Day One	
07:00 – 08:00	Registration, refreshments
08:00 – 10:30	**Session One** **Opening and Welcome:** *Conference Chair, Prof Manoj Maharaj* **Guest Speakers** *Jennifer Bachus: Principle Deputy Assistant Secretary Bureau of Cyberspace and Digital Policy, US State Department* *Joost Bunk, First Secretary, Netherlands Mission to South Africa* *Neal Kushwaha, National Security Centre of Excellence (NSCOE) Centre d'excellence pour la sécurité nationale (CdESN/COESN), Canada* **Discussions and Questions:** *Facilitator, Prof Manoj Maharaj* **Sponsors' Address** *Dimension Data – TBC* *MANCOSA University – Trisha Govender* *Snode, Mr Nithen Naidoo* **Address on behalf of the University of Stellenbosch and introducing the Honourable Deputy Minister:** *Prof Bruce Watson, University of Stellenbosch* **Opening Address** *Deputy Minister Department of Communications and Digital Technologies,* *The Honourable Mohlopi Phillemon Mapulane*
10:30 – 11:00	Networking Break, Refreshments
11:00 – 13:00	**Session Two** **Emerging issues in Cybersecurity – Quantum Computing and AI** **Session Chair: Dr. Jabu Mtsweni**
11:00 – 11:40	**Keynote Talks** **Presenter:** Prof. Francesco Petruccione **Affiliation:** University of Stellenbosch **Presenter:** Dr. Jabu Mtsweni **Affiliation:** Head, Information and Cyber Security Centre, Council for Scientific and Industrial Research
11:40 – 12:00	**Research papers** **Presenter:** Shirdhar Singh

		Affiliation: UKZN **Title:** 1. Towards Authenticity of Large-Language Model Computations using Zero-Knowledge Proof Validations **Presenter:** Ntshuleko Makondo **Affiliation:** TUT **Title:** 2. The latest developments in Quantum Computing in Cybersecurity for Financial Sector: Opportunities and Challenges
	12:00 – 13:00	Panel Discussion
13:00 – 14:00		**Lunch**
14:00 – 16:00		**Session 3** **Metaverse and Big Data, Information Warfare** **Session Chair: Prof. Kennedy Njenga**
	14:00 – 15:00	**Keynote Talks** **Presenter:** Distinguished Prof. Oleg Smirnov **Affiliation:** South African Radio Astronomy Observatory **Presenter:** Noelle Van der Waag-Cowling **Affiliation:** Cyber Program Lead, Security Institute for Governance and Leadership, Stellenbosch University **Presenter:** Prof. Bret van Neikerk **Affiliation:** DUT, Chair, International Federation of Information Processing Working Group on ICT in Peace and War
	15:00 – 15:20	**Research papers** **Authors: Heinke Lubbe,** Rudi Serfontein, Marijke Coetzee **Affiliation:** NWU **Title:** 3. A review of the security state of ADS-B: Threats and Mitigations **Presenter:** Sifiso Mgaga **Affiliation:** CSIR **Title:** 4. Secure Authentication Using Zero Knowledge Proof and Biometrics: A Review
	15:20 – 16:20	**Panel Discussion**
16:30 – 19:30		**Cocktail Reception**

Day Two	
08:00 – 10:30	**Session Four** **Cybersecurity for a Sustainable Future: Strengthening Resilience in Developing Countries** **Session Chair: Dr Kiru Pillay**
08:00 – 08:10	Opening and Welcome Prof. Bruce Watson
08:10 – 09:10	Keynote Talks **Presenter:** Muhammad Ali **Affiliation:** CEO WWise **Presenter:** Moliehi Makhumane **Affiliation:** Research Consultant, Cyber Diplomacy and International Security, United Nations Institute for Disarmament Research **Presenter:** Abdul-Hakeem Ajijola **Affiliation:** Chair, African Union Cyber Security Expert Group
09:10 – 09:30	**Research Papers** **Presenter:** Mkhululi Tyukula **Affiliation:** CSIR **Title:** 5. Cloud Computing Adoption by Developing Nations: Cybersecurity and National Security Implications **Presenter:** Thomas Appiah **Affiliation:** Ghana Communications Technology University **Title:** 6. Assessing the cybersecurity framework of developing countries: A case study of Ghana (Online)
09:30 – 10:30	Panel Discussion
10:30 – 11:00	**Networking Break, Refreshments**
11:00 – 13:00	**Session Five** **Securing the Network** **Session Chair:** Professor Kanshukan Rajaratnam
11:00 – 11:40	Keynote Talks **Presenter:** Shameer Amir **Affiliation:** CEO, Younite **Presenter:** Fabian Yamaguchi **Affiliation:** CTO, Whirly Labs, Associate Professor Extraordinary, Stellenbosch University
11:40 – 12:00	**Research Papers**

		Presenter: Faith Lekota (UJ), **Marijke Coetzee (NWU)** **Title:** 7. Enhancing Cybersecurity Incident Response and Resilience for South Africa's Critical Infrastructure **Presenter:** Ross Holder **Affiliation:** CSIR **Title:** 8. Enhancing Biosecurity and Combating Livestock Theft Through Cybersecurity Technologies **Presenter:** **Crestinah Mudau,** Mkhululi Tyukala, Heloise Meyer **Affiliation:** CSIR **Title:** 9. Mobile Application Security Assessment Platform (mSAP)
	12:00 - 13:00	Panel Discussion
13:00 – 14:00		Lunch
14:00 – 16:15		**Session Six** **Emerging issues in Cybersecurity Awareness, Training, and Development** **Session Chair: Jeanette Morewane (TBC)**
	14:00 – 14:40	**Keynote Talks** **Presenter:** Kerissa Verma **Affiliation:** Vodacom, Vodafone **Presenter:** Lee-Anne Major **Affiliation:** HR and Training Manager NIL Data (EC Council) **Presenter:** Anna Collard **Affiliation:** World Economic forum's Global Future Council, WEF Cybersecurity Skills Development Working Group
	14:40 – 15:20	**Research Papers** **Presenter:** Ndumiso Mahlangu **Affiliation:** ?? **Title:** 10. A framework for promoting cybersecurity awareness: South Africa **Presenter:** Ebenezer Malcalm **Affiliation:** GCTU **Title:** 11. Analysis of the effect of Artificial Intelligence on the academic performance, creativity and innovation of tertiary students in Ghana (Online) **Presenter:** **Baswibile Matamane** , Kennedy Njenga **Affiliation:** UJ **Title:** 12. On information security of SNS users and AI use in social engineering

		Authors: **Maoneke, PB**; Masuku, D; Wayi-Mgwebi, I; and Ngqondi, T. **Affiliation:** UM **Title:** 13. Citizen's Participation in MOOCs on Cyber-security: A Case of a Government's Upskilling Initiative
	15:20 – 16:15	Panel Discussion
16:15 – 16:30		**Session Seven** Closing

Paper Abstracts

1. **Shirdhar Singh**

   UKZN

   Towards Authenticity of Large-Language Model Computations using Zero-Knowledge Proof Validations

Abstract: Large-Language Models (LLMs) have become a playground for users and developers. However, they are limited in their range of knowledge. As such, the intention to provide systems with the most relevant information created the need to supplement this base knowledge (training data) with refined information to create 'expert-GPT' systems capable of greater understanding and interpretation than traditional GPT-models. Such systems have led to open-source projects capable of localising GPT models for private and business use-cases. This, however, sparks the concern of integrity and authenticity of LLMs in professional and personal environments where sensitive or mission-critical data are fundamental to operations and can therefore not afford to be factually incorrect, have malicious intentions, or be wielded by unauthorised personnel. In the above case, providing misleading data to the computation could yield incorrect and inaccurate results causing an output to become untrustworthy. Therefore, there is a dire need to create a more secure means of authentication, one that can validate multiple sources and ensure that the data is reliable to be used in the GPT computation. For this, we look to Zero-Knowledge Proofs as they are a modular and scalable proof system that can validate the legitimacy of models, data, and users without revealing sensitive/unnecessary information. Our work proposes the use of Zero-Knowledge Proofs for this purpose. Promising results not only validate desirability and feasibility, but also the viability of this approach.

2. **Ntshuxeko Makondo, Topside E. Mathonsi, Tshimangadzo M. Tshilongamulenzhe**

   Tshwane University of Technology

   The latest developments in Quantum Computing in Cybersecurity for Financial Sector: Opportunities and Challenges

Abstract: This study reviews the influence of Quantum Computing (QC) on banking cybersecurity. The paper opens with an introduction of QC and its essential concepts. This paper delves deeper into the benefits and drawbacks of QC. Furthermore, the study discusses how Quantum Computing will impact the banking sector in the future. According to the study's conclusions, Quantum technology can dramatically disrupt financial institutions and provide new avenues for innovation. This underscores the importance of corporations investing in expanding their Quantum Computing expertise while also addressing the potential risks and barriers associated with this technology. The study goes on to emphasize the need of staying ahead of the curve by investing in Quantum Computing and reaping its potential benefits for financial organizations.

3. Heinke Lubbe

???

A review of the security state of ADS-B: Threats and Mitigations

Abstract: The Automated Dependent Surveillance-Broadcast system (ADS-B) is a novel method of tracking air traffic that promises to provide the necessary precision to enhance situational awareness. Airlines and air traffic controllers also benefit from the operational improvements introduced by ADS-B, leading to reduced chances of air traffic incidents. The Federal Aviation Administration has therefore enforced ADS-B's deployment. However, the intrinsic nature of ADS-B introduces several security concerns. This paper provides a critical review and analysis of the security of the ADS-B system. A review of proposed mitigations highlights the need for a better alternative to anticipate and mitigate potential security threats.

4. Madau/Ntshangase

CSIR

Secure Authentication Using Zero Knowledge Proof and Biometrics: A Review

Abstract: Secure authentication is a very crucial feature to maintain privacy and security of sensitive data such as biometrics. Zero Knowledge Proof (ZKP) is one of cryptographic techniques widely used to improve privacy and security by allowing one party to prove to another party that they know a piece of information, without revealing the information itself. In this study, we conducted a review using the PRISMA framework to explore the use of ZKP and biometrics for authentication, its applications, and different protocols. Our findings highlight the significance of multi-party authentication scenarios and identify fingerprints, face, and iris as commonly used biometrics with ZKP. The Schnorr original method emerges as a widely employed ZKP protocol. Lastly, we provide future directions for leveraging ZKP in secure authentication systems.

5. Tuyukula

??

Cloud Computing in Developing Nations: Beyond Cybersecurity to National Security Implications

Abstract: Since the introduction of the first platform called Amazon Web Services (AWS) by Amazon in 2006, cloud computing has revolutionized the way organizations procure, use, and manage information technology (IT) services worldwide. The cloud eliminates the need for organisations to build their own physical infrastructure prior to bringing their services to life. As such, it helps organisations shorten the time and effort it takes to bring their services to

their target audience. Recently, governments from both developed and developing nations have begun to transition their systems to cloud-based platforms. However, this migration brings forth significant threats, especially in the realms of cybersecurity and geopolitical stability. These challenges extend beyond mere technical vulnerabilities, potentially threatening the national security of the nation and need to be taken into consideration before the developing nations can fully adopt cloud computing. As such, this paper aims to highlight these challenges in developing nations, emphasizing that they are not limited solely to cybersecurity but have broader implications for national security.

6. Eric Appiah

GCTU

Assessing the cybersecurity framework of developing countries: A case study of Ghana

Abstract: The focus of this paper is to assess the effectiveness of Ghana's cybersecurity policies, laws, and directives in addressing the evolving landscape of cyber threats and vulnerabilities. We relied on the literature and expert opinions to investigate the cybersecurity measures and policies of the country. With the help of NVivo software, we analysed legal documents, policy frameworks, and interview data with relevant stakeholders. These stakeholders include government officials, legal experts, cybersecurity practitioners, and private sector representatives. The findings reveal that whereas Ghana is making giant strides in enhancing its cybersecurity architecture through the establishment of a legal foundation for cybercrime prevention and data protection, there are still loopholes and vulnerabilities that could increase the cyber threats faced by the country. We find discrepancies between policy intent and practical implementation, which has the potential to undermine the effectiveness of policies, directives, and legal frameworks instituted by the country. A thorough analysis of relevant data revealed that there are key areas that require improvement, and these include capacity building for institutions and regulatory agencies, improving collaboration among different sectors, enhancing public–private partnerships, and promoting cybersecurity education and awareness among key stakeholders and the public. Furthermore, the study underscores the need for periodic reviews and updates to legal frameworks and directives to align with the evolving cybersecurity landscape. By using Ghana as a case study, this paper contributes to the intellectual discourse on cybersecurity effectiveness in developing nations. Additionally, the evaluation of the existing policies and legal structures is important in providing valuable insights that can inform policy reviews and strategic interventions. This paper thus serves as a guide for Ghana and similar countries as they strive to develop a more robust cybersecurity environment that will foster innovation and economic development.

7. Maritje Coetzee

NWU

Enhancing Cybersecurity Incident Response and Resilience for South Africa's Critical Infrastructure

Abstract: Cyberattacks targeting critical infrastructure (CI) have become a global concern, with ransomware attacks posing a significant threat. Following international best practices, South Africa must safeguard its critical infrastructures against these evolving threats. This paper presents incident response recommendations to bolster the resilience of South Africa's critical infrastructure in the face of attacks such as ransomware and other cyber threats. The current state of critical infrastructure protection in South Africa, as defined by the National Cybersecurity Policy Framework (NCPF), is reviewed, and challenges to be addressed are identified. European aviation CSIRT structures are described to provide more insight into current best practices. The paper offers a set of recommendations, including establishing a coordinated incident response network to strengthen the incident response capabilities of South Africa's critical infrastructure.

8. Holder

CSIR

Enhancing Biosecurity and Combating Livestock Theft Through Cybersecurity Technologies

Abstract: The South African livestock is extremely vulnerable to periodic transboundary or high-impact diseases. These outbreaks of diseases, such as Foot and Mouth negatively impact the domestic trade and exportation of certain livestock products or species. Currently, South Africa has been barred from exporting meat and meat products due to the lack of animal traceability system that ensures that infected animals are isolated, and their movement is controlled electronically. Besides the transboundary diseases, the South African livestock is also prone to theft for immediate slaughter and sell or for sell to neighboring countries. The impact of stock theft is enormous and involves economic loss due to food security and employment opportunities in farms, animal cruelty, and human safety in terms of crimes and illicit meat consumption. There is currently insufficient enforcement of animal's movements, treatment, vaccination, and health information related to animal health status. This lack of enforcement compounds the issues related to disease outbreaks, as guarantees regarding these diseases cannot be given to trade partners even though animal movements need to be recorded by law. This paper presents a livestock identification and traceability system, for South Africa which exploits the RFID tags, and software development tools and enhance unique identification of individual animals and their traceability. The system has showed promising results since its pilot deployment is six (6) South African provinces.

9. **Mudau**

CSIR

Mobile Application Security Assessment Platform (mSAP)

Abstract: In recent years, the proliferation of smartphones has led to the development of mobile applications with capabilities previously exclusive to computers. However, if not properly vetted, these applications can pose significant security and privacy risks to users. Notably, there have been widely reported security incidents involving high-ranking businessmen and world leaders through their mobile devices. A pressing concern arises: how can we ascertain the security of the applications we install on our smartphones? How can we ensure they function as advertised and only perform tasks chosen by the user? This paper introduces the initial phase of the Mobile Application Security Assessment Platform (mSAP). mSAP is designed to evaluate the security of mobile applications before installation, ensuring they operate as intended and safeguard user data.

10. **Ndumiso Mahlangu**

UNISA

A framework for promoting cybersecurity awareness: South Africa

Abstract: In today's technology-driven landscape, safeguarding information systems is imperative. Industries heavily depend on digital tools, emphasizing the need for secure practices. Adherence to computer usage principles is vital for end-users and organizations, forming the foundation for system integrity. Neglecting these principles exposes vulnerabilities, exploited by malicious actors. Cybersecurity breaches cause substantial harm, leading to financial losses. Breaches often result from inadequate knowledge and lax security measures, with detection typically occurring post-attack. End-users are susceptible to sophisticated cybercriminal tactics. As internet user numbers surge, so do cyber-attacks' frequency and sophistication, presenting a formidable challenge. This study introduces a governance framework to fortify defenses against cyber-attacks, safeguarding organizations and end-users. By establishing a structured procedural foundation, this framework aims to proactively mitigate cybersecurity risks in an era characterized by escalating digital reliance.

11. **Ebenezer Malcalm, Esther Aseidu, Ruhiya Abubakar, Isaac Boakye, Theresa Obuobisa Darko, Nusrat Jahan Abubakar, Afia Nyarko Boakye**

GCTU

Analysis of the effect of Artificial Intelligence on the academic performance, creativity and innovation of tertiary students in Ghana

Abstract: This study aimed to explore the effects of Artificial Intelligence (AI) on the academic performance, creativity, and innovation of tertiary students in Ghana. A mixed method

research approach was employed where the explanatory sequential design was used. Qualitative data was collected through semi-structured interviews with 10 respondents, consisting of five students and five educational experts from tertiary schools in Ghana. Quantitative data on the other hand was collected from 510 students. The qualitative data was analyzed using thematic analysis, and the findings were triangulated through member checking and peer review. Quantitative data on the other hand was analyzed using STATA. The study found that there was a significant negative impact of AI on creativity and innovation, but had a positive impact on academic performance. The qualitative data on the other hand further emphasized that while AI can be a helpful tool for students, there are potential negative consequences if students become overly reliant on it. The participants noted that students are relying heavily on AI to complete their work, rather than putting in the effort to truly understand the concepts they are learning. The educators also noted that students become frustrated when they do not have access to AI during exams or quizzes, highlighting the potential impact on their academic performance. The study also found that AI has the potential to perpetuate biases if the data it's trained on is biased. This could have significant implications for academic research and grading, as the AI may be relying on biased sources or criteria. Furthermore, the study found that overreliance on AI may hinder the development of critical thinking skills, which are essential for future success in academic and professional settings. This has potential implications for their academic performance and future career prospects. Overall, the study highlights the need for continued research and thoughtful integration of technology in educational settings. Educators and students need to be aware of the potential drawbacks of AI and take steps to ensure that AI is used in a way that enhances, rather than hinders, their academic success.

12. Njenga

UJ

On information security of SNS users and AI use in social engineering

Abstract: The paper explores the possibility that as artificial intelligence (AI) gains traction in social network site (SNS) usage, this novel technology will be used for nefarious purposes, detrimental to SNS information security posture. Using the constructs developed by Rogers in the diffusion of innovation theory, the paper tests the readiness of AI to carry out sophisticated phishing attacks. A quantitative deductive approach was used to measure this readiness. An online survey instrument was distributed to practitioners familiar with AI technology in Gauteng province of South Africa. Findings indicate that the constructs, relative advantage, complexity and compatibility will strongly influence readiness of AI adoption in phishing attack campaigns. The implications for these findings are discussed in the main paper.

13. Maoneke

UM

Citizen's Participation in MOOCs on Cyber-security: A Case of a Government's Upskilling Initiative

Abstract: Little has been done to establish the uptake of skills development and up-skilling initiatives that are being facilitated by the National Electronic Media Institute South Africa (NEMISA). Some of these initiatives are based on Massive Open Online Courses (MOOCs) that brings in an interesting subject of navigating challenges of human computer interaction in the process of learning the subject matter. This study explores secondary data to establish the interest in participating in cybersecurity skills development by South African citizens. The study use data that was accessed from Coursera's MOOCs platform. This dataset was accessed through NEMISA. Study findings confirm that citizens do have an interest in enhancing skills with a particular bias towards enhancing information technology skills, cybersecurity skills included. However, descriptive statistics used to analyze the dataset suggest the numbers of students on enrolment, active participation, dropout, and course completion differ according to course. There are also findings that do not align with expectations. For instance, the data set shows a high dropout rate and inactivity on both courses that have been reported to be demanding and less demanding according to the literature. Findings in this study can be used to formulate future research and motivate a continued use of MOOCs in promoting skills development.