Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

# The Potential Benefits and Challenges of a BRICS+ Agency for Cybersecurity Intelligence Exchange

Masike Malatji*, Walter Matli
Graduate School of Business Leadership (SBL), University of South Africa (UNISA), South Africa.

*Received 25 Aug. 2023; Accepted 09 Nov. 2023; Available Online 30 Dec. 2023.*

## Abstract

The Brazil, Russia, India, China, South Africa (BRICS) nations lack a cohesive cybersecurity framework for intelligence exchange. The proposed expansion of the BRICS bloc calls for a BRICS+ agency dedicated to cybersecurity information sharing and analysis. Information Sharing and Analysis Centres (ISACs) are successful not-for-profit entities that centralise resources for gathering, analysing, and disseminating cybersecurity intelligence. However, founding a BRICS+ ISAC confronts challenges such as coordination complexity, financial constraints, trust deficits, linguistic diversity, and disparate legislative landscapes. This paper proposes a novel hybrid ISAC architectural model that amalgamates centralised and decentralised elements, presenting a tailored solution for the multifaceted needs of the expanding BRICS+ entity. The innovation of this model lies in its capacity to enhance cybersecurity resilience, promote efficient intelligence exchange, elevate the BRICS+ international standing, and solidify inter-nation collaboration, while being flexible enough to cater to the specific legal, cultural, and technological variances across member countries. The proposed model's uniqueness and adaptability position it as the premier choice for actualising the BRICS+ vision for a unified cyber front.

## I. Introduction

South Africa assumed chairmanship of the Brazil, Russia, India, China and South Africa (BRICS) bloc from China on January 1, 2023, under the theme "*BRICS and Africa: Partnership for mutually accelerated growth, sustainable development and inclusive multilateralism*" [1]. BRICS countries are emerging economies that have grown in economic and political influence [2]. The increasing reliance on technology and the Internet in these countries necessitates addressing cybersecurity threats and vulnerabilities, including cyber attacks on critical infrastructure (CI) [3], [4]. These countries face common opportunities and challenges in cyberspace, such as malicious use of artificial intelligence (AI) [5], making cybersecurity cooperation essential [6]. An effective tool used successfully in other regions for cybersecurity cooperation is the information sharing and analysis centre (ISAC), an organisational formation that collects, processes, analyses, disseminates, and presents information on cybersecurity threats and vulnerabilities [7]–[9].

To this end, there has been growing interest in establishing a BRICS ISAC to promote collaboration

**Keywords:** Cybersecurity, BRICS+, Incident response, Information sharing, ISAC, Threat intelligence.

Production and hosting by NAUSS

* Corresponding Author: Masike Malatji
Email: malatm1@unisa.ac.za

doi: 10.26735/LUKH3275

and cooperation among the BRICS countries on cybersecurity issues [10]. For example, both the 13th BRICS Summit, hosted by India on 09 September 2021, and the 14th BRICS Summit, hosted by China on 23 June 2022, highlighted security in the use of modern information and communication technologies (ICTs), or cybersecurity, as one of the key initiatives to pursue collaboratively through the Global Security Initiative (GSI) [11], [12]. Recognising mounting global risks and challenges, the GSI was proposed to address the current global security dilemma and provide guidance for building a world with universal security and lasting peace [12].

However, there are also challenges to be considered for the establishment of a BRICS ISAC, including coordination, funding, trust, language barriers, and legal and regulatory issues [10], [13]. Researchers such as Belli [3], [14] have recently explored new legal and regulatory concepts such as cyber defence and cyber warfare legislative frameworks in the BRICS countries. Other researchers such as Wanglai [6] highlighted the existence of the working group of experts of the BRICS member countries on security pertaining to the use of ICTs to promote sharing of information and best practices on cybersecurity, establishment of nodal points in member countries and effective coordination against cybercrime. However, there is no indication by Belli [3], [14] and Wanglai [6], and in the latest literature pertaining to the BRICS Summits (13th Summit in 2021 and 14th Summit in 2022) [11], [12], that there is one single body responsible for the coordination of BRICS cybersecurity information sharing and analysis. This paper explored the potential benefits and challenges of establishing a BRICS ISAC and to propose the potential architectural model that could be used for cybersecurity intelligence exchange in the bloc.

The rest of the paper is structured as follows: Following the introduction of the research aim in this section, Section II of the paper outlines the methods adopted for the exploration of the potential benefits of a BRICS agency for cybersecurity information sharing and analysis. Whereas Section III discusses related works on the potential benefits and challenges of ISACs and their architectural models in general, Section IV specifically discusses the potential benefits and challenges of a BRICS ISAC and its architectural model. The paper concludes with Section V where recommendations for future research are also put forward.

## II. Research Design and Approach

This study adopted a scoping review approach, underpinned by an analytical framework, to investigate the viability and implications of establishing a BRICS ISAC. The analytical framework for this study is grounded in the following key concepts:

- *ISACs*: ISACs are not-for-profit, member-driven organisations that facilitate the sharing and analysis of cybersecurity information among members. They play a vital role in enhancing cybersecurity resilience and fostering collaboration between public and private sector stakeholders [7]–[9].
- *BRICS*: The BRICS nations are a diverse grouping of emerging economies with growing geopolitical and economic significance. Cybersecurity cooperation among BRICS nations is essential for addressing the shared challenges posed by cyber threats [2].
- *Hybrid ISAC architectural model*: A hybrid ISAC architectural model combines centralised and decentralised elements to provide flexibility and scalability, while also addressing the unique needs of the member states [15]–[17].

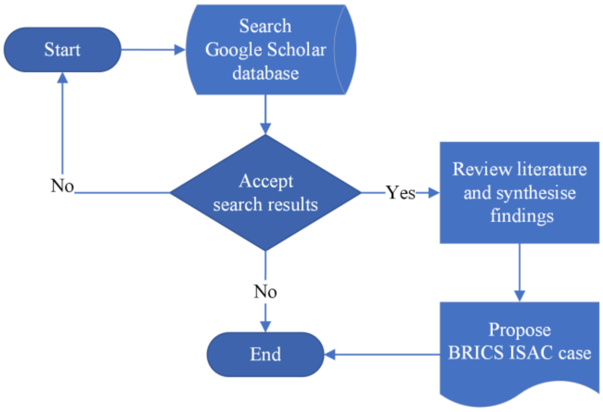
Start
Search Google Scholar database
Accept search results
No
Yes
Review literature and synthesise findings
No
End
Propose BRICS ISAC case

Fig.1. Research Procedure Overview.

The research process involved the following steps:

1. Literature search: A literature search was conducted in Google Scholar to identify scholarly and grey literature on the concept and operationalisation of ISACs, with a focus on the BRICS nations and cybersecurity collaboration.
2. Relevance filtering: The resulting literature was subjected to a relevance filter to discard documents that did not directly contribute to understanding the establishment of an ISAC within the BRICS context or that lacked empirical or theoretical depth. The remaining papers were subjected to a thematic synthesis.
3. Thematic synthesis: The thematic synthesis involved identifying and categorising the potential benefits and challenges of establishing a BRICS ISAC according to emerging themes. This synthesis informed the subsequent construction of an argument for the suitability of a hybrid architectural model for the proposed BRICS ISAC.

The general view of the potential benefits and challenges of establishing an ISAC and architectural models are discussed in the next section.

## III. Related Works

### *A. BRICS + Concept*

In March 2017, the concept of a 'BRICS Plus' to build a new platform for south-south cooperation to promote the establishment of broader partnerships and facilitate common development and prosperity of emerging markets on a larger scale was proposed [18], [19]. Like the BRICS-Outreach Summit, the BRICS Plus is a forum for BRICS-related initiatives to interact and/or collaborate with nations that are not a part of the BRICS grouping [20]. Foreign ministers from nations such as Saudi Arabia, Egypt, Argentina, United Arab Emirates (UAE), Nigeria, Indonesia, Thailand, Kazakhstan and Senegal have already attended a BRICS Plus meeting [20].

This paper therefore adopted the BRICS Plus, or BRICS+, formation for the proposed BRICS ISAC establishment. As of the writing of this paper, the 15th BRICS Summit, which was held in Johannesburg, South Africa from August 22 to 24, 2023, had formally invited six nations to join the BRICS bloc starting January 1, 2024 [21]. To quote the South African President, Cyril Ramaphosa, "*We have decided to invite the Argentine Republic, the Arab Republic of Egypt, the Federal Democratic Republic of Ethiopia, the Islamic Republic of Iran, the Kingdom of Saudi Arabia and the United Arab Emirates to become full members of BRICS. The membership will take effect from 1 January 2024"* [21]. This paper therefore adopted the BRICS Plus, or BRICS+, formation for the proposed BRICS ISAC establishment.

### *B. Overview of ISACs*

According to the European Union (EU) agency for cybersecurity, popularly known as the European Network and Information Security Agency [15], ISACs are non-profit organisations that provide a central resource for gathering information on cyber threats (in many cases to CI) as well as enable bidirectional sharing of information between the private and public sectors. Originally, the ISAC concept was initiated by the government of the United States of America (USA) around 1998 to be industry-based associations expected to serve as a mechanism for gathering, analysing, appropriately sanitising and disseminating private sector cybersecurity information to both industry and the government [8], [22].

They achieve this by digging deeper into their sectors to provide secure and trusted information and analytical capabilities to stakeholders that could be in the water, transportation, real estate, oil and natural gas, maritime, ICT, and aviation sectors [23]. Accordingly, ISACs are designed to interconnect industry and governmental organisations, forming public-private partnerships, with the aim of improving cybersecurity posture for all parties involved [22], [24]. Furthermore, ISACs operate as service systems for effective joint response to cyber compromise by multiple stakeholders [25]. According to the National Institute of Standards and Technology (NIST) [26], [27], [28], and [29] some of the ISAC functions and responsibilities include:

- **Incident response:** ISACs are tasked with managing response and recovery efforts when a security incident takes place. This involves determining the incident's characteristics and extent, evaluating the impact, and implementing corrective actions to mitigate future occurrences.
- **Vulnerability management:** ISACs are responsible for identifying and addressing vulnerabilities in an organisation's systems and networks. This includes identifying and prioritising vulnerabilities based on their potential impact and implementing measures to mitigate or eliminate those vulnerabilities.
- **Threat intelligence:** ISACs use technological platforms to gather and analyse data on emerging cyber threats, such as new malware variants and sophisticated cyber espionage activities. These platforms automate data collection, integrate multiple data sources, and use real-time analytics and ML algorithms to enhance predictive capabilities. By leveraging such platforms, ISAC members gain actionable intelligence that enables them to take a more proactive cybersecurity stance and anticipate potential attacks. This dynamic and informed approach to threat intelligence is crucial for maintaining an up-to-date understanding of the threat landscape and devising effective countermeasures.
- **Guidance and support:** ISACs regularly furnish direction and assistance to member organisations concerning safeguarding against evolving threats or vulnerabilities, which are continually progressing due to technological advancements such as AI, cloud computing, blockchain, and other digital technologies. The aid and guidance may incorporate best practices, training, or technical support.

Whereas ISACs and security operations centres (SOCs) are both dedicated entities or teams within an organisation that are responsible for monitoring and analysing data to identify potential cybersecurity risks and implementing measures to mitigate those risks, there are some key differences between them [7], [24], [25], [30]:

- **Scope:** ISACs are typically focused on a specific industry or sector, such as energy or water. They collect and analyse data on emerging threats and vulnerabilities within that industry or sector and provide guidance to member organisations on how to protect against those threats. SOCs, on the other hand, are typically focused on a specific organisation or group of organisations and are responsible for protecting those organisations against all types of cyber threats.
- **Membership:** ISACs are usually membership-based, with organisations paying a fee to join and receive the benefits of membership. SOCs, on the other hand, are usually established and funded by a specific organisation or group of organisations.
- **Functions and responsibilities:** ISACs and SOCs both have a range of functions and responsibilities, including incident response, vulnerability management, threat intelligence, and guidance and support. However, the specific tasks and responsibilities of ISACs and SOCs may vary depending on their scope and membership.

Overall, ISACs and SOCs are both important components of an organisation's cybersecurity strategy with ISACs having diverse functions and responsibilities that vary depending on the specific focus and membership of the ISAC [27]. Thus, operating an effective ISAC would require overcoming a number of challenges as highlighted by ENISA [15]. Some of the most pertinent challenges are discussed in the next section.

### *C. Benefits and Challenges of an ISAC*

In addition to what has already been highlighted in the previous sections, some of the benefits of establishing an ISAC include [26], [27]:

- **Improved cybersecurity:** ISACs can help organisations to improve their cybersecurity posture by providing access to threat intelligence, best practices, and other resources.

- **Enhanced incident response:** ISACs can help organisations to respond to security incidents more quickly and effectively by providing access to incident response expertise and resources, and by facilitating the sharing of information among member organisations.
- **Greater collaboration:** ISACs facilitate collaboration among member organisations, allowing them to share information and resources and work together to address common security challenges.
- **Cost savings:** By providing access to shared resources and expertise, ISACs can help organisations to reduce the cost of implementing and maintaining their own cybersecurity programs.

There are, however, several challenges to be considered when establishing and operating an effective ISAC and these include [15], [26], [27]:

- **Limited resources:** Many organisations struggle to allocate sufficient resources, e.g. staff or funding, to their ISACs, resulting in inadequate staff or technology. This can hinder the ability of an ISAC, or similar formation, to effectively monitor and analyse data, and to respond to incidents in a timely manner.
- **Skills shortage:** There is a shortage of skilled professionals with expertise in cybersecurity, which can make it difficult for organisations to staff their ISACs. This can lead to a reliance on automated tools such as the application of AI in cybersecurity, which may not be able to fully address the complexity and diversity of modern cyber threats.
- **Lack of standardisation:** Without clear policies and procedures in place, it may be difficult for analysts to consistently gather, analyse, and disseminate information.
- **Data overload:** With the proliferation of big digital data, analysts may be overwhelmed by the volume, variety and velocity of information they need to process.
- **Limited expertise:** Analysts may not have the necessary skills or experience to effectively analyse and interpret complex datasets.
- **Lack of collaboration:** Without proper communication and collaboration among analysts and other stakeholders, it may be difficult to effectively share information and insights.
- **Insufficient training:** Analysts may not have received adequate training to effectively carry out their duties.
- **Limited access to information:** Analysts may not have access to all the information they require to properly analyse and interpret data.
- **Limited ICT infrastructure:** Organisations may not have the necessary technology or tools to effectively support the operations of an ISAC.
- **Legal, regulatory and ethical considerations:** Organisations may face legal and ethical challenges when collecting, storing, and sharing information due to, for example, data privacy legislations.
- **Coordination:** Setting up an ISAC involves coordinating the efforts of multiple organisations, which can be a complex and time-consuming process. Ensuring that all member organisations are on board with the idea and willing to contribute resources and expertise could be a challenge.
- **Trust:** Sharing sensitive information about cybersecurity threats and vulnerabilities requires a high level of trust among the member organisations

Having delineated the challenges to be considered when establishing and operating an effective ISAC, it is imperative to broaden our perspective and explore the manifestation and operation of ISACs in various other regions of the world.

### *D. ISACs in Other Regions of the World*

There are several examples of countries that have established ISACs to enhance their national cybersecurity posture. For example, the USA has a number of sector-specific ISACs, such as the Financial Services ISAC and the Electricity ISAC, as well as a national ISAC known as the Cybersecurity and Infrastructure Security Agency (CISA) [31], [32]. CISA works closely with USA federal agencies, state and local governments, and private sector partners to be the national coordinator for CI security and resilience and operationally lead federal cybersecurity functions and responsibilities [32].

The United Kingdom (UK) has established the UK National Cyber Security Centre (NCSC) to provide guidance and support to critical organizations, the public sector, industry, small and medium-sized enterprises, and the general public regarding cybersecurity [33]. Despite leaving the EU, the NCSC produced good practice indicators that aided EU member states in meeting the Network and Information Security (NIS) Directive's principles and objectives [34]. Furthermore, the UK created the Cyber Security Challenge UK, a non-profit organization that brings together government, academia, and industry to identify fresh cybersecurity talent with the requisite skills and diverse backgrounds the industry needs and demands [35]. This challenge incorporates a variety of ISACs that concentrate on specific sectors, including finance, energy, and healthcare, and collaborates with industry partners to improve the UK's CI's resilience and capacity through training initiatives [35].

Other countries that have established ISACs or similar organisations include Canada, which has the Canadian Cyber Threat Exchange and the Canadian Centre for Cyber Security [36], [37], and Australia, which has the Australian Cyber Security Centre [38]. Therefore, a number of countries have established ISACs or similar organisations to enhance their national cybersecurity posture by facilitating the exchange of information and analysis related to cybersecurity threats and incidents. These organisational formations serve as a hub for the collection, analysis, and dissemination of cybersecurity information, and provide a range of value-added services to their members, including intelligence briefings, incident response support, and training and education [27]. To be effective in promoting collaboration and cooperation on cybersecurity issues among members, an ISAC must be configured through an appropriate architectural model.

### *E. ISAC Models*

There are several architectural models that organisations can consider when designing and implementing an ISAC. Some of these models include [15]–[17]:

- Centralised: The ISAC functions as a central hub for aggregating, processing, and analysing information from diverse sources, ultimately disseminating it to a network of "spokes," or member organisations, who utilize it to enhance their security posture. This approach enables improved efficacy and coordination, although its successful implementation necessitates substantial resources.
- Decentralised: Multiple ISACs function independently but opt to exchange information and resources voluntarily. Information sharing and analysis activities are performed by individual organisations or smaller regional ISACs. While this approach may be more feasible for organisations with limited resources, it may also lead to a lack of standardisation and coordination. Nonetheless, this model enables organisations to benefit from the expertise and resources of multiple ISACs without being reliant on any single one.
- Hybrid model: This model combines elements of the centralised and decentralised models, allowing organisations to choose the level of involvement and collaboration that best suits their needs.

ENISA [15] identified three informal categorisations of ISAC models in Europe, namely country-focused, sector-specific, and international collaboration models. The country-focused model encompasses cooperation and collaboration initiatives at a national level, with the goal of bringing together all experts or cyber security incident response teams to facilitate smoother and more effective information sharing and analysis [15]. The sector-specific ISAC model is tailored to specific CI sectors such as energy, water, transportation, and healthcare [15]. Finally, the international collaboration ISAC model seeks to unite multi-stakeholder members from across Europe and beyond, recognising that cybersecurity threats transcend national borders. Notably, these ENISA models are variations of the three ISAC models discussed earlier. Ultimately, determining the most appropriate architectural model for any given entity or group of entities hinges on their specific needs and objectives.

## IV. Discussions of the Proposed BRICS+ Agency For Cybersecurity

The paper includes a consolidated list of all the organisations discussed in this section and throughout the manuscript in Table I, listing their purpose and country of origin.

TABLE I
List of Organisations Discussed In the Paper

| Organisation | Purpose | Country |
|---|---|---|
| Brazilian National Computer Emergency Response Team (CERT.br) | Handling computer security incidents and providing alerts on cybersecurity matters | Brazil |
| National Cyber Defence Centre (CDCiber) | Safeguarding the nation's cyberspace by coordinating various cybersecurity initiatives | Brazil |
| Armed Forces' Cyber Defence Command (ComDCiber) | Protecting the armed forces' digital infrastructure and ensuring the security of military operations in the cyberspace domain | Brazil |
| National School for Cyber Defence (ENaDCiber) | Training military personnel in cybersecurity and cyber defence techniques | Brazil |
| Federal Security Service (FSB) | National security, including counterintelligence and cybersecurity | Russia |
| Federal Protective Service (FSO) | Security and counter-surveillance functions, potentially including cyber protections for federal agencies | Russia |
| Indian Computer Emergency Response Team (CERT-In) | Responding to computer security incidents, reporting on vulnerabilities and promoting effective security practices | India |
| National Technical Research Organization (NTRO) | Technical intelligence gathering and ensuring the security of India's critical infrastructure | India |
| National Computer Network Emergency Response Technical Team/ Coordination Centre of China (CNCERT or CNCERT/CC) | Coordinating response to internet security incidents in national networks and promoting the country's cybersecurity policy | China |
| Ministry of Public Security (MPS) | Law enforcement and security, which includes cyber policing and anti-cybercrime efforts | China |
| Electronic Communications Security (Pty) Ltd - Cyber Security Incidents Response Team (ECS-CSIRT) | Responding to cybersecurity incidents affecting electronic communications for organs of state only | South Africa |
| National Cybersecurity Hub (National CSIRT) | Acting as the central point for collaboration on cybersecurity incidents, policies, and standards | South Africa |
| South African Police Service (SAPS) | Crime prevention and investigation, which encompasses cybercrimes | South Africa |

### *A. Overview of ISACs or Similar Formations in Each BRICS Country*

BRICS countries have established various cooperation mechanisms, such as the BRICS Summit, BRICS Political Parties, Think Tanks and Civil Society Organisations Forum, and the BRICS Business Council [6], [39]–[41]. These nations have also set up institutions like the New Development Bank and the Contingent Reserve Arrangement to promote cooperation [39]–[41]. In the area of security, there has been an increasing interest in creating a BRICS ISAC or a similar organisation to address cybersecurity challenges and foster cooperation among the BRICS member countries [42], [43]. At the national level, each BRICS country has established agencies or entities that function as hubs for collecting, processing, analysing, disseminating, and presenting information concerning cybersecurity threats and vulnerabilities.

*1) Brazil*

The Brazilian government has several agencies and units that are responsible for cybersecurity, including the Brazilian National Computer Emergency Response Team, National Cyber Defence Centre, Armed Forces' Cyber Defence Command, and National School for Cyber Defence [44], [45].

*2) Russia*

The Russian government has several agencies and units that are responsible for cybersecurity, including the Federal Security Service and Federal Protective Service [46].

*3) India*

The Indian government has several agencies and units that are responsible for cybersecurity, including the Indian Computer Emergency Response Team and the National Technical Research Organization [47].

*4) China*

The Chinese government has several agencies and units that are responsible for cybersecurity, including the National Computer Network Emergency Response Technical Team/Coordination Centre of China and the Ministry of Public Security [47], [48].

*5) South Africa*

The South African government has several agencies and units that are responsible for cybersecurity, including the Electronic Communications Security—Cyber Security Incidents Response Team in the State Security Agency, National Cybersecurity Hub in the Ministry of Communications and Digital Technologies, and the South African Police Service [49].

These agencies work to protect the BRICS member countries' CI and information systems from cyber threats and to respond to cyber incidents. The paper did not provide an overview of ISACs or similar formations of the countries that are expected to join BRICS (Saudi Arabia, Iran, Egypt, Ethiopia, Argentina, and the United Arab Emirates). Nevertheless, some of the potential benefits and challenges pertaining to the establishment of a BRICS+ ISAC are discussed in the next section.

### *B. Benefits and Challenges of a BRICS+ ISAC*

There are several potential benefits of establishing a BRICS+ ISAC. An ISAC can facilitate improved information sharing about cybersecurity threats and vulnerabilities in a timely and secure manner, which can help member countries stay ahead of potential cyber attacks and respond more effectively to incidents when they occur [10]. Furthermore, a BRICS+ ISAC could enhance collaboration by sharing knowledge, expertise, and resources to address common cybersecurity challenges more effectively [13]. A BRICS+ ISAC could also contribute to greater resilience by sharing information and working together, helping to build more robust and resilient cybersecurity capabilities and reduce the member countries' vulnerability to cyber attacks [43]. Finally, a BRICS+ ISAC could enhance the member countries' reputation as responsible actors in the global cybersecurity landscape by demonstrating a commitment to addressing cybersecurity issues. Fig. 2 summarises the key benefits of establishing a BRICS+ ISAC.

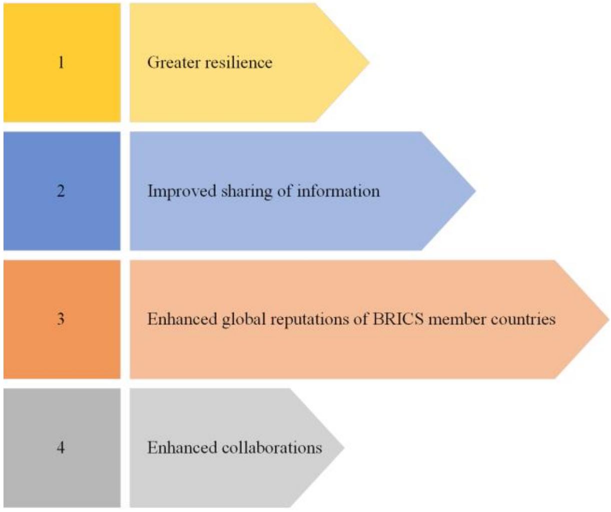
1
Greater resilience
2
Improved sharing of information
3
Enhanced global reputations of BRICS member countries
4
Enhanced collaborations

Fig. 2. Potential benefits of establishing a BRICS+ ISAC.

The potential benefits of establishing a BRICS+ ISAC, as presented in Fig. 2, align with those discussed in Section III of the reviewed literature. These include improved cybersecurity, enhanced incident response, greater collaboration, and cost savings. However, the establishment of a BRICS+ ISAC also poses several challenges that must be considered. Fig. 3 summarises the key challenges of establishing a BRICS+ ISAC.

Coordination is one such challenge, given that it involves the coordination of multiple countries and organisations, which can be complex and time-consuming. Funding is another significant challenge, as an ISAC requires substantial resources, including staff, equipment, and infrastructure, and securing buy-in from all member countries may prove difficult [10], [13]. Trust is also a critical factor to consider as sharing sensitive information about cybersecurity threats and vulnerabilities requires a high level of trust among the member countries, which may be challenging due to political or other tensions. Language barriers may also pose a challenge in ensuring effective communication among the countries. Moreover, navigating legal and regulatory issues, such as data protection laws and privacy concerns, could be a challenging process. It is essential to ensure that the ISAC follows all relevant laws and regulations within member countries [3], [10], [13], [14], [43].

The potential challenges of establishing a BRICS+ ISAC, as shown in Fig. 3, align with the challenges discussed in Section III of the reviewed literature. These include limited resources, skills shortages, lack of standardisation, data overload, limited expertise, lack of collaboration, insufficient training, limited access to information, limited ICT infrastructure, legal and ethical considerations, coordination, and trust [10], [13], [43]. Addressing the potential challenges of establishing a BRICS+ ISAC will involve multifaceted strategies tailored to the unique contexts of the member nations. Next we discuss the potential solutions to the challenges identified in Fig.. 3.

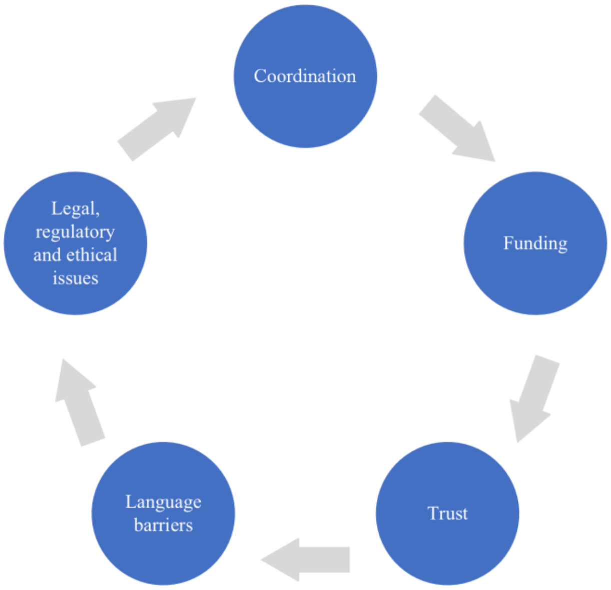

Fig. 3. Potential challenges of establishing a BRICS+ ISAC.

### *C. Addressing the Challenges of Setting up a BRICS+ ISAC*

We can learn from existing international cybersecurity collaborations, such as the European Cybercrime Centre (EC3) within Europol, USA's CISA, Cooperative Cyber Defence Centre of Excellence (CCDCOE), and others, to overcome the potential challenges of establishing a BRICS+ ISAC:

- **Coordination:** BRICS+ coordinators should establish a clear governance structure with defined roles, responsibilities, and decision-making processes. Similar to the EU's NIS Directive, which sets network and information security requirements for all EU members [50], BRICS+ could develop a framework for joint operations with protocols for coordinating activities. This could be modelled on the practices of the North Atlantic Treaty Organisation (NATO)'s Cooperative Cyber Defence Centre of Excellence [51]. Lastly, BRICS+ should engage in regular joint exercises to conduct cybersecurity drills, similar to the Cyber Storm exercises led by the USA's Department of Homeland Security [52], which can improve coordination among member countries.

- **Funding:** BRICS+ should develop a shared financial contributions protocol based on gross domestic product (GDP), similar to the United Nations (UN) General Assembly's regular budget assessments [53]. BRICS+ should also explore external funding from international organisations like the World Bank, which funds cybersecurity initiatives in developing countries [54]. Additionally, BRICS+ should pursue public-private partnerships to engage with private sector stakeholders for investments or in-kind contributions, similar to those by CISA in the USA [55].
- **Trust:** BRICS+ should pursue mutual legal assistance treaties (MLATs) to strengthen legal cooperation and trust, similar to the Budapest Convention on Cybercrime [49]. BRICS+ should also develop confidence-building measures (CBMs) to establish transparency and predictability in state behaviour, similar to the Organisation for Security and Cooperation in Europe (OSCE)'s cybersecurity CBMs [56]. Finally, BRICS+ should set up secure communication channels using cryptographic methods [57] and secure platforms to maintain the confidentiality and integrity of shared data.
- **Language barriers:** BRICS+ should develop multilingual digital platforms to ensure that all participants can access information in their native languages. With the rise of generative AI and large language models like ChatGPT, Google Bard, and Bing Chat, the need for dedicated translators for real-time translation during meetings and documentation may diminish, like the UN's linguistic services. However, BRICS+ should encourage cross-language training among member countries' cybersecurity teams to facilitate better direct communication.
- **Legal, Regulatory,** *and Ethical Issues*: BRICS+ should aim for harmonisation and alignment of cybercrime laws and regulations, drawing upon the examples of the General Data Protection Regulation (GDPR)'s impact on privacy laws worldwide [58]. Moreover, a charter that outlines the ethical use of shared information and the commitment to respecting privacy and civil liberties should be developed. Finally, BRICS+ should create standard operating procedures that are legally vetted to govern the sharing and use of data, ensuring compliance with various national laws and norms.

To effectively promote cooperation and collaboration on cybersecurity matters among BRICS+ member countries, an appropriate architectural model must be adopted for the ISAC.

### *D. Architectural Model of a BRICS+ ISAC*

BRICS+ ISACs can be implemented using different architectural models, including centralised, decentralised, and hybrid models, as shown in Fig. 4.

One option for the BRICS+ ISAC is the centralised model where one node serves as a central hub for information collection, processing, analysis, dissemination, and presentation for each member country, as shown in Fig. 4. This model allows the BRICS+ ISAC to operate as a central hub that collects and analyses information from member countries and disseminates it back to all members, enabling easy and speedy sharing of information [13]. However, this model may be less flexible and responsive to the unique requirements of individual members [13]. Moreover, the entire system depends on the central hub, and if it fails or experiences technical glitches, the entire system will be affected [17].

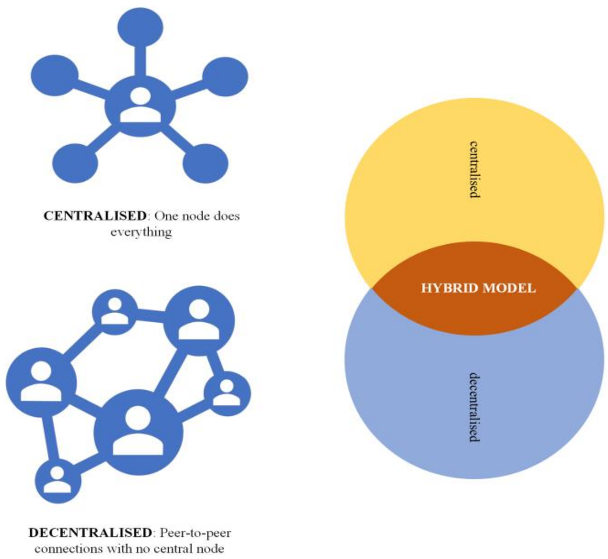
CENTRALISED: One node does everything
centralised
HYBRID MODEL
decentralised
DECENTRALISED: Peer-to-peer connections with no central node

Fig. 4. Potential architectural model for establishing a BRICS+ ISAC.

The decentralised model, as depicted in Fig. 4, is another option for the BRICS+ ISAC, where each member country operates its own separate ISAC and shares information directly among peers (member countries' ISACs) without going through a central hub [13]. Compared to the centralised model, this model allows for faster information sharing and collaboration on cybersecurity issues among member countries [17]. Moreover, the decentralised model is generally more resilient as there are more connections available for information transfer [17]. However, this peer-to-peer approach lacks value-added services such as information analysis, aggregation and correlation, which a centralised hub could provide [17]. Additionally, the cost involved in establishing and maintaining trusted communication channels in this peer-to-peer architecture could be a significant disadvantage [17].

The third option for the BRICS+ ISAC is the hybrid model, which incorporates both the centralised and decentralised architectures [13], [17]. Under this model, a central hub is responsible for collecting and analysing cybersecurity information, while member countries also maintain their own ISACs that can share information directly with one another. This approach offers the advantage of assigning different information sharing and analysis functions to different levels or components of the central ISAC as [17], giving BRICS+ member countries the flexibility to choose the level of collaboration that suits them best. Ultimately, the most effective architectural model for a BRICS+ ISAC will depend on several factors, including the member countries' size and complexity, the level of trust and cooperation among them, and the resources and capabilities available to support the ISAC.

Through careful consideration of these factors and collaboration to develop a suitable architectural model, the member countries can ensure the success and sustainability of the BRICS+ ISAC [13], [17].

## V. Conclusion

This paper explored the potential benefits and challenges of establishing a BRICS+ ISAC for cybersecurity, proposing a multifaceted architectural model that could be adopted. A BRICS+ ISAC would not only facilitate the exchange of information and analysis related to cybersecurity threats and incidents, but will also act as a catalyst in enhancing the overall cybersecurity posture of each member country. This enhancement would be rooted in collaborative intelligence, shared resources, and coordinated response mechanisms.

However, the path to realisation is fraught with potential challenges that require meticulous attention, such as building trust among diverse stakeholders, ensuring secure and ethical information sharing, acquiring sustainable funding, and maintaining long-term operational sustainability. The paper delved into various architectural models, including centralised, decentralised, and hybrid structures, with a particular emphasis on the hybrid model. This model emerges as a viable option, demonstrating flexibility and adaptability to create an effective BRICS+ ISAC system that can operate in a range of scenarios, accommodating the unique legal, cultural, linguistic and technological landscapes of the member nations.

Future research should venture into the intricate governance strategy and mechanics of setting up and operating an effective BRICS+ ISAC, including legal frameworks, ethical considerations, technological infrastructure and human capital development. Overall, the establishment of a BRICS+ agency for cybersecurity information sharing and analysis should transcend mere technological collaboration; it must symbolise a concerted effort towards a unified cybersecurity front. It could provide significant benefits to the BRICS+ grouping, requiring careful planning, strategic alignment, and consideration of potential challenges. By working together in this pioneering endeavour, the BRICS+ nations will not only enhance their individual cybersecurity posture. They will be contributing to building a more secure, resilient and interconnected global digital environment. This would be reflecting their shared commitment to the collective security and prosperity of the emerging digital world.

## Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

## Conflict of Interest

Authors declare that they have no conflict of interest.

## References

[1] SABC, ‘SA holds 2023 presidency in BRICS’, SABC News - Breaking news, special reports, world, business, sport coverage of all South African current events. Africa’s news leader. Accessed: Jan. 03, 2023. [Online]. Available: https://web.archive.org/web/20230103115845/https://www.sabcnews.com/sabcnews/sa-holds-2023-presidency-in-brics/

[2] I. Denisov, A. Kazantsev, F. Lukyanov, and I. Safranchuk, ‘Shifting Strategic Focus of BRICS and Great Power Competition’, *Strateg. Anal.*, vol. 43, no. 6, pp. 487–498, 2019, doi: 10.1080/09700161.2019.1669888.

[3] L. Belli, *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham, SWITZERLAND: Springer International Publishing AG, 2021a. Accessed: Nov. 19, 2022. [Online]. Available: http://ebookcentral.proquest.com/lib/unisa1-ebooks/detail.action?docID=6450854

[4] M. Malatji, ‘Industrial control systems cybersecurity: Back to basic cyber hygiene practices’, in 2022 *International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Prague, Czech Republic, 2022, pp. 1–7. doi: 10.1109/ICECET55527.2022.9872810.

[5] K. A. Pantserev, ‘Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity’, *Vestn. RUDN Int. Relat.*, vol. 22, no. 2, Art. no. 2, 2022, doi: 10.22363/2313-0660-2022-22-2-288-302.

[6] G. Wanglai, ‘BRICS cybersecurity cooperation: Achievements and deepening paths’, *China Int. Stud.*, vol. 68, pp. 124–139, 2018.

[7] D. P. David, M. M. Keupp, and A. Mermoud, ‘Knowledge absorption for cyber-security: The role of human beliefs’, *Comput. Hum. Behav.*, vol. 106, p. 106255, 2020, doi: 10.1016/j.chb.2020.106255.

[8] Z. Rashid, U. Noor, and J. Altmann, ‘Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem’, *Future Gener. Comput. Syst.*, vol. 124, pp. 436–466, 2021, doi: 10.1016/j.future.2021.05.033.

[9] J. M. Salomon, ‘Public-Private Partnerships and Collective Cyber Defence’, in 2022 *14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, 2022, pp. 45–63. doi: 10.23919/CyCon55549.2022.9810912.

[10] N. Kshetri and S. Rangarajan, ‘Establishing an information sharing and analysis center (ISAC) for addressing cyber threats in BRICS countries’, *J. Cybersecurity*, vol. 2, no. 3, pp. 231–247, 2016.

[11] BRICS, ‘XIII BRICS Summit- New Delhi Declaration’, 2021. Accessed: Jan. 03, 2023. [Online]. Available: https://web.archive.org/web/20220713184307/https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-51.pdf

[12] BRICS, ‘Yang Jiechi Chairs the 12th Meeting of BRICS National Security Advisers and High Representatives on National Security’. Accessed: Jan. 03, 2023. [Online]. Available: https://web.archive.org/web/20220705230339/http://brics2022.mfa.gov.cn/eng/dtxw/202206/t20220616_10704504.html

[13] M. A. Babar and N. Kshetri, ‘Challenges and issues in establishing an information sharing and analysis center (ISAC) in developing countries’, *J. Cybersecurity*, vol. 1, no. 1, pp. 23–37, 2015.

[14] L. Belli, ‘Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation’, *Afr. J. Inf. Commun.*, vol. 28, pp. 1–14, 2021b, doi: 10.23962/10539/32208.

[15] ENISA, ‘Information Sharing and Analysis Center (ISACs) - Cooperative models’, ENISA. Accessed: Jan. 04, 2023. [Online]. Available: https://web.archive.org/web/20221124125759/https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/

[16] C. Johnson, M. Badger, D. Waltermire, J. Snyder, and C. Skorupka, ‘Guide to Cyber Threat Information Sharing’, National Institute of Standards and Technology, NIST Special Publication (SP) 800-150, 2016. doi: 10.6028/NIST.SP.800-150.

[17] Z. Fathi, A. J. Rafsanjani, and F. Habibi, ‘Anon-ISAC: Anonymity-preserving cyber threat information sharing platform based on permissioned Blockchain’, in 2020 *28th Iranian Conference on Electrical Engineering (ICEE)*, Tabriz, Iran, May 2020, pp. 1–5. doi: 10.1109/ICEE50131.2020.9261029.

[18] E. Y. Arapova, ‘The “BRICS Plus” as the First International Platform Connecting Regional Trade Agreements’, *Asia-Pac. Soc. Sci. Rev.*, vol. 19, no. 2, pp. 30–46, 2019, doi: https://doi.org/10.1177/21582440211054128.

[19] A. Sokolov, S. Shashnov, and M. Kotsemir, ‘From BRICS to BRICS plus: selecting promising areas of S&T Cooperation with developing countries’, *Scientometrics, vol.* 126, no. 11, pp. 8815–8859, Nov. 2021, doi: 10.1007/s11192-021-04142-3.

[20] K. Kipgen and S. Chakrabarti, 'The Politics Underpinning the BRICS Expansion', *J. Lib. Int. Aff.*, vol. 8, no. 3, pp. 445–458, 2022, doi: https://e-jlia.com/index.php/jlia/article/view/773.

[21] South African Government, 'President Cyril Ramaphosa: Media briefing remarks announcing outcomes of the XV BRICS Summit | South African Government'. Accessed: Aug. 25, 2023. [Online]. Available: https://www.gov.za/speeches/president-cyril-ramaphosa-media-briefing-remarks-announcing-outcomes-xv-brics-summit

[22] M. He, L. Devine, and J. Zhuang, 'Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach', *Risk Anal.*, vol. 38, no. 2, pp. 215–225, 2018, doi: 10.1111/risa.12878.

[23] S. E. Jasper, 'U.S. Cyber Threat Intelligence Sharing Frameworks', *Int. J. Intell. CounterIntelligence*, vol. 30, no. 1, pp. 53–65, 2017, doi: 10.1080/08850607.2016.1230701.

[24] R. Leszczyna, 'Standards with cybersecurity controls for smart grid-A systematic analysis', *Int. J. Commun. Syst.*, vol. 32, no. 6, p. e3910, 2019, doi: 10.1002/dac.3910.

[25] C.-H. Han, 'Blockade-detection-response based security operations dashboard design', *Comput. Hum. Behav. Rep.*, vol. 4, p. 100143, 2021, doi: 10.1016/j.chbr.2021.100143.

[26] NIST, 'Guide to Cyber Threat Information Sharing', National Institute of Standards and Technology, NIST SP 800-150, 2016. doi: 10.6028/NIST.SP.800-150.

[27] M. Csoka, 'Information and security analysis centers: A comprehensive overview', *Int. J. Inf. Secur. Cybercrime*, vol. 7, no. 1, pp. 1–8, 2018.

[28] R. J. Raimundo and A. T. Rosário, 'Cybersecurity in the Internet of Things in Industrial Management', *Appl. Sci.*, vol. 12, no. 3, Art. no. 3, 2022, doi: 10.3390/app12031598.

[29] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, 'Threats and Opportunities with AI-Based Cyber Security Intrusion Detection: A Review', *Int. J. Softw. Eng. Appl.*, vol. 13, no. 5, 2022, doi: https://ssrn.com/abstract=4323258.

[30] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, 'Challenges and performance metrics for security operations center analysts: a systematic review', *J. Cyber Secur. Technol.*, vol. 4, no. 3, pp. 125–152, 2020, doi: 10.1080/23742917.2019.1698178.

[31] T. Wallis and R. Leszczyna, 'EE-ISAC—Practical Cybersecurity Solution for the Energy Sector', *Energies*, vol. 15, no. 6, Art. no. 6, 2022, doi: 10.3390/en15062170.

[32] CISA, 'ABOUT CISA | CISA'. Accessed: Jan. 04, 2023. [Online]. Available: https://web.archive.org/web/20221231195909/https://www.cisa.gov/about-cisa

[33] NCSC, 'What we do'. Accessed: Jan. 04, 2023. [Online]. Available: https://web.archive.org/web/20230101013620/https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

[34] T. Wallis, C. Johnson, and M. Khamis, 'Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive', *Inf. Secur. Int. J.*, vol. 48, pp. 36–68, 2021, doi: 10.11610/isij.4812.

[35] Cyber Security Challenge UK, 'Who we are - Cyber Security Challenge UK'. Accessed: Jan. 04, 2023. [Online]. Available: https://web.archive.org/web/20220808170500/https://cybersecuritychallenge.org.uk/who-we-are

[36] S. Carvin and Centre for International Governance, 'Canada and Cyber Governance: Mitigating Threats and Building Trust', Centre for International Governance Innovation, 2019. Accessed: Jan. 04, 2023. [Online]. Available: https://www.jstor.org/stable/resrep26129.19

[37] G. Hale and C. Bartlett, 'Managing the Regulatory Tangle: Critical Infrastructure Security and Distributed Governance in Alberta's Major Traded Sectors', *J. Borderl. Stud.*, vol. 34, no. 2, pp. 257–279, 2019, doi: 10.1080/08865655.2017.1367710.

[38] A. Williams, 'Beyond 2000: The Rise of Australian Cyber Warfare Capability', in *International Conference on Cyber Warfare and Security*, Reading, United Kingdom: Academic Conferences International Limited, 2020, pp. 549-555,XVIII. doi: 10.34190/ICCWS.20.043.

[39] J. Kirton and M. Larionova, 'The First Fifteen Years of the BRICS', *Int. Organ. Res. J.*, vol. 17, no. 2, pp. 7–30, 2022, doi: 10.17323/1996-7845-2022-02-01.

[40] L. Zongyi, 'China and BRICS', in *Locating BRICS in the Global Order*, Routledge India, 2023, pp. 221–236.

[41] Y. Li and Q. Liu, 'A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments', *Energy Rep.*, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[42] K. Huang, M. Siegel, and S. Madnick, 'Systematically Understanding the Cyber Attack Business: A Survey', *ACM Comput. Surv.*, vol. 51, no. 4, p. 70:1-70:36, 2018, doi: https://doi.org/10.1145/3199674.

[43] S. Rangarajan and N. Kshetri, 'Cybersecurity challenges and issues in BRICS countries', *J. Cybersecurity*, vol. 2, no. 2, pp. 123–138, 2016.

[44] L. M. Hurel and L. C. Lobato, 'Cyber security governance in Brazil: Keeping silos or building bridges?', in *Routledge Companion to Global Cyber-Security Strategy*, Routledge, 2021.

[45] M. Garcia, F. Mendonça, and R. De Oliveira Albuquerque, 'Assessments on National Cyber Capability: A Brazilian

Perspective in a Comparison with Spain', in *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, Madrid, Spain, Jun. 2022, pp. 1–6. doi: 10.23919/CISTI54924.2022.9866889.

[46] J. Kluge, 'The future has to wait: 5G in Russia and the lack of elite consensus', *Post-Sov. Aff.*, vol. 37, no. 5, pp. 489–505, 2021, doi: 10.1080/1060586X.2021.1967071.

[47] M. Sharma, 'India and China: Warnings ignored?', in *National Cyber Emergencies: The Return to Civil Defence*, Routledge, 2020.

[48] W. Lu, Y. Zhang, W. Wen, H. Yan, and C. Li, *Cyber Security - 19th China Annual Conference, {CNCERT} 2022, Beijing, China, August 16-17, 2022, Revised Selected Papers*, vol. 1699. in Communications in Computer and Information Science, vol. 1699. Beijing, China: Springer, Cham, 2022.

[49] M. Malatji, A. L. Marnewick, and S. Von Solms, 'Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa', *Sustainability*, vol. 13, no. 1, Art. no. 1, 2021, doi: 10.3390/su13010291.

[50] EU Directive 2016/1148, 'EUR-Lex - 32016L1148 - EN - EUR-Lex'. Accessed: Nov. 07, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[51] J. Tarien, 'National cyber defence policies and the role of international cooperation', *Connections*, vol. 19, no. 1, pp. 5–7, 2020.

[52] K. Geers, 'Live Fire Exercise: Preparing for Cyber War', *J. Homel. Secur. Emerg. Manag.*, vol. 7, no. 1, 2010, doi: 10.2202/1547-7355.1780.

[53] UN GA Resolution 70/245, 'a/res/70/245'. Accessed: Nov. 07, 2023. [Online]. Available: https://undocs.org/Home/Mobile?FinalSymbol=a%2Fres%2F70%2F245&Language=E&DeviceType=Desktop&LangRequested=False

[54] World Bank, 'World Bank and partners announce new global fund for cybersecurity', World Bank. Accessed: Nov. 07, 2023. [Online]. Available: https://www.worldbank.org/en/news/press-release/2021/08/16/world-bank-and-partners-announce-new-global-fund-for-cybersecurity

[55] CISA, 'Partnerships and collaboration'. Accessed: Nov. 07, 2023. [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration

[56] OSCE, 'Confidence and Security Building Measures'. Accessed: Nov. 07, 2023. [Online]. Available: https://www.osce.org/secretariat/107484

[57] A. Lohachab, A. Lohachab, and A. Jangra, 'A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks', *Internet Things*, vol. 9, p. 100174, 2020, doi: 10.1016/j.iot.2020.100174.

[58] EU, 'Complete guide to GDPR compliance'. Accessed: Oct. 28, 2023. [Online]. Available: https://gdpr.eu/