An evaluation of the challenges encountered by the South African police service with regard to the fourth industrial revolution

Grace Moipone Betty Vuma (a) Jacob Tseko Mofokeng (b) Adewale Olutola (c) Moses Morero Moteki (d)∗

(a,b,c,d) Tshwane University of Technology, 2 Aubrey Matlakala St, Soshanguve, Pretoria, 0001, South Africa

INTRODUCTION

The 4IR differs in speed, scale, complexity, and transformative power from previous industrial revolutions (Smith & Pourdehnad, 2018). Owing to, amongst other factors, globalization and the rapid evolving of new digital technologies, some careers are becoming obsolete and being replaced by new ones, causing the changing faces of crime and victimization. Schwab (2016) is of the view that the three (3) previous industrial revolutions liberated humankind from animal power, made mass production possible, and brought digital capabilities to billions of people.

The main difference between previous revolutions and the 4IR is the pace of change. Thus, while this industrial revolution builds strongly on the preceding digital revolution, the pace and scope of technological innovation makes it distinct (Genesis Analytics, 2017). The 4IR offers huge potential to transform and realign public service delivery processes by the SAPS. The SAPS is standing at an important moment in the history of technology.

The global, digitally enabled 4IR is already the fastest period of innovation ever. It is underpinned by rapid advances in technologies including BI, AI, Robotics, IoT, Data Analytics, Nanotechnology and Biotechnology, to name a few. The disruption of the public-sector market among other traditional markets and industries is already underway. These technologies, as observed by McKinsey (2016), can assist local and central governments to accelerate service delivery. Therefore, as noted by Shava and Hofisi (2017), the advent of new technologies enables citizens to express their opinions through social networks (Facebook, WhatsApp, Twitter) and...
other online platforms which are fundamental in facilitating e-participation, thereby, enhancing social accountability of governments. In an effort to limit the scope of this paper, its main focus is on the challenges faced by the SAPS when dealing with 4IR. Finally, the paper concludes on prevailing lessons learned, and provide some practical guidance on what can be done to address these challenges.

The introductory part of this study revealed that the implications of the fourth industrial revolution (4IR) in the SAPS – Gauteng province are yet to be fully understood. Based on the abovementioned background, it appears that the SAPS digital strategy is not designed to address social problems and the use of new 4IR technologies which could increase its capacity to better serve citizens directly. For example, robotics coupled with IoT, AI, Computerized Algorithms, Mobile Sensors, 3-D printing, and machine-to-machine communications could provide automation beyond the physical. For instance, enhancing service delivery at inaccessible terrains through drones thus enhanced service delivery in crime prevention. The SAPS still does not utilise sophisticated methods of different technologies in the investigation and combating of crime, no proper training when comes to the use of technology.

**Theoretical framework**

**Human Capital Theory (HCT)**

Human Capital Theory (HCT) originated in the 1700s when Smith (1776) claimed that education forms the basis of human capital in every society, allowing and sustaining economic growth. Smith (1776) determined that the acquisition of valuable skills and knowledge by one nation's inhabitants increases individual human capital, while at the same time increasing the general wealth of that nation. Kupe (2019) therefore argues that universities, globally and in South Africa, are expected to contribute to the advancement and development of their societies by investing in their graduates. In this regard, government, the private sector and students themselves are investing in the acquiring of human capital through, for example, a relevant university education (Alan, Altman & Roussel, 2008). This needs to be supported by teaching and learning policies that produce excellently educated, emotionally intelligent students equipped with adequate skills for the 4IR workplace (Kupe, 2019).

Expertise about techniques to detect criminals who commit crimes using sophisticated technology methods and to prosecute them is yet to be realised in South Africa. Reports of the arrest and conviction of this criminals are frequent yet not from the CJS. The implications based on the findings on 4IR in South Africa are compelling and require concerted effort from all relevant stakeholders within the CJS. Though the SAPS due to competing priorities, has not yet codify this crime for consumption by the public, it is essential that the official statistics made known to the public. The researchers are of the view that SAPS can also educate their officers about crimes involving 4IR. The challenges facing SAPS officers can be resolved through education the officers and taking them through training of utilising sophisticated technological methods.

**A thematic analysis**

The researcher used the interviews to collect data. The interviews are gathered from more than one person because the goal is to identify differences and similarities across participants in a sample. In-depth interviews were used by the researcher, and the reason being that in-depth interviews are conducted with unique individuals or a small number of people (Creswell, 2014:15). The advantages of the interviews are: Firstly, considerable input from each participant and an independent view is obtained on a situation. Secondly, participants can discuss intimate and confidential issues without fear, and no peer group pressure creates bias. Additionally, allows a rapport to build between participants and interviewer and can accommodate widely scattered participants. Thirdly, better for heterogeneous participants who may not gel in a group and allows the interviewer to see the surrounding home or office of the respondent. The study used a semi-structured interview schedule as it allowed the researcher to use the pre-planned schedule, and it allowed for elaborate discussions between the participants and the researcher. The interviews where in-depth and done on a one on one this was done to illicit detailed information. The interviews took place at locations that were chosen by the participants and the duration ranged from 20-40 minutes, this was dependent on how much information the participants were willing to share.

Thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data as it organises and describes data in detail (Braun & Clarke, 2006). At the heart of thematic analysis, the familiarisation of data by the researcher is important. Data familiarisation was possible because the researchers personally conducted audio-recorded interviews and transcribed them. This process allowed the researchers to familiarise themselves with the data for expedited and insightful analysis.

Following this thematic transcription, the scripts were analysed using NVivo version 8 software. This software organised the raw data so that it was possible to link and compare thematic issues within and across documents. The list of “starter nodes” was generated from an initial entry in a project journal in the software where the questions and assumptions brought to the report were outlined. The software gave results that allowed for a deeper examination and management of the qualitative data that might not be possible in traditional coding.

Two distinct types of coding were used in the analysis. The first was descriptive coding, which described the cases in this study. This process-related both to the coding of information in categories and the creation of attributes to clarify them. The second type was analytical coding, which was done by selecting source content to interpret and reflect on the meaning of the data to arrive at new
ideas and categories. The process entailed gathering material that could be rethought and reviewed given the growing understanding of the inter-relationship of the categories in the data.

Therefore, the following themes were identified during the fieldwork process:

**Theme 1: Lack of capacity and resources to deal with 4IR crimes**

It was clear that SAPS in Gauteng province did not have capacity and resources to deal with 4IR crimes. The capacity and resources which lacking is: Human resources and physical resources (technological tools) to investigate, combat and to trace the sophisticated crimes caused by the perpetrators. SAPS lack human resources which are capable to investigate 4IR crimes, it was difficult to trace, and locate criminals using technological tools.

**Theme 2: Limited skills, expertise and training to deal with 4IR crimes**

SAPS in Gauteng province have limited skills, expertise and training to deal with 4IR crimes, the sophisticated crimes committed by criminals is hard for the SAPS to comprehend as the personnel in the service currently have limited skills, expertise and training. It was clear during data collection that the SAPS personnel have to undergo proper training, to upgrade their skills and expertise. Specialized skills are needed to intensify and to ensure that the criminals who commit crimes using technology are apprehended and arrested.

**Theme 3: Lack of capacitated and skilled multi-disciplinary unit within the CJS**

There is a need for a capacitated and skilled multi-disciplinary unit which will solely deal with 4IR crimes which involve sophisticated technological tools. It was clear during FGD’s and KII that criminals utilize software programs and sophisticated technological tools which makes hard for the SAPS to investigate, combat, arrest and prosecute those who are committing this type of crime. A multi-disciplinary unit will assist the SAPS to re-focus, deal and combat 4IR which is currently difficult for SAPS to control and prevent.

**Theme 4: Underdeveloped network infrastructure and cybercrime detection and prevention**

It was clear during data collection that there was a gap between the SAPS and network service providers. It was a challenge for the SAPS to get necessary information from the service providers regarding ongoing cases or to provide information of the criminal’s especially online conversations.

**Discussion**

It should be noted that findings such as those given below were similar among all the selected participants, regardless of the department the participants worked. Examples of some of the remarks regarding their experiences in terms of using 4IR in the SAPS were similar. The participants indicated their understanding about the concepts within the 4IR by the SAPS Gauteng Province. However, the participants from the SAPS provided different definitions about their understanding of 4IR. These are some of their responses quoted verbatim in italics, and no corrections of their language were made:

“*In short it is the digitalization of processes and implementation of the cyber technology and artificial technology to perform tasks previously performed by humans/animals*” (Participant 2).

“*The automation of various processes (manufacturing/industrial) using modern technology*” (Participant 3).

“*4IR can be described as a world where individuals move between digital domains and offline reality with the use of connected technology to enable and manage their lives*” (Participant 4).

“*The way the world interacts with technology, altering the way we conduct businesses, connect with one another and how electronic and digital world communicate and interact with each other, changing life as we know it*” (Participant 12).

“*The integration of new and pre-existing technologies into the everyday lives of people in general in reasonably, foreseeable and sometimes in unexpected ways*” (Participant 7).

Based on the above, the participants showed understanding of what 4ID entails. Their responses shows that they understand that 4ID involve technology and very complex and sophisticated technological tools, skills and expertise. However, participants provided different definitions about the concepts in question and everyone explained it the way they understand it.

When asked about their understanding of artificial intelligence, these are some of their responses quoted verbatim, and no corrections of their language were made:

“*This is intelligence demonstrated by missionary. It is a simulation of human intelligence in a mission*” (Participant 6).

“*It is human Intel in machines or robots that is programmed to think or act like human beings and replace human beings*” (Participant 14).

“*Collection of data, analysing of data to predict future trends, to act out of historic events based on predefined structures or data sets*” (Participant 20).
“Is intelligence demonstrated by machines, unlike the natural intelligence displayed by humans and animals, leading IA textbooks define the field as the study of “intelligent agents”: any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. Colloquially, the term “artificial intelligence” is often used to describe machines (or computers) that mimic “cognitive” functions that human associate with the human’s minds, such as “learning” and “problem solving” (Participant 15).

“Machines that is sentient and intelligent. Intelligence demonstrated by machines to act on available demand and to distinguish pictures and this may include genome editing and technology embedded within human bodies” (Participant 21).

When asked about their understanding of Cyberspace and Cyber-physical systems, these are some of their responses quoted verbatim, and no corrections of their language were made:

“The entirety the online sphere is cyberspace and electronic computer networks in which online communication take place” (Participant 21).

“Everything that happens in the digital environment, cloud management, data storage, transactions, whether gaming of business or just informational, irrespective of human interaction or not” (Participant 23).

“Is a local domain within the information environment consisting of the interdependent network or information systems infrastructures including the Internet, telecommunications networks, computer systems, an embedded processors end controllers” (Participant 30).

“Is a computer system in which in mechanism is controlled all monitored my computer-based algorithms. In cyber physical systems, physical and software components are deeply intertwined, able to operate on different spatial and temporal scales, it exhibits multiple and distinct behaviour modalities, and interact with each other in ways that change with context. Examples of CPS include smart grid, autonomous automobile systems, medical monitoring, industrial control systems, robotic systems, an automatic pilot avionics” (Participant 25).

“Theft off property information, gaming artefacts, digital espionage and theft of information, hacking of user data, crimes whereby computers are used as the instrument, i.e., pornography, human trafficking, terrorism etc.” (Participant 11).

“Cybercrime also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud trafficking in child pornography an intellectual property, stealing identities, or violating privacy” (Participant 17).

“Is a crime that involves a computer and a network. The computer may have been used in the Commission of the crime, or it may be the target. Cybercrime may threaten a person, computer or a Nations Security and financial health” (Participant 27).

When asked about their understanding of what are different types of cyber-crimes, these are some of their responses quoted verbatim, and no corrections of their language were made:

“Scams, Hacking, cyber bullying, application fraud, online harassment, cyber stalking” (Participant 6).

“Internet fraud, identity fraud, emails fraud” (Participant 37).

“Advance fee fraud or 419 scams, business email compromise, online gambling, crypto currency theft, malware, child sexual exploitation” (Participant 33).

“Ransome ware, financial theft on scams, human trafficking, theft of data, child pornography” (Participant 32).

“Steganography, denial of service attacks, computer viruses, ATM fraud” (Participant 26).

Based on the above the participants highlighted the different types of cyber-crimes which they may have experienced or dealt with at their different works places. Most of the participants studied Information communication technology but they still lacked skills and expertise to deal with sophisticated cyber-crimes committed by criminals. When asked about the challenges, gaps and or limitations that the SAPS Gauteng Province face when policing cybercrimes. These are some of their responses quoted verbatim, and no corrections of their language were made:

“Lack of training, skilled personnel, lack of software and tools, funds for specific licensing, no access to monitor cyber space” (Participant 13).

“Service providers such as ISP’s and network providers I'm not corporative when contacted to provide information which could assist investigators” (Participant 38).

“Ill equipped personnel, lack of relevant in state-of-the-art equipment, underdeveloped network infrastructure and major lakes in IT training in cybercrime detection and prevention” (Participant 31).

“Technology to investigate cybercrime” (Participant 8).
Developments in creating policies. Poor security control regarding cybercrime. The lengthy development and implementation process of policies, existing policies that are outdated” (Participant 5).

Based on the above, the participants highlighted that the SAPS lack training, skilled personnel and software and tools, they indicated that funds are the problems in terms of getting proper licensing and tools to fight and monitor cyber-crimes. When asked how these challenges can, gaps and all limitations are resolved by SAPS Gauteng Province. These are some of their responses quoted verbatim, and no corrections of their language were made:

“Government to invest in the fight against crime. Lack of funding limits the possibilities and grows inside it core protectors” (Participant 28).

“Awareness campaigns. Compel service providers to cooperate” (Participant 39).

“Identified need by cybercrime should be addressed by TMS in other relevant authorities” (Participant 19).

How can SAPS Gauteng Province establish and maintain cyber policing unit or online visible policing? These are some of their responses quoted verbatim, and no corrections of their language were made:

“There must be a very good relationship between the SAPS in the private sector, because the private sector has the necessary resources and skills to police cybercrime. Policing of cybercrime is the responsibility of everyone who has access to the Internet. The police officials do not have the adequate skills and knowledge to prevent cybercrime. Police at local stations like next Prince in handling cyber related crimes, therefore it would be very important that a special investigation unit like the Hawks be implemented. All when is off cybercrime to the public is really important because people don’t report these crimes. The SAPS need to train more officials around cybercrime prevention, prosecution and sentencing” (Participant 19).

“With the national command centre, similar to 10111 but this one will focus solely on cybercrime” (Participant 35).

“By installing cameras in all areas and monitoring all criminal events on a 24/7 basis through an operational centre with all stakeholders. Crimes that already occurred can be tracked through the same systems. They can track the group from the scene to where they started to commit crimes by blocking identify gadgets like phones, templates and other systems like GPS in trackers” (Participant 37).

“Employment of skilled personnel from private sector, there are a lot of cyber boffins in the country” (Participant 39).

When asked about the processes which can be included in a framework for policing in the 4IR’s by SAPS Gauteng Province? These are some of their responses quoted verbatim, and no corrections of their language were made:

“Autonomy from political influence in terms of direction. In-house research and development initiative programs. Extensive scrutiny of both human and machine vetting” (Participants 6).

“Total revamp off police system integration, cloud computing and access to the state-of-the-art technologies” (Participants 19).

“Better allocation of resources regarding policing of these crimes. Better training for all police officials. Cybercrime awareness to the public. The SAPS must use social media better” (Participants 10).

“Cyber command centre. Social medium monitoring solution. Training of members by accredited and qualified institutions on a regular basis as technology continues to evolve” (Participants 14).

“Automation of processes. Big data analytics. Cloud technology” (Participants 33).

Identified study challenges and themes

i. Lack of capacity and resources to deal with 4IR crimes
ii. Recommendation and strategy to improve theme 1

The study recommends that IT capacity and resources within SAPS has to be developed in order to ensure that the SAPS in Gauteng province are able to investigate, combat and to trace the sophisticated crimes caused by the criminals. The SAPS need to allocate funds to buy IT equipment’s, software’s and head hunt personnel which have skills, knowledge and capacity to curb, investigate and combat 4IR crimes.

i. Limited skills, expertise and training to deal with 4IR crimes
ii. Recommendation and strategy to improve theme 2

The study recommends that the SAPS personnel in Gauteng should be taken for training to improve their skills and expertise. The study further recommend that the SAPS personnel have to go overseas and undergo same training which FBI and other international federal agencies are going through. It is important to have specialized skills and expertise especially the organization like SAPS, it has constitutional obligation to protect and safeguard the inhabitants of the republic.

Identified study challenges and themes

i. Lack of capacity and resources to deal with 4IR crimes
ii. Recommendation and strategy to improve theme 1

The study recommends that IT capacity and resources within SAPS has to be developed in order to ensure that the SAPS in Gauteng province are able to investigate, combat and to trace the sophisticated crimes caused by the criminals. The SAPS need to allocate funds to buy IT equipment’s, software’s and head hunt personnel which have skills, knowledge and capacity to curb, investigate and combat 4IR crimes.

i. Limited skills, expertise and training to deal with 4IR crimes
ii. Recommendation and strategy to improve theme 2

The study recommends that the SAPS personnel in Gauteng should be taken for training to improve their skills and expertise. The study further recommend that the SAPS personnel have to go overseas and undergo same training which FBI and other international federal agencies are going through. It is important to have specialized skills and expertise especially the organization like SAPS, it has constitutional obligation to protect and safeguard the inhabitants of the republic.
Lack of capacitated and skilled multi-disciplinary unit within the CJS

Recommendation and strategy to improve theme 3

The study recommends that the SAPS should be capacitated and have highly skilled multi-disciplinary unit which will deal solely with 4IR crimes. The multi-disciplinary unit will assist the SAPS to re-focus, deal and combat 4IR crimes. The study further recommends that the SAPS should purchase and utilize software programs and sophisticated technological tools which will assist to investigate, combat, arrest and prosecute those who are committing 4IR crimes.

Underdeveloped network infrastructure and cybercrime detection and prevention

Recommendation and strategy to improve theme 4

The study recommends that the SAPS should work closely with network service providers. This will assist the SAPS to get necessary information from the service providers regarding ongoing cases and to provide information of the criminal’s especially online conversations.

Conclusion

The study has made a huge impact in terms of closing the gaps in combating 4IR crimes. The study would help the SAPS and the role players involved in combating 4IR crimes. The literature review has indicated that 4IR crimes in South Africa are hard for the SAPS to comprehend, investigate and combat it. The study has also made contributions by conducting legal and theoretical frameworks which would help to combat and reduce 4IR crimes in South Africa especially the SAPS in Gauteng Province. The participants of the study highlighted that there must be a very good relationship between the SAPS and the private sector, because the private sector has the necessary resources and skills to police cybercrime. Policing of cybercrime is the responsibility of everyone who has access to the Internet. The police officials do not have the adequate skills and knowledge to prevent cybercrime.

Acknowledgement

Author Contributions: Conceptualization, GV., JM., AO., MM.; Methodology, GV., JM., AO., MM.; Data Collection, GV., JM., AO., MM.; Formal Analysis, GV., JM., AO., MM.; Writing—Original Draft Preparation, GV., JM., AO., MM.; Writing—Review And Editing, GV., JM., AO., MM. All authors have read and agreed to the published the final version of the manuscript.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to that the research does not deal with vulnerable groups or sensitive issues.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Conflicts of Interest: The authors declare no conflict of interest.

References

Arntz, M., Gregory, T. & Zierahn, U. (2016). The risk of automation for jobs in OECD countries: A comparative analysis. In OECD Social, Employment, and Migration Working Papers 189; OECD: Paris, France.
Andress, J. & Winterfield, S. (2014). Cyber warfare: Techniques, tactics and tools for security practitioners (2nd Ed.). Waltham, MA: Elsevier.
Anderson, R. (2017). Closing the phishing hole - fraud, risk and nonbanks. In Federal Reserve Bank of Kansas City, Conference on Nonbanks in the Payments System (1-16).
Adams, R. (2020). Research to determine the potential impact of the fourth industrial revolution on the current and future regulation of gambling in South Africa. Available from: http://repository.hsrc.ac.za/handle/20.500.11910/15237.
Alexy, M. & Burges, M. (2015). Perceptions of Cyber stalking among college students. Available from: https://www.researchgate.net/publication/31325303_Perceptions_of_Cyberstalking_Among_College_Students
Atieno, O. (2009). An analysis of the strengths and limitation of qualitative and quantitative research paradigms. Available from: https://www.sciencesocialis.lt/pec/node/242
Benyera, E. (2019). Policing and the 4IR into a policing resource and not curse. Department of political science: UNISA.
Benyera, E. (2020). Police, Policing and the 4IR: Turn the 4IR into a policing resource and not curse. UNISA: Department of Political Science.
Buchanan, B. (2017). The cyber security dilemma. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001
Bossler, M. and Berenblum, T. (2019). Introduction: New directions in Cybercrime research. Available from: https://www.tandfonline.com/doi/full/10.1080/0735648X.2019.1692426
Bogdanoski, M. (2013). Cyber Terrorism- Global Security Threat. Available from: http://eprints.ugd.edu.mk/6849/
Berger, R. (2016). The Industries 4.0 Transition Quantified. How the Fourth Industrial Revolution is Reshuffling the Economic, Social and Industrial Model; Roland Berger: Monachium, Germany.
Blanchet, M., Rinn, T., Von Thaden, G. & De Thieulloy, G. (2018). Industry 4.0: The New Industrial Revolution - How Europe Will Succeed. Hg. v. Roland Berger Strategy Consultants GmbH: München. Available online from: https://www.iberglobal.com/files/Roland_Berger_Industry.pdf [Date of accessed on: 20 June 2018].

Gordon, R. J. (2016). The Rise and fall of American Growth: The U.S. Standard of Living since the Civil War; Princeton University Press: Princeton, NJ, USA, 2016. [Google Scholar].

Greenberg, D. F., & Roush, J. B. (2009). The effectiveness of an electronic security management system in a privately owned apartment complex. Evaluation review, 33(1), 3-26.

Groff, E., & McEwen, J. T. (2008). Identifying and Measuring the Effects of Information Technologies on Law Enforcement Agencies: The Making Officer Redeployment Effective Program: a Guide for Law Enforcement. Alexandria, Va: Institute for Law and Justice.

Haggerty, K. (2008). Book Review: Evidence-Based Crime Prevention, Theoretical Criminology, 121-126.

Hanusch, H. & Pyka, A. (2017). The Principles of Neo-Schumpeterian Economics. Camb. J. Econ. (2007), 31, 275-289.

Harris, A. and Lurigio, A. (2017). Crime Prevention and Soft Technology: Risk Assessment, Threat Assessment, and the Prevention of Violence, 103-132, in Byrne, J. And Rebovich, D. (2007). The New technology of Crime, Law and Social Control (Monsey).

Harris, C. (2007). Police and Soft Technology: How Information Technology Contributes to Police Decision Making, In: Byrne, J. and Rebovich, D. (2007). The New technology of Crime, Law and Social Control, Monsey, NY: Criminal Justice Press, 153-183.

Hermann, M., Pentek, T. & Otto, B. (2016). Design principles for industry 4.0 scenarios. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5-8 January 2016, 3928-3937.

Hier, S. (2014). Risky spaces and dangerous places: Urban surveillance, social disorder and CCTV. Social and Legal Studies, 13(4):541-554.

Publisher’s Note: SSBFNET stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2022 by the authors. Licensee SSBFNET, Istanbul, Turkey. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).