Towards an Active Cyber Defence Framework for SMMEs in Developing Countries

Nombeko Ntingi, Jaco du Toit and Sebastian von Solms
Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa

nntingi@gmail.com
jacodt@uj.ac.za
basievs@uj.ac.za

Abstract: Small, medium, and micro enterprises (SMMEs) are obliged to adopt digital technologies to render services to their clients and remain competitive. The COVID-19 global crisis has accelerated the cyberfication of systems and services. The move to digital platforms has afforded SMMEs opportunities to offer their services to a broader geographical area. However, this has also presented opportunities for cybercriminals to invade the digital infrastructure. Adopting digital transformation has put SMMEs in a vulnerable position since they need to manage their cybersecurity while lacking the necessary skills and ICT infrastructure. The inability of SMMEs to defend themselves against cyberattacks compels them to outsource their security needs to external security service providers. These external security service providers offer security services based on a hierarchical operating model. Essential security services are offered at a lower level. If the paying clients require advanced security services, they may be provided as an add-on to the contractual agreement resulting in additional cost. This paper explores the active cyber defence (ACD) approach to enhance cybersecurity defence while minimising service costs. Therefore, the primary objective and outcome of this paper are to identify some of the essential drivers that will contribute towards developing the active cyber defence framework for SMMEs in developing countries. For purposes of clarity, essential drivers are the gaps highlighted during the literature review and will be referred to as "essential drivers" throughout the paper. The essential drivers, together with suggested recommendations, will be consolidated. The essential drivers were drawn from existing literature by going through peer-reviewed academic papers and company whitepapers. To achieve the primary objective, we need to establish whether SMMEs are utilising the services of external security service providers. The external security service providers will be referred to as "Security Operation Centre - SOC as a service" throughout the paper. The secondary objective of this paper is to determine whether SMMEs are utilising the SOC as a service and if they do, whether they realise value for money.

Keywords: SMMEs, Active Cyber Defence, Proactive, Artificial Intelligence, SOC as a Service, Security Service Provider

1. Introduction

According to a report conducted by Abbosh & Bissell (2019), organisations are more dependent on the digital economy and the internet than they have ever been in the last ten years. Large and small enterprises are obliged to adopt the digital economy to render their businesses efficiently and effectively to realise business value while expanding their client base. These enterprises are affected by cyber risks, such as reputational, financial, and regulatory consequences, irrespective of their sizes, geographical locations, or industries (Accenture/Poneman Institute, 2019). This is due to the ever-changing landscape of the cybersecurity domain. SMMEs are the softer target and easier to penetrate due to the inefficiency of their current cybersecurity defences (Weiss & Muegge, 2019). Cyber defenders face a huge task as they need to close all loopholes in ICT systems, whereas cybercriminals only need one weak point to penetrate through. It is not a myth that cybercriminals are always one step ahead of cyber defences and that cyber defences must always play catch-up. As cyberattacks become more sophisticated, more innovative, and proactive methods of hardening cyber defences are required.

When dealing with advanced or determined cybercriminals, such as state or state-sponsored attackers, the current passive cyber defence approaches are no longer enough, as they are just one part of the solution (Broeders, 2021). States and non-state organisations must bolster their defence mechanisms through proactive measures. One concept that nation-state and non-state organisations can use to complement passive cyber defences is Active Cyber Defence (ACD) (Burke, 2020).

This paper's primary objective is to identify some of the essential drivers that will contribute towards developing the active cyber defence framework for SMMEs within the same industry, in developing countries. To achieve the primary objective, we will also determine whether the SMMEs are utilising the SOC as a service and whether they are realising value for money.

The rest of the paper is organised as follows: Section 2 conceptualises active cyber defence. Section 3 gives background literature on the cybersecurity landscape of SMMEs in developing countries. Section 4 discusses the role of SMMEs in the economies of developing countries. Section 5 discusses the advanced cybersecurity solution –Security Operation Centres (SOCs), as implemented in large enterprises. Section 5 also discusses the

SOC as a service and highlights the SOC operating models. Section 6 discusses the optimisation of ACD using Artificial Intelligence (AI). Section 7 consolidates essential drivers that have been identified and suggest recommendations. Section 8 concludes the paper and highlights observations for future studies.

2. Conceptualisation of 'Active cyber defence'

In this section, we will briefly discuss the concept of active cyber defence (ACD) and its originality. According to Denning & Strawser (2017), ACD originates from the military or nation-state organisations, and it is derived from the active air and missile defence from the US Department of Defence. "Active air and missile defence is defined as the direct defensive action taken to destroy, nullify, or reduce the effectiveness of air and missile threats against friendly forces and assets" (Denning & Strawser, 2017).

The views on ACD are conflicting, with some scholars perceiving ACD as an intrusive concept that engages in hacking back. A comparative study on the US, Israeli and Germany states that ACD is an actively deployed countermeasure, with the countermeasures conducted during the ACD operations categorised as *defence with a twist, hack-back and persistent engagement and defending forward* (Herpig, Morgus & Sheniak, 2020). The *defence with a twist* countermeasure involves utilising defence security tools, with some tools having active and evasive capabilities (Herpig, *et al*., 2020). The *hack back* countermeasure involves using invasive tools to trace back the origins of the adversary with the intention of retaliating (Herpig, *et al*., 2020). The *persistent engagement and defending forward* involves using cyber capabilities to act even before the adversary attacks, disrupting the threat's capabilities from its source (Herpig*, et al*., 2020). From this comparative study, it can be deduced that ACD involves both offensive and defensive operations. However, Broeders (2021) defines active cyber defence as a concept that allows organisations to go beyond passive defences by implementing proactive cyber defence mechanisms for their own ICT networks. Organisations are not allowed to trace back where the cyberattack originated from or retaliate against cyber attackers beyond the perimeters of their own ICT networks (Broeders,2021).

As illustrated in Figure 1 below, by dotted lines on the active-defensive quadrant, the ACD falls on the active-defensive quadrant of the cyber counterintelligence (CCI) model (Ntingi, Duvenage, du Toit & von Solms, 2022). Even though the tools and techniques used to conduct activities of active cyber offence and active cyber defence are the same, active cyber defence aims to strengthen the cyber defences of an organisation rather than intrusive actions towards the adversaries (Duvenage, Jaquire & von Solms., 2020a; Ntingi, *et al*., 2022).

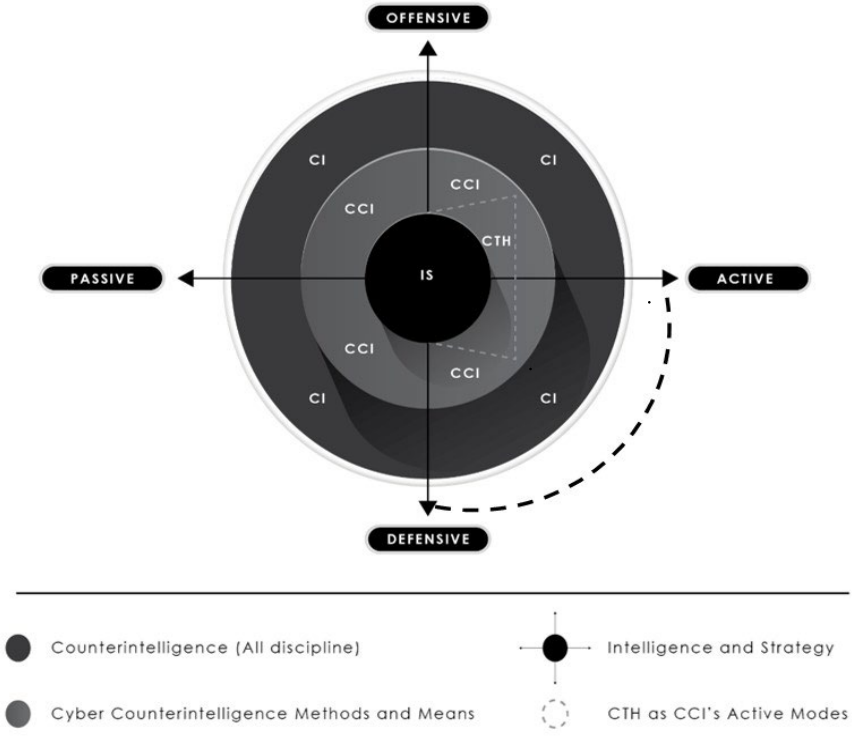

Figure 1: Cyber Threat Hunting as part of Cyber Counterintelligence (Ntingi, *et al*., 2022)

Our focus is on the cybersecurity operations of organisations, particularly SMMEs, to strengthen their cyber defences and actively defend their ICT systems without resorting to intrusive actions against adversaries.

Having discussed the active cyber defence concept, we will now discuss the cybersecurity landscape of developing countries.

3. Cybersecurity landscape of SMMEs in the developing countries

To be able to achieve the primary objective of the paper, which is to identify the essential drivers that will contribute towards the development of the active cyber defence framework, it is imperative that we foreground that with a brief discussion of the cybersecurity landscape of SMMEs in developing countries. This background information will highlight and strengthen the need to develop an ACD framework for SMMEs within the same industry, in developing countries. Organisations of all sizes, large and small, are taking advantage of the benefits that come with internet usage because it broadness the scope of service delivery. Digital transformation allows organisations to compete on a global scale and reduce the turnaround time of service delivery. According to a report by Verizon (2019), 43% of SMMEs in South Africa were victims of security breaches. A review conducted by Ncubukezi, Mwansa & Rocaries (2020) on SMMEs in the Western Cape, South Africa, states that SMMEs do not prioritise cybersecurity risk assessment and analysis. The review further states that there are no unanimous cybersecurity best practices across various industries (Ncubukezi, *et al*., 2020). Consequently, this leads to different cybersecurity approaches used to maintain cybersecurity hygiene (Ncubukezi, *et al*., 2020).

A study conducted on South African SMMEs by Kabanda Tanner & Kent (2018) reveals that the organisational internal factors, such as budget, management support, and attitudes, hinder the perception towards cybersecurity implementation. Consequently, these factors are regarded as impediments to implementing cybersecurity in SMMEs'environment (Kabanda *et al*., 2018). Additionally, SMMEs lack the know-how to identify cyber breaches, which causes delays in responding to cyber breaches, worsening the impact and adversely affecting business continuity.

While the cybersecurity state of SMMEs in developing countries is dire, a study by Mimecast (2022) reveals that organisations are becoming more aware of the need to implement and strengthen their cyber defences. There is a growing recognition that a lack of cyber preparedness is a major risk factor (Mimecast, 2022). 96% of the respondents reported that their organisations either already have or are developing cyber defence strategies (Mimecast, 2022).

The following subsection will group the essential drivers that were identified in this section.

3.1 Essential drivers identified in section 3.

These essential drivers are the identified challenges confronting SMMEs in developing countries. The essential drivers have been identified in section 3 above.

- Different cybersecurity approaches are used to maintain cybersecurity hygiene.
- Lack of financial resources.
- Limited or lack of advanced cybersecurity skillsets.

Flowing from the discussion, it is evident that even though SMMEs are willing to embrace cyber defences, there are still challenges confronting them, such as a limited budget and a lack of necessary skill sets to carry out cyber defence operations. The following section will discuss the role of SMMEs in the economies of developing countries.

4. The role of SMMEs in the economy of the developing countries

The role of SMMEs in the economies of developing countries cannot be understated. SMMEs are considered economic drivers and vehicles for job creation. Statistics South Africa, StatsSA (2019) estimated a labour force of about 14,7 million in the third quarter of 2020, with SMMEs accounting for approximately 45% of employment. Furthermore, SMMEs contributed 39% of the turnover of South Africa's gross domestic product (GDP) in the first quarter of 2019 (StatsSA, 2019). Additionally, SMMEs are part of the supply chain as they act as third-party contractors and provide services to large organisations. Considering the role of SMMEs in the economies of the countries, to stay competitive and relevant in the borderless economies and advancement of technology, they are compelled to embrace technology to offer their services efficiently to their clients. Adopting technology by SMMEs is a critical enabler in expanding business and client engagement. However, the adoption

of digital transformation brings with it cybersecurity challenges. While digital transformation has many benefits and opportunities in the ways in which organisations conduct their businesses, it also exposes them to significant cybersecurity risks.

The ever-changing landscape of the cybersecurity domain is faced with evolving cyber risks. The principal cyber risks that face organisations, as stated by the Institute of Risk Management (2014.), include business operational risk, reputational risk, and legal and compliance risk. SMMEs being part of the supply chain may present opportunities as the weakest link for cybercriminals to violate the supply chain and attack large organisations (de Vicente Mohino, Mallouli, Ruiz & van Haastrecht, 2021). Due to the exposure of SMMEs to cyberattacks, it is prevalent for SMMEs to adopt emerging proactive approaches towards the safeguarding of ICT infrastructure.

It is against this background that there is a need for SMMEs to implement and strengthen cyber defence technologies tailored to meet their specific needs. The following section will briefly discuss the technology solution, known as Security Operation Centres (SOCs), as currently implemented in large enterprises. The SMMEs can also adopt the SOC, but there is a need to adapt it to suit SMMEs' environments.

5. Security operation centres (SOCs) - as implemented in large enterprises

This section will briefly discuss the SOC as implemented in large enterprises. Furthermore, the SOC as a service and its operating models will be discussed. The concept of community SOC will also be introduced in subsection 5.3. Briefly, a community SOC concept services a group of companies in the same industry. The objective of this section is not to highlight all the SOC operating models but to highlight some of the models and find gaps that can be enhanced for the specific needs of SMMEs.

The SOC is defined as a centralised organisational unit whose primary functions are to continuously detect, analyse and respond to cybersecurity threats (Vielberth, Bohm, Fichtinger & Pernul, 2020; National Institute of Standards and Technology, 2018). Many organisations are building SOCs to combat the actions of adversaries. The function of the SOC is accomplished using a combination of people, technology, and processes (Vielberth, *et al*., 2020). SOCs in large enterprises can also implement advanced functions, such as threat hunting, incident analysis and response to highly sophisticated threats. These advanced functions are regarded as optional in the SOC environment due to their complexity and the high levels of expertise required (Kaspersky, 2019). SOCs are large and complex, necessitating large budgets, advanced skillsets, and advanced technologies. The SOC can either be operated internally within the organisation or externally through the SOC as a service. According to a survey conducted by Crowley & Pescatore (2018), enterprises that have built their own SOCs are confronted by various challenges in establishing well-run efficient SOCs. Some of the challenges include a lack of skilled staff, a lack of automation, a lack of integrated tools, and being overwhelmed by too many alerts (Crowley & Pescatore,2018). Due to SMMEs being just as vulnerable to cyberattacks as large enterprises and yet lack the necessary resources and skillsets to defend themselves against these cyberattacks, they are compelled to outsource security functions to SOC as a service (Weiss & Muegge,2019; Gupta & Zhdanov, 2012). Mihindu & Khosrow-shahi (2020) also asserts that with constraints confronting SMMEs, such as limited budget, SMMEs need a new and perhaps a different approach towards implementing cyber defences.

Having discussed the fundamentals of the SOC, we will now discuss the SOC as a service. The discussion will aid in establishing whether SMMEs fully utilise these cybersecurity services and, if not, highlight the factors that act as barriers to that.

5.1 SOC as a service

This section will briefly discuss the SOC as a service and highlight its operating models that can be adapted to better suit the cybersecurity needs of SMMEs in developing countries. According to Harrison (2020), to run a 24 x 7 SOC, organisations need to employ at least a minimum of 5 full-time professionals. Due to budgetary constraints and a lack of skills, enterprises, including large and small, have resorted to outsourcing their cybersecurity needs to third-party organisations. SOC as a service is, therefore, an answer to resource-constrained enterprises.

SOC as a service follows an operating model when delivering its services to its paying clients. In this section, we will discuss managed security service providers (MSSP) and managed detection and response providers (MDR) operating models. The role of these external service providers differs in how they offer their services to their paying clients. Both MSSPs and MDRs deliver security functions to their clients based on the contractual

agreement. According to TechTarget (2021), MSSPs often provide basic SOC services such as security management and monitoring services. This means that if a cybersecurity breach or intrusion is detected, the cybersecurity provider only alerts the client. Unless specified on the contractual agreement as an add-on, the advanced cybersecurity functions will be at an additional cost.

According to Zimmerman (2014); Vielberth, *et al*., (2020), the operating model is categorised into three tiers. The most basic services are offered at the first tier, with advanced cybersecurity services offered at the higher-level tiers. Red Canary Webinars (2022) also states that MSSPs offer their services using a tiered approach, with tier 1 services as basic services and tier 2 and 3 services being advanced security services offered at an additional cost. In contrast, MDRs are specialised services that offer more advanced and complex security functions to their paying clients (TechTarget, 2021). It is worth noting that the delivery of SOC services is scattered, hence a need for consolidation of the current operating models.

Now that we have discussed the operating model of the SOC as a service, in subsection 5.2, we will continue to address the secondary objective. In the interest of clarity, we will re-emphasise our secondary objective.

For us to be able to achieve this primary objective, we need to investigate the secondary objective.

- The secondary objective of this paper is to investigate whether SMMEs are utilising the SOC as a service and whether they realise value for money.

5.2 Utilisation of SOC as a service by the SMMEs

The aim of this section is to investigate the utilisation of SOC as a service by SMMEs and the challenges confronting them in optimally utilising SOC services. One of the challenges facing enterprises in implementing SOC as a service is that the service providers may use different security tools that cannot be integrated with each other (Kaspersky, 2019). Furthermore, these service providers might not support certain applications used in SMMEs. If the application is not part of the list supported by the external service provider, then SMMEs might have to consider procuring additional ICT infrastructure.

As mentioned in subsection 5.1, the delivery of SOC services is scattered. For enterprises to fully enjoy the benefits of SOC as a service, they may need to combine the services of MSSPs and MDRs to supplement the security functions of the other. Some functionalities offered by these services may be irrelevant to the needs of SMMEs and may therefore escalate the cost of cybersecurity implementation. For SOC as a service to deliver its services, some organisations might require significant changes in sourcing additional ICT infrastructure (Schatz, 2014). Organisations would be forced into "locked-in", resulting in rising costs of switching to other service providers, thereby compelling them to use the cybersecurity service providers even when their security needs are no longer met (Schatz, 2014).

The challenges mentioned in this subsection are some of the major impediments to SMMEs not utilising the

SOC as a service. It is for this reason that developing a community SOC framework for SMMEs in developing countries is imperative. Having highlighted the impediments to utilising SOC as a service, we will now introduce the concept of a community SOC.

5.3 Conceptualising a community SOC

In this section, we will introduce the concept of a community SOC. According to a survey conducted by Abbosh & Bissell (2019) on building trust in the digital economy, 86% of respondents thought that in the near future, a code of conduct for businesses in the same industry would be necessary to build resilience and foster trust among them. Based on this notion, developing a community SOC framework for SMMEs in the same industry would be feasible and assist in reducing the cost of implementing active cyber defences. The idea of a community SOC is to provide services to SMMEs from a specific community in the same industry and serve as a central and intermediate SOC that feeds into a higher-level SOC.

The UK government promotes the creation of community SOCs, termed Warning, Advice and Reporting Point (WARP), for public sector communities. The WARPs are made up of members that have a collective interest, such as the same business sector or geographical area. The responsibility of the WARPs is to act as a single point of contact and provide information security warnings and advice services to communities in the same industry (NLAWARP, 2018). For example, the defence industry WARP acts as a single point of contact for cyber incidents that pose risks, specifically to the Ministry of Defence. The critical cyber incidents are escalated from the local WARP to a higher-level cyber centre with advanced capacity (NLAWARP, 2018).

In South Africa, the National Cybersecurity Policy Framework (NCPF) recommends the establishment of relevant additional computer security response teams (CSIRTs) that will serve as a point of contact for that specific sector for cybersecurity matters, as well as coordinate cybersecurity incident response actions for that sector (State Security Agency, 2015). NCPF encourages collaboration and coordination among various stakeholders, including government agencies, the private sector and civil society. The community SOC framework for SMMEs can easily operate within the confines of the NCPF. Having highlighted the need for developing a community SOC, we will now highlight how artificial intelligence can be used to optimise the active cyber defences in the SMMEs' environment.

5.4 Essential ACD framework drivers identified in section 5.

The following essential drivers were identified in section 5 above.

- Lack of automation.
- SOCs are large and complex, necessitating large budgets, advanced skillsets, and advanced technologies.
- Lack of integrated tools, different security tools that cannot be integrated with each other.
- SOC professionals are overwhelmed by too many alerts.
- SOC services are scattered (MSSPs, MDRs), offering different services. For enterprises to fully enjoy the benefits of SOC as a service, they may need to combine the services of MSSPs and MDRs to supplement the security functions of the other resulting in escalating implementation costs.
- For SOC as a service to deliver its services, some organisations might require significant changes in sourcing additional ICT infrastructure.

6. Optimisation of ACD using Artificial Intelligence (AI)

In this section, we will look at how artificial intelligence (AI) can be used to optimise active cyber defence. Firstly, we will briefly discuss artificial intelligence in the context of cybersecurity. Our aim is to highlight how AI technology can be used to optimise active cyber defences in SMMEs' community SOC environment. Digital transformation with themes like digital sales, cloud computing, big data, or artificial intelligence is crucial for the innovative power and future competitiveness of most SMMEs (Lloyd, 2020). According to Burke (2020), SOCs rely on human expertise and specialised skills and knowledge to perform SOC functions. As already mentioned in the previous sections, most organisations and specifically the SMMEs, are unable to benefit from the SOC capabilities due to their limited or lack of advanced cybersecurity skillsets. This is where AI technology fits in in terms of automating complex processes.

AI, as defined by Vähäkainu & Lehto (2019), is the intelligence that is formed artificially to solve complex problems in computers. AI assists in automating complex processes to identify cyberattacks and to react to information system breaches. As the ACD concept aims to increase the automation within an enterprise to help strengthen cyber defences Burke (2020), AI can act as a problem solver in the automation of data processing and threat detection.

According to Burke (2020), the United Kingdom (UK) and the United States of America (USA) are among the countries that incorporate defensive AI technologies into their cybersecurity strategies. Duvenage, Jaquire & von Solms (2020b) state that the convergence of emerging technologies such as AI, the Internet of Things, Big Data, and social media is important in strengthening efforts to cybersecurity defences. Furthermore, Duvenage*, et al*., (2020b) also alludes that these technologies are not only useful for large organisations and nation-states but also for smaller organisations with limited resources.

As the number of cyberattacks grows, so are the costs of discovering the cyberattacks, and emerging technologies may be the answer to finding and reversing this trend. Accenture/Poneman Institute (2019) states that organisations should aim to implement technologies such as AI that reduce the rising costs of discovering a cyberattack. Organisations seek to gain a competitive edge in the market by implementing cyber defence solutions, while cyber threat actors are also actively seeking new ways of launching cyberattacks (Burke, 2020). AI has seen adoption within the cybersecurity domain and can be used for the automated detection and classification of malware and automated threat alerting on network traffic and endpoint data sources (Burke, 2020).

In the following section, we will consolidate the essential drivers that were identified in subsections 3.1, and 5.4.

7. Implications of essential drivers for the development of an active cyber defence framework

7.1 Gaps in the current operating models of SOC as a service

It is worth noting that the essential drivers highlighted in this section are not exhaustive, as the paper is part of an exploratory and ongoing research project. The challenges highlighted in the sections above contribute to the essential drivers necessary towards the building of an active cyber defence framework for SMMEs in developing countries. They will all be consolidated in this section. The essential drivers that will contribute towards the active cyber framework have been consolidated and are listed in Table 1 below. The recommendations will address the identified challenges confronting SMMEs in developing countries. These recommendations will form part of the requirements that can be implemented to develop the ACD community SOC framework.

Table 1: Essential drivers for active cyber defence framework for SMMEs in developing countries.

Essential driver/existing gap	Recommendations
• Different cybersecurity approaches are used to maintain cybersecurity hygiene.	• Develop a unanimous framework for SMMEs in the same industry. This framework will be termed a community SOC framework.
• Lack of financial resources.	• The community SOC framework will relieve the cost burden because the SMMEs will share the cost of implementing the cybersecurity defences.
• Limited or lack of advanced cybersecurity skillsets.	• The advanced skills will be shared across the SMMEs serving a particular community SOC.
• SOC services are scattered (MSSPs, MDRs), offering different services.	• Consolidate SOC services to minimise implementation costs.
• SOC as a service use different tools than those of SMMEs and might not be integrated into the SMMEs'environment.	• Propose a uniform technology for the community SOC. SMMEs in the same industry.
• SOC functions are human-intensive and require huge volumes of data. • Lack of automation, lack of integrated tools, and being overwhelmed by too many alerts. • Complex processes, analysts overwhelmed by too many alerts.	• Automation of data processing and threat detection through AI. Automation will aid in minimising the need for intensive human intervention and reduce the cost of implementation. • Propose essential cyber defence tools that can be integrated into a single platform. • Create universal use cases for the community SOC.

8. Conclusion

Several topics were discussed to achieve the objective of the paper. The following topics were covered: (2) conceptualisation of active cyber defence, (3) cybersecurity landscape of SMMEs in developing countries, (4) the role of SMMEs in developing countries' economies, (5) SOCs as implemented in large enterprises, and (6) optimisation of ACD using AI. The discussed topics, essential drivers and recommendations, viewed in combination, are essentially all factors that decisively influence the development of the ACD community SOC framework.

In concluding this paper, we propose incremental work that will ultimately complete the proposed active cyber defence community framework for SMMEs in developing countries. The proposed future work will detail how the recommendations will be implemented. The paper highlighted and consolidated the essential drivers needed to develop an ACD community framework. Our point of view is that SMMEs need not spend excessive amounts of money to be able to access active cyber defence technologies, nor should a limited budget hinder them from accessing these technologies. The SMMEs should be able to utilise these technologies and still be economically sustainable, hence the proposed solution for ACD community SOC for SMMEs. As far as this paper is concerned, it contributes towards a PhD project of an ACD community framework, that will be expanded on in future work.

References

Abbosh, O. & Bissell, K., 2019. *Securing the digital economy: Reinventing the Internet for Trust.* [Online]
Available at: https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf
[Accessed 08 01 2023].

Accenture/Poneman Institute, 2019. The Cost of Cybercrime. *Network Security,* 2019(3), pp. 4-4.

Broeders, D., 2021. Private active cyber defense and (international) cyber security—pushing the line?. *Journal of Cybersecurity,* 7(1).

Burke, A., 2020. *Robust artificial intelligence for active cyber defence.* [Online]
Available at: https://www.turing.ac.uk/sites/default/files/2020-08/public_ai_acd_techreport_final.pdf
[Accessed 06 01 2023].

Crowley, C. & Pescatore, J., 2018. *The Definition of SOC-cess? SANS 2018 Security Operations Center Survey.* [Online]
Available at: https://www.sans.org/white-papers/definition-soc-cess-sans-2018-security-operations-center-survey/
[Accessed 27 12 2022].

Crowley, C. & Pescatore, J., 2019. *Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey.* [Online]
Available at: https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf
[Accessed 10 10 2022].

Denning, D. E. & Strawser, B. J., 2017. Active Cyber Defense APPLYING AIR DEFENSE TO THE CYBER DOMAIN. In: G. Perkovich & A. Levite, eds. *Understanding cyber conflict: 14 analogies.* Washington, DC: Georgetown University Press, pp. 206-208.

Duvenage, P., Jaquire, V. & von Solms, S., 2020a. A Cyber Counterintelligence Matrix for Outsmarting Your Adversaries. *Journal of Information Warfare,* 19(1), pp. 1-10.

Duvenage, P., Jaquire, V. & von Solms, S., 2020b. *Cyber Counterintelligence: Some Contours towards the Academic Research Agenda.* Chester, Academic Conferences and Publishing International Limited.

Harrison, B., 2020. *What is a Security Operations Center (SOC)?.* [Online]
Available at: https://blog.cygilant.com/blog/what-is-a-security-operations-center-soc
[Accessed 06 01 2023].

Herpig, S., Morgus, R. & Sheniak, A., 2020. *Active Cyber Defense- A comparative study on US, Israeli and German approaches.* [Online]
Available at: https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf
[Accessed 07 12 2022].

Institute of Risk Management, 2014. *Cyber risk.* [Online]
Available at: https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf
[Accessed 06 01 2023].

Jaquire, V., Duvenage, P. & von Solms, S., 2021. *Some Cybersecurity Governance Imperatives in Securing the Fourth Industrial.* United Kingdom, Academic Conferences International Limited, pp. 187-194.

Kabanda, S., Tanner, M. & Kent, C., 2018. Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce,* 13 07, 28(3), pp. 269-282.

Kaspersky, 2019. *Barriers to an effective Security Operations Center.* [Online]
Available at: https://www.kaspersky.com/enterprise-security/security-operations-center-soc
[Accessed 27 12 2022].

Mihindu, S. & Khosrow-shahi, F., 2020. *Collaborative Visualisation embedded Cost-efficient, Virtualised Cyber Security Operations Centre.* Melbourne, IEEE.

Mimecast, 2022. *Confronting the new wave of cyberattacks: The State of Email Security 2022.* [Online]
Available at: www.mimecast.com
[Accessed 27 12 2022].

Ncubukezi, T., Mwansa, L. & Rocaries, F., 2020. *A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses.* s.l., IEEE Xplore.

Ntingi, N., Duvenage, P., du Toit, J. & von Solms, B., 2022. *Effective Cyber Threat Hunting: Where and how does it fit?.* Chester, Proceedings of the 21st European Conference on Cyber Warfare and Security, pp. 206-213.

Schatz, D., 2014. Thoughts on Managed Security Services Provider Engagement. *ISSA Journal,* pp. 26-31.

StatsSA, 2019. *How large is the small business footprint?.* [Online]
Available at: https://www.statssa.gov.za/?p=12264
[Accessed 11 12 2022].

Vähäkainu, P. & Lehto, M., 2019. *Artificial intelligence in the cyber security environment Artificial intelligence in the cyber security environment.* Stellenbosch, RSA, Proceedings of the 14th International Conference on Cyber Warfare and Security.

Verizon, 2019. *2019 DBIR: Summary of Findings.* [Online]
Available at: https://enterprise.verizon.com/resources/reports/dbir/2019/summary-offindings/
[Accessed 28 12 2022].

Vielberth, M., Bohm, F., Ines, F. & Pernul, G., 2020. *Security Operations Center: A Systematic Study and Open Challenges.* Regensburg, IEEE Access.

Weiss, M. & Muegge, S., 2019. Conceptualizing a New Domain Using Topic Modeling and Concept Mapping: A Case Study of Managed Security Services for Small Businesses. *Technology Innovation Management Review,* 9(8), pp. 55-64.