Advancing cybersecurity capabilities for South African organisations through R&D

Zubeida Casmod Khan and Nenekazi Nokuthala Penelope Mkuzangwe

Council for Scientific and Industrial Research, Pretoria, South Africa

zdawood@csir.co.za

nmkuzangwe@csir.co.za

1 Abstract

There is a growth of cyber-attacks in South Africa. Seeing that there are over 38 million Internet users in South Africa, this is no surprise. The South African government has published the National Cybersecurity Policy Framework (NCPF) and Protection of Personal Information Act (POPIA) to move towards mitigating cyber threats due to the increase of the presence of South African organisations and citizens in cyber space. This demonstrates that there is a need for organisations to have a clear roadmap to implement and improve on their own cybersecurity capabilities. South African organisations need to take a proactive stance in cybersecurity because businesses rely heavily on technology for day-to-day operations. Currently cyber-attacks cost South African organisations over R2 billion, and the current work-from-home arrangement that most organisations have implemented will only worsen the situation. While a cybersecurity roadmap will differ in every organisation based on the organisation's vision, goals, and objectives, along with their information technology (IT) and operations technology (OT), a starting point is perhaps the identification of key research and development (R&D) areas together with key activities that organisations can focus on in order to improve their cybersecurity capabilities. Cybersecurity capabilities are tools that organisations use to strengthen their organisation and protect themselves from potential cyber threats. The purpose of this study was to investigate R&D areas that organisations should invest in for the purpose of improving their cybersecurity capabilities. There are various subfields in cybersecurity that can be explored for organisations to advance their cybersecurity capabilities. Five integral R&D dimensions were identified together with key activities and are presented and discussed. A conceptual framework is also presented which maps the R&D dimensions and activities to the main pillars of cybersecurity, i.e., People, Processes, and Technology. South African organisations could reference the framework and adapt it for their business needs to protect themselves against potential cyber threats.

Keywords: cybersecurity, cyber threat, cybersecurity capability, cyber-attack, research and development.

2 Introduction

Since the COVID-19 pandemic, many professionals are working from home, which has resulted in the growth of cyber-attacks at an alarming rate. In South Africa, critical infrastructure such as its rail, port and pipeline company, Transnet, has been targeted in an act of cyber warfare (Slabbert and Peyper, 2021). Most organisations have systems with data that are connected to the Internet which opens avenues for cybercrime. The cybersecurity statistics of South Africa demonstrate that most organisations have not been able to protect their computer systems. Kaspersky announced that South Africa faced millions of cyber-attacks in 2020 (Kaspersky, 2020).

It is essential that organisations protect themselves from such threats as there is an increased presence in cyber space with cybersecurity. To do this, cybersecurity capabilities need to be developed or improved. The problem is that organisations are unclear on how to enhance their cybersecurity capabilities. The importance of enhancing cyber capabilities is emphasised by the Employment and Labour minister of South Africa, Thulas Nxes, stating that the South African government plans to also ramp up its cybersecurity capabilities following the cyber-attack on Transnet (Business Tech, 2021). While the South African government has promulgated the National Cybersecurity Policy Framework (NCPF) and Protection of Personal Information Act (POPIA), there has not been a national cybersecurity strategy, highlighting key research and development (R&D) activities that need to be investigated to strengthen cybersecurity capabilities.

To solve this problem of insufficient cybersecurity capabilities for organisations, the researchers aim to investigate the cybersecurity capabilities that other countries have invested in, and to categorise these

capabilities in a theoretical framework, together with key activities. This is elucidated in a cybersecurity capability R&D framework.

The remainder of the paper is structured as follows. Section 3 provides an outline of work on cybersecurity R&D areas other countries focus on to strength their cybersecurity capabilities while Section 4 introduces the R&D dimensions which have been categorized. Section 5 presents the R&D framework, and the work is concluded in Section 6.

3 Related Works

This section presents existing literature on the cybersecurity research and development areas that are proposed to enhance cybersecurity capabilities in other countries. According to Di Franco (Franco, 2018), there is a need for multi-disciplinary research in modelling and designing future system in order to make them more easily understandable. This will assist with understanding how people adopt and use new technologies and how risks are perceived in digital space (Franco, 2018). The output of this research will address the rapid societal change and risks brought by the digital transformation (Franco, 2018). Another challenge recognised by the work (Franco, 2018) is those associated with the shortage of cybersecurity experts; this roots from issues at a curriculum level. Other noteworthy cybersecurity R&D areas recognised by the work of Di Franco (Franco, 2018) include Artificial Intelligence (AI), and Quantum Technology. AI techniques are expected to enhance cybersecurity by either automating certain routine tasks or assisting human system managers to monitor, analyse, detect and respond to adversarial threats to cyber systems (Institute for Information Infrastructure Protection, 2003) (Whitehouse, 2016).The impact of quantum technologies in security can be divided into those technologies that can defeat the existing data encryption systems and those that can provide secure communication that is resistant to quantum computing attacks (Franco, 2018). According to (ID Quantique, 2020), a technology that can protect from both classical and quantum computing attacks is well suited for protecting national security communication.

In addition to the aforementioned key R&D areas identified by Di Franco (Franco, 2018), the Federal Cybersecurity Research and Development Strategic Plan (Whitehouse, 2016) identifies trustworthy distributed digital infrastructure (TDDI), privacy, and secure hardware and software as priority points. TDDI is an important element in promoting the growth of new industries that will help drive a nation's economic growth (Whitehouse, 2016). TDDI will enable the distribution of computing to new network edge, acceleration of the roll-out of next generation telecommunication and information communications infrastructure such as Fifth-Generation and post Fifth-Generation wireless networks (Whitehouse, 2016). Cybersecurity aspects of privacy involves protecting the collection, disclosure, and use of an individual's private information, including identity; patterns of behaviour; and economic, social, or other discriminators (Whitehouse, 2016). Secure hardware and software enable the development of resilient and survivable cyber capabilities (Whitehouse, 2016).

Wireless networks include not only wireless telecommunications but a diverse set of end devices such as sensors, process controllers, and information appliances for home and business users and domain specific networks, such as vehicular communication networks and sensor networks; has been listed as one of the key research areas as there are many security concerns with it (Institute for Information Infrastructure Protection, 2003). Other R&D areas identified (Institute for Information Infrastructure Protection, 2003) include metrics and models, and Law, Policy, and Economic Issues, and digital forensics. Digital forensic assists with uncovering what happened during the cyber-attack, that is, how the incident happened, who did it, how to respond to it and how to stop it from happening in the future (DRS, 2018). This can help in building threat intelligence database, etc. (DRS, 2018). Therefore, (National Research Foundation: Singapore, 2021) suggests that applied research should be conducted for acquiring digital evidence and forensics in order to reduce the analysis time required to comprehensively locate and evaluate digital evidence in diverse, disperse and multi-tenanted systems.

Other cybersecurity measures that exist in literature include cyber-threat information and intelligence, network security protocols and cybersecurity governance. Cyber-threat information and intelligence is about indicators (system artifacts or observables associated with an attack), tactics, techniques, and procedures, security alerts, threat intelligence reports and recommended security tool configurations can help an organisation to identify, assess, monitor, and respond to cyber-threats (Johnson, Feldman and Witte, 2017). Where threat intelligence is threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes. Sharing cyber threat information with other organisations gives an organisation access to knowledge, experience and capabilities of the other organisations and helps the organisation gain a more complete understanding of the threats the organisation may face (Johnson, Feldman and Witte, 2017). Using this knowledge, an organisation can make threat-

informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies (Johnson, Feldman and Witte, 2017).

Network security protocols preserve the security and integrity of the data over a network. Different methodologies, techniques, and processes are involved in these protocols to secure the network data from any illegitimate attempt to review or extract actual data content (Reddy, 2020).

To establish and maintain effective cybersecurity governance program, (Swinton and Hedges, 2019) suggests that organizations should clearly define risk management policies, strategy, and goals and ensure that standardised processes are repeatable. Furthermore, (Swinton and Hedges, 2019) suggests that cybersecurity governance should be measurable and enforced so that there is accountability for compliance across all personnel levels. The organisations should ensure that senior leadership remains engaged for the lifecycle of the cybersecurity governance program and adequate resources are available to meet the organisation's basic cybersecurity governance and compliance needs (Swinton and Hedges, 2019).

4 Exploring R&D dimensions

Following the literature overview in the previous section, key R&D areas were identified and defined as dimensions. The selected R&D dimensions can be used to enhance organisations' cyber defence capabilities to address emerging cybersecurity risks. Recommendation activities are grouped together for each R&D dimension. The following sections provide the identified R&D areas to focus on.

4.1 Cybersecurity governance

This refers to the set of people, processes, and tools that are used to ensure that cyber risks are mitigated in an organisation. It is vital that organisations have a framework for how to deal with both attempted and successful cyber-attack. This framework must explain how an organisation can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks. The framework can be used as a tool for aligning policies, business, and technological approaches to manage the cybersecurity risks (National Institute of Standards, 2014).

The framework also enables organisations to describe their current cybersecurity posture and target state of cybersecurity, identify, and prioritise opportunities for improvement within the context of a continuous and repeatable process, assess progress toward the target state and communicate cybersecurity risks to internal and external stakeholders (National Institute of Standards, 2014).

As organisations are moving towards the use automation technologies to enhance their functionality, this may introduce new/unknown operational risks and design security vulnerabilities associated with these technologies, which may lead to cybersecurity risks. This calls for research into the understanding of both operational, vulnerabilities, and cybersecurity risks associated with using these technologies. It further requires redefining cybersecurity governance in order to accommodate the handling of the risks associated with using automation technologies (Deloitte, 2019) . In order to establish and maintain effective cybersecurity governance the following R&D recommendations are made:

- Research on how to develop a cybersecurity framework for managing cybersecurity risks (e.g., investigate best practice cybersecurity frameworks such as the NIST framework).
- Research on risks associated with adopting automation technology, operational, design, and cybersecurity related frameworks.
- Develop a cybersecurity framework that is aligned to the organisation's business drivers and security considerations that are specific to the use of the organisation's technology (both manual and automated).

4.2 Cybersecurity enabling techniques and technologies

Technologies, specifically those that enable good cybersecurity, need to be adapted for organisational use. In this R&D area we group together the following techniques and technologies: Artificial Intelligence (AI), Quantum Information Science (QIS), Trustworthy Distributed Digital Infrastructure (TDDI), secure hardware and software and vulnerability investigation technologies, secure communication, network protocols, wireless network security and remote, access security.

AI: AI can enhance cyber-attack deterrence, protection, detection, and response (Whitehouse, 2016). Furthermore, AI/ML can be used not only as a defensive measure in the context of cyber warfare but as an offensive tool also (Cummings, 2017). However, the adoption of AI is subjected to the challenges which include the reasoning and outcomes of AI algorithms/techniques being not understandable which may lead to incorrect

decisions, attacks on AI algorithms, etc (Institute for Information Infrastructure Protection, 2003). Therefore, the following R&D recommendations are made:

- Investigate the AI based technologies that can be used in the context of cybersecurity/cyber warfare (cyber-attack monitoring, deterrence, protection, detection, response, and as an offensive tool).
- Invest on meeting the requirements associated with the deployment of these technologies that include obtaining big datasets for training and testing the technologies, high computing machines for the implementation of these technologies and big data storage that is secure.
- Research on gaining understanding of attacks against these technologies and tools to protect these technologies from those attacks (Whitehouse, 2016).
- Research onto the risks associated with adopting these technologies and how they can be mitigated.
- Investigate legal and ethical issues associated with employing AI in cyber warfare.
- Implement AI technologies to monitor, analyse, detect, and respond to adversarial threats to cyber systems. This is typically used for external threats.
- Develop methodologies to validate and interpret results from AI systems against human perceptions and expectations (Institute for Information Infrastructure Protection, 2003).
- Develop definitions, models, and metrics of security and trust that can be used to evaluate AI cybersecurity systems and AI-based cybersecurity controls (Whitehouse, 2016).

QIS: QIS can enhance protection from cyber-attacks (Whitehouse, 2016). Quantum technologies can provide secure communication that is resistant to quantum computing attacks and promise to achieve a higher level of security than classical computing limits (Whitehouse, 2016). However, it can also be used to defeat existing data encryption systems (Whitehouse, 2016). Therefore, understanding quantum capabilities and finding ways to overcome their fundamental limits is vital (Whitehouse, 2016). The following R&D recommendations are made:

- Conducting research to gain understanding of which quantum technologies exists, how they can be used to enhance cybersecurity and their vulnerabilities and adoption.
- Investigate the deployment requirements of such technologies.
- Investigate the cybersecurity risks associated with using such technologies and how they can be mitigated.
- If such home-grown technologies cannot be obtained, partner with home companies/organisations that can conduct R&D of those technologies, their deployment requirements and cybersecurity risks and mitigations.

TDDI: TDDI assists in facilitating next-generation telecommunications and information communications infrastructure such as 5G wireless network, IoT etc (Institute for Information Infrastructure Protection, 2003). These technologies are part of the fourth industrial revolution (4IR) technologies and since the 4IR technologies are being increasingly used, it is at the best interest of organisations and countries to start preparing for the adoption of these technologies. Therefore, in order to prepare for the adoption of these technologies, the following R&D recommendations are made:

- The starting point for adoption of the relevant 4IR technologies is to conduct research to gain understanding of the distributed digital infrastructure that is needed to enable the deployment of the relevant 4IR technologies.
- Research into gaining understand of which 4IR technologies are relevant to the organisation's business.
- Research to gain understanding of the operation and deployment of the infrastructure and technologies.
- Research to gain understanding of security risks that are associated with the infrastructure and technologies and ways to mitigate those risks.

Secure Hardware and Software and Vulnerability Investigation Technologies: Secure hardware and software to enhance the protective and detective aspect of cybersecurity (Whitehouse, 2016). However, hardware, firmware, and software tend to have design defects that present security vulnerabilities (Whitehouse, 2016). Therefore, the following research recommendations are made:

- Develop mechanisms and tools that verify the security properties of hardware before its deployed (Institute for Information Infrastructure Protection, 2003).
- The development of security solutions to patch vulnerabilities and prevent unauthorised program modification in order to protect against future attacks.
- Investigate technologies for investigating system vulnerabilities, discovering unauthorised hardware modifications and unauthorised programs and obtain them through R&D if not available (ATLA, 2020).
- Obtain/develop system vulnerability investigation personnel.

- Conduct research to gain understanding of penetration testing methods and their implementation or recruit penetration testing professionals to implement penetration testing or train some employees to become penetration testers through courses/workshops.

Network Security Protocols: Network security protocols play an important part in protecting network traffic both in wired and wireless networks. These protocols use encryption and authentication to protect these networks. Traditional encryption algorithms tend to be heavy for wireless devices such as sensors (ID Quantique, 2020). Encryption can be broken by quantum computing attacks. This means, there is a need for developing encryption/data protection algorithms/techniques that are suitable for use on wireless devices and resistant to quantum computing attacks. Therefore, the following recommendations are made in order to enhance network security protocols functionality:

- Investigate and develop quantum computing resistant encryption algorithms that can be used in the protocols.
- Investigate and develop encryption algorithms or data protection algorithms that are appropriate to be used with wireless network devices.

Wireless Network Security: The adoption of wireless network technologies/devices is growing among organisations. According to (Institute for Information Infrastructure Protection, 2003), some of these devices tend to have limited power, processing, storage etc., that limit their security capabilities. Furthermore, security solutions for wired networks may not be usable in wireless networks due to the unfair differences between these network systems capabilities (Institute for Information Infrastructure Protection, 2003). Therefore, the following research recommendations are made in order to enhance wireless security capability of an organization:

- Research and develop security solutions for an organisation's wireless networks that include vulnerability investigation of their wireless systems.
- Investigate traffic monitoring and analysis technologies to gain an understanding of the state of the network.

4.3 Cybersecurity capacity building

To put cybersecurity into practice, an organisation needs experts on the topic, whether they are hired or outsourced. To achieve this capacity in terms of cybersecurity experts, the following R&D recommendations are made:

- Hire or outsource diverse postgraduate graduates and computer science researchers.
- Hire or outsource employees with cybersecurity skills and certifications based on the gaps determined during the skills audit.
- Identify private and public entities that can enable the development of novel research and technology.
- Identify cybersecurity institutions for training staff members.

4.4 Cyber threat intelligence

This is of the utmost importance to determine the components of the organisation's software system that needs to be protected and the type of security threats to protect the component against attacks. Cyber-attacks are continuously increasing in frequency and sophistication and this presents significant challenges for organisations that must defend their data and systems from capable threat actors (Johnson *et al.*, 2016).

Joining cyber threat information and intelligence sharing communities helps the organisation to gain understanding of threats that it can face. The knowledge obtained from sharing can be used to make threat-informed decisions regarding defence capabilities, threat detection techniques and mitigation strategies (Johnson *et al.*, 2016). Researchers recommends the use of standardised data representation formats (e.g., Structured Threat Information Expression (STIX)) and transport protocols (e.g., Trusted Automated Exchange of Intelligence Information (TAXII)) to make the sharing of cyber-threat information and intelligence easier (Johnson *et al.*, 2016). Data representation formats provide a reporting structure and language that can be used to capture descriptions of threats. Transport protocols are mechanisms/protocols for the transportation of threat information/intelligence.

Organisations need to join cyber-threat information and intelligence sharing communities and invest in technologies that enable cyber-threat information and intelligence sharing and the personnel to operate these technologies. Recommendations for keeping up to date with existing and new cyber threats are as follows:

- Determining the components of a system that needs to be protected and the type of security threats to protect the component against.

- Implementing cyber threat analysis training.
- Investigate existing local and international cyber threat information sharing communities.
- Joining cyber-threat information and intelligence sharing communities (locally, South African Cyber Hub and internationally) that are of relevance to the domain of the business.
- Obtaining technologies that enable automated cyber-threat information and intelligence sharing.
- Investigating and adopting the data representation formats and transport protocols used by these sharing communities.
- Securing personnel to work/operate these technologies. The adoption of standardised data formats and transport protocol will require a capable workforce.

4.5 Cybersecurity awareness building

People are at the centre of successful cybersecurity at an organisation. However, people typically think of cybersecurity as an isolated IT office problem, or something that is difficult to achieve (Institute for Information Infrastructure Protection, 2003). This indicates that there is a need to empower employees/citizens with the knowledge and a sense of shared responsibility to practice safe and informed behaviours in the cyberspace (Franco, 2018). At an organisation level, the following recommendations are made in order to educate employees to practice safe and informed behaviours in the cyberspace:

- Conduct cybercrime awareness and prevention campaigns. Enforce these campaigns and training at all levels of an organisation from top to bottom level, i.e., from the CEO to the intern level.
- Conduct periodic training across the organisation using a combination of eLearning, workshops, policy rollouts, simulated phishing emails, blogs, social media posts, articles, risk assessments, and surveys.
- Participation in cyber games by employees. According to (Awojana and Chou, 2019), game based learning allows learners to actively learn and practise the right way things should be done, while having fun. This approach leads to effectiveness on cybersecurity awareness training and practical skill acquisition for learners from diverse backgrounds.
- Investigating local and international cyber conferences for attendance and participation. Invest in allowing employees to attend cyber conferences such as Black Hat[1].
- Identify organisations to develop technologies and tools for cybersecurity awareness.

5 R&D Framework

The dimensions with tasks explored in the aforementioned section are used to drive the R&D framework. The framework, shown in Figure 1, is built upon the three pillars of cybersecurity, i.e., People, Processes, and Technology (PPT) which is harmonised to deliver a holistic approach to drive cybersecurity R&D.

People is all about the personnel involved in cybersecurity R&D. This involves employees, training institutions, communication mechanisms etc. Processes encompasses the rules, regulations, frameworks, campaigns etc. that the R&D dimensions relate to, while technology involves the systems, applications, hardware, software, etc. that are relate to the R&D. Each pillar of PPT are closely related to each other and each have an important role to play for organisations' cyber security. Organisations are encouraged to look at the pillars, i.e., PPT and implement the key activities for each pillar to ensure adequate security.

In the following sections, each pillar is introduced, together with its goal, and key activities. The key activities are devised from summarising the R&D recommendations from Section 4 and mapping it to a pillar (i.e., PPT).

5.1 People

Every employee of an organisation has a role to play in terms of cyber security. People need to partake in several tasks and activities to ensure effective cyber security of an organisation. Thus, the main goal for this pillar is: *to prepare people in an organisation by training and other human-centric, interactive activities to ensure that an organisation's IT systems are secure.* Therefore, this pillar is linked to the **cybersecurity awareness, cyber threat intelligence,** and **cybersecurity capacity building** R&D dimensions of the framework. The activities associated with these R&D dimensions that can be adopted in this pillar are as follows:

- Identify organisations to provide tools and technologies for cyber security awareness training.
- Invest in and implement cyber security awareness training, cyber security campaigns and game participation.
- Identify private and public institutions to collaborate with the organisation to build capacity.

[1] https://www.blackhat.com/us-21/

- Identify cyber security training institutions where the personnel can be trained or up skilled since training is an on-going activity as cyber security progresses and criminals use sophisticated and novel attacks to gain access to organisations.
- Invest in and implement cyber threat intelligence training or secure personnel to perform cyber threat intelligence. This includes hiring computer science graduates as well as hiring experience individuals and outsourcing if needed.

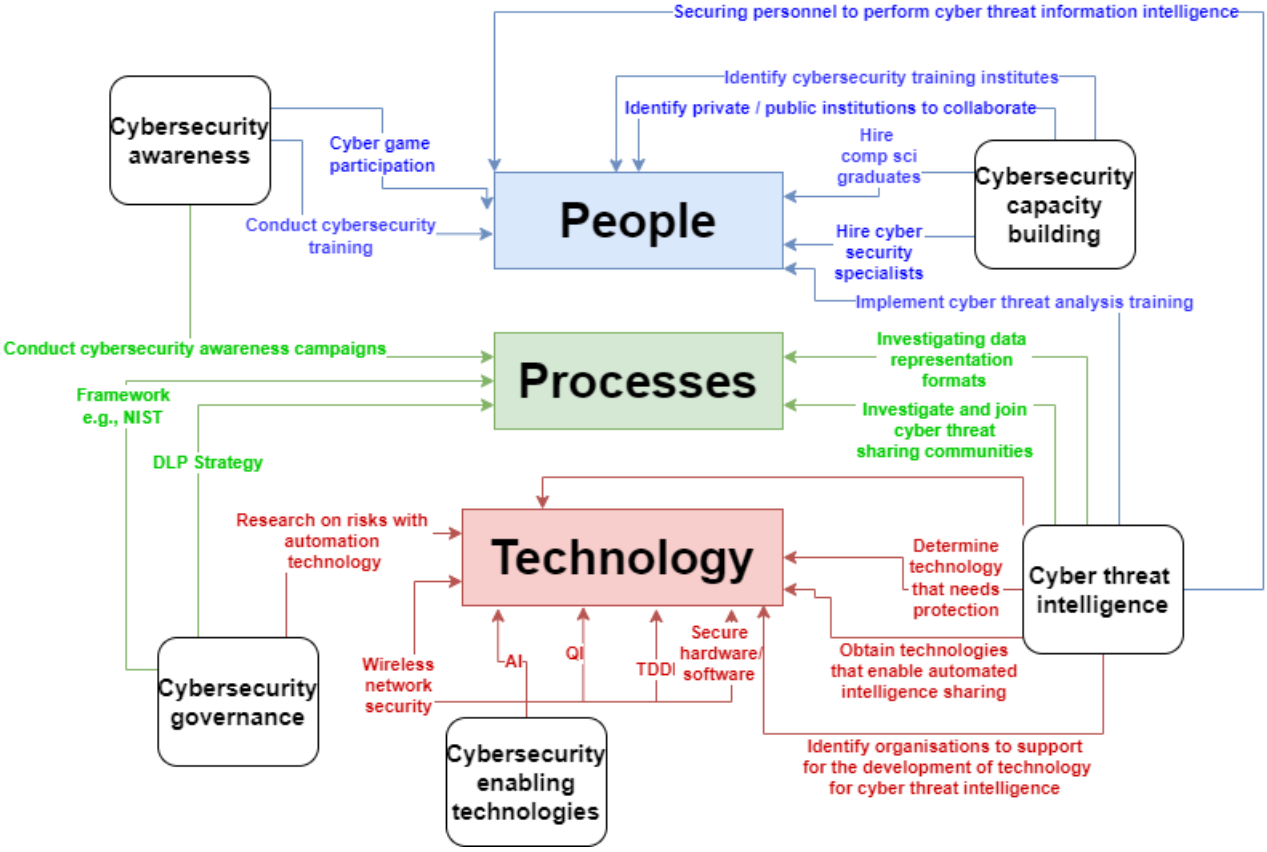

Figure 1: R&D framework for cybersecurity capabilities for organisations.

5.2 Processes

Processes are steps that need to be taken to ensure cyber security and protection of an organisation. This involves the policies, procedures and other practises that should be taken by an organisation. The main goal that organisations should seek for this pillar is: *"to continuously adapt and improve information security processes to ensure adequate response to security incidents and reduce cyber risk."* This pillar is linked to **cybersecurity governance**, and **cyber threat intelligence** R&D dimensions of the framework.

The activities associated with these R&D dimensions that can be adopted in this pillar are as follows:

- The development and implementation of cyber security awareness training, cyber security campaigns and game participation plans.
- The development and implementation of cyber security frameworks e.g., NIST.
- Implement DLP processes to protect sensitive information of the organisation.
- Investigate and join cyber threat sharing communities that can be joined to share intelligence.
- Investigate data representation formats and transport protocols used by cyber threat intelligence sharing communities.

5.3 Technology

Technology is used by people to automate processes to enforce cyber security for an organisation. The main goal that organisations should seek for this pillar is: *"to utilise cyber security technologies to ensure the confidentiality, integrity, and availability of organisational data."* This pillar is linked to **cybersecurity**

governance, **cyber enabling technologies** and **cyber threat intelligence** R&D dimensions of the framework.

The activities associated with these R&D dimensions that can be adopted in this pillar are as follows:

- To perform research on risks associated with adopting automation technology.
- To implement AI technologies to monitor, analyse, detect and respond to adversarial threats to cyber systems.
- To implement technologies that enables information sharing for cyber security threats.
- To use secure hardware and secure software to enhance the security of the organisation's technology.
- To determine the technology that needs to be protected.
- TDDI and QIS are not widely used in most information systems yet, but organisations should monitor technology for when there are operational as it will change the nature of cyberattacks.
- Implement software security solutions for the organisations' wireless networks.
- Identify private and public institutions that can enable and support for the development of research and technology for cyber threat intelligence tailored to the organisation at hand.

6 Conclusion

The increase in cybersecurity breaches in South Africa demands for organisations to equip themselves for protection. While the South African government has recently promulgated the NCPF and POPIA, a national strategy has not been published. This could cause organisations to be indifferent to cybersecurity measures that need to be taken to protect themselves. To solve this problem, the researchers have explored cybersecurity R&D areas of other counties and categorised these as dimensions with task recommendations. This has been conceptualised and the researchers presented a R&D framework for cybersecurity capabilities built upon the PPT pillars of cybersecurity. Organisations can now adopt this R&D framework for business needs towards achieving cybersecurity.

The proposed framework opens a plethora of avenues for future research. It would be beneficial to create strategies for certain types of organisations, i.e., the telecommunications industry, electricity industry etc. which would enable various sectors to further protect themselves.

7 References

ATLA (2020) *R&D Vision Toward the Realization of a Multi-Domain Defense Force and Beyond Explanatory Documentation*. Available at: https://www.mod.go.jp/atla/en/policy/pdf/rd_vision_full.pdf (Accessed: 17 February 2021).

Awojana, T. and Chou, T.-S. (2019) 'Overview of Learning Cybersecurity Through Game Based Systems', in *Proceeding of the 2019 Conference for Industry and Education Collaboration, CIEC 2019*. New Orleans, LA: Advances in Engineering Education.

Business Tech (2021) 'South Africa building database of security specialists as it recovers from major cyber attack', *Busuness Tech*, August. Available at: https://businesstech.co.za/news/it-services/510640/south-africa-building-database-of-security-specialists-as-it-recovers-from-major-cyber-attack/ (Accessed: 23 November 2021).

Cummings, M. 'Missy' L. (2017) *Artificial Intelligence and the Future of Warfare*. Available at: https://www.chathamhouse.org/publication/artificial-intelligence-and-future-warfare (Accessed: 11 October 2018).

Deloitte (2019) *Future of Risk in the Digital Era | Deloitte US*. Available at: https://www2.deloitte.com/us/en/pages/advisory/articles/risk-in-the-digital-era.html (Accessed: 19 November 2021).

DRS (2018) *The importance of digital forensics in cyber security*, *DRS*. Available at: https://www.drs.co.za/the-importance-of-digital-forensics-in-cyber-security/ (Accessed: 22 February 2021).

Franco, F. Di (2018) *Analysis of the European R&D priorities in cybersecurity Strategic priorities in cybersecurity for a safer Europe*. Available at: https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity/at_download/fullReport.

ID Quantique (2020) *The impact of quantum technology on national security - ID Quantique*, *ID Quantique*. Available at: https://www.idquantique.com/the-impact-of-quantum-technology-on-national-security/

(Accessed: 17 February 2021).

Institute for Information Infrastructure Protection (2003) *CYBER SECURITY RESEARCH AND DEVELOPMENT AGENDA*. Available at: https://web.stanford.edu/class/msande91si/www-spr04/readings/week8/2003_Cyber_Security_RD_Agenda.pdf (Accessed: 22 February 2021).

Johnson, C. *et al.* (2016) *NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing*. doi: 10.6028/NIST.SP.800-150.

Johnson, C., Feldman, L. and Witte, G. (2017) *ITL BULLETIN FOR MAY 2017 CYBER-THREAT INTELLIGENCE AND INFORMATION SHARING*. Available at: https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2017-05.pdf (Accessed: 22 February 2021).

Kaspersky (2020) 'South Africa, Kenya and Nigeria saw Millions of Cyber Attacks in 2020 and the Year is not over yet', *Africa newsroom*, September. Available at: https://kaspersky.africa-newsroom.com/press/south-africa-kenya-and-nigeria-saw-millions-of-cyber-attacks-in-2020-and-the-year-is-not-over-yet?lang=en (Accessed: 23 November 2021).

National Institute of Standards (2014) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. doi: 10.6028/NIST.CSWP.04162018.

National Research Foundation: Singapore (2021) *National Cybersecurity R&D Programme*. Available at: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme (Accessed: 17 February 2021).

Reddy, P. (2020) *Network Protocols and Its Security*, *Mediuam*. Available at: https://priya-reddy.medium.com/network-protocols-and-its-security-47d68f356666 (Accessed: 22 February 2021).

Slabbert, A. and Peyper, L. (2021) 'Transnet attack is cyber warfare', *Citypress*, 1 August. Available at: https://www.news24.com/citypress/business/transnet-attack-is-cyber-warfare-20210801 (Accessed: 23 November 2021).

Swinton, S. and Hedges, S. (2019) *Cybersecurity Governance, Part 1: 5 Fundamental Challenges*. Available at: https://insights.sei.cmu.edu/blog/cybersecurity-governance-part-1-5-fundamental-challenges/ (Accessed: 19 November 2021).

Whitehouse (2016) *FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN*. Available at: https://www.nitrd.gov/groups/csia/. (Accessed: 17 February 2021).