Africa's Contribution to Academic Research in Cybersecurity

Author(s): S von Solms

Source: *Journal of Information Warfare*, Spring 2019, Vol. 18, No. 2 (Spring 2019), pp. 60-73

Published by: Peregrine Technical Solutions

Stable URL: https://www.jstor.org/stable/10.2307/26894671

Africa's Contribution to Academic Research in Cybersecurity: Review of Scientific Publication Contributions and Trends from 1998 to 2018

S von Solms

Department of Electrical Engineering Science
University of Johannesburg Johannesburg,
South Africa

Email: svonsolms@uj.ac.za

Abstract: *Contributions of scientific knowledge in cybersecurity are made by researchers globally, where the focus and scope differ based on the development and challenges in cybersecurity faced by each country. This study examines the publication contributions and trends of African researchers in the field of cybersecurity for a period of 20 years (1998 to 2018). Drawing data from various leading scientific databases, this paper looks at the publication patterns and contributions of cybersecurity research from Africa. This study shows that South Africa is at the forefront of cybersecurity research in Africa, but that many other African countries are starting to make research contributions in this field.*

Keywords*: Cybersecurity, Information Security, Influence, Technology, Research*

Introduction

Economic growth and various elements of social progress are largely due to advancements in technology (World Bank 2008), where new trends in technology due to the Fourth Industrial Revolution have already impacted the global business ecosystem and social welfare. This revolution has provided opportunities for innovation, improved productivity, advanced manufacturing technologies, and sophisticated communication methods amongst many (Heeks & Stanforth 2015; Signé & Signé 2018). However, this transformation in the use of technology brings forth an increased exposure to cyberattacks and other cyber-related threats. As the global landscape of cyber threats is changing as quickly as technology itself, research and innovation in the field of cybersecurity must keep pace with the changes.

Across Africa, countries are becoming an increased target for cybercriminals due to the increase of Internet penetration and a lack of corresponding cybersecurity expertise. Due to the borderless nature of cybercrime and other cyber-related threats, many of the global cybersecurity issues prevalent worldwide are also affecting Africa. The African landscape has proven to be a hotbed for cybercriminals, as many are exploiting African nations with weaker network and information security controls (Alfreds 2015; United Nations Economic Commission for Africa [UNECA] 2014). Cybercrime, such as identity theft, fraud, and espionage, has the highest growing rate in Africa

(Symantec Corporation 2013). The Africa Cybersecurity Report in 2017 indicated that cyberattacks cost Africa approximately $3.5 billion annually and that over 90% of African organisations, particularly small and medium enterprises (SMEs), do not have the skills, resources, or funding to protect, detect, and respond to cybersecurity threats (Africa Cybersecurity Report 2017). The African continent is ill-prepared to deal with information security threats due to a lack of technical know-how, cybersecurity legal frameworks, funding, and skilled professionals (van Heerden, von Solms & Vorster 2018; Musuva-Kigen, Mueni, Ndegwa 2015).

Against the backdrop of these reports, the question that emerges is whether the status of African cybersecurity in any manner reflects the production of scientific publications in this field. This study aims to analyse the contribution and trends in cybersecurity research in Africa during the last 20 years. This study will indicate the condition of cybersecurity research in Africa and could help to further drive progress, growth, and direction in the field.

History of Cybersecurity and the African Landscape

The field of cybersecurity has developed as networks and network-related technology have developed. The early days of computing regarded computers as devices for making calculations, storing data, and automating simple business processes (Bourgeois 2014). As these computers evolved in the mid-1980s, businesses began to see the need to connect their computers together to collaborate and to share resources. Computers were connected to communicate with each other, forming small networks (Bourgeois 2014). The combining of these telecommunications and information systems led to the forming of Information Technology (IT) departments within organisations. The networking architecture was a client-server architecture in which users could log in to the local network to access various resources on the network, mainly within their own organisation (Bourgeois 2014). During this time, information security was an active field of research mainly related to the infiltration of lone standing computers and small computer networks, as well as to the protection of data on these computers. In South Africa, the first computer science departments were established in the 1970s, including those at the University of Stellenbosch (University of Stellenbosch 2018), Rand Afrikaans University (now University of Johannesburg) (University of Johannesburg 2011) and the University of Pretoria (University of Pretoria 2012). African research prior to 1990 focussed on protecting the physical computer infrastructure and ensuring continuous operation (Gerber & von Solms 2001).

The precursor to the Internet, ARPANET, started the notion of connected computer networks which could communicate with other networks running a proprietary protocol. In the 1980s, many computers were added to the Internet at an increasing rate, mostly from government, academic, and research organisations (Bourgeois 2014). South Africa has a history with Internet research, which started during this time when researchers at Rhodes University established an email link to the Internet in 1988 (TENET 2014). The late 1980s saw a string of computer network nuisance attacks, including the first computer worm in 1989, namely the Morris worm. The Morris worm was the world's first self-replicating computer worm which spread so rapidly that it effectively shut down a large part of the Internet (Julian 2014). The cybersecurity field can be generally traced back to the establishment of the first Computer Emergency Response Team (CERT) in the late 1980s, established as a central point for co-ordinating responses to cyber-related emergencies, such as the Morris worm. As the Internet was still in its infancy, these attacks were manageable, but industry

reacted to these attacks by starting to develop various preventative and detective security products (Julian 2014). Research in this era still included physical protection, but moved towards technical controls, such as authentication, access controls, the secure use and storage of data in databases, and the encryption of data (Gerber & von Solms 2001).

The early popularity of the Internet was driven by its telecommunication function using electronic mail (email). The introduction of the World Wide Web project in 1990 provided users with a user-friendly way to navigate the Internet, where the first commercial web browser, Netscape Navigator, became available in 1994 (Bourgeois 2014). Residential Internet services were available from 1997, and the Tertiary Education and Research Network of South Africa (TENET) launched in 2000 (TENET 2014). The creation of online content was highly technical which limited creation of content to a small number of skilled individuals. Internet browsing was, therefore, mostly limited to viewing and downloading content, not uploading and sharing. In this era, viruses started to become more prevalent and caused systems to fail but had no strategic objective or financial motivation (Julian 2014). There exist many instances of individuals hacking their way through security features of companies without doing any harm but simply seeing what they could do. One such incident on African soil was traced to a 15-year-old boy who hacked into computer systems of the South African telecommunications company, Telkom, in 1998 but did no harm, even though he was able to (van Heerden, von Solms & Mooi 2016). The age of computer viruses led to the inception of anti-virus technologies to detect the signatures of viruses and to stop them from executing (Julian 2014). These incidents also gave birth to cybersecurity awareness, which drove companies and individuals to realise the risks of reading emails from untrusted sources, opening attachments, and other unwanted intrusions (Julian 2014). The first International Federation for Information Processing Conference on Information Security and Privacy Protection (IFIP SEC Conference) was held on African soil in 1995 in Cape Town, South Africa, with the theme "Information security—the next decade".

In the late 1990s and early 2000s, the commercialisation of the Internet enabled companies to start online commerce (Bourgeois 2014). The creation of Web 2.0 applications provided users the ability to create custom web content and interactive websites without requiring advanced knowledge of programming to put information online (Bourgeois 2014). Poor business models as well as the lack of cybersecurity knowledge by many companies enabled cyberattacks to become more targeted with clear financial motivation. This era saw the first serial data breach of credit card numbers, followed by multiple attacks of the same nature. Companies realised the financial consequences of bad security structures as the intervention of authorities were required, and victims had to be compensated for the theft and exploitation of regulated data (Julian 2014). These consequences motivated companies to develop and implement more sophisticated security systems to arm themselves against cyberattacks (Julian 2014). In the early 2000s, individuals were targeted by phishing email scams, including romance, advance-fee, and the 'Nigerian Prince' emails, which put West African countries on the cybercrime map (Cabrera 2017). Unsuspecting victims were convinced to transfer large amounts of money to the scammers who contacted them via email. International and regional organisations also started to developed conventions, agreements, and guidelines, which included The Council of Europe Convention on Cybercrime (2001), The European Union Directive on attacks against information systems (2013) and the African Union Convention on Cyber Security and Personal Data Protection (2014) (Schjølberg 2017).

In the current landscape, cybercrime and other cyber-related attacks are extremely diverse, ranging from personal information theft to sophisticated attacks on a country's critical infrastructure. The range and impact of these attacks are further accelerated by the high level of connectivity of technology across the globe. High focus is placed on understanding the risk of cybercrime and other cyber-related attacks, which includes cybersecurity awareness and education to enable users of technology to safely navigate the technological landscape and to manage the risks related to cyberattacks (Julian 2014). The utilisation of technology and the implementation of business practices to secure data and sensitive information requires cybersecurity knowledge. However, in the changing landscape, cybersecurity knowledge and practices must continue to adapt to the changing technologies, which would require individuals, organisations, and governments to develop cyber-resilience—the ability to prepare for and recover from known and unknown cyber-related threats (Collier *et al.* 2015).

The establishment of cybersecurity knowledge and cyber-resilience in Africa requires a broad and comprehensive approach, which includes education and research (Dalton, Jansen van Rensburg & Westcott 2017). As cyber-related skill sets are in high demand but in short supply, tertiary education and research done at African universities must aim to expand the pool of cybersecurity professionals and to create resilient societies. Based on a broad search on the used databases, the author found that the following African countries run formal cybersecurity-related university undergraduate or postgraduate degrees: South Africa (9), Tunisia (3), Nigeria (2), Egypt (2), Kenya (1), Ghana (1) and Ethiopia (1). Various African countries also have cybersecurity-related certifications or short courses. Considering the limited number of formal tertiary education programmes throughout Africa on cybersecurity, this research aims to determine the scale and impact of cybersecurity-related research throughout Africa.

Methodology and Information Sources

As noted in the introduction, this study aims to analyse the trends in cybersecurity research from African-based researchers over the last 20 years. To determine research trends and contributions, peer-reviewed scholarly articles and professional academic journals were utilised to gain insight into scientific outputs (Tijssen 2007). Only English-language journals and peer-review conferences with good international reputations were considered. This was done by drawing data from two reputable databases, IEEE Xplore and Scopus. IEEE Xplore is a digital library containing scientific and technical content published by the IEEE (Institute of Electrical and Electronics Engineers) and its publishing partners on electrical engineering, computer science, and electronics). Scopus is the largest abstract and citation database of peer-reviewed literature, which includes scientific journals, books, book chapters and conference proceedings. The author notes that other reputable databases exist, but the utilised databases allow for the capture and analysis of published articles through integrated search tools. The following steps were followed in this research process:

Step 1: The period 1998 to 2018 was considered for this research as this period covers most of the cybersecurity history, as described in the second section of this paper.

Step 2: IEEE Xplore and Scopus were selected as appropriate databases as they publish content in the applicable field and provide integrated tools for data capture and analysis.

Step 3: The key words and search terms selected for this research were

cybersecurity
cyber AND security cyber
AND safety information
security information AND
security.

These search terms were considered due to their relevance to the cybersecurity-related fields and to relevant history.

Step 4: The metadata of each paper in the selected databases was searched for the above key words. When an applicable paper was found, the following information was stored in a database:

Title of paper
Year of publication
Authors
Author affiliations
Keywords
Name of conference proceedings or journal
Number of citations.

Step 5: From the search results collected in the database in Step 4, all duplications were removed.

Step 6: After a search in the author-affiliation field, each paper (co)authored by at least one author with an African affiliation was marked as an "African contribution". All other publications were marked as "Other publications".

There exist multiple African corporations conducting cybersecurity research in Africa. Note that this search does not include corporate research into cybersecurity, as this study only considers the contribution of academic research from African academic institutions. This search is not an exhaustive study as not all academic databases were considered in this study. However, the search was of sufficient size to provide an accurate view of trends in African cybersecurity publications.

Results

The data collection method discussed in the methodology section of this paper was followed, using the IEEE Xplore and Scopus databases. In total, 8,484 academic papers were collected, which included papers published in conference proceedings, book chapters, academic books, and journal articles. The determined trends are presented in the subsequent sections.

Publications per year of African countries

The first result shows the total number of African publications included in IEEE Xplore and Scopus databases from 1998 to 2018. The total number of publications for African countries per year are shown in Figure 1, below.

It can be seen from the graph in **Figure 1**, below, that the number of publications is increasing annually, with an exponential increase in publications within the last two years. The year 2016 saw approximately 58 publications from the African continent on cybersecurity, which increased to 100 in 2017 and approximately 375 in 2018, based on numbers from the databases identified. The dotted line in the figure indicates the trendline.

To put these publication values in perspective of the global average, the total number of publications from Africa in relation to the total number of publications worldwide were calculated:

$$\frac{\text{\# African publications}}{\text{\# Total publications}} \times 100$$

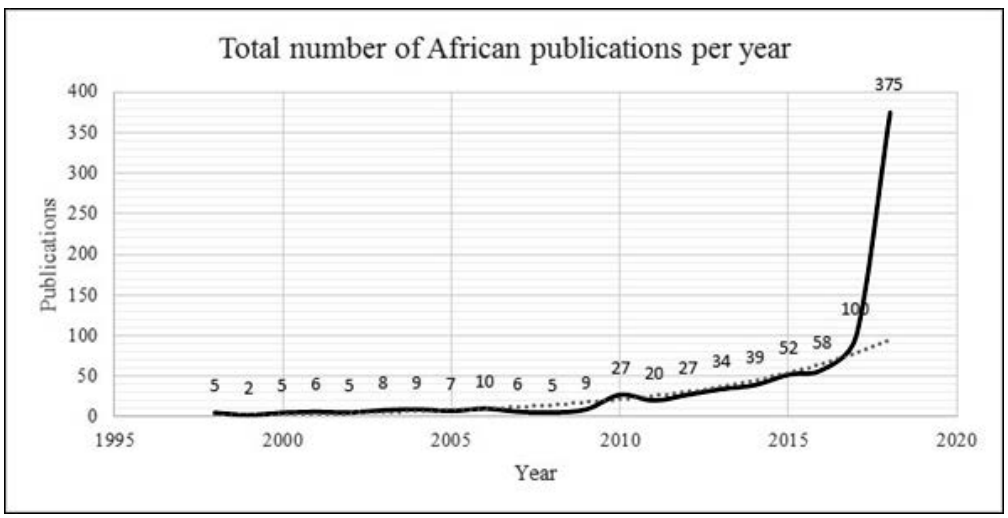

Figure 1: Total number of publications per African countries per year

The graph in **Figure 2**, below, shows the percentage of African publications per year from 1998 to 2018. The dotted line in the figure indicates the trendline.

It can be seen from **Figure 2** that the African percentage of publications has grown to approximately 10% of the global cybersecurity publications since 2015. The graph shows an upwards trend, which indicates a continuous increase in cybersecurity research from African countries.

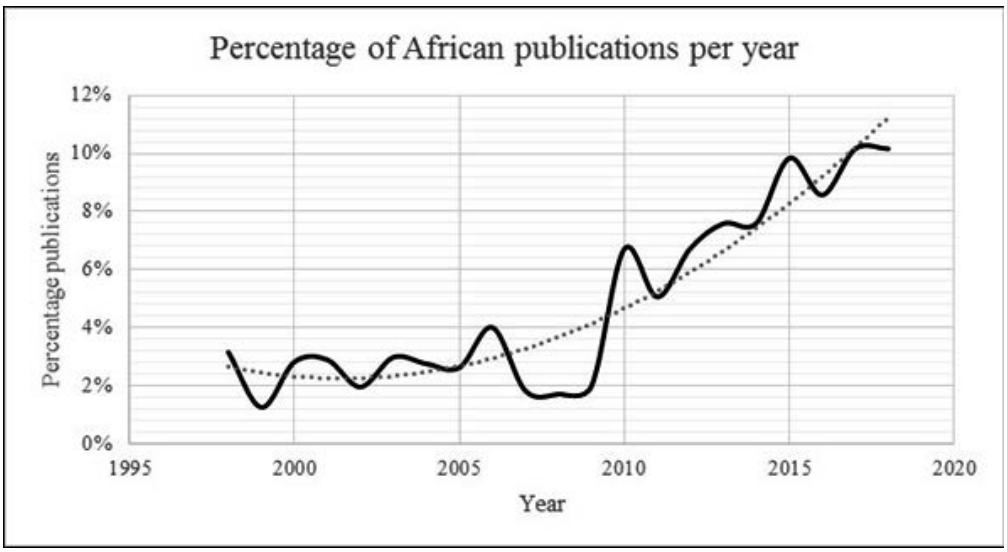

Figure 2: Percentage of African publications per year

Citations of African publications

In addition, the impact of the African publications was investigated. The citation impact of academic articles is often used as an indicator of international scientific impact, which in turn reflects to some degree their scientific relevance and quality (Waltman 2015). This study follows the same approach, that is, the number of citations were used as an indication of the scientific relevance of the publications. The researcher acknowledges that the citation count is not the only indication of scientific relevance, as citations accrue over time. Other factors indicating scientific relevance can include acceptance rate of the conference or journal, as well as the impact factor of the journal.

Figure 1, above, shows that between 1998 and 2004 less than 10 African publications per year were found in the searched databases. However, the average number of citations for these publications vary between 80 and 150 per paper. This average citation value indicates that, although publications from African authors was approximately 3% of the global number of publications, they were publications of scientific relevance and quality. Many of the older works are seminal work in cybersecurity, which are still referenced in cybersecurity research.

The top 10% of African publications with the highest number of citations as well as the top 10% of other publications with the highest number of citations were collected. The average number of citations of the top 10% of both African and other publications were calculated. The results are shown in **Figure 3**, below.

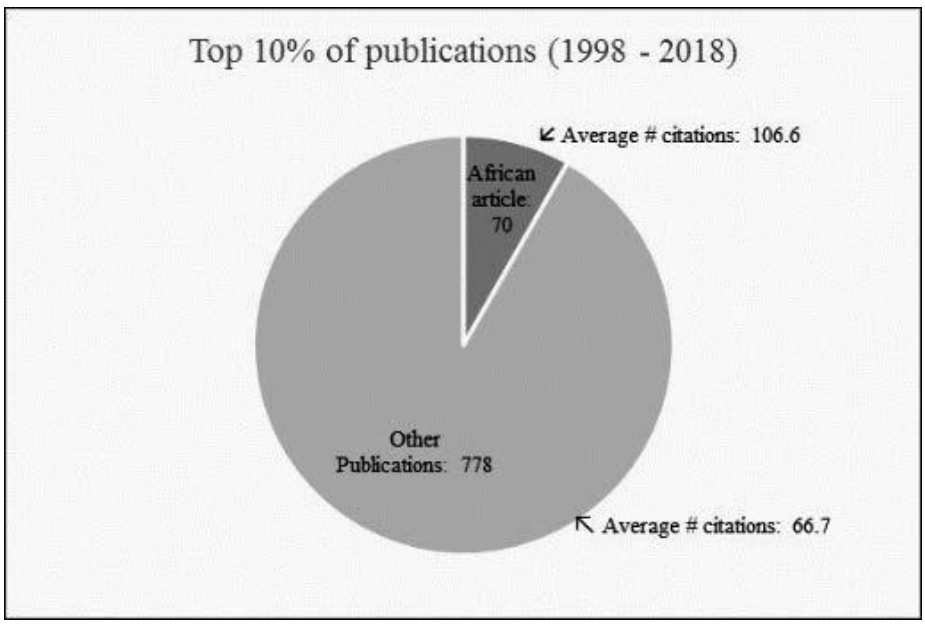

Figure 3: Average citations of top 10 % of publications (1998-2018)

The top 10% of articles were determined:

The top 10% of the other publications were a total of 778 articles.
The top 10% of the African articles were determined to be a total of 70 papers.

The following was found regarding citation count:

Average number of citations for other publications was equal to 66.7.
Average number of citations for Africa articles was equal to 106.6.

Although the African continent produced fewer publications, the average number of citations per paper are higher for the top-cited papers, showing global impact of the research done on the African continent.

African countries publishing in cybersecurity

The final investigation was to determine the contribution made by African countries to cybersecurity research. **Figure 4**, below, indicates the total number of publications from contributing African countries over the total of 20 years.

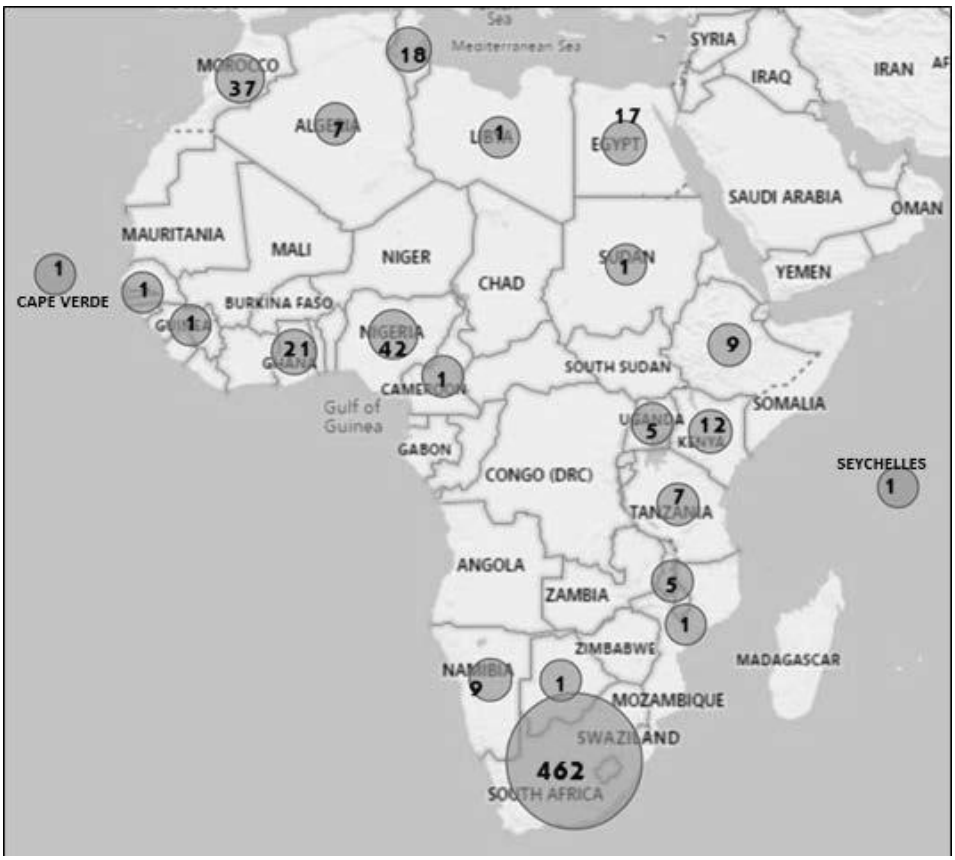

Figure 4: Total number of publications from contributing African countries

Figure 4 shows that South Africa has made the largest contribution to cybersecurity research on the African continent over the last 20 years. The other African countries' publications are considerably fewer in number than those of South Africa, with Nigeria, Morocco, and Ghana at 42, 37, and 21 total publications, respectively. South African researchers have contributed to cybersecurity research since 1998, while the other African countries are only now starting to conduct research in this field. To indicate the increase in the number of African countries conducting cybersecurity-related research, **Figure 5**, below, shows the number of African countries that published research in the field of cybersecurity since 1998.

As stated above, South Africa is the only country that has conducted cybersecurity research since 1998. However, the number of contributing countries is steadily increasing. From 2015 to 2017, eight African countries have contributed to cybersecurity research, with that number increasing to 18 countries in 2018. The total number of African countries contributing to this field has been increasing significantly since 2011.

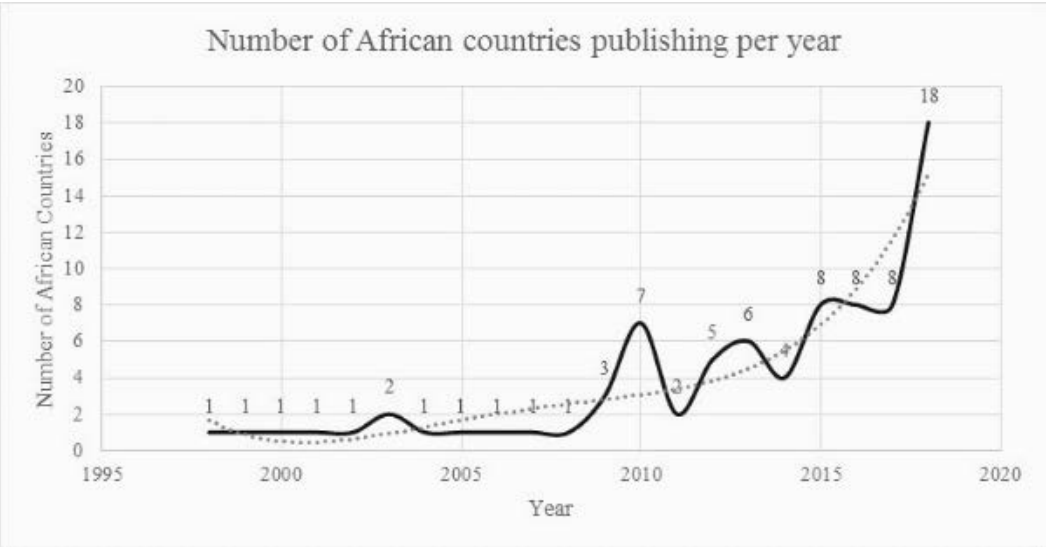

Figure 5: Total number of African countries conducting research in cybersecurity

The research trends seen in **Figure 5** are consistent with the Internet rollout timelines of African countries. Residential Internet services in South Africa were available from 1997, and the Tertiary Education and Research Network of South Africa (TENET) launched in 2000 (TENET 2014). A high growth in Internet access in Africa was only seen from 2005, when mobile Internet drastically increased Internet penetration throughout Africa (Nyirenda-Jere & Biru 2015). Between July 2010 and July 2011, a total of 45,498 km of terrestrial fibre optic network was rolled out across Africa, linking an additional 53,885 million people across Sub-Saharan Africa to broadband Internet. In December 2012, Africa's international Internet bandwidth reached 1.479 Tbps and passed 2 Tbps in June 2014 (Hamilton Research 2019). It can also be seen that countries running formal undergraduate and postgraduate cybersecurity-related programs, including South Africa, Nigeria, Ghana, Tunisia, Egypt, and Kenya, have produced higher numbers of research publications.

Discussion

The results presented in the above sections indicate that South Africa is the African country with the longest history related to cybersecurity research in the academic space. It was shown that, although the African continent produced approximately 10% of cybersecurity-related research, the average number of citations is higher for those top-cited papers than it is for the articles published in the rest of the world: the average number of citations for African articles is 106.6 compared to 66.7 for the rest of the world. The higher average citation rate of the top African papers compared to the global average indicates the global impact of the research done on the African continent.

The trends show that more and more African countries are joining cybersecurity research, with only one country (South Africa) conducting cybersecurity research in 1998 and at least 18 countries in 2018. The results show that, although there are limited academic institutions in Africa where a formal cybersecurity-related degree can be obtained, the number of research publications is increasing. This study shows that South Africa has been and still is at the forefront of cybersecurity research on the African continent, but that many African countries are starting to make research contributions in this field.

The most frequently used words found in the titles of the African publications are included in the word cloud shown in **Figure 6**, below. From this figure, along with the general cybersecurity-related topics such as information, cybersecurity, security, and technology, topics such as health, development, education, and learning are also featured in African cybersecurity-related research.

Figure 6: Word cloud indicating the most frequent words in African research paper titles (https://worditout.com)

Conclusion

Research and innovation can generate advances that help cybersecurity keep up with the evolving cyber risks and, in turn, create a trusted and resilient digital environment. Although the participation of African countries in cybersecurity research is growing, the number of countries participating in research in this field is still very low.

To support progress in cybersecurity research in more African countries, research should be pursued that integrates insights from different disciplines and around the globe. For African universities to conduct original cybersecurity research, it is imperative that researchers have access to content and examples from the African continent which are conducted in the African context as well as from first-world research content. In many cases throughout Africa, African university libraries are not open access, and Africa cannot see its own research—it only has open access to first-world content. African university libraries should upgrade their libraries so that African researchers can obtain content and research from the African continent and context.

African cybersecurity research can also be supported by the development of more ambitious, challenge-led research funding organisations as well as the continuation of dedicated cybersecurity conferences and summits on the African continent. Academic and corporate cybersecurity events enable cybersecurity researchers from Africa and across the globe to come together and share ideas, initiatives, and solutions in the cybersecurity space. Such meetings also enable researchers to facilitate deeper cooperation across Africa and the globe. The support of governments and pri-

vate organisations in academic conferences as well as other well-resourced strategic initiatives will also support growth in African cybersecurity research.

This research shows that popular themes in African cybersecurity research include health, development, education, and learning. In the last decade, African research relating to the Internet of Things and Industry 4.0 (4IR) shows a massive increase. However, only 4% to 14% of the published research in these areas includes research relating to cybersecurity. Africa, like the rest of the world, is faced with the rapid advancement of 4IR and the potential that 4IR technologies offer. Given the convergence of multiple digital fields as well as the speed required for 4IR technologies, cybersecurity will become a pillar of Industry 4.0. Consequently, cybersecurity research in this field must become a future topic for African cybersecurity research.

The scope and progression of 4IR and future trends in technology, health, and education are almost inconceivable, but it is definitely the case that connectivity and convergence will be the backbone of future technologies and organisations. Translation of innovative ideas and approaches from research will create a strong supply of reliable, proven solutions to difficult-to-predict cybersecurity risks. These advances are necessary to meet the cybercrimes and other cyber-related attacks that will inevitably increase as new technology is adopted at a great pace in African countries and around the globe.

References

Africa Cybersecurity Report 2017, 'Achieving cyber security resilience: Enhancing visibility and increasing awareness', *Serianu*, viewed 16 August 2019, <http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf>.

Alfreds, D 2015, 'Cyber criminals target Africa', *Times Live*, viewed 16 August 2019, <https://www.timeslive.co.za/news/sci-tech/2015-12-22-cyber-criminals-target-africa/>.

Bourgeois, D 2014, *Information systems for business and beyond, The Saylor Academy*, viewed 16 August 2019, <https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond.pdf>.

Cabrera, E 2017, 'The culture of cybercrime in West Africa', *Trend Micro*, viewed 16 August 2019, <https://blog.trendmicro.com/category/cybercrime/>.

Collier, Z, Panwar, M, Ganin, A, Kott, A & Linkov, I 2015, 'Security Metrics in Industrial Control Systems', *Cyber Security of Industrial Control Systems, Including SCADA Systems*, ed. E Colbert & A Kott, Springer, New York, NY, US.

Dalton, W, Jansen van Rensburg, J & Westcott, J 2017, 'Building cybersecurity resilience in Africa", *Proceedings of 12th International Conference on Cyber Warfare and Security (ICCWS 2017)*, Academic Conferences and Publishing International Ltd, pp. 112-20.

Gerber, M & von Solms, R 2001, 'From risk analysis to security requirements', *Computers and Security*, vol. 20, no. 6, pp. 577-84.

Hamilton Research 2019, 'Terrestrial network rollout increases Africa's fibre reach by 54 million', *Africa bandwidth maps*, viewed 16 August 2019, <http://www.africabandwidthmaps.com/?p=2394>.

Heeks, R & Stanforth, C 2015, 'Technological change in developing countries: Opening the black box of process using actor-network theory', *Development Studies Research*, vol. 2, no. 1, pp. 33-50.

Julian, T 2014, 'Defining moments in the history of cyber-security and the rise of incident response', *Infosecurity Group*, viewed 16 August 2019, <https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/>.

Musuva-Kigen, P, Mueni, F & Ndegwa, D 2016, 'Africa cyber security report 2016', *Serianu Cyber Threat Intelligence Team*, Lavington, Nairobi, KE.

Nyirenda-Jere, T & Biru, T 2015, 'Internet development and Internet governance in Africa', *Internet Society*, viewed 16 August 2019, <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Internet%20development%20and%20Internet%20governance%20in%20Africa.pdf>.

Signé, L & Signé, K 2018, 'Global cybercrimes and weak cybersecurity threaten businesses in Africa', *Africa in focus: Brookings*, viewed 16 August 2019, <https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/>.

Symantec Corporation 2013, *Internet security threat report 2013, 2012 Trends*, vol. 1, viewed 22 January 2019, <https://www.insight.com/content/dam/insight/en_US/pdfs/symantec/symantec-corp-internet-security-threat-report-volume-18.pdf>.

Schjølberg, S 2017, 'The history of cybercrime (1976-2016)', *Korean Institute of Criminology,* vol. 11, no. 12, pp. 1-5.

TENET 2014, 'TENET: The Tertiary Education and Research Network of South Africa', viewed 22 January 2019, <https://www.tenet.ac.za/>.

Tijssen, R 2007, 'Africa's contribution to the worldwide research literature: New analytical perspectives, trends, and performance indicators', *Scientometrics,* vol. 71, pp. 303-27.

Van Heerden, R, Von Solms, S & Mooi, R 2016, 'Classification of cyber attacks in South Africa', *Proceedings of IST-Africa*, IIMC International Information Management Corporation Ltd, pp. 34-45.

United Nations Economic Commission for Africa (UNECA) 2014, 'Tackling the challenges of cybersecurity in Africa', *Policy Brief*, viewed 25 September 2019, <https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf>.

University of Johannesburg 2011, 'The Academy for Information Technology celebrates its 40th birthday', *Faculty of Science Newsletter*, viewed 16 August 2019, <https://www.uj.ac.za/faculties/science/Documents/Newsletter/Newsletter%20July%202011%20Academy%20of%20Computer%20Science%20Applied%20Mathematics%20Statistics.pdf>.

Univeristy of Pretoria 2012, 'University of Pretoria Historical Overview', *Internet Archive: Wayback Machine*, viewed 25 September 2019, <https://web.archive.org/web/20120401175118/http://web.up.ac.za/default.asp?ipkCategoryID=9792>.

University of Stellenbosch 2018, 'More than a hundred years of science', *Faculty of Science*, viewed 16 August 2019, <https://www.sun.ac.za/english/faculty/science/about-us/our-history>.

Van Heerden, R, Von Solms, S & Vorster, J 2018, 'Major security incidents since 2014: An African perspective', *Proceedings of IST-Africa*, IIMC International Information Management Corporation Ltd, pp. 1-7.

Waltman, L 2015, 'A review of the literature on citation impact indicators, *Journal of Informetrics*, vol. 10, no. 2, pp. 365-91.

World Bank 2008, *Global economic prospects 2008: Technology diffusion in the developing world*, World Bank Publications, Herndon, VA, US.