The Conceptualisation of a National Malware Intelligence Laboratory for South Africa

Wian Gertenbach, André McDonald, Mfundo Masango, Ele Mukondeleli, Ethan Buckinjohn, Rendani Mmbodi, Molebogeng Latakgomo, Ndabe Hhlongwane and Namosha Veerasamy
Council for Scientific and Industrial Research, Pretoria, South Africa

WGertenbach@csir.co.za
AMcdonald@csir.co.za
MMasango1@csir.co.za

Abstract: South Africa has become an increasingly attractive target for cybercriminals, with malware and ransomware attacks on critical national infrastructure and public institutions rising in both frequency and severity. High-profile incidents, such as ransomware attacks on Transnet, the Department of Justice, and the Government Employees Pension Fund (GEPF) highlight the scale of the threat. These attacks result in severe operational disruption and financial losses, often due to inadequate readiness and response mechanisms. This paper presents the conceptualisation of a national malware intelligence laboratory (NMIL) for South Africa, designed to strengthen domestic readiness and response to malware-related threats. A literature study was carried out to determine the main gaps. This was complemented by a stakeholder interview and questionnaire. This led to a gap analysis, and the examination of existing models as reference for the proposed design of the NMIL. This process not only identifies systemic weaknesses in the national cyber defence capabilities of South Africa but also evaluates how an NMIL could be integrated into existing national cybersecurity processes. The gap analysis revealed limited coordination of malware intelligence sharing across sectoral computer security incident response teams (CSIRTs), the potential to improve the ability of the National Cybersecurity Hub (CSHUB) to aggregate and disseminate actionable threat data, and insufficient hands-on exposure to malware in current cybersecurity education and training programs. In response, the paper introduces a framework and reference model that defines NMIL functions and its manner of integration into the national cybersecurity ecosystem. Specifically, the laboratory would provide high-quality malware intelligence to the CSHUB, including sample analysis results, threat profiling, and advisory support on removal tools, to improve effective response coordination. Additionally, the laboratory would offer access to a sandboxed training environment to educational institutions, thereby adding greater depth to cybersecurity education and promoting national cybersecurity readiness. The framework and reference model is developed using a systems engineering approach, to detail the NMIL's information flows, interfaces and functional domains. It is anticipated that the formal process resulting in conceptual laboratory provides a replicable approach for institutionalising national malware laboratories. This model offers both strategic and operational insights for South Africa as well as other developing countries.

Keywords: Malware analysis, Malware threat intelligence, Malware laboratory, Skills development

1. Introduction

In the last decade, malware attacks have evolved significantly in sophistication, resulting in a global influx of attacks on critical infrastructure and services. Emerging trends in the adoption of sophisticated criminal business models – particularly those leveraging affiliate distribution networks that function as a malware-as-a-service ecosystem – pose a significant threat to developing countries that lack adequate defence capabilities (Gajjar and Taherdoost, 2024). This threat is realised in South Africa, which faces an annual increase in malware attacks as criminals shift their focus more towards developing countries (Henrico and Els, 2025). A national survey conducted by the Council for Scientific Research (CSIR) in 2024 found that malware attacks were the most common incident type reported by South African organisations, accounting for 65% of incidents reported (Ngejane, 2024). Ransomware is especially prevalent, with attacks on South African public entities such as Transnet, the Department of Justice, and the Government Employees Pension Fund (GEPF) documented and publicised in the last five years (Greig, 2024; Moyo, 2024; Timcke et al., 2023). In a survey conducted by Sophos in 2025 on 154 South African organisations that were hit by ransomware in the previous year, 58% of respondents stated that the most common cause of attacks was a lack of expertise (Sophos, 2025). Interpol reported that ransomware remains one of the most prevalent forms of cybercrime across Africa, with South Africa ranking second in the number of ransomware threats detected in 2024 (Interpol, 2025).

Despite legislative advancements in South Africa such as the establishment of the Cybercrimes Act (Act 19 of 2020), and National Cybersecurity Hub (CSHUB), systemic gaps remain in malware threat intelligence sharing, malware analysis capacity, and the integration of hands-on training (Henrico and Els, 2025). These challenges signify the need for improved national malware threat intelligence, stronger national coordination, and investing in hands-on cybersecurity training to develop skills in digital forensics, malware analysis and open-source

intelligence (Interpol, 2025). To address these gaps, the paper introduces the conceptualisation of a South African national malware intelligence laboratory (NMIL) as a critical component in advancing domestic readiness against malware-related threats and a supportive capability that strengthens upstream defensive functions. A structured process was applied, using a cause-effect analysis informed by literature, inputs from academic and cybersecurity professionals through interviews and questionnaires, to identify the root causes of poor malware readiness. This led to the conceptualisation of a laboratory model to address these root causes.

The paper presents several contributions. The process through which the NMIL was conceptualised, as presented in section 2, is replicable and can be used in different scenarios. The gap analysis, presented in section 3, identifies specific gaps that arise within the South African cyber defence context and was used to conceptualise the proposed solution. In section 4, a framework that defines a solution (the NMIL) to address the gaps identified, as well as a reference model that serves as a blueprint for implementing and validating NMILs in general, is developed. Section 5 explains the limitations of the study as well as recommendations and future work.

2. Process for Conceptualisation of a National Malware Intelligence Laboratory

The conceptualisation of the NMIL requires a structured process to ensure that the proposed NMIL framework is evidence-based and addresses critical gaps that are contextually relevant in South Africa. The process combines theoretical perspectives on the state of domestic malware-related attacks, practical examples from international laboratory models that demonstrate clear benefits, and an examination of domestic realities through an interview and questionnaire. This approach ensures that the NMIL framework reflects international best practices while simultaneously remaining responsive and relevant to local challenges and constraints.

The first step involved a literature survey to understand the local need for addressing the increase in malware-related attacks and to identify critical gaps in domestic cybersecurity capabilities. Several sources were studied to ensure maximal coverage. Industry reports from cybersecurity vendors, academic publications, news articles, and reports by research organisations provided practical insight into the South African threat landscape and skills shortages. International technical architectures and implementation approaches for cybersecurity laboratories and malware analysis capabilities were studied to understand how other nations structure their malware intelligence capabilities and integrate them with existing cybersecurity frameworks. The review served to identify the need for a practical solution, like a national malware laboratory, to support malware intelligence sharing and analysis in national resilience, and how its functions may integrate into existing national computer security incident response teams (CSIRTs) and related institutions. This step provides the conceptual foundation to identify the functions that an NMIL should perform, specifically in the domains of malware threat intelligence sharing and addressing critical skills shortages. The outputs of the literature review were synthesised into a cause-effect diagram to visualise relationships between the root cause (malware-related incidents in the public sector) and underlying systemic gaps.

The cause-effect analysis led to the identification of two critical gaps that contribute to the country's struggling cyber resilience, namely the lack of relevant skills to address malware-related attacks, and ineffective coordination of malware threat intelligence sharing between sectoral CSIRTs. These gaps were explored in a gap analysis to fully understand their effects on national resilience. The gap analysis was supported by a questionnaire and interview with stakeholders across research institutions and academia. The goal was to obtain additional evidence – not publicly available form academic publications or articles – from industry experts who work closely with entities that play a role in threat intelligence sharing, as well as to understand the role of malware-related content in formal education. Although a broader set of stakeholder engagements were planned, only one in-depth interview and one academic questionnaire response were successfully completed during this phase. As the study was explorative and conceptual in nature, these engagements were treated as validation inputs rather than statistically representative samples.

The interview provided qualitative insight into operational challenges faced by national cybersecurity teams, specifically coordination between CSIRTs in the public sector and the lack of available malware analysis infrastructure. The academic response was used to confirm challenges related to malware content in higher education curriculums, specifically the lack of skilled lecturers and adequate infrastructure for practical training.

The structured process established a solid foundation to derive a suitable framework and reference model for a NMIL. The framework defines the functions of the NMIL that address the gaps identified. This includes the NMIL's core domains of operation to establish it as a technical, strategic, and educational hub. The reference model provides a system representation of the NMIL's inputs, processes, outputs, and information flows. The

framework together with the reference model serves as a blueprint for how the laboratory would interface with its stakeholders and integrate into South Africa's cybersecurity ecosystem.

3. Findings: Gap Analysis and Root Causes

The rise in successful malware-related breaches in the South African public sector can be attributed to various causes. During the gap analysis, various causes were identified and investigated. The most significant cause is the public sector's poor malware readiness posture (Siphambili et al., 2024). Evidence for this cause is the number of successful malware-related attacks on critical public entities in recent years. A few high-profile attacks that have occurred in recent years includes the City of Johannesburg, the Department of Justice, GEPF and Transnet (Moyo, 2024; Ngejane, 2024; Pieterse, 2021; Siphambili et al., 2024; Timcke et al., 2023). The reasons for these attacks vary per incident. Henrico and Els (2025) note that the main cause stems from systemic weaknesses and a lack of relevant skills to protect and respond to incidents. Section 3.1 explores the systemic weaknesses, evaluating the challenges faced by current systems and entities to combat malware-related attacks. Section 3.2 explores the reason why skills shortages in the malware analysis domain are a reality.

3.1 Intelligence Sharing and Infrastructure Gaps

An important question to consider is whether systems, processes and policies are already in place to prevent the rise of successful malware-related attacks, and whether they are adequate. As a central role player, the South African National CSHUB acts as an advisory to other sectoral CSIRTs to improve the effectiveness of incident response activities. The CSHUB is mandated under the National Cybersecurity Policy Framework (NCPF) to focus on collaboration with stakeholders in the public and private sectors to facilitate incident coordination, information dissemination, public cybersecurity awareness and the promotion of national standards (State Security Agency, 2015). Unfortunately, various challenges exist in this coordination plan. To uncover the specific reasons, the authors interviewed a key stakeholder of the CSHUB to provide insight into the current challenges it faces.

The most pressing challenge currently faced by the CSHUB and other CSIRTs is the effective distribution of local malware intelligence, according to (Ngobeni, 2025), the interviewee. Although infrastructure and standard operating procedures (SOPs) for threat intelligence sharing exist, their adoption is still in an immature phase. There is an overall reluctance from public and private institutions to participate in intelligence sharing, mainly due to the fear of reputational damage and competitiveness. As a result, current infrastructure and processes that facilitate intelligence sharing are not fully utilised, thereby leading to the neglect of sustained operations. Furthermore, there is insufficient integration of threat intelligence sources with the CSHUB, which hinders their ability to share critical information that may help to prevent malware-related incidents. Specific sources include findings from dark web monitoring, which is rich in unconventionally obtainable information and resources. This integration could greatly strengthen the CSHUB's position as a hub of proactive intelligence.

Ngobeni (2025) explains that South Africa's cybersecurity infrastructure is still at an infant stage, and official government support structures are inadequate to aid or resolve critical issues. This leads the departments to rely on weak internal IT support (this also points to a weak cybersecurity workforce) rather than robust incident response units. In incidents involving malware, other service providers are rather employed. However, their services are typically too costly for government departments, and security clearance requirements can also pose challenges. Additionally, there is a noted absence of adequate virtual infrastructure for testing and compliance, indicating current setups are insufficient for proactive malware handling or simulation. Overall, these issues are still neglected due to the NCPF being a non-binding policy rather than law, limiting enforcement and development of the necessary infrastructure and processes.

3.2 Skills and Educational Gaps

A critical factor contributing to South Africa's malware-readiness challenges is its increasing cybersecurity skills gap (de Jager et al., 2023). There is a significant lack of technical skills in cyber forensics and threat intelligence, especially under recently graduated individuals entering the workforce. Thomson et al. (2019) explain a few causes, including the insufficient integration of general cybersecurity education in undergraduate computer science curricula, a lack of educators specialised in cybersecurity, and a curriculum overload, which prevents the addition of more content. Practical, hands-on training is also not featured in most curriculums, as undergraduate programs focus mostly on theoretical concepts (de Jager et al., 2023). There is a shift in modern education to include more experimental and practical training for self-learning, which is currently lacking in tertiary education for cybersecurity-related topics (Steyn et al., 2021). A questionnaire was provided to experts in the educational field with the purpose of gaining additional input, (apart from the literature study), on the current level of

exposure that computer science and information technology students receive regarding cybersecurity, and especially malware concepts. The questions were designed to explore how academic programs address malware-related topics, how well students are prepared for real-world incidents, and what kind of institutional support could improve teaching and research in this domain.

The first question aimed to determine at what stage of tertiary education students are introduced to malware-related content, such as detection, analysis, and reverse engineering. The respondent indicated that such exposure typically occurs only at the Honours level and is limited to those who specifically choose a cybersecurity specialisation. This highlights that undergraduate programs lack the incorporation of cybersecurity topics, including malware, leaving most students without foundational knowledge in this area.

The second question assessed how effectively current curricula prepare students to deal with real-world cyber threats like ransomware and malware-as-a-service. The respondents noted that students are not sufficiently exposed to these advanced and evolving threat models. One of the main reasons cited was the difficulty in balancing a wide range of required topics within the Association for Computer Machinery (ACM)-aligned CS curriculum. This is strengthened by Thomson et al. (2019)'s findings on curriculum overload, and suggests that while institutions follow recognised guidelines, practical threat engagement is often exchanged for theoretical or foundational topics.

The third question focused on identifying the main skill gaps among graduates entering the cybersecurity workforce. The respondent revealed that the most pressing issue is the lack of real-world, hands-on experience. The current education model's focus is on breadth (broad, theoretical knowledge) over depth (practical, hands-on skills), leaving graduates unprepared for workplace demands (Manson and Pike, 2014). Graduates may understand theoretical concepts but often struggle to apply them in practical malware analysis or defence contexts, underscoring the need for experiential learning opportunities.

The fourth question explored the perceived value of integrating malware-related content into computer science curricula and asked for suggestions on how to effectively support this inclusion. The respondent mostly supported the idea, with one recommending the introduction of general malware knowledge at the undergraduate level and more advanced, practical work at the postgraduate level. There was an emphasis on the need for well-equipped laboratory environments where students can safely conduct malware analysis. The respondent also pointed to a shortage of qualified lecturers in this field, highlighting a broader capacity issue within academia. This challenge is highlighted by Thomson et al. (2019), who note that some computer science educators are not specialised in security, and may not have the necessary knowledge to effectively integrate and teach cybersecurity topics.

The final question inquired whether access to a national malware intelligence laboratory, with features like anonymised datasets, sandbox environments, expert guidance, and training resource, would add value to current curricula. The respondent agreed that such an initiative would directly address the current lack of suitable laboratory environments mentioned earlier. This indicates strong support for collaborative, centralised infrastructure that could enhance both education and research capabilities in malware analysis.

The questionnaire response and literature findings reveal a consistent theme: while there is academic interest in malware-related topics, exposure remains minimal, practical experience is limited, and institutional capacity is constrained. A national malware intelligence laboratory could therefore serve as a crucial bridge between theory and practice, equipping students and educators with the necessary tools, data, and expertise to become a capable workforce in South Africa.

3.3 Summary of Gaps

The gap analysis showed that various factors contribute to the country's struggle to combat malware-related attacks. Cybersecurity infrastructure and intelligence sharing processes are not optimised or utilised to its full potential, which ultimately results in private and public sector entities seeking solutions from external service providers. For government departments, this is a major challenge, as reliance on private service providers is often constrained by limited budgets, the confidential nature of projects, and the strict clearance requirements involved. The lack of specialised cybersecurity skills, particularly in incident response and malware analysis, leads to a decrease in readiness. Recently graduated cybersecurity practitioners often lack the practical knowledge needed to be applied to complex situations, which stems from the limited exposure to practical scenarios involving malware during their studies. In section 4 a solution is proposed that directly addresses the identified gaps in a framework that can be replicated by countries facing similar issues.

4. Proposed Framework: National Malware Intelligence Laboratory (NMIL)

The NMIL is conceptualised to address the identified gaps outlined in section 3. The gaps are classified in three groups, namely infrastructure and tooling gaps, intelligence sharing gaps, and skills and educational gaps. Table 1 shows a mapping of gaps to the direct NMIL response and its outcome. This structure helped guide the derivation of the NMIL's functional domains, which is based on a similar design described by Svajcer (2015). Although not addressing the same gaps as the NMIL, Svajcer (2015) explains the typical requirements for a malware laboratory, with emphasis on malware sample acquisition from diverse sources, analysis systems, and end-user systems. The NMIL follows a similar structure but includes an important intelligence generation function and educational system.

Table 1: Identified Gaps Mapped to the NMIL's Response and Expected Outcomes

Identified Gap	NMIL Response	Expected Outcome
Infrastructure and tooling gaps.		
Absence of virtualised infrastructure for tool testing and compliance.	Dedicated virtual environment where malware removal tools can be evaluated and developed to comply with national standards.	Capability to safely test and validate malware removal tools, ensuring readiness for real-world deployment.
Lack of hands-on malware analysis in prevention and response to public incidents.	Dedicated malware collection capability and sandbox environments for analysis.	Improved national capacity for malware research, enabling effective knowledge sharing.
Intelligence sharing gaps		
Lack of rich information sources.	Dark web monitoring and information gathering from various sources.	Broader and more comprehensive threat intelligence coverage, resulting in early threat detection.
Lack of specialised hardware to facilitate intelligence sharing.	Platform to process intelligence from a variety of sources and share it with the CSHUB to distribute to sectoral CSIRTs.	A robust intelligence processing system that enables efficient data correlation and dissemination among stakeholders.
Skills and educational gaps.		
Lack of practical training in universities.	Development of practical training material, in the form of laboratory scenarios.	Increased number of graduates with practical malware analysis experience.
Lack of access to infrastructure for practical training.	Provides universities with access to virtualised infrastructure to experiment and expose students to malware.	Improved access to specialised environments for students, lecturers and researchers to enhance skill development.

Existing malware laboratories—such as those operated by ANSSI (France), JPCERT/CC (Japan) and the United States Cybersecurity and Infrastructure Security Agency (CISA)—focus on technical analysis and indicators of compromise (IOC) dissemination within their national ecosystems. Academic labs address training or research functions separately. However, no existing models integrate malware intelligence, national coordination, and practical skills development in a manner tailored to South Africa's unique challenges. The NMIL therefore adapts international laboratory principles to address these specific national gaps.

In short, the NMIL would function as a technical hub for malware analysis and intelligence production as well as an educational hub for practical training and capacity building. Section 4.1 details the architecture of the reference model, which translates its functional domains into a system-level representation. Its integration with external systems is explained in section 4.2 , with information flows between systems clearly defined.

4.1 Conceptual Architecture

The NMIL operates in four key functional domains, namely malware collection, preservation and analysis, threat intelligence generation and sharing, education and training, and tool development and innovation. Figure 1

shows a diagram of the internal NMIL system and how the different functional domains interact with each other. Each functional domain consists of different sub-system modules that realise the goals of the NMIL.

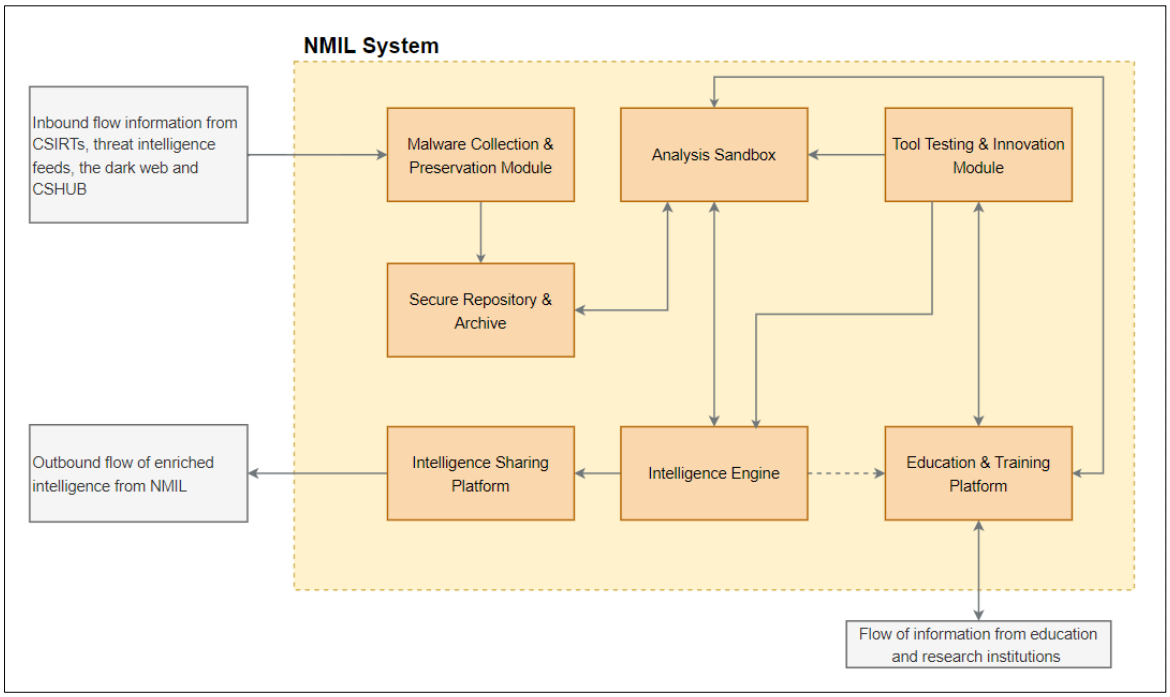

Figure 1: Internal NMIL System with Functional Domains

4.1.1 Malware collection, preservation and analysis

The NMIL is equipped with tools and hardware to collect, preserve and analyse malware, which ensures the acquisition and curation of malware samples from diverse sources, including the dark web, incident reports, the CSHUB, and international threat feeds. Collected samples are maintained in a secure repository with metadata describing their origin, behaviour, and IOCs. Analysis of these samples involve applying static and dynamic analysis techniques to dissect malware and understand its execution patterns, persistence mechanisms, and attack vectors. Through this process the NMIL generates technical insights in the form of analysis reports that enable the profiling malware to be used as actionable intelligence.

The Malware Collection and Preservation Module's main responsibility is to gather, register, label, and prepare inbound malware samples for secure storage and future use. Each incoming sample is assigned a unique identifier and labelled with essential metadata, including its type, hash value, origin, timestamp and source. This process ensures sample traceability from the point of origin and establishes a digital record of provenance and chain of custody for forensics and analysis purposes. A typical requirement for malware laboratories is the ability to collect malware as soon as it is located publicly or on the dark web (Svajcer, 2015). This module interfaces with the dark web and constantly monitors and scrapes information and malware samples to be processed by the NMIL. Registered samples are transmitted to the Secure Repository and Archive to maintain a catalogue of all collected samples. Transmission takes place over a secure data exchange channel to ensure that all content is isolated from other segments of the NMIL network. This prevents potentially dangerous artifacts from compromising the integrity of the NMIL. The repository enforces strict access and transfer protocols to prevent unauthorized handling or accidental exposure.

The repository interfaces directly with the Analysis Sandbox. The sandbox is an isolated, virtual environment designed to safely execute and observe malware behaviour without risking contamination of other sub-systems. It allows the simulation of different reproducible virtual environments to monitor malware behaviour in specific scenarios. This is ideal for testing new and existing malware removal and defence tools, which are developed and documented in the Tool Testing and Innovation Module. The sandbox is equipped with the necessary tools to perform static, dynamic, and code analysis. Analysts and researchers, with the required access rights, can copy samples from the repository to the sandbox to run experiments, test tools, perform research and return structured behavioural reports back to the repository once analysis is complete. Analysis results and reports also

feed into the Intelligence Engine, where observed tactics, techniques and procedures (TTPs) are mapped against frameworks such as MITRE ATT&CK (Svajcer, 2015).

The sandbox also interfaces with the Education and Training Platform. This allows access for registered students and instructors to experiment with malware practically without the risk of compromising their personal computers or equipment. The sandbox's function is thus twofold: To provide an operational environment to generate technical results for critical stakeholders, and to provide an experimental and learning environment where researchers and students can freely test, learn, and teach the principle of malware analysis.

4.1.2 Threat intelligence generation and sharing

This domain is responsible for the generation and sharing of actionable intelligence. The Intelligence Engine is responsible for the translation of technical findings from the Analysis Sandbox – such as behavioural indicators, IOCs and TTPs – into actionable insights by applying correlation, enrichment, and classification techniques to derive meaningful insights. The main goal of this module is to ensure that intelligence is operationally useful to security practitioners and NMIL stakeholders. Once validated, the refined intelligence is shared through the Intelligence Sharing Platform, ensuring secure transmission to external entities.

The Tool Testing and Innovation Module interacts with the Intelligence Engine by providing performance data and detection insights from various security tools – existing and custom developed – tested within the NMIL's environment. The Intelligence Engine processes these findings into actionable information, which can be shared to stakeholders in the form of tool recommendations.

Specific results processed by the Intelligence Engine are shared with the Education and Training Platform to be integrated with training material. In Figure 1, this interface is denoted with a dotted line and is one-directional. This means that the Education and Training Platform cannot access the Intelligence Engine directly. The Intelligence Engine shares information on a case-to-case basis, as some intelligence might be sensitive. As such, only specifically curated information is shared with the Training and Education Platform.

4.1.3 Support for education and training

The NMIL facilitates practical, hands-on knowledge transfer and training through its Education and Training Platform. It offers universities and academic institutions access to the Analysis Sandbox to support practical skills capacity building. The platform hosts various educational material developed from technical analysis findings, intelligence generation (carefully curated not to reveal sensitive stakeholder information), and tool experimentation, which is made available to educational institutions through university lectures and as online resources.

Additionally, research outputs are generated by the NMIL and published, facilitating academic collaboration. Leveraging real-world malware data and samples, the NMIL becomes a desired platform for experimental learning and a capable workforce development.

4.1.4 Tool experimentation, development and innovation

The sandboxed nature of the NMIL allows for experimentation with various malware removal and endpoint detection and response tools. Insights gained from testing these tools can be presented to stakeholders in the form of consultations. The Tool Testing and Innovation Module facilitates this capability and allows the research and development of new and existing malware prevention, removal and defence tools. It interfaces with the sandbox to allow the deployment of these tools in different scenarios. Documentation and tool-readiness reports feed into the Intelligence Engine, providing strategic insights to external entities on tool usage and deployment. The Tool Testing and Innovation Module also interfaces with the Education and Training Platform to allow students to experiment and learn how to use and develop industry-grade tools.

4.2 Data and Intelligence Flows

The diagram in Figure 2 illustrates the interaction and information flow between the NMIL and its key stakeholders in the South African cybersecurity landscape. At the centre, the NMIL System acts as the hub for malware intelligence generation and knowledge sharing. It interfaces with several external systems – its stakeholders – and facilitates the flow of information to and from the different systems.

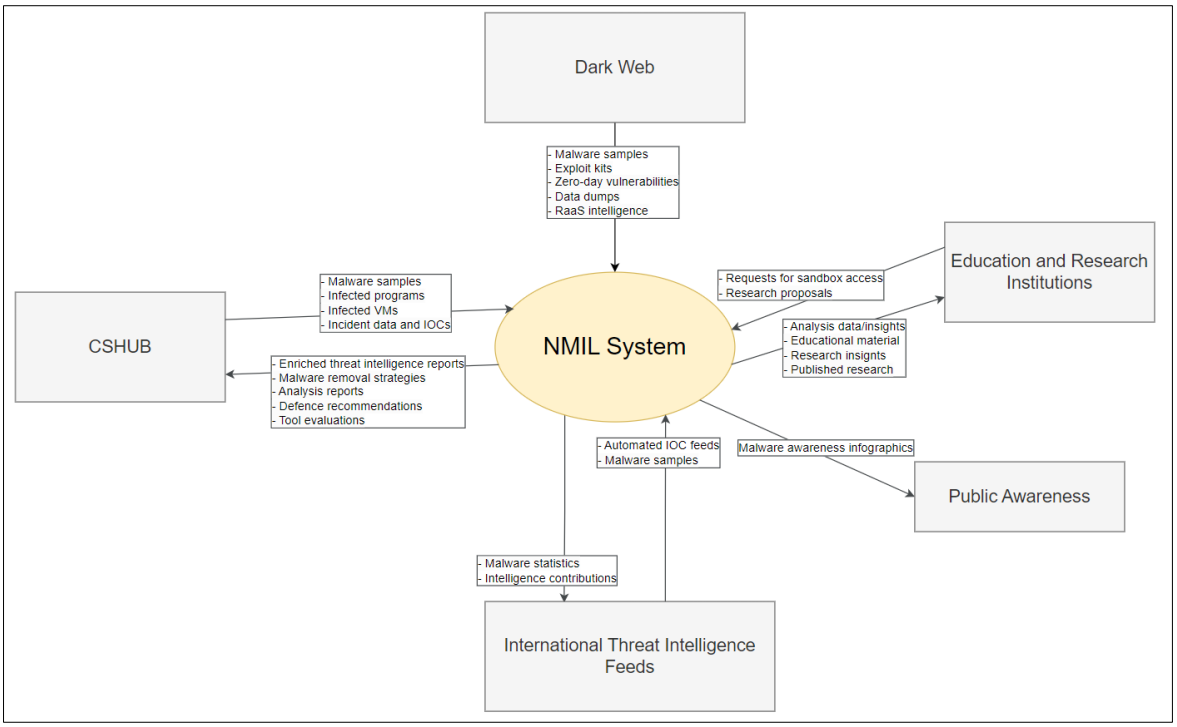

Figure 2: National Malware Intelligence Laboratory System Context Diagram

While the NMIL is not designed to function as a Security Operations Centre (SOC), its outputs naturally align with the higher-tier analytical functions commonly found in SOC structures. In a tiered SOC model, Tier 1 and Tier 2 teams typically perform alert monitoring, initial triage, and basic investigation (Cassetto, 2025). More advanced malware reverse engineering, deep-dive incident reconstruction, and threat intelligence correlation activities are performed by Tier 3 teams. In this context, the NMIL should be viewed as a national-level extension of Tier 3 analytical capability, rather than an operational SOC service. When organisations or sectoral CSIRTs escalate complex malware-related incidents that exceed their internal capacity, NMIL provides specialised analysis, tooling insights, and enriched intelligence. This positioning ensures the NMIL complements—rather than replaces—existing SOC and CSIRT functions, by supplying advanced technical outputs that feed back into frontline operational teams and national coordination structures such as the CSHUB.

The NMIL's interface with the CSHUB is bidirectional. It receives malware samples, infected programs and virtual machines (VMs), and incident data, which is then processed internally through its modules and platforms (see Figure 1) to produce actionable outputs. These elements can also be obtained from other sources, such as international threat intelligence feeds or dark web intelligence. The NMIL provides the CSHUB with enriched malware intelligence, removal and defence strategies, analysis reports, and tool evaluation results. This can then be used by the CSHUB to share with its own stakeholders (the sectoral CSIRTs), to fulfil its role in the national cybersecurity ecosystem.

The Dark Web acts as a source of threat intelligence, providing the NMIL with critical inputs which include malware samples, exploit kits, zero-day vulnerabilities, data dumps, and general information on the developments of ransomware-as-a-service. This information feeds into the NMIL for analysis and enrichment. Enriched intelligence is distributed to other systems such as the CSHUB and international threat intelligence feeds.

Education and Research Institutions interact with NMIL through requests for sandbox access, learning material and research proposals, enabling academic collaboration and experimental research on malware behaviour. In turn, NMIL shares analysis data and insights, learning material, research findings, and published papers, fostering a knowledge-sharing ecosystem that supports cybersecurity education and innovation. Knowledge-sharing is also enabled by the NMIL's interaction with the public. The NMIL produces malware awareness infographics for the public based on current threat trends and intelligence findings from international feeds and the dark web. This helps inform the public and organisations about emerging threats and best practices for protection.

The International Threat Intelligence Feeds component represents NMIL's external integration with global cybersecurity networks. NMIL provides malware statistics and intelligence contributions to international partners, while receiving automated IOC feeds and malware samples in return. This ensures South Africa's participation in the broader global cyber intelligence community, promoting mutual threat detection and prevention.

5. Limitations and Future Work

The findings presented in this paper are exploratory and primarily conceptual. Stakeholder input was based on one practitioner interview and one academic response, which limits generalisability of the results. However, these engagements provided valuable first-hand confirmation of the infrastructure, educational and information sharing gaps identified in the literature. The proposed NMIL framework should therefore be viewed as a proof-of-concept model grounded in initial evidence.

Future work will focus on system development and pilot integration with the CSHUB to assess its operational feasibility. Performance metrics will be defined to evaluate the NMIL's effectiveness. Further stakeholder engagement, particularly with educational institutions and the CSHUB, will support the NMIL's alignment with the national cybersecurity objectives and its integration into higher education for sustainable skills development.

6. Conclusion

This paper conceptualised a national malware intelligence laboratory (NMIL) for South Africa to address growing malware-related threats. A structured process was used by combining a literature review, a cause-effect analysis and limited stakeholder interaction to identify two key gaps in the South African cybersecurity landscape: insufficient malware analysis infrastructure and weak intelligence sharing, alongside limited exposure to practical training in computer science curricula.

The proposed NMIL integrates four functional domains: malware collection, preservation and analysis; threat intelligence generation and sharing; education and training; tool development and validation. These functional domains address the identified gaps through enhanced intelligence sharing mechanisms with the CSHUB and by developing a capable workforce through access to sandboxed training environments.

As a conceptual framework and model, the NMIL provides a replicable blueprint for enhancing cyber defence capabilities in other developing countries. Future work will focus on pilot implementation, expanded stakeholder engagement, and performance evaluation metrics to validate its operational and educational effectiveness.

Ethics Declaration: No ethical clearance was required for the completion of research activities mentioned in this paper.

AI Usage Declaration: Generative artificial intelligence (AI), specifically large language models (LLMs), were used to enhance writing, fix grammatical issues and provide summaries of literature for dissemination of information. No tools were used to write original content. AI tools used to aid the writing process include ChatGPT and Claude.

References

Cassetto, O., 2025. SOC Analyst Tier 1 vs. Tier 2 vs. Tier 3: Key Differences & Responsibilities [WWW Document]. Radiant Security.

de Jager, M., Futcher, L., Thomson, K.-L., 2023. An Investigation into the Cybersecurity Skills Gap in South Africa. In: Human Aspects of Information Security and Assurance, IFIP Advances in Information and Communication Technology. Springer, Cham, pp. 237–248.

Gajjar, V.R., Taherdoost, H., 2024. Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies. In: Proceedings - 2024 5th International Conference on Mobile Computing and Sustainable Informatics, ICMCSI 2024. Institute of Electrical and Electronics Engineers Inc., pp. 668–676.

Greig, J., 2024. LockBit takes credit for February shutdown of South African pension fund [WWW Document]. The Record.

Henrico, S., Els, S., 2025. Cyber Attacks in South Africa: Geopolitical and legal implications. African Security Review 1–25.

Interpol, 2025. Interpol Africa Cyberthreat Assessment Report 2025.

Manson, D., Pike, R., 2014. The case for depth in cybersecurity education. ACM Inroads 5, 47–52.

Moyo, A., 2024. Justice department suffers another cyber attack [WWW Document]. ITWeb. URL https://www.itweb.co.za/article/justice-department-suffers-another-cyber-attack/rW1xLv5nJkx7Rk6m (accessed 9.15.25).

Ngejane, H., 2024. DATA BREACHES IN SOUTH AFRICA: SURVEY REPORT.

Ngobeni, S., 2025. Interview by W. Gertenbach. Unpublished interview conducted in Pretoria on 25 August 2025.

Pieterse, H., 2021. The Cyber Threat Landscape in South Africa: A 10-Year Review. The African Journal of Information and Communication 28, 1–21.

Siphambili, N., Mahlasela, O., Baloyi, E., Mukondeleli, E., 2024. A Review of the South African Public Sector's Capability in Combating Ransomware. In: 2024 4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC). IEEE, pp. 493–499.

Sophos, 2025. The State of Ransomware in South Africa 2025.

State Security Agency, 2015. The National Cybersecurity Policy Framework.

Steyn, A.A., Botha, A.J.M., Coetzee, D., Villiers, M. de, 2021. Interactive Learning: Introducing a First-Year Systems' Analysis and Design Course. pp. 171–186.

Svajcer, V., 2015. Building a Malware Lab in the Age of Big Data. In: 25th Virus Bulletin International Conference. Prague.

Thomson, K.-L., Futcher, L.A., Gomana, L., 2019. Towards a framework for the integration of information security into undergraduate computing curricula. South African Journal of Higher Education 33.

Timcke, S., Gaffley, M., Rens, A., 2023. The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. The African Journal of Information and Communication (AJIC) 1–28