the outset of this chapter, as it may provide a background to when the researcher refers to the term as a response to threats. Bester (2023:43) defines cybersecurity as follows:

> Cybersecurity is a flexible security process through which individuals constantly interact 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 applying knowledge to risk perception and precautionary behaviour while being fully aware of physical and cyberspace vulnerabilities.

There is a shift in how cyberspace is conceptualised from a multidisciplinary view of security (Bester, 2023). Cyberspace is considered a new domain of warfare. It demands a new approach to understanding the role of security and the position of the armed forces in securing this digital domain (United States Army Joint Chiefs of Staff, 2018). (4) The human aspect of cybersecurity is not void of vulnerabilities; therefore, countries and organisations have invested in cyber-awareness to reduce the notion of users involuntarily being victims of cybercrime. Furthermore, with the increasing threat rate, it is evident that there is more focus on creating cybersecurity awareness among cyberspace users. Thus, it is argued that there is a growing dialogue internationally and locally on cybersecurity, which positions cyber threats at the centre of security agendas. In this way, the logic of security travels to new and emerging domains is highlighted; thus, ST is an applicable framework to explore emerging threats in social landscapes (Philipsen, 2018).

Cyberspace has increased the vulnerability of users' data and advanced the level of dependence on technology. This is due to the increasing trend of internet-connected device use. Furthermore, this level of vulnerability impacts data housed in government organisations and may even increase the likelihood of cyber threats if no adequate security measures are implemented. Therefore, with the increase in use, the organisation or entity responsible for user data must ensure that precautionary measures are employed against cyber threats and

potential attacks (Toch, Bettini, Shmueli, Radaelli, Lanzi, Riboni & Lepri, 2018). The storage of volumes of data in organisations also exposes the organisations to threats such as data breaches and privacy concerns, which ultimately places user information and sensitive organisational information at risk (Toch *et al.*, 2018).

Zukic (2020) highlights that advancing the cybersecurity knowledge of military members is essential as the space is evolving, which also results in an ever-changing threat landscape, thus posing a significant threat to national security and human security in cyberspace. Bester (2023) contends that the armed forces have a complex relationship with cyberspace and emerging technology, which can be likened to a double-edged sword. It is argued that cyberspace is continuously being integrated into the function of the armed forces, especially with the employment of operational and strategic military activities where intelligence gathering, surveillance systems and reconnaissance activities are carried out (Sayler, 2020). According to Martin (2020), technology and cyberspace have the potential to amplify forces, yet they also present security risks to personnel. Adding to the importance of the human being at the centre of cybersecurity, one may argue that there is an expectation that the armed forces context is the primary actor within a security cluster that is responsible for advancing national cybersecurity and protecting the cyber sovereignty of the state (Kolton, 2017).

This chapter takes the positionality of securitisation theory (ST) to understand how cybersecurity threats are understood among senior South African National Defence Force (SANDF) military officers. Furthermore, this chapter aims to explore cyber threats as emerging security challenges within the SANDF. Ultimately, this chapter contributes to research on new conceptualisations of security by focusing on cyber threats and using ST as a theoretical guide in positioning how this new and emerging threat is framed.

What is Securitisation Theory?

It is argued that ST focuses on elements associated with war and conflict, particularly when viewing the securitisation procedure as successful. This level of success may not necessarily imply that all facets of the theory were "ticked on the list;" it indicates the resolution of addressing existential threats that were resolved using an extraordinary measure (Lucke, 2016). To describe ST, the constituent elements of its definition must be identified. The definition of ST is as follows:

> The discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object and to enable a call for urgent and exceptional measures to deal with the threat (Buzan & Waever, 2003:491).

In their definition, Buzan and Waever (2003) suggest that there is movement in understanding and communicating threats. The definition posed echoes the process where an issue moves from the political realm and transforms into an existential threat. This transformation of the threat is done by the securitising actor, which enforces the value and importance of the threat to an audience that may or may not agree with the threatened object of reference. Bester (2023) notes that an existential threat may threaten the survival of a referent object. However, Philipsen (2018) cautions that not all threats can be classified as existential or demand an emergency response.

Dos Santos (2018) considers the role of the state an important facet of the securitisation process, and its role is central to its emphasis on how domestic and international issues are threatened and addressed by its existential measures (Bote, 2019; Egloff & Cavelty, 2021). Eroukhmanoff (2018) adds that ST offers a rational process through which security procedures are announced and elevated to deal with existential threats. The chapter suggests that ST's linear process may not apply in non-Western contexts when considering cybersecurity threats. The researcher puts forth that in the context of SA, the securitising actors (the state and an authorised representative) have acknowledged cyber threats as threatening the national

security interests of the state and civil society, thus ultimately challenging SA's position on establishing cyberspace sovereignty (Republic of South Africa, 2018).

Philipsen (2018) notes that the traditional notion of ST can be challenged by the idea of who may speak of security. Traditionally, ST emphasises that actors in positions of authority are a pre-condition for speaking of security and possibly proclaiming the significance of the threat. Instead, Philipsen (2018) argues that speaking of security should be the primary condition under which authority is exercised. Egloff and Cavelty (2021) argue that ST considers constructing policies linked to security agendas. Therefore, a threat might be classified as objective and even, to a certain extent, described as existential. However, the securitisation process's success is achieved when threats are established and presented successfully in the political domain (Buzan, Waever, & De Wilde, 1998).

In terms of politics, the Copenhagen School (CS) first considered public issues to be politicised, after which they were securitised (Hama, 2017). Based on this view, securitisation is elevating political issues beyond normal political practices designed to respond to security threats and vulnerabilities (Hama, 2017). Egloff and Cavelty (2021) assert that ST is grounded in the speech act theory, which purports that the use of language can be a performative act. Security speech acts containing performative power can reconstruct and change social reality. This might impact how security is described within social and political contexts. Additionally, the security utterances made by the securitising actors may influence the response to certain threats (Stritzel, 2007). It is important to note that the ST process is understood in its sequential format.

Based on the information in Figure 11.1, it is evident that securitisation follows a logical process where security measures are introduced and elevated to deal with existential threats (Eroukhmanoff, 2018). It can be argued that the linear progression of ST might not be applicable in some contexts. Within the context of the SANDF, the securitising actor (the state and authorised representative), in this case, lends itself

to the activity where the Minister of Defence openly declares cyber threats and attacks a security challenge for security clusters in the nation-state. The SA Minister of Defence also acknowledges that cyber threats impact national security interests, highlighting the human element as a potential actor that may challenge cyber sovereignty at risk (Republic of South Africa, 2018). Therefore, the state and the human element are considered referent objects worth protecting through security measures. It is worth noting that the new SA Minister of Defence indicated in the budget speech debate on the Defence Vote 2022/2023 (Republic of South Africa, 2022) that cybersecurity is one of the SANDF's chief defence concerns by highlighting the following: "… protecting South Africa's intangible sovereignty through support to the National Cyber Resilience Initiative and ensuring Defence Digital Protection" (Republic of South Africa, 2022, par. 44).

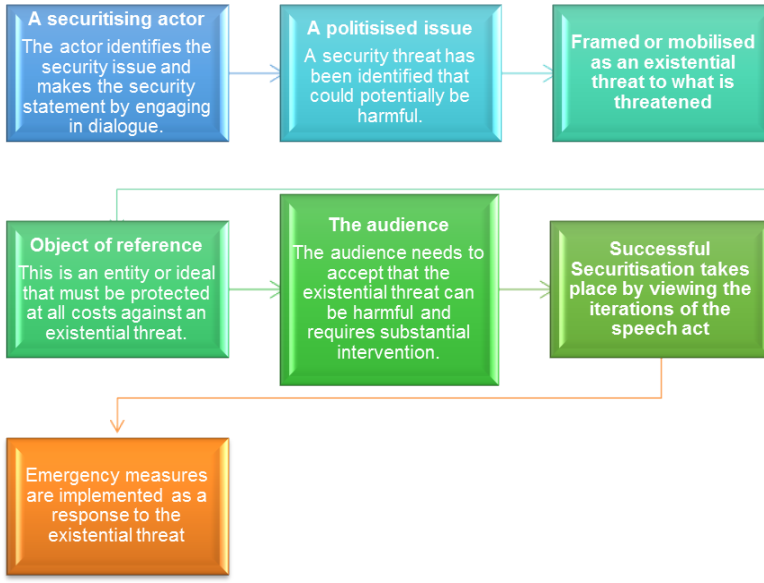

Figure 11.1: The logical flow of the securitisation process

Within the social context, the politician-state-centred view of the ST may be countered by a new way of thinking that

questions this monopoly on an issue carrying the label of being securitised when the state as an organ of power must proclaim a specific issue to be a realistic threat to its citizens so that adequate measures can be taken to counteract or mitigate the threat. Philipsen (2018) notes that the traditional notion of ST can be challenged by the idea of who may speak of security. Traditionally, ST emphasises that actors in positions of authority are a pre-condition for speaking of security and possibly proclaiming the significance of the threat. Instead, Philipsen (2018) suggests that speaking of security should be the condition of authority.

Buzan and Waever (2003) define the securitisation process as the transition of an ordinary security issue progressing to a level where the securitising actor classifies it (the security issue) as an existential threat. The existential threat can be narrowly defined as the threat to survival (May *et al.*, 1958). However, Philipsen (2018) cautions that not all identified threats might be classified as existential or require an emergency response. Furthermore, Van Ooijen (2020) believes that the threat response through emergency measures and the verbalisation of threats by the securitising actor is measurable by scale. This may typically be performed by the rate of execution of measures and how well the audience responds to the value placed on the referent object. However, it is noted that this measurement may not be applicable in all contexts as the sequential nature of ST may not occur in a rigid fashion. Philipsen (2018) indicates that security iterations develop over time and that the securitisation process may not necessarily be the same across all contexts as new meanings are added systematically. This impacts the way securitisation is carried out in different contexts.

The positioning of ST and its relevance to cyber threats

This chapter positions itself within the security studies discipline and explores cybersecurity as a new emerging threat within the South African armed forces context. By applying social network theory, one can recognise how cyber threats are communicated

to South African military officers and understand the response patterns to threats and attacks emerging from a digital landscape. This section of the chapter engages with the often-overlooked actors within the security process, such as the South African military officer. The traditional perspective of ST is that the state is the central element in the securitisation process (Buzan & Waever, 2003). ST entails the subjective process of managing and understanding elevated security threats against a recognised object of reference (Bester, 2023). ST highlights the process of framing a threat as existential, therefore demanding an extraordinary response. Once the threat has been identified in the political realm, it is escalated by the securitising actor to a point that requires extraordinary responses through security mechanisms. Herein rests the focal point of the theory.

Aydindag (2021) puts forth that after the threat has been identified and communicated by a securitising actor, a call is issued in the political community to enable exceptional measures relating ST to cyber threats. The South African Government has advanced the narrative regarding cyber threats and attacks by developing its defensive measures and creating a cyber command within its military. Furthermore, the nation-state is also developing its national legislation framework on cybersecurity by employing the National Cybersecurity Policy Framework (Republic of South Africa, 2015) and the Cybercrimes Bill (Republic of South Africa, 2019). These two legislative frameworks indicate the advancement SA has made in addressing cybersecurity threats. However, the slow-paced ratification of these policies is not necessarily in line with the advancement and complexities of cyber threats (van Niekerk, 2017).

Importance of the human element

The SANDF serves in a democratic dispensation and is subject to the state's civil authorities (Janse van Rensburg, 2019). It is worth noting that civil control of the military denotes the hierarchical nature of armed forces, which serve the executive branch of the state (Aldis & Drent, 2008). The SANDF is an important element in the pursuit of establishing

national security. Van't Wout (2019) argues that the capability of an armed force is only as good as the human capital being continuously developed and recruited. Additionally, cybersecurity training and awareness creation are crucial for equipping the human element with the necessary security behaviour and knowledge to effectively counteract threats in a digital space.

Four central reasons exist in support of why the human element is considered the weakest link in the cybersecurity chain, and they are: (1) Deception and exploitation of the human element by nefarious actors may result in sensitive organisational information being disclosed (Zwilling, Klien, Lesjak, Wiechetek, Cetin & Basim, 2020; Rauf, 2019). Thus, when linking it to the context of the armed forces, it might be possible for military members to be psychologically targeted to disclose restricted information about strategic activities. (2) The internet is integrated into everyday life, especially with mobile devices. Therefore, the connection between organisational and personal information being shared on convenient communication platforms, such as social media platforms, may pose a security risk to the online security credibility of the organisation and may compromise the military members' devices (Ani, He & Tiwari, 2019). (3) The role of the voluntary and involuntary points of access in organisational network systems, through the actions of the human element, may lend itself to the notion that the military member might be vulnerable to being a medium through which malicious software is passed (McMahon, 2020; Rauf, 2019). (4) The online security behaviour and the protocol used for responding to threats might be influenced by individual levels of security awareness (Zwilling *et al*., 2020).

The South African military officer is closely integrated into the civilian domain and functions within the broader armed forces community. The military member is allocated specific security mandates and responsibilities. This duality is mainly linked to the notion that cyberspace is ephemeral and the threats originating from this space may target anyone. The researcher adds that this view lends itself to the argument that the human element is vulnerable and may act as a security challenge for

the SANDF and the sovereignty of the nation state. Furthermore, cyber threats are unconventional and necessitate that the armed forces context and human capital adapt to the challenges the cyber domain offers, as the adversary is often unseen.

The role of the speech act in cyber securitisation

The previous section of the chapter emphasised the role of the human element and its position with ST. This section of the chapter offers a brief discussion on the role of the speech act in ST. An emergency measure is actioned based on the seriousness of the security threat. This statement aligns with the view that security is performative; in other words, to speak security, one must do security. It is worth noting that the SA military officer takes on a performative stance within the ST process (Bester, 2024). The SA military officer may also be in a vulnerable position and be susceptible to cyber threats. These military members may also be impacted by the deployed security responses. The coordination of cybersecurity efforts in the nation state has become the responsibility of the SANDF, as noted by the National Cybersecurity Policy Framework (Republic of South Africa, 2015a). One may put forth that the acting of security and speech acts that were performed by various actors beyond the military elevated the importance of cyber threats. Consequently, the SANDF is becoming a key actor responsible for maintaining cyber defence. This responsibility allows the military officer to enter the practice of security. Floyd (2020) highlights that ST is not a once-off event but rather a political process where issues are transformed into security threats over a period of time. Floyd (2020) suggests that the process of securitisation commences with the securitising actor, who engages in a speech act or makes a securitising move. The speech aims to announce a referent object being vulnerable to a threat (Floyd, 2020). This is followed by the audience, who must agree with the speech being verbalised and the securitising move. Once the audience accepts the narrative, the deployment of an emergency response is required to manage the perceived threat (Floyd, 2020). When linking this to cyber threats and attacks, the discourse regarding the severity of the attacks

increases the coordination process, ensuring accountability and maintaining cyber defence measures. These acts of ensuring cybersecurity connect with the notion that the SA military officer speaks due to the political elite engaging in the speech act and the security incidents that have transpired.

Methodology

This section of the chapter explores the methodological considerations of this particular study. The methodology section explores the research design, sampling descriptions, and data collection process. The data analysis is also briefly covered in this section of the chapter.

Research design

This study utilised an interpretivist approach to explore the perceptions of cybersecurity within the SANDF. The study used a cross-sectional design. The cross-sectional design is employed within research studies to explore a phenomenon at a particular time (Setia, 2016). In this study, the researcher explores the role of ST within the SANDF by specifically focusing on the perceptions of cybersecurity and how threats are framed. Furthermore, the recruited participants were recruited using a non-probability sampling method. Homogenous purposive sampling, a non-probability method, was used to obtain key information regarding security orientation from participants (Creswell, 2007). Homogenous purposive sampling is a technique that seeks to attain participants who have common sampling traits and experiences (Laerd Dissertation, 2012). All participants in this study served in the military and were of senior rank. It is important to note that ethical standards were maintained throughout the study.

Sample size and research participants

The researcher recruited participants located at the South African National Defence College (SANDC), which is a site where professional military training is offered. The SANDC is

a military training institution where senior military officers undergo professional training for promotional purposes (Bester, 2023). Biographical factors such as age and gender were not considered as these factors were not essential for this study's aims and objectives. Due to a sampling limitation associated with the military officers' academic obligations, the researcher could, ultimately, only recruit 13 participants.

Data collection and data analysis

The data collection approach used in this study was qualitative, which was employed to obtain perceptions of cybersecurity in the context of the armed forces. The researcher conducted 13 semi-structured interviews to extract views on (1) cybersecurity orientation, (2) cybersecurity training, (3) the organisation's approach to cybersecurity and (4) security culture. A set of pre-determined questions were designed for the interviews. The questions focused on aspects related to how threats are constructed in the armed forces context, the level of importance placed on cybersecurity in the SANDF context and the narrative associated with cyber threats in the organisation. The 13 senior military officers were purposively selected, and all semi-structured interviews were conducted at the SANDC. The interviews offered a bird's-eye view of the qualitative features of how threats are constructed and elevated to a point of importance among South African military officers. Qualitative Content Analysis (CA) was used to analyse the data received from the 13 interview transcripts. Qualitative CA is a type of analysis that explores the written, verbal and visual messages from the social world (Bester, 2023). Krippendorff (2004:18) describes CA as "a research technique for making replicable and valid inferences from texts to the contexts of their use."

Themes

Three main themes emerged from the data analysis: (1) awareness and knowledge of cyberspace and its connected dangers; (2) culture of digital security among officers; and (3) perception as an important aspect for senior military officers.

This section of the chapter explores the qualitative narratives regarding how military officers construct cyber threats and considers the importance of cybersecurity.

Theme 1: Awareness and knowledge of cyberspace and its connected dangers

The theme 'awareness and knowledge of cyberspace and its connected dangers' speaks to the notion that military officers need to be acquainted with cyberspace and cyber threats. The theme also focused on the level of awareness military officers have pertaining to the potential implications of cyber threats in the workplace. Sohrabi and Von Solms (2016) highlight that when individuals accumulate experiences, these contribute to their knowledge of events. In the context of this theme, awareness and knowledge related to cyberspace also refer to the participants' level of familiarity with cyberspace, which might be linked to how well they respond to security threats. Thus, the focus should shift to the skills and the capacity to prevent, manage, and alleviate the risk of exposing sensitive data (Ashenden, 2008). The purpose of this theme links to the participant's awareness of the threats in cyberspace and indicates that they were equally cognisant of the practices that went hand in hand with remaining active in cyberspace. This outlook was, for example, corroborated by Participant 2, who argued:

> I believe that the organisation should employ cybersecurity policy more strongly. If there is a presentation during the Officer Commanding period once a month, to indicate that there were seven violations on social media and counter-M should look at this to create that awareness on rules and order within cyberspace (Participant 2, senior military officer).

When analysing the extracted narrative produced by Participant 2, it became clear that the senior military officer was referring to violations within cyberspace and highlighting that the organisation should be more active in enforcing policies and

directives, which linked up with creating awareness of cyber threats. From an ST perspective, it is clear that elevating the threat has been identified. However, enforcing policies as a security measure has not yet been performed or accepted. This also highlights the argument that securitisation may occur over a long period, and not all actors and processes may occur logically.

Theme 2: Culture of digital security among officers

The theme addresses the culture of digital security among military officers. Cybersecurity awareness emerged as an important factor in constructing a digital-orientated organisation. The notion of a digital culture being linked to online awareness was evident from the narratives of Participant 1. This narrative described urgency relating to cybersecurity awareness as a challenge in the SANDF. In addition, urgency as a challenge was revealed specifically during the coding process, as the narratives indicated that there was a need for the organisation to improve and accelerate addressing cybersecurity. The relevant narratives of participants in this respect are captured in the following extracts:

> There is no level of awareness culture in the SANDF concerning cybersecurity. I would score cybersecurity it as a 4 out of 10, which is at its worst, because the majority of officers save DOD information on their personal USB sticks or email it to their personal accounts and do not worry about whether their emails are hacked (Participant 1, senior military officer).

The culture of digital security in the excerpt above showed that the participant considered the cybersecurity efforts made by the SANDF concerning. The application of security behaviour is also coming into question, as extremely limited information sharing practices were actively applied, thus reflecting how well digital technology is integrated into the everyday operational activities within the organisation.

Theme 3: Perception as an important aspect for senior military officers

The theme focused on perception and how military members felt about cybersecurity efforts made by the SANDF. Perception is an important factor in predicting reactions to certain events and a reflection on the behavioural response exhibited (Saban, Rau & Wood, 2021). It can be argued that there is a link between the security perceptions of users and the level of awareness that is displayed. When the perception of cybersecurity is low, the activity to secure information decreases. Thus, the researcher indicates that perception of cyber threats and attacks may have a role to play when employing security protocols. Furthermore, perceptions of certain issues in organisations may impact how employees respond to certain events. In addition, this perception may also infer to how employees respond to change, roles and developing social identities (Saban *et al*., 2021).

> Currently, yes, uhm, I don't think there is good control over it. There are people posting on the DOD web and there's undisciplined comments being made and stuff. So, I think it can be a big threat in general, and I do believe that most people are not very secure (d). We know about the dangers, but I don't think we are doing enough. I have the ability to access my phone and laptop with my thumb scanner, but now I am thinking I should have actually applied it and I haven't (Participant 2, senior military officer).

When analysing the qualitative extract from Participant 2, it is clear that there is extremely limited control over the information being shared on media sites. This view extends to the point where the senior military officer has little trust in fellow military members concerning security behaviour. Furthermore, it is also clear from the extract that security behaviour is not actively applied, and directives are not adhered to as military members post carelessly. Although the military officer is aware of the threat information, certain guidelines and best practices are not consistently followed in their application and employment. This view also extends to the ST, where the essence is that a

response needs to follow from threat verbalisation (speech-act). Therefore, speaking security and doing security, in this case, may not necessarily be applicable. However, the researcher adds that not all threats require an emergency response and for this reason, the haphazard application of guidelines and best practices might be sufficient, as the threat does not constitute an emergency measure.

Discussion

The discussion of this chapter starts with the statement that securitisation may take place over a long period and may or may not complete this process in some contexts (Bester, 2024). It is important to note that, historically, institutionalised security actors such as political institutions and military establishments may have more claim to ST than new actors entering the securitisation space. However, newer securitising actors may also challenge the established conceptualisations of security. The traditional view is that the armed forces are utilised to secure the interest of the state. It is often the state that may utilise the military as a response to a threat. This chapter included cyber threats as an emerging conceptualisation of ST. The newer or emerging conceptualisation of ST invites newer actors to challenge the current nuances about security and may challenge the status quo. It is important to note that not all facets of ST may be suitable in the context of cyber threats in the context of SA armed forces. This is because the researcher explored cybersecurity at the individual level and did not opt to view the elevation of cyber threats at a macro level, where the state and its actors are primary drivers for threat elevation and the deployment of security responses.

It is clear from the qualitative excerpts that the SANDF acknowledges that cyber threats are a serious security challenge. Furthermore, the participants also indicate that the perceptions of senior SA military officers of cybersecurity play an important part in how organisations view and respond to threats. It is worth stressing that the referent object in the case of ST takes on dual roles: (1) the SANDF as an organisation within the SA security cluster and (2) the senior military officer as the

human element. The reason for this duality is that the SANDF is an important actor within the SA security cluster, which is primarily responsible for maintaining national security and performing strategic operational activities that align itself to coordinating cybersecurity in the nation state (Van der Waag-Cowling, 2017; Republic of South Africa, 2015). Philipsen (2018) indicates that security actors must perform and speak security. The importance of the SA military officer takes on two positions in the securitisation process: (1) the senior SA military officer is accountable for the implementation of security measures as instructed by the organisation; (2) the senior SA military officer must announce cyber threats as a security challenge for the organisation and NS, and that emergency measures need to be implemented. The senior SA military officer takes on a very influential position, especially since senior ranking officers can inform decision-making and implement the directives used in the organisation to address security issues. The military officer generally takes on a role where they are accountable for executing plans and operations. This position corresponds with the concept of the securitising actor, which actively identifies and articulates the threat along with its associated risks. It is worth noting that the securitising actor does not necessarily have to be associated with the political elite or more influential decision makers. Philipsen (2018) indicates that new actors may intervene and challenge the traditional conceptualisations of security. However, these newer actors may still rely on established views of security.

Philipsen (2018) notes that to speak about security, one must capture the reality of the threat. The senior SA military officers indicated in their narratives that the threat of cyber-attacks is challenging and that they apply security behaviour. However, there is a dissonance in their perception of the elevation of cyber threats and the emergency response employed. The researcher notes that the element of power might be one of the deciding factors when distinguishing anyone to become a securitising actor. However, it is worth indicating that historically institutionalised actors are more established than emerging actors attempting to enter the

securitisation process. These historically institutionalised actors have power in the speech act, and their claim on legitimising threats is more accepted than newer actors. Furthermore, there are many referent objects that need to be protected through emergency responses. The researcher argues that while the state might be considered the referent object under the traditional perspective of ST due to its national interests and sovereignty, it is imperative to note that other referent objects may also require attention (Hirsch Ballin, Dijstelbloem & De Goede, 2020). Thus, the researcher believes that in the context of the SANDF and cybersecurity, additional layers of referent objects require survival. Due to cybersecurity being ephemeral and being integrated into people's daily lives, one cannot be fixed on the premise that cyber threats (non-traditional) may only threaten the state and its sovereignty. Newer actors entering the security debate may challenge existing elements of "what" and "who" constitute a referent object other than the state (Bester, 2023).

Conclusion

Cyber threats in the South African context are pervasive and challenges cyber sovereignty. The findings suggest that perceptions of cyber threats are important as they establish the legitimacy of securitisation. The result of the securitisation of cyber threats is cybersecurity. Cybersecurity does not just constitute the process of employing technical capabilities, it also includes applying best practices and guidelines. Education and training as an emergency response to threats should be ongoing and with the perspective that securitisation may occur over a prolonged period. ST denotes the process through which a normal threat transitions from the ordinary to existential, therefore acting as a threat to an individual's safety. Cyber threats have no boundaries, and their impact is often felt offline. Thus, the voice of the human factor remains an important element in the widened approach to ST, as it provides an alternative view of security conceptualisations. This chapter positioned cybersecurity within the wider ST security debate by arguing that SA senior military officers are valuable

actors within the securitisation process. The perceptions of cybersecurity prove to be a crucial factor when ascertaining the current process of how cyber threats are elevated and responded to. The perceptions of SA military officers also provided a snapshot into how cybersecurity, as a response to threats, is approached by the SANDF. However, in terms of the notion that threats need to be responded to rapidly, cybersecurity in the SANDF context has yet to be allocated a status that deems it fit as an emergency response to the rising threat level in the broader societal context. The chapter concludes by stressing that while cybersecurity is a non-traditional threat, the manner in which the securitising actor speaks and responds is in a peculiar position, which reflects the disconnect between the perceived impact of the threat and the actual resources allocated to indicate its level of importance.

Acknowledgements

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

References

Aldis, A., & Drent, M. E. 2008. *Common norms and good practices of civil-military relations in the EU*. Groningen: Harmonie Papers.

Ani, U.D., He, H., & Tiwari, A. 2019. Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, 21(1):2-35. https://doi.org/10.1108/JSIT-02-2018-0028

Ashenden, D. 2008. Information security management: A human challenge? *Information Security Technical Report*, 13, 195201. [Retrieved 18 October 2023] http://www.sis.pitt.edu/jjoshi/courses/IS2621/Spring2014/Paper1.pdf https://doi.org/10.1016/j.istr.2008.10.006

Aydindag, D. 2021. Copenhagen school and securitization of cyberspace in Turkey. *Propósitos y Representaciones*, 9(1):1-19. http://dx.doi.org/10.20511/pyr2021.v9nSPE1.e850

Bester, K. J. 2023. Exploring the perceptions and views on cybersecurity among South African military officers. Unpublished Doctoral dissertation. Stellenbosch: University of Stellenbosch. https://doi.org/10.1007/978-3-031-43059-6_15

Bester, K.J. 2024. Cybersecurity awareness from the perspective of the South African National Defence Force military officer. In: E. Jakaza, H. Mangeya & I. Mhute (eds). *Crisis and Disaster Management Communication in Sub-Saharan Africa*. 273-294. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-43059-6_15

Bote, D. 2019. *The South African national cyber security policy framework: A critical analysis*. Unpublished master's thesis. North West University.

Buzan, B. & Waever, O. 2003. *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511491252

Buzan, B., Waever, O. & De Wilde, J. 1998. *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner. https://doi.org/10.1515/9781685853808

Cavelty, M. & Egloff, F.J. 2021. Attribution and knowledge creation assemblages in cybersecurity politics. *Journal of Cybersecurity*. 7(1):1-12. https://doi.org/10.1093/cybsec/tyab002

Creswell, J.W. 2007. *Qualitative inquiry and research design: Choosing among five approaches.* 2nd edition. London: SAGE.

Dos Santos, M.C. 2018. Identity and discourse in securitisation theory. *Contexto Internacional*, 40(2):229-248. https://doi.org/10.1590/s0102-8529.2018400200003

Eroukhmanoff, C. 2018. Securitisation theory: An introduction. In: S. McGlinchey, R. Walters, & C. Scheinpflug (eds). *International relations theory*. Boston: E-International.

Floyd, R. 2020. Securitisation and the function of functional actors. *Critical Studies on Security,* 9(2):81-97. https//doi.org/10.1080/21624887.2020.1827590

Gazula, M.B. 2017. *Cyber warfare conflict analysis and case studies*. Unpublished master's thesis. Cambridge, MA: Massachusetts Institute of Technology.

Hama, H.H. 2017. State security, societal security, and human security. *Jadavpur Journal of International Relations,* 21(1):1-19. https://doi.org/10.1177/0973598417706591

Hansen, L. & Nissenbaum, H. 2009. Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53(4):1155-1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hlase, E. 2018. *The securitisation of cyberspace in South Africa: The tension between national security and civil liberties*. Unpublished master's thesis. Pretoria. University of Pretoria.

Hirsch Ballin, E., Dijstelbloem, H. & De Goede, P. 2020. The extension of the concept of security. In: E. Hirsch Ballin, H. Dijstelbloem, & P. De Goede (eds). *Security in an interconnected world: A strategic vision for defence policy*. New York: Springer Cham. 13-40. https://doi.org/10.1007/978-3-030-37606-2

Janse van Rensburg, W. 2019. Twenty years of democracy: An analysis of parliamentary oversight of the military in South Africa since 1994. Unpublished doctoral dissertation. Stellenbosch: Stellenbosch University.

Kolton, M. 2017. Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence. *Cyber Defence Review*, 2(1):119-154. [Retrieved 17 October 2023] http://www.jstor.org/stable/26267405

Krippendorff, K. 2004. *Content analysis: An introduction to its methodology*. Thousand Oaks, CA: SAGE.

Laerd Dissertation. 2012. *Purposive sampling*. [Retrieved 22 December 2022] https://dissertation.laerd.com/purposive-sampling.php#:~:text=Homogeneous%20sampling%20is%20a%20purposive,%2C%20occupation%2C%20etc

Letho, M. & Henselmann, G. 2020. Non-kinetic warfare: The new game changer in the battle space. In: B.K. Payne & H. Wu (eds). *Proceedings of the 15th International Conference on Cyber Warfare and Security*. Academic Conferences International. 316-325. https://doi.org/10.34190/ICCWS.20.033

Lucke, R. J. 2016. How securitization theory can benefit from psychology findings. Presented at: *ECPR General Conference*, Prague, Czech Republic. Panel: Advances in political psychology: methodological and theoretical contributions. 7-10 September. [Retrieved 21 August 2023] https://opus4.kobv.de/opus4-uni-passau/frontdoor/deliver/index/docId/621/file/Lucke_Robin_Securitization_Psychology.pdf

Martin, G. 2020. Uncontrolled use of social networks a security risk for the SANDF. *Defence Web*, 12 March. [Retrieved 11 December 2023] https://www.defenceweb.co.za/sa-defence/sa-defence-sa-defence/uncontrolled-use-of-social-networks-a-security-risk-for-the-sandf/

May, R. 1958. Contributions of Existential Psychotherapy. In R. May, E. Angel, & H.F. Ellenberger (Eds.), *Existence: A New Dimension in Psychiatry and Psychology* (pp. 37-91). Basic Books/Hachette Book Group. https://doi.org/10.1037/11321-002

McMahon, C. 2020. In defence of the human factor. *Frontiers in Psychology*, 11:1390. https://doi.org/10.3389/fpsyg.2020.01390

Mulazzani, F. & Sarcia, S.A. 2011. Cyber security on military deployed networks. Conference presentation at: *Third International Conference on Cyber Conflict.* Talinn, Estonia. [Retrieved 28 November 2023] https://ccdcoe.org/uploads/2018/10/CyberSecurityOnMilitaryDeployed Networks- Mulazzani-Sarcia.pdf

Philipsen, L. 2018. Performative securitization: From conditions of success to conditions of possibility. *Journal of International Relations and Development*, 23:39-163. https://doi.org/10.1057/s41268-018-0130-8

Rauf, A. 2019. *The importance of* [the] *human factor in cybersecurity.* [Abstract]. National University of Sciences and Technology. [Retrieved 17 January 2020] https://www.researchgate.net/publication/332539716_The_Importance_of_Human_Factor_in_Cybersecurity/citation/download

Republic of South Africa. 2022. *Department of Defence. Budget Vote 2022/23.* South African Government. [Retrieved 24 August 2023] https://www.gov.za/speeches/minister-thandi-modise-defence- dept-budget-vote-202223-24-may-2022-0000

Republic of South Africa. 2018. *Department of Defence. Budget Vote 2018/19.* South African Government. [Retrieved 27 July 2023] https://www.gov.za/speeches/minister-nosiviwe-mapisa-nqakula-defence-dept-budget-vote-201819-18-may-2018-0000

Republic of South Africa. 2015. *National Cybersecurity Policy Framework.* State Security Agency. South African Government. Pretoria: Government Printer.

Saban, K.A., Rau, S., & Wood, C. A. 2021. SME executives' perceptions and the information security preparedness model. *Information and Computer Security*, 29(2), 263-282. https://doi.org/10.1108/ICS-01-2020-0014

Sayler, K.M. 2020. *Artificial intelligence and national security.* Congressional Research Service Report. [Retrieved 29 March 2023] https://sgp.fas.org/crs/natsec/R45178.pdf

Schwarz, K.J. 2016. *The securitization of cyberspace through technification*. Unpublished master's thesis. Blacksburg, VA: Virginia Polytechnic Institute and State University.

Setia M.S. 2016. Methodology Series Module 3: Cross-sectional Studies. *Indian Journal of Dermatology*, 61(3):261-264. https://doi.org/10.4103/0019-5154.182410

Stritzel, H. 2007. Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations,* 13(3), 357-383. https://doi.org/10.1177/1354066107080128

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D. & Lepri, B. 2018. The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys,* 51(2), 1-27. http://doi.acm.org/ 10.1145/3172869

US Army Joint Chiefs of Staff. 2018. *Joint publication on cyber operations.* [Retrieved 10 March] https://wwwjcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Van der Waag-Cowling, N. 2017. South Africa and the cyber warfare threat: A strategic overview. *Civil–military cooperation and international collaboration in cyber operations*. Institute for Leadership and Strategic Studies: Symposium Monograph Series. Georgia, USA: University of North Georgia Press. [Retrieved 15 October 2023] https://web.ung.edu/media/university-press/ILSS%20Monograph%202017.pdf

Van Niekerk, B. 2017. An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, 20:113-132. https://doi.org/10.23962/10539/23573

Van Ooijen, M. 2020. Cyber securitization or cyberization of conflict? On the militarization of cyber security in Estonia. Unpublished master's thesis. Utrecht: Utrecht University.

Van't Wout, C. 2019. Develop and maintain a cybersecurity organisational culture. CSIR Research Space. Conference presentation at: *Fourteenth International Conference on Cyber Warfare and Security*. Stellenbosch, South Africa. 28 February–1 March. http://hdl.handle.net/10204/11345

Zukic, A. 2020. *Assessing the role of the military in national cybersecurity efforts*. Unpublished master's thesis. Fort Leavenworth, KS: U.S. Army Command and General Staff College.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. & Basim, H.N. 2020. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1):82–97. https://doi.org/10.1080/08874417.2020.1712269