Research Challenges for Cybersecurity and Cyberwarfare: A South African Perspective

Trishana Ramluckan[1], Brett van Niekerk[1], and Louise Leenen[2]
[1]University of KwaZulu-Natal, Durban, South Africa
[2]University of the Western Cape and CAIR, Cape Town, South Africa
ramluckant@ukzn.ac.za
vanniekerkb@ukzn.ac.za
lleenen@uwc.ac.za

Abstract: The International Institute for Strategic Studies (2018: 6) states that "cyber capability should now be seen as a key aspect of some states' coercive power ... This has driven some European states to re-examine their industrial, political, social and economic vulnerabilities, influence operations and information warfare, as well as more traditional areas of military power." Cybersecurity is often incorrectly assumed to be a purely technical field, however there are numerous multidisciplinary aspects. The very nature of cybersecurity and operations in cyberspace is disruptive, and this is true for many disciplines attempting to introduce cybersecurity research into their offerings. This can provide challenges to researchers and students where methodologies that do not necessarily follow disciplinary norms are prejudiced against by old-school thought. Foundational understanding of concepts may also hinder multi-disciplinary research, as specific terminology that is used in cybersecurity may be considered colloquial or have different meanings in other disciplinary settings. The experimental, observational and mathematical research methodologies often employed by computer scientists do not address the political or legal aspects of cybersecurity research. Research methods for cybersecurity generally apply and teach the limited scientific methods for creating new knowledge, validating theories, and providing some critical insights into to the cybersecurity arena. This paper aims to investigate the South African national and institutional perspectives for higher education and research, identify challenges, and propose interventions to facilitate multidisciplinary research into cybersecurity and cyberwarfare in South Africa. Legislature and policies, organisational structures, processes, resources, and historical and socio-economic factors will be discussed as to the influence on cybersecurity research. A review and analysis of international efforts for multidisciplinary research in higher education institutions will provide for a basis to propose a framework for South African higher education institutions to effectively implement cybersecurity research.

Keywords: Cybersecurity, Cyberwarfare, Higher education, Multidisciplinarity, Research methods

1. Introduction

In today's 'global' society, research methodology challenges require collaboration by researchers from multidisciplinary backgrounds. However, multidisciplinary research is not without its challenges which may result from training as well as the scientific culture. Regarding cybersecurity research, it can be said to currently be of a strict scientific methodology, with little to no involvement or collaboration with other disciplines thereby restricting innovation in such a diverse field. By definition research refers to "a search for knowledge" and a systematic method of identifying a problem, collecting and collating information, developing hypothesis and analysing them to form grounded conclusions and provide viable recommendations.

There is now a growing request by research policy-makers for the change and adaptation of research methodologies to allow for collaboration and multidisciplinarity, to gain the most value from a "shared research methodology". Although the idea of multidisciplinarity appears good on paper, there is limited literature on collaborative research between disciplines. While there are numerous terms such as "multi-disciplinarity", "trans-disciplinarity" and "inter-disciplinarity", the area of collaborative research remains idealist and its practicality is yet to be established.

Cybersecurity refers to "the measures that are taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (Merriam-Webster, 2018) while cyber warfare is defined as the "use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes". From the definition of cybersecurity, it can be seen as a purely technical area. However, cybersecurity and cyber-warfare are unique areas as they combine the social sciences including political sciences as well the technical sciences. Therefore, it becomes

essential for the development and practice of multidisciplinarity research methodologies with reference to cybersecurity and cyberwarfare.

Desk research was conducted for the paper. For the desk research information was gathered using existing resources, including the press, the Internet, analytical reports and statistical publications. This was then followed by the collation of data.

Figure 1 illustrates South Africa's standing in international research. A Scopus search for publications with a title or keyword including 'cybersecurity' or 'cyber-security' was performed, and South Africa was 13th with 149 publications.

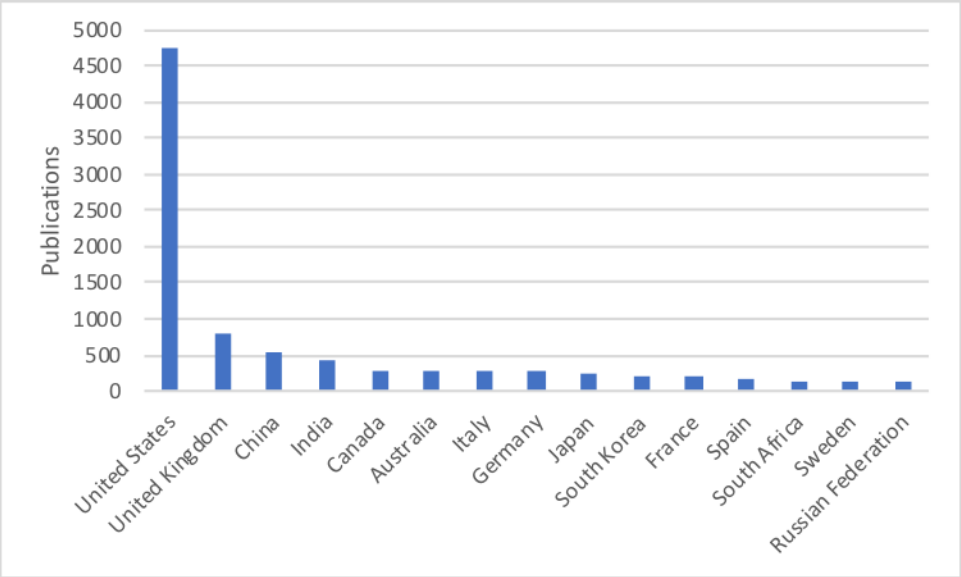

Figure 1: South Africa's standing in international cyber-security research, source: (Scopus, 2019)

2. The Social and Technical Elements of Cybersecurity and Cyberwarfare

The most well-known “hacking” incident was that used in the 2016 US elections. According to media reports 13 Russian nationals and three other entities were charged with conducting an illegal "information warfare" by attempting to disrupt the 2016 presidential election in order to influence the election outcome. This according to Matishak (2018), had cost millions of dollars, time and labour resources. The purpose of the campaign, conducted through a Russian “Troll Farm”, was to spread distrust towards the presidential candidates and the US political system. This incident was termed as “cyber-warfare” or “election hacking”. The general definition of hacking is “the gaining of unauthorized access to data in a system or computer” (Merriam-Webster, 2018). However, this was not a technical hack, as no system was infiltrated by an unauthorised user. Instead fake online accounts were created to influence the voters. Similar concepts were considered by Cybenko, Giani, and Thompson (2002) in what they termed "cognitive hacking".

Furthermore, the Irish Republican Army had subsequently begun an operation using social media platforms i.e. Facebook, Twitter, Instagram and YouTube to influence the US people in their choice of Presidential candidate. This was apparently done through the creation of fake bot accounts and false or misleading advertising (Matishak, 2018). The key example is that the IRA trolls produced materials promoting Trump e.g. #TrumpTrain, as well as anti-Clinton hashtags on Twitter, such as #Hillary4Prison. Further to this the alleged trolls had also encouraged minorities either to not vote or to vote for a third-party candidate starting in the latter half of 2016. This is a key element reflecting psychological warfare in cyber-space.

The technical side of hacking may refer to the plot which included the operation in the middle of 2016, which involved malware on “at least ten of the Democratic Congressional Campaign Committee’s (DCCC) computers", which may have stolen employees’ passwords, and lead to the indictment leaks. This further enabled the “hackers” to illegally monitor the Democratic Party’s activities. This allowed the publication of the retrieved files by DC Leaks, Guccifer 2.0 and what is believed to be WikiLeaks (Matishak, 2018).

Cybersecurity is relevant at a tactical or technical level, as well as a strategic international level. Traditional concepts of deterrence and state sovereignty are questioned when it comes to cybersecurity (Davis, 2015). The role of cyber in military and intelligence applications is uncertain. There is debate surrounding the applicability of traditional military theorists such as Sun Tzu, Clausewitz and Jomini (Duggan, 2016), or if a new theory of war is required. The head of the British MI6, Alex Younger, indicated that intelligence needs to fuse traditional intelligence with modern technological methods (Fitsanakis, 2018). Attempts are being made to ascertain the relevance of current international humanitarian laws regarding war to cyber-space (Schmitt, 2017). Liaropoulos (2014) illustrates the dualistic technical and socio-political nature of cyber-conflict through a discussion of theoretical paradigms.

Cybersecurity and cyberwarfare consist of many elements both technical and social, which requires a multidisciplinarity approach to be able to fully analyse/understand it. This creates numerous challenges in the field of research.

3. Challenges in Cyber Security Research

3.1 Global Challenges

The shortage of cybersecurity skills is a global problem and it has become critical ($(ISC)^2$, 2018; Florentine, 2015). The $(ISC)^2$'s Cybersecurity Workforce Study of 2018 estimates a global shortage of just under 3 million positions. Governments, civil society, business and the military are competing to recruit within a small pool of cybersecurity professionals. Universities and research institutions are struggling to compete against all these other sectors to find and retain researchers and lecturers in this field.

Awareness of the discipline amongst potential researchers and workers is often not adequate. School leavers need to be educated about the opportunities in the field. Raytheon and the National Cybersecurity Alliance published the result of a study in 2015 that indicated 67 % of men and 77 % of woman in the US and 62 % of men and 75 % of woman globally, did not receive any counselling in high school or secondary schools on careers in cybersecurity (Florentine, 2015).

Women are under-represented in the cybersecurity and this creates another challenge in the field. The $(ISC)^2$ Cybersecurity Workforce Study (2018), fielded in North America, Latin America, Asia Pacific and Europe, found that women represent only 24% of the workforce overall. Willes-Ford (2018) found that although women 50% of the U.S, workforce comprise of women, only 10-15% of the U.S. cybersecurity workforce consist of women, Foley et al. (2017) lodged a study that found women only comprised 11% of the global cybersecurity workforce and 10% in the Asia-Pacific region. This study's key findings are concerning:

- Fifty-one percent of women in the filed report widespread discrimination and stereotype bias;
- The lack of flexibility in work hours and long work hours is a primary obstacle;
- Women feel their opinions are not valued by their employers;
- Women persistently face wage inequality;
- The attrition of women from the ICT, Science and Engineering fields start in primary school and the current number of female graduates are declining. It is possible that the perception women may have of the cybersecurity career could be a deterrent to choosing this field. Jessica Ortega of SiteLock noted that "Women often don't see tech or security as viable career paths because they're often considered masculine professions" (Bradford, 2018). In addition to the problem of attracting women to the industry, retainment is also problematic. Women frequently leave the field after a brief tenure according to a study by Georgetown University Center on Education and the Workforce 2011 (Hechinger Report, 2018). Willis-Ford (2018) conducted a comprehensive study on the perceived barriers on retaining women in cybersecurity and found that lack of mentorship, the Imposter Phenomenon and hostile work environments are noteworthy barriers. The Imposter Phenomenon is when a suitably qualified individual feels inadequate to satisfy the requirements of a position. A hostile work environment include elements such as harassment and a lack work/life balance.

Availability of data is often considered as a problem for academic cybersecurity research. Corporations and governments are unwilling to provide too much detail on successful cyber-attacks, and to get access to detailed network information to test new algorithms or systems is very difficult. In nations where there are

laws mandating public announcements of data breaches, data will be more readily available; in countries without this requirement there will be limited information on cyber-attacks available. The legal mandates however, are usually for data breaches of personal information, and do not necessarily require public notification of other cyber-attacks that do not affect data. Therefore there is even less available data on cyber-attacks against industrial systems, making specific research into this area even more challenging.

Data cleanliness and consistency is problematic. Vendor and computer security incident response team (CSIRT) reports often differ in the categorisation of data, which limits the accuracy of analysis. Some vendors and CSIRT also change their categorisations from year to year (Pretorius, 2016). For instance, if a researcher is focussing on the transportation sector, it could be combined with utilities in one year, and categorised on its own in another year. Most cyber-attack techniques rely on secrecy and deception; when conducting research, it is important to filter through possible erroneous reports (for example news reports that are sensationalist and based on conjecture). The reliability of data collected based on human perceptions also needs to be considered; for example, a respondent may report that their organisation has not been a victim of a cyber-attack, however they may not yet be aware that an attack has occurred (van Niekerk, 2011).

As stated by James Brokenshire, the Minister for Crime and Security, "governments cannot deliver a safer online world. We need to work closely with industry to ensure that safe infrastructure and services can be provided to the public and share information and skills (OGL, 2017)." Jansen van Vuuren & Leenen (2018) identified roles for government, business and academia to work together to build cybersecurity capacity and capability in South Afrrica but these results are applicable globally. Educational institutions must be supported to initiate new cybersecurity qualifications. Businesses should embark and expand in capability building initiatives such as the participation in cybersecurity awareness in schools as well as career guidance of young people. The businesses can also support curricula development by providing threat and attack information to allow for current and local relevance. The implementation of cybersecurity exercises gives opportunities of hands-on learning, and can enhance interest in these careers. In addition, business can sponsor bursaries, support internships, and help to conduct cybersecurity exercises.

3.2 Challenges in South Africa

In South African Higher Education, the National Qualifications (NQF) structure remains rigid and does not allow for a multidisciplinary approach. With the diversity of cybersecurity, a multidisciplinary approach is required. The South African NQF structure sets the boundaries, principle and guidelines, which provides the vision, as well as the philosophical foundational base for the construction of the qualifications system.

Whilst multi-disciplinary research is advocated at South African institutions, implementing it in practice is often problematic. To establish a strong national research capacity, inter-institutional collaboration is required; however, they cannot even achieve effective collaboration internally. A concept known as vertical progression ensure that to do a post-graduate in Computer Science or Politics, a student requires an undergraduate major in that discipline. However, due to institutional structures, it is very difficult for a student to major in both a technical science and a social science. The various disciplines can be very territorial and have strict expectations. This presents challenges for students wishing to do a postgraduate with a cybersecurity topic as the project can be considered too technical for social science disciplines, however it is not technical enough for computer science. Prospective students may therefore lose enthusiasm and opt not to register, or choose another topic.

Cybersecurity is a discipline that has been growing rapidly but is still a young discipline. There are still no specialised cybersecurity degree courses in South Africa. This is partially due to the limited number of academics specialising in cybersecurity and the fact that most universities do not have lecturers that can teach a sufficiently broad range of cybersecurity topics. Most active researchers were trained in other related disciplines such as Computer Science, Statistics, Engineering, or Information Systems. This creates challenges due to different research approaches and the fact that a large percentage of researchers have not been working in the discipline for a long time. They often have steep learning curves and need to modify approaches and perceptions to adjust to the cybersecurity domain. Often in industry cybersecurity professionals emerge from accountants and auditors due to the function of auditing security controls on financial information systems. They then attempt to consider postgraduate studies related to cybersecurity without the necessary background.

The schooling system in South Africa provides a very weak grounding in Science, Technology, Engineering, and Mathematics (STEM) subjects. For those going into a technical cybersecurity field, the necessary skills and knowledge can be provided through the undergraduate programmes. For those going through the social sciences, and then into cybersecurity, they may then struggle to understand the technical concepts required.
Government support is also lacking. Whilst countries such as the US and UK have established accreditation programmes supported by the military and intelligence communities (Government Communications Headquarters, 2016; National Security Agency, 2016), South Africa does not have a dedicated support programme from government. Therefore, cyber-security research projects need to compete with all the other disciplines. The government should include cybersecurity specifically as a scarce-skill and allocated dedicates funding to post-graduate research in this discipline. There is a mandate that the national Council for Scientific and Industrial Research conducts research on behalf of the military, so there is limited engagement directly between the academia and the military. However, the South African Cybercrimes Bill has indicated that the military, law enforcement, and intelligence agencies should engage with academia to develop the necessary skills (Minister of Justice and Correctional Services, 2017). A possible hinderance to the implementation of this is the general lack of funding for tertiary institutions.

In South Africa, there is a limited core of researchers, with little or no evidence of younger researchers coming through: this is evidenced by the high prevalence of specific South African authors, with limited publications coming from a variety of other authors who do not appear to continue with research (van Niekerk, 2015). This could indicate a future shortage should the existing researchers leave the South African research environment. Whilst there is a global under representation of women in cybersecurity, the strong political mandate to deliver on employment equity in South Africa is difficult to meet when it is almost impossible to find any suitable candidates.

4. Discussion

In an online society, cybersecurity and cyber-war challenges involve more than just the technical issues. Cybersecurity extends into every aspect of modern society, as critical infrastructure from basic healthcare providers to the power grid, is now fully dependent on technology. This creates the need for a multidisciplinary approach towards cybersecurity and cyberwarfare as it should consist of people, processes and technology. This concept, also known as the “Golden Triangle”, was made popular by Bruce Schneier, a cyber-security and privacy expert, in the 1990’s and states that “operational efficiency requires an approach that optimises the relationships between people, process & technology” (Banks, 2016).

Although cyber networks have a technical component, they also have a social one. As such cybersecurity threats become social threats (University of Nevada Cyber Research Centre, 2018). Therefore, a multidisciplinarity research approach to cybersecurity becomes imperative. This approach combines numerous branches of learning, with the sole purpose of achieving the same objective. The concept of multidisciplinarity research involves an in-depth inquiry into the problem for ascertaining the main hypothesis, but also combines different academic approaches and methods. Molteberg and Bergstrom (2000) have argued that “Multidisciplinary Studies appear to be both applied and action or policy-orientated” and is considered as a “progressive scholarly method.” Therefore, modern research is becoming more multidisciplinary in nature. With reference to Choudhary (2015), a multidisciplinary research approach provides for international cooperation linking the key principles in areas from policy development to cybersecurity.

With the broad scope of cybersecurity, defining an expert in the field is difficult. Does someone who graduate with a doctorate with a focus of student awareness of cybersecurity topics qualify as an expert, if they are unable to implement technical cybersecurity solutions? If someone has a deep knowledge of firewall rules, but does not understand the international relations of cyber-conflict, can they be considered as cybersecurity experts? With such a diverse set of perspectives, cybersecurity should be a discipline on its own and not reside under other disciplines such as computer science. Researchers and students of cybersecurity should then receive a grounding of the different perspectives prior to specialising through research in one specific area. This requires dedicated postgraduate degrees for cybersecurity to be implemented within South Africa. Dedicated degrees will allow for students to register without external disciplinary constraints negatively affecting promising research.

Additional modules should be made available to students specifically to develop skills critical thinking and analytic techniques. As Beebe and Pherson (2015) indicate, these skills are required for academic research as well as intelligence analysis; therefore, they are critical for students intending to conduct research in cybersecurity. Given that the available data and information in South Africa is imperfect or incomplete, and the secret nature of cyber-attacks, the need for critical thinking and analytical skills to provide a coherent view through research is required.

In South Africa, the average time to detect a breach is 150 days, followed by an average of 40 days to contain the breach (Moyo, 2018). As the average time to detect a breach is nearly 5 months, obtaining human perceptions or feedback may be erroneous due to not yet having detected a breach. Whilst the Protection of Personal Information (POPI) Act does require organisations to publicly disclose the occurrence of data breach, the Act is not fully implemented, therefore companies can still opt not to report a breach, however the breaches may be discovered and/or disclosed by third parties. This indicates that there will be a lack of data on all cyber-attacks in the country. Efforts should be made to engage with industries and the relevant government departments for them to supply desensitised data that can be used in cybersecurity research. For technical research, an alternative is for there to be initial research projects that use simulation and emulation to generate synthetic data that can be used.

Given the general lack of available funding for tertiary institutions in South Africa, it is imperative that some of the funding that is available be dedicated to cybersecurity research. Alternative funding mechanisms to allow engagements between government functions (governance, military, law enforcement, and intelligence agencies) and academia should be provided to ensure mutual support towards developing a sustainable national cybersecurity skills base. It is imperative for South African researchers to collaborate to motivate for dedicated cybersecurity research funding and partnerships. Of the funding that is available, there should be a portion dedicated towards cybersecurity research to provide impetus to the established researchers to foster young academics in the field.

Diversity in the workplace is good for any business (Bradford, 2018; Shaban, 2016) and the cyber workforce can only benefit from higher numbers of women and other minorities (currently within the field). Shaban (2016) found that diversity in terms of social background in a workforce usually leads to improved innovation, ideas and creativity. In South Africa, an effort should be made to attract recruits from previously disadvantaged backgrounds.

5. Conclusion

There remain challenges both within a national and international context, which include the rigidity of the NQF Educational structure and lack of monetary resources in South Africa, and the lack of cyber skills both nationally and internationally. Further to this is the aspect of critical thinking, which is usually not taught at any level of education in South Africa. The traditional scientific research methodologies used by scientists fail to address the political and social elements of cybersecurity research. Research methods for cybersecurity is accustomed to maintaining the “traditional” means for creating new knowledge and validating theories in cyber. In this era of rapid movement in technology, society, and various socio-economic problems, research with connections to different disciplines such as political science may provide the ideal solution. The purpose of research is to provide a solution for the betterment of society. By its nature, cybersecurity and cyber warfare involves a “human element “and cannot be studied or researched in isolation i.e. as a purely technical field. South African institutions need to implement multi-disciplinary research, with dedicated postgraduate degrees in cybersecurity, in order to circumvent the challenges faced do to the current siloed study areas that are currently present. Dedicated funding should be allocated to cybersecurity research, particularly for women and previously disadvantaged demographics.

Acknowledgements

The second author received funding by the South African National Research Foundation, Grant no. 115059.

References

Banks, C. (2016). People, process & technology – why is it important to consider all 3? [online], accessed 16 February 2019, https://analyze.co.za/people-process-technology-important-consider-3/.

Beebe, S.M., and Pherson, R.H. (2015) *Cases in Intelligence Analysis: Structured Analytic Techniques in Action*, 2nd ed., Los Angeles: Sage.

Bradford, L. (2018) "Cybersecurity Needs Women: Here's Why," *Forbes*, 8 October, [online], accessed 4 February 2019, https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#3d4590d647e8.

Choudhary, A. (2015). Multidisciplinary Research. [online] , accessed 24 January 2019, https://www.lawctopus.com/academike/multidisciplinary-research/

Cybenko, G., Giani, A., and Thompson, P. (2002) "Cognitive Hacking: A Battle for the Mind", *Computer* 35(8), pp. 50 – 56.

Davis, P.K. (2015) "Deterrence, Influence, Cyber Attack, and Cyberwar," *International Law and Politics*, vol. 47, pp. 327-355.

Duggan, P. (2016) Why Special Operations Forces in US Cyber-Warfare? *The Cyber Defense Review* 1(2), January 8, pp. 73-79 [online], accessed 16 February 2019, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/US_Special_Operations_Duggan_Oren.pdf?ver=2018-08-01-090209-853

Fitsanakis, J. (2018) MI6 spy chief outlines 'fourth generation espionage' in rare public speech, 4 December, [online], accessed 16 February 2019, https://intelnews.org/2018/12/04/01-2449/.

Florentine, S. (2015) "Closing the cybersecurity talent gap, one woman at a time," CIO, 17 November, [online], accessed 4 February 2019, https://www.cio.com/article/3005637/cyber-attacks-espionage/closing-the-cybersecurity-talent-gap-one-woman-at-a-time.html.

Foley, M., Dewey, L., Williamson, S., Blackman, D., Creagh, A., Davidson, L., and Zhu, M. (2017) *Women in Cyber Security Literature Review*, UNSW Canberra Australian Centre for Cybersecurity, June, [online], https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-literature-review.pdf.

Government Communications Headquarters. (2016) *GCHQ certifies six more Masters' degrees in Cyber Security*, May 23, [online], accessed 11 April 2017, https://www.gchq.gov.uk/news-article/gchq-certifies-six-more-masters-degrees-cyber-security.

The Hechinger Report. (2018) "Jobs in cybersecurity are exploding: Why are woman locked out?" *Transmosis*, 4 May, [online], accessed 4 February 2019, https://transmosis.com/jobs-in-cybersecurity-are-exploding-why-are-women-locked-out/.

International Institute for Strategic Studies. (2018) "Editor's Introduction: Western technology edge erodes further," *The Military Balance*, 118(1), pp. 5-6.

(ISC)2. (2018). *Cybersecurity Workforce Study 2018: Professionals Focus on Developing New Skills as Workforce Gap widens*, [online], accessed 4 February 2019, https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

Jansen van Vuuren, J. and Leenen, L. (2018) "Cybersecurity and Capacity Building for South Africa," *Proceedings of the 13th Human Choice and Computers Conference (HCC 13)*, September, Poznan, Poland.

Liaropoulos, A. (2014) "Cyberconflict and Theoretical Paradigms: Current Trends and Future Challenges in the Literature," *Proceedings of the 13th European Conference on Cyber Warfare and Security*, 3-4 July, pp. 133- 139.

Matishak, M. (2018). What we know about Russia's election hacking. Politico. [online]. Accessed 29 January 2019, https://www.politico.eu/article/russia-hacking-us-election-what-we-know/

Merriam-Webster. (2018). Merriam-Webster Dictionary. Encyclopaedia Britannica [Online], 27 January 2018, https://www.merriam-webster.com/dictionary/cybersecurity

Merriam-Webster. (2018). Merriam-Webster Dictionary. Encyclopaedia Britannica [Online], 27 January 2018, https://www.merriam-webster.com/dictionary/electionhacking

Minister of Justice and Correctional Services. (2017) *Cybercrimes and Cybersecurity Bill*. Republic of South Africa.

Molteberg, E & Bergstrom, C. (2000) Our Common Discourse: Diversity and Paradigms in Development Studies, [online], accessed 3 February 2019, https://www.researchgate.net/publication/242094789_Our_Common_Discourse_Diversity_and_Paradigms_in_Development_Studies

Moyo, A. (2018) "SA's Average Data Breach Costs Escalate," *ITWeb*, 12 July, [online], accessed 3 February 2019, https://www.itweb.co.za/content/Pero37ZgOnXMQb6m.

National Security Agency. (2016) *Centers of Academic Excellence in Cybersecurity*, May 3, [online] accessed 11 April 2017, https://www.nsa.gov/resources/educators/centers-academic-excellence/.

OGL. (2017). Industrial Strategy Building a Britain fit for the future. HM Government, London, [online], accessed 3 February 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf

Pretorius, B. (2016) *Cyber-Security and Governance for Industrial Control Systems (ICS) in South Africa*, Masters Dissertation, Durban, South Africa: University of KwaZulu-Natal.

Schmitt, M.N. (2017) *Tallinn Manual 2.0: On The International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

Scopus. (2019). Analysis of Search Results, [online], accessed 4 February 2019, https://www.scopus.com.

Shaban, A. (2016). "Managing and Leading a Diverse Workforce: One of the Main Challenges in Management," *Social and Behavioural Sciences*, vol. 230, pp. 76-84.

University of Nevada. (2018) *Cybersecurity Research*, [online], accessed 31 January 2019, https://www.unr.edu/cybersecurity/research

van Niekerk, B. (2011) *Vulnerability Assessment of Modern ICT Infrastructure from an Information Warfare Perspective*, Doctoral Thesis, Durban, South Africa: University of KwaZulu-Natal.

van Niekerk, B. (2015) "An Information Operations Roadmap for South Africa ," *10th International Conference on Cyber Warfare and Security,* 24-25 March, South Africa, pp. 347-357.

Willis-Ford, C. (2018) "The Perceived Impact of Barriers to Retention on Women in Cybersecurity", Thesis, University of Fairfax, [online], accessed 17 February 2019, https://www.researchgate.net/publication/329754528_THE_PERCEIVED_IMPACT_OF_BARRIERS_TO_RETENTION_ON_WOMEN_IN_CYBERSECURITY.