

Artificial Intelligence as a tool for improving policing in Zimbabwe

Tenson Ngwenya^a, Mqemane Tshababa^b, Edmore Chijoko M^c, Edward Tshuma^d, Stephen Makaza^e

Abstract

This paper reviews literature on the use of Artificial Intelligence (AI) in improving policing efficiency. The paper makes a case for a better understanding and adoption of AI as a policing and criminal investigation strategy for use by police organisations. The authors document the historical developments of AI as well as the benefits that accrue from using AI in policing. The challenges affecting the successful implementation of AI are also highlighted to build sustainable AI systems for crime management in Zimbabwe. Using the Innovations Diffusion theory and the System theory, the authors highlight how organisations such as the Zimbabwe Republic Police take up and utilise technological innovations to their advantage. The benefits that can accrue from AI include crime prevention and detection through Unmanned Aerial Systems, Facial Recognition Systems, Gunfire Detection, DNA Analysis, AI Security Cameras, Pre-trial Release, Parole, and Public safety video and image analysis. The conclusions drawn from the discussion show glaring gaps between the Zimbabwean context and advances made in other countries. The challenges of using AI as a policing strategy in developing countries include the culture, technology and law enforcement processes that include those related to standards of safety and performance, acquisitions, intellectual property and data rights. Given the challenges and benefits of AI, strategies for enhancing law enforcement can, therefore, be easily forecasted. Meaningfully investing in Information Communication Technologies by governments in developing countries is the starting point for enhancing law enforcement through Artificial Intelligence. Human capital capacitation is also another critical area that should be reinforced by sustainable strategies for employee retention.

Keywords: *Artificial Intelligence, Criminal Investigations, Crime Prevention, Law, Policing, Technology*

^{a,c,d,e}Zimbabwe Republic Police Staff College [An Affiliate College of the University of Zimbabwe]

^b Department of Psychiatry, Social and Behavioural Sciences, National University of Science and Technology, Zimbabwe

Corresponding Author – Tenson Ngwenya: thamungwenya78gmail.com

Introduction

While the Fourth Industrial Revolution has brought numerous advantages to the contemporary policing society, the Zimbabwe Republic Police is yet to fully exploit the technologies associated with this revolution. The need to fully embrace these technologies cannot be overemphasised due to the challenges that are replete in the modern policing landscape. The Zimbabwe Republic Police in its quest to be abreast with the rest of the world is making frantic efforts to adopt AI to improve crime management. The organisation is still grappling with traffic enforcement, with traffic-related crimes and accidents on the increase. The number of wanted persons moving freely within and out of Zimbabwe is also on the increase. Cases of motor vehicle thefts are also a cause for concern to the Zimbabwe Republic Police and the public. This paper outlines how the Zimbabwe Republic Police can benefit from fully adopting AI systems such as Unmanned Aerial Vehicles (UAV), Automated Fingerprint Indexing System (AFIS), Gunpowder Detection System (GDS), DNA Analysis System, Public Safety Video and Image Analysis (PSVIA), AI Security Cameras (AISC), and Robotics for law enforcement.

Historical development of Artificial Intelligence (AI)

The technological revolution has altered the way people live, work, and relate to one another. The response to this revolution has summoned an integrated and comprehensive approach involving all stakeholders of the global polity, from the public and private sectors to academia and civil society (Schwab, 2016). According to Schwab (2016), the first industrial revolution used water and steam power to mechanize production, on the other hand, the second used electric power to create mass production. The third used electronics and information technology to automate production. The fourth industrial revolution is building on the third and is the digital revolution that has been occurring since the middle of the twentieth century (Schwab, 2016). The fourth Industrial Revolution is characterised by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.

The advent connection of billions of people by mobile devices, with unprecedented processing power, storage capacity, and access to knowledge has brought in a rare fit in the fourth industrial revolution. Emerging technology breakthroughs in fields such as artificial intelligence, robotics, the Internet of Things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology,

materials science, energy storage, and quantum computing have been the order of the day.

The term artificial intelligence (AI) refers to an artificial creation of human-like intelligence that can learn reason, plan, perceive, or process natural language (Burell, 2016). AI started in the early forties until the benchmark development in 1950. John McCarthy pioneered who adopted the name of Artificial Intelligence (Popescu et al., 2010). The main milestones at the end of the sixties until the middle of eighties were adding domain knowledge, development of knowledge-based systems and success of rule-based expert systems, such as DENDRAL, MYCIN (Schmidhuber, 2007). Rising of machine learning started in 1986 with major advances in machine learning algorithms and applications.

In the middle of the nineties, AI was classified as science, where the integration of learning, reasoning, knowledge was represented in addition to AI methods used in vision, language and data mining (Popescu et al., 2010). In 1998, COPLINK was created at the Artificial Intelligence Laboratory at the University of Arizona at Tuscon, as a revolution in artificial intelligence technology that depended on pooling the available various information sources that can be brought to improve police officers' information (Oatley et al., 2006).

With time, the level of knowledge management played an effective role in law enforcement. This entailed moving from the stage of using office applications to applying artificial intelligence in replacement of police officers (Gottschalk, 2008). Gonzales et al. (2005) opine that in 2004, a wide range of intelligence methods was available to support law enforcement such as crime analysis, crime pattern analysis, geographic analysis, investigative analysis such as network analysis, telephone record analysis, and bank record analysis. In addition, strategic analysis intelligence includes threat assessments, target profiles, and strategic targeting. (Gonzales et al., 2005). This study sought to establish the extent to which the ZRP has adopted artificial intelligence in its operations and how it is deriving efficiency in its operations from such technology.

The concept of Artificial Intelligence (AI)

The concept of Artificial Intelligence concerning its use in policing refers to a system that can receive inputs from the environment, interpret and learn from such inputs (Schmidhuber, 2007). According to Gottschalk (2008), the system then exhibits related and flexible behaviours and actions that help law enforcement organisations to achieve their goal of managing crime overtime.

This section provides a review of the historical development of AI as well as the framework for the application of AI in law enforcement organisations.

Figure 1: Framework for AI and Crime Investigations

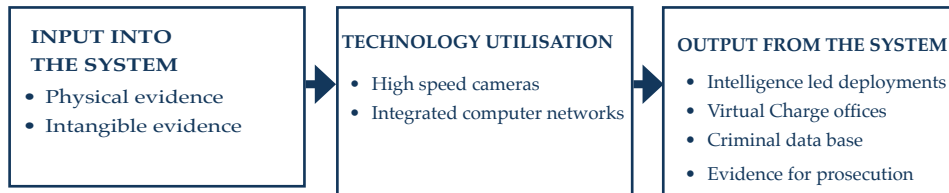


Figure 1 indicates that physical evidence obtained from the crime scenes such as fingerprints, footprints, tyre impressions and other materials left at the crime scene will be uploaded into the system using digital recording equipment. In addition, intangible evidence such as modus operandi will be recorded into the system. The information will be processed through technological devices such as high-speed cameras and computers that will be integrated on a network and the server operated at the Police General Headquarters. This will ensure quick information dissemination to remote points of access like police stations in Zimbabwe as well as outside links with SARPCCO and INTERPOL. The output from the system will entail deployments that are led by intelligence obtained from the system. Deployments will cover areas prone to crime, times at which criminals operate as well as types of criminals involved. This will enable the police officers to be better equipped for the assigned tasks. The system will also allow for the creation of virtual charge offices through internet connectivity. Virtual charge offices will enable members of the public to report any criminal activities at the comfort of their homes or offices. This will enable police officers to react quickly to crime scenes thus improving the detection and recovery rates. Database of criminals will be maintained in the system and this will enable police officers to quickly track down criminals. Of paramount importance is that the system will provide scientific evidence for use in the prosecution of criminal cases.

Theoretical Review

This paper is anchored on the Innovations Diffusion and Systems Theories as discussed below.

Innovations diffusion theory

The spread of artificial intelligence use by law enforcement organisations is a classic example of the types and phases of diffusion of innovations theory. Everett Rodgers advanced this Theory in 1962. According to Jen and Annette (2002), diffusion relates to the process through which an innovation trickles down to the social system members through certain channels over time. Innovation adoption occurs when an organization transforms a thought into an actual practice (Dearing, 2009). The adoption rate is the speed at which organisations in the security sector take up and accept innovation.

According to Dearing (2009), the innovation curve is bound to reach critical mass in the adoption curve. This Diffusion of innovations model aids security organisations in comprehending the adoption of available technology in crime management over time. The model is especially useful to organisations when they are launching a new technology-oriented service (Dearing, 2009). Security service organisations adopt innovations for diverse reasons including detection, investigation and arrest of criminals (Rogers et al., 2004).

Crime in different countries is taking a new twist where it is becoming complicated with each day. Security organisations are employing different strategies that are meant to better manage crime in their respective countries. Some have turned to technology to enhance their operational efficiency. Though the use of technology in crime management came into being long back, only a limited number of security organisations have fully embraced it. The internet saw the coming into fruition of different police-public interactions. This marked a new era in the crime management landscape as the crime management process is aided by ubiquity and instantaneity.

Utterback and Abernathy (1975) posited that the two types of innovations are product innovations centred on the market itself and consumer needs and process innovations, which are focused on the company itself as it seeks to improve the efficiency of operations. While incremental innovations are typically internal improvements, radical innovations provide firms with something new and different from any process previously used by the organization (Marvel & Lumpkin, 2007). The ability to innovate may also reposition the organization among others within the same industry (Lanzolla & Suarez,

2012). Crime in Zimbabwe has evolved from being physical in nature such as assaults, robbery and murder to highly sophisticated transgressions such as cybercrime which has shown its head through fraud, card cloning, online child sexual assaults and cyberbullying. Such an evolution calls for the ZRP to continually innovate through employing both process and strategy innovation. To enhance its operational efficiency, the ZRP has to adopt both incremental and radical innovations by positioning itself well to deal with the new wave of criminal sophistry.

Wolfe (1994) grouped adopters into five categories, which are the early adopters, the early majority, innovators, laggards and finally the late majority. Innovators comprise a small percentage of the adoption groups and rarely face immediate mimicking because of how far ahead this group is about other organisations. They are, according to Redmond (2002), willing to break with tradition and habit to take on the innovation. They are opinion leaders amongst the social system and can help increase the rate of adoption (Rogers et al., 2004). Early majority adopters interact with peers and move slowly to adopt, preferably after watching all earlier users and opinion leaders gain success (Dearing, 2009). Developed countries are innovators in security services. They impart the innovations to developing countries like Zimbabwe. This is usually done through world bodies like Interpol and SARPCCO (International Criminal Police Organisation, 2019).

The speed and degree of each innovation are influenced by several factors such as the relative advantage which relates to the level at which a new idea is thought of as preferable to the idea it comes after, compatibility, the proportion to which the new idea is aligned to the needs espoused by the adopter and complexity of implementation (Rogers et al, 2004). The ZRP has been lagging in the adoption of artificial intelligence in its operations. This paper seeks to identify the factors that impede the ZRP in embracing artificial intelligence in its operations.

The Theory has been criticised because much of its evidence, including the adopter categories, does not originate in the security services sector and it was not developed to explicitly apply to the adoption of new behaviours or security innovations. The Theory also does not take into account an individual's resources or social support to adopt the innovation. Despite these setbacks, the theory has been used successfully in many fields including communication, agriculture, public health, criminal justice, social work, and marketing.

Systems Theory

The Systems Theory views organisations as open social systems that must interact with their environments to survive (Broom, 2006). Organisations depend on their environments for several essential resources: customers who purchase the product or service, suppliers who provide materials, employees who provide labour or management, shareholders who invest, and governments that regulate. Katz and Kahn, who adapted General Systems Theory to organisational behaviour (Katz & Kahn, 1966), first applied the open-systems approach.

The approach identifies organisational behaviour by mapping the repeated cycles of input, throughput, output, and feedback between an organisation and its external environment (Robbins, 2009). Systems receive input from the environment either as information or in the form of resources. Concerning law enforcement organisations, the input can be in the form of information from the community since most organisations have embraced the concept of community policing (Popescu, 2012). The systems then process the input internally, which is called throughput, and release outputs into the environment in an attempt to restore equilibrium to the environment (Robbins, 2009). The system then seeks feedback to determine if the output was effective in restoring equilibrium. The systems approach focuses on the means used to maintain organizational survival and emphasize long-term goals rather than the short-term goals of the goal-attainment approach.

According to Broom (2006), systems can be considered either open or closed. Open organizations exchange information, energy, or resources with their environments, whereas closed systems do not (Broom, 2006). No social systems can be completely closed or open, they are usually identified as relatively closed or relatively open. The distinction between closed and open systems is determined by the level of sensitivity to the external environment. Closed systems are insensitive to environmental deviations, whereas open systems are responsive to changes in the environment (Broom, 2006).

Law enforcement agencies can use the concept of Systems Theory to implement protocols for regular feedback to the organisation, thereby aligning it with the desires of the public in the environment they serve (Ahmad, 2012). According to Ahmad (2012), this theory is also important for enabling security organisations to understand the role of research and feedback in creating a thoroughly analysed and consistent crime management strategy.

The throughput which is the analysis of information and creation of strategy helps law enforcements agents to conceptualize and justify not only the research budget but also the need for making decisions that strategically align with the needs of the public (Townesley, 2008).

Systems Theory, however, is not without some shortcomings. Robbins (1990) noted that one criticism of this approach is that its focus is on the means necessary to achieve effectiveness rather than on organizational effectiveness itself. Robbins (1990) further points out that measuring the means, or process, of an organization can be very difficult when compared to measuring specific end goals of the goal-attainment approach.

Uses of AI in policing

Police organisations are attempting to use AI in a variety of ways to address crime. Broadly, AI is used to detect crimes and prevent future crimes. According to Pierson (2012), law enforcement agencies across the world are being trained on what to look for at crime scenes and how to handle digital evidence. Gaming consoles, Echo devices and even Fitbits have provided valuable information to help solve crimes (Pierson, 2012). Many criminals do not appreciate the power of these devices to contradict alibis and catch lies. Detectives for analysis when trying to solve a crime then use these digital devices.

Police officers can now have body cameras on when on patrol. These cameras can provide another set of eyes to sort through an interaction after engaging criminals. McCarthy et al. (2006) indicate that the cameras can improve self-awareness to prevent unacceptable behaviour such as accepting bribes on the part of police officers and those they interact with since they will be aware that their interactions will be recorded. This is a big deterrent for bad behaviour. The Zimbabwe Republic Police is still lagging in this technological development.

Collins (2012) opines that some police cars are equipped with GPS projectiles that can be shot via remote control and hook onto the back of an alleged perpetrator's vehicle. These allow officers to know where a suspect is located and therefore prevent high-speed and dangerous car pursuits. Smart sensors have been developed that can be fixed to the inside of an officer's gun to track how the gun is being used including whether it has been upholstered or discharged. This information could prove valuable in criminal trials where scientific evidence is required to secure the conviction of accused persons.

Agencies across the world are moving toward more data-driven approaches to solving crimes. Machine learning is particularly skilled at identifying patterns and can be quite useful when trying to discern a *modus operandi* (M.O.) of an offender (Gottschalk, 2007). Digital tools can speed up this work and find connections that might take humans much longer to uncover (ibid). These types of algorithms might prove useful to detect serial crimes committed by the same individual or group.

Zuev and Fedyanin (2012) highlight that there is a new officer in Dubai to help fight crime, but although the officer puts on a police cap, the officer is one hundred percent robot. Dubai police plan to have robotic officers make up a quarter of the force by 2030 (Zuev & Fedyanin, 2012). It can speak six languages and is designed to read facial expressions. It has a computer touch screen where people can report a crime (ibid). The robot is deployed mainly to tourist spots and is equipped with a camera that sends live images back to police headquarters to identify wanted suspects (Zuev & Fedyanin, 2012). Although the robot cop can help deter crime and relieve some tasks from its human counterparts, humans are still expected to make arrests. Moran (2012) opines that other robots are deployed around the world to collect evidence, investigate and detonate bombs and for crowd control among other things.

AI for crime prevention

Collins et al. (2012) aver that the goal of any society should not be to just catch criminals but to prevent crimes from happening in the first place. AI can be used to predict future crime spots. Predicting police organisations use big data and machine learning to try to predict when and where crime will take place (Collins et al, 2012). By analysing existing data on past crimes, law enforcement agencies can predict when and where new crimes are most likely to occur (Collins et al, 2012). This is based on the observation that certain crime types tend to cluster in time and space (Collins et al., 2012). Buscema and Tastle (2013) state that using historical data and observing where recent crimes took place, predictions where future crimes will likely happen can be made. For example, a rash of burglaries in one area could correlate with more burglaries in surrounding areas soon enough. Buscema and Tastle (2013) opine that this technique is called real-time epidemic-type aftershock sequence crime forecasting. The system highlights possible hotspots on a map and the police then consider patrolling the areas more heavily (Buscema & Tastle, 2013).

AI can be used in the prediction of who will commit a crime. According to Zuev and Fedyanin (2012), facial recognition and gait analysis try to predict if an individual will commit a crime before it happens. The system detects if there are any suspicious changes in the behaviour or unusual movements of people (Zuev & Fedyanin, 2012). For example, if an individual seems to be walking back and forth in a certain area repeatedly indicating they might be a pickpocket or casing the area for a future crime, the system will track the individual over time (Zuev and Fedyanin, 2012).

AI for crime detection

City infrastructure is becoming smarter and more connected. This provides cities with sources of real-time information, ranging from traditional security cameras to smart lamps that can be used to detect crimes as they happen (Al-Ma'aitah, 2013). Arrests have been made through evidence collected from connected digital devices. This is the landmark breakthrough for law enforcement as a result of the Internet of Things (IoT), artificial intelligence and robots (Reed, 2011). There are certainly benefits to applying this new technology to help fight crime, but it also raises some challenging questions regarding the right to privacy and security breaches.

Unmanned Aerial Systems

Unmanned Aerial Systems such as drones have become a necessity in the policing landscape. The police at times need air support to get an aerial vantage point both during scene attendance and in crime prevention. Helicopters have been relied on to this effect. The emergence of Unmanned Aerial Vehicles (UAVs) commonly known as drones has seen the development of Unmanned Aerial Systems where drones are connected, controlled and tasked using a network of integrated systems which are cheaper to acquire, maintain, easy to deploy and save lives by keeping officers off danger situations than helicopters. AI and machine learning have seen the development of drone swarms which can be used by the police to patrol a large area at once and also in search and rescue missions. UAVs have proved to be a tactical tool in many situations including accident scene reconstruction, border patrols for illicit trafficking and crown control amongst others. UAVs can be fitted with cameras that take images ranging from the visible to the infrared spectrum thus are capable of being deployed during any time (day/night). LIDAR cameras can also be mounted on drones to acquire 3D images of the area under surveillance. These drones can be equipped with AI-based programmes to sense parameters that can be

regarded as criminal activities for example geo-fencing can be used to detect encroachment into restricted areas.

Facial recognition system

A facial recognition system is an AI system of algorithms that are used to automatically encode already existing image profiles stored in a database and compare them to the sample (input) image. The result thereof is a match to the suspect. This enables quick identification and tracking of missing persons and criminal suspects. A network of CCTV cameras has to be put in place to have a large base to collect data (images) in addition to photographs taken by the police of suspects and accused persons. Some authorities argue that CCTVs makes our habitat safe but others say it infringes on people's privacy. However, according to Interpol, "650 criminals, fugitives and persons of interest/missing persons" have been accounted for in four years since the launch of Interpol's Facial Recognition System (IFRS) which has a database of 160 countries feeding images into it since 2016. To avoid garbage in garbage out, and facial recognition system is as powerful as its input data, thus the algorithms become more effective with more images in the database and continuous machine learning. Police in countries like China, the USA and Russia have since deployed facial recognition systems with effective arrests being made though at times wrong suspects can be apprehended when their faces appear to be similar to real criminals.

AI Security Cameras

Grover and Bramer (2007) aver that while police organisations listen for crime, many others are using cameras to watch for it. Townsley and Johnson (2008) indicate that in 2015, Hikvision, a Chinese company that is a major security camera producer, announced they would be using chips from Movidius (an Intel company) to create cameras able to run deep neural networks right on board. The system uses AI to perform tasks like facial recognition, license plate reading, and unattended bag detection (Townsley and Johnson, 2008). The video processing traditionally took place on a centralized hub or in the cloud. On the contrary, these cameras process the videos within themselves and as such make the process faster and cheaper (Townsley and Johnson, 2008). Townsley and Johnson (2008) aver that the cameras can also reduce the need for using significant bandwidth since only relevant information needs to be transmitted. There has been a 65% drop in crime in Sea Point and South Africa following the introduction of this camera system (Townsley and Johnson, 2008).

DNA analysis

AI can also benefit the law enforcement community from a scientific and evidence-processing standpoint (Azuela et al, 2006). According to Gonzales et al (2005), biological material, such as blood, saliva, semen, and skin cells, can be transferred through contact with people and objects during the commission of a crime. DNA technology has advanced to allow forensic scientists to detect and process low-level, degraded, or otherwise unviable DNA evidence that could not have been used previously (Gonzales *et al*, 2005). It follows therefore that decades-old DNA evidence from violent crimes such as sexual assaults and homicide cold cases is now being submitted to laboratories for analysis.

Pre-trial Release and Parole

After being charged with a crime, most individuals are released until they stand trial. In the past deciding, who should be released pre-trial or judges using their best judgement (Alimadad et al, 2013) mainly did what an individual's bail should be set at. In just a few minutes, judges had to attempt to determine if someone is a flight risk, a danger to society, or at risk to harm a witness if released. This was an imperfect system open to bias.

Alimadad et al, (2013) indicate that the city of Durham, in the United Kingdom, is using AI to improve the system of deciding to release a suspect. The program, Harm Assessment Risk Tool (Hart), was fed five years' worth of criminal data. Hart uses that body of data to predict if an individual is a low, medium or high risk. The city has been testing the system since 2013 and comparing its estimates to real-world results. The city claims Hart's predictions that an individual would be low risk were accurate 98% of the time, and predictions that an individual would be high risk were accurate 88% (Alimadad et al, 2013). The intent is for Hart to advise authorities on which suspects are most likely to commit another crime.

Schmidhuber (2007) states that jurisdictions in the United States have been using more basic risk assessment algorithms for over a decade to make decisions about the pre-trial release and whether or not to give the individual parole. One of the most popular algorithms is Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), which is used throughout all Wisconsin and numerous other locations (Schmidhuber, 2007). An analysis by the New York Division of Criminal Justice Services found COMPAS's recidivism scale worked effectively and achieved satisfactory predictive accuracy (Schmidhuber, 2007). On the other hand, the COMPAS came under fire after analysis indicated that the system indirectly contained a strong racial bias. It was found that black

defendants who did not recidivate over two years were nearly twice as likely to be misclassified as higher risk compared to their white counterparts (ibid).

Public safety video and image analysis

Rigano (2019) states that video and image analysis is used in the criminal justice and law enforcement communities to obtain information regarding people, objects, and actions to support criminal investigations. However, the analysis of video and image information is very labour-intensive, requiring a significant investment in personnel with subject matter expertise (Rigano, 2019). Video and image analysis is also prone to human error due to the sheer volume of information, the fast pace of changing technologies such as smartphones and operating systems, and a limited number of specialized personnel with the knowledge to process such information.

According to Moran (2012), AI technologies provide the capacity to overcome such human errors and to function as experts. Traditional software algorithms that assist humans are limited to predetermined features such as eye shape, eye colour, and distance between eyes for facial recognition or demographics information for pattern analysis (Moran, 2012). AI video and image algorithms not only learn complex tasks but also develop and determine their own independent complex facial recognition features/parameters to accomplish these tasks, beyond what humans may consider (ibid). These algorithms have the potential to match faces, identify weapons and other objects, and detect complex events such as accidents and crimes both in progress and after the fact.

Gunfire Detection

According to Oately (2006), AI uses smart city infrastructure to triangulate the location of a gunshot. According to Pierson (2012), individuals immediately report only about 20% of gunfire events to the police. Even when people report gunfire, they often provide vague or potentially inaccurate information. The system can therefore alert authorities in effectively real-time with information about the type of gunfire and a location that can be as accurate as 10 feet (Pierson, 2012). Multiple sensors pick up the sound of a gunshot and their machine learning algorithm triangulates where the shot happened by comparing data such as when each sensor heard the sound, the noise level, and how the sound echoed on buildings (Pierson, 2012). Pierson (2012) indicates that this has been in use in cities including New York, Chicago, San Diego and Cape Town.

Challenges encountered by police organisations in the use of AI

It is difficult to have technology that is so strategically important being developed commercially by a relatively small number of companies. In addition to the shift in funding sources, several challenges related to technology, process, personnel, and culture continue to impede the adoption of AI by law enforcement agencies.

Technology

Bell et al (2010) aver that a wide variance exists in the ease of adaptability of commercial AI technology for law enforcement purposes. In some cases, the transition is relatively seamless. For example, the aircraft maintenance algorithms, many of which were initially developed by the commercial sector, will likely require only minor data adjustments to account for differences between aircraft types. In other circumstances, significant adjustments are required due to the differences between the structured civilian environments for which the technology was initially developed and the more complex enforcement environments required in policing (Bell, 2010). For example, commercial semiautonomous vehicles have largely been developed in and for data-rich environments with reliable GPS positions, comprehensive terrain mapping, and up-to-date information on traffic and weather conditions obtained from other networked vehicles. In contrast, the enforcement variant of such a vehicle would need to be able to operate in locations where map data are comparatively poor such as rural areas and in which GPS positioning may be inoperable due to adversary jamming. Moreover, semi-autonomous or autonomous enforcement technologies would likely need the ability to operate in remote areas a capability not inherent in most commercial sector technologies (McNeill, 1982).

Process

Law enforcement processes that include those related to standards of safety and performance, acquisitions, and intellectual property and data rights present a challenge to the integration of AI in police operations (Galway et al, 2006). Often, civilian and police standards of safety and performance are either not aligned or are not easily transferable (Galway et al, 2006). Galway et al (2006) postulate that a failure rate deemed acceptable for a civilian AI application may be well outside of tolerances in a law enforcement environment where greater precision is a must or vice versa. These factors may create a barrier to the smooth transfer of commercially developed AI technology to law enforcement

operations (ibid). Police organisations may need to adjust their acquisitions processes to account for rapidly evolving technologies.

Personnel

Law enforcement organisations face challenges when it comes to recruiting and retaining personnel with expertise in AI due to research funding and salaries that significantly lag behind those of commercial companies (Grover *et al*, 2007). Such challenges stem from quality-of-life factors, as well as from a belief among many technology workers that they can achieve large-scale change faster and better outside the government than within it (Grover *et al*, 2007). AI experts would be willing to serve in government if officials could create a more compelling sense of purpose and a technical environment within the government that would maximize their talents (ibid). If police organisations are unable to recruit and retain the appropriate experts, law enforcement AI applications could be delayed, deficient, or lacking in appropriate safeguards and testing.

Culture

The cultural divide between law enforcement and commercial technology companies may also present challenges for AI adoption (Cummings, 2017). Some companies are not at liberty to work with police organisations due to ethical concerns over the government's use of AI in surveillance or weapon systems (ibid). Cultural factors within the law enforcement establishment may also impede AI integration. The integration of AI into existing systems alters standardized procedures. Some law enforcement agents are unwilling to accept AI-generated analysis, arguing that their jobs are at risk of being replaced.

EMPIRICAL REVIEW

Artificial intelligence in law enforcement in Jordan

Suhaib, Alzou'bi, Haitham, Alshibly and Mohammad Al-Ma'aitah carried out a study on artificial intelligence in law enforcement in 2014. The study focused on law enforcement in Jordan. The research sought to review other works and papers that focused on using the new digital technology in one of the crucial aspects of life. It also sought to introduce success tools of developed countries in this field as well as summarize the Jordanian situation on the use of AI in law enforcement.

The methodology used in the research involved conducting a critical review of prior researches, scanning the literature efficiently as well as reviewing the information in the texts and evaluating it. It also involved reviewing the status in Jordan concerning using AI as a sort of supportive tool for making decisions in addition to conducting meetings and direct questions with decision-makers.

The study by Suhaib, Alzou'bi, Haitham, Alshibly and Mohammad Al-Ma'aitah found out that the prediction techniques used in law enforcement in Jordan were limited to be understood or revealed due to high strict code of security in the country's Security Directorates and Bodies. It also found out that GIS and the statistical analysis that depend on repeatability and potential correlations were used in the operational policing and enforcing law In Jordan. Computer crimes were recorded in Jordan, but there was no information to understand how the law was applied in such cases.

Basing on the findings, the research recommended that Jordan had to make efficient contributions in AI and Law international conferences, so that its success stories may give a good view for the upcoming future regarding AI. It also recommended that an in-depth search on the use of AI in enforcing the law in Jordan have to be done by incorporating universities and related agencies. The research also recommended that effective evaluation methods must be conducted on time so that the police and other relevant departments may judge properly the effectiveness of AI in police work.

Artificial intelligence and robotics for law enforcement

The INTERPOL's Innovation Centre, the United Nations Interregional Crime, and Justice Research Institute (UNICRI), researched on embracing artificial intelligence and robotics for law enforcement in Singapore in 2018. The objectives of the study were to gain insights and foresight of AI and robotics in law enforcement as well as identifying the latest innovations and new technologies in the application of AI and robotics.

The key findings of the study were that AI and robotics were new concepts for law enforcement and there were expertise gaps that should be filled to avoid law enforcement falling behind. The study also found that many countries were exploring the application of AI and robotics in the context of law enforcement. Some countries had explored further than others and a variety of AI techniques were materializing according to different national law enforcement priorities. There is, however, a need for greater international coordination on this issue.

The research found out that AI and robotics were significantly enhancing law enforcement's surveillance capabilities and, there was a need to address privacy concerns associated with these technologies, including issues such as when and where it is permissible to use sensors.

The research recommended that law enforcement should take steps to ensure fairness, accountability, transparency and that the use of AI and robotics are effectively communicated to communities. It also recommended that security organisations should advance their understanding of and prepare for the risk of malicious use of AI by criminal and terrorist groups, including new digital, physical, and political attacks. The research further recommended that law enforcement needs to continuously monitor the new technology landscape to ensure preparedness. To this end, the INTERPOL Police Technology and Innovation Radar, a worldwide overview of new, emerging technologies and their use in police practice should support this endeavour.

Impact of artificial intelligence on crime and crime prevention

Joy Wang of Australian National University (ANU) carried out a study on the impact of artificial intelligence on crime and crime prevention in 2019. The study sought to outline some of the likely limits and potential of AI applications as a crime enabler or crime fighter. The focus of the study was on the criminogenic potential as well as the preventative role of Artificial Intelligence.

The study found out that investment and interest in developing machine learning (ML) technologies that underpin AI capabilities across the industry, civil and military applications have grown exponentially in the past decade. It also emerged from the study by Wang et al. (2019) that the potential weaponisation of AI applications such as computational marketing, 'deep' fake images or news and enhanced surveillance, was posing challenges to democracies and human rights. The study observed that poorly implemented ethical, accountability and regulatory measures provide opportunities for criminal activities as well as the potential of accidents, unreliability and other unintended consequences.

The authors recommend that automated decision-making technology should not be relied upon as a sole decision-making tool. Scepticism is necessary when evaluating an AI's performance. The authors also recommended that AI applications must be used to enhance many existing surveillance systems incorporating and aggregating data from different sources including fusing individual biometric data with expenditure and activity transaction records to create 'whole of life' behavioural classifiers.

The role of artificial intelligence and expert systems in the implementation of National Development Strategy 1 (NDS1)

The NDS1, which is a Zimbabwean Government strategy of achieving its National Vision of achieving an upper-middle economy by 2030, has as one of its priority areas, 'the anchoring of crimemanagementon automation, digitalisation, computerisation and smart policing.' The papers, therefore, makes a point on how Zimbabwean Government could fully integrate Artificial Intelligence and Expert Systems as a driver for implementing NDS1. It highlighted how the police, what benefits, could use Artificial Intelligence and Expert Systems could be realized from integrating its current government programs to enhance the implementation of NDS1.

Recommendations

The authors recommend that the Zimbabwe Republic Police engage with technology-driven stakeholders for ease of integration of AI. The paper recommends that governments prioritize resources allocation for the implementation of AI systems. Above the political will, the authors suggest that there should be a buy-in from the citizenry.

Conclusion

While the ZRP is making frantic efforts to adopt AI, a lot of groundwork still needs to be covered for the successful implementation of AI in its operations. From the literature reviewed and discussions made, the authors conclude that the full integration of systems such as unmanned aerial vehicles, ATMs, AFIS, ANRS, Gunpowder Detection System, DNA Analysis System, Public safety video and image analysis, AI Security Cameras, Artificial intelligence and robotics for law enforcement will go a long way in resolving the criminal sophistry bedevilling the policing world. The challenges highlighted in this paper are not insurmountable if there is a prioritization of resources and a buy-in from the citizenry.

References

- Ahmad, I., Kamruzzaman, J., and Habib, H., and Habibi, D. (2012). Application of artificial intelligence to improve quality of service in computer networks. *Neural Comput&Applic*, Volume 21, Pages 81–90.
- Alimadad, A., Ghaseminejad, A. H., Borwein, P., Christopher, C., Brantingham, P., Li, J., Brantingham, P., Pollard, N., Dabbaghian-Abdoly, V., Rutherford, A., Ferguson, R., Van Der Waal, Alexa and Fowler, E. (2008). Using Varieties of Simulation Modelling for Criminal Justice System Analysis. Ch 19 In Liu, L. & Eck, J. *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*. Premier Reference Source. USA.
- Al-Ma'aitah, M. A. (2013). Security Concerns in E-payment and the Law in Jordan. *IJACSA International Journal of Advanced Computer Science and Applications*, Volume 4, Pages 179-183.
- Azuela, J. H. S., Ritter, G., Serra J., and Cortés, U. (2006). Special Issue: Advances in Artificial Intelligence. Instituto Politécnico Nacional Centro de Investigación en Computación.
- Bell, P., Dean, J. and Gottschalk, P. (2010). Information Management In Law Enforcement: The Case Of Police Intelligence Strategy Implementation. *International Journal of Information Management*, Volume 30, Pages 343–349.
- Broom, G. M. (2006). An open-system approach to building theory in public relations. *Journal of Public Relations Research*, 18(2), 141-150.
- Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 2053951715622512.
- Buscema, M., and Tastle W. J. (ED). (2013). *Intelligent Data Mining in Law Enforcement Analytics; New Neural Networks Applied to Real Problems*. Springer Dordrecht Heidelberg New York London. *International Journal of Advanced Information Technology (IJAIT)* Vol. 4, No. 4, August 2014
- Collins, I. M., Breathnach, O., and Felle, P. (2012). Electronic Clinical Decision Support Systems Attitudes and Barriers to Use in the Oncology Setting. *Ir J Med Sci*, Volume 181, Pages 521–525.

- Cummings, M. (2017). *Artificial intelligence and the future of warfare*. London: Chatham House for the Royal Institute of International Affairs.
- Dearing, J. W. (2009). Applying diffusion of innovation theory to intervention development. *Research on social work practice*, 19(5), 503-518.
- Galway, L., Charles, D., and Black, M. (2008). Machine learning in digital games: a survey. *ArtifIntell Rev*, Volume 29, Pages 123-161.
- Gonzales, A. R., Schofield, R. B., Herraiz, D. S. (2005). Intelligence-Led / Policing: The New Intelligence Architecture. Bureau of Justice Assistance. NCJ 210681.
- Gottschalk, P. (2007). *Knowledge Management Systems in Law Enforcement: Technologies and Techniques*. Indea Group Inc. USA.
- Jen Friis & Annette Millner (2002) Mobile sports betting, unpublished article, IT University.
- Lanzolla, G., & Suarez, F. F. (2012). Closing the technology adoption-use divide: The role of contiguous user bandwagon. *Journal of Management*, 38(3), 836-859.
- MacNeil, B. J. (1982). *Critical issues in medical technology*. Boston: Auburn House.
- Marvel, M. R., & Lumpkin, G. T. (2007). Technology entrepreneurs' human capital and its effects on innovation radicalness. *Entrepreneurship Theory and Practice*, 31(6), 807-828.
- McCarthy, J., Minsky, M. L., Rochester, N., and Shanno, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence August 31, 1955. *AI Magazine* Volume 27, Pages 12-14.
- Moran, L. (2011). <http://www.dailymail.co.uk/news/article-2053617/Professor-John-McCarthy-Father-artificial-intelligence-dies-aged-84.html>.
- Oatley, G., Ewart, B., and Zeleznikow, F. (2006). Decision support systems for police: Lessons from the application of data mining techniques to "soft" forensic evidence. *Artificial Intelligence and Law*, Volume 14, Pages 35-100.
- Pierson, R. M. (2012). Can Artificial Intelligence Detect Crime Before It Happens?. <http://www.lockergnome.com/news/2012/08/25/can-artificial-intelligence-detect-crime-before-it-happens/>.

- Popescu, V. A., Popescu, G., and Popescu, K. R. (2010). The amazing world of the Internet-Challenges of the Internet Age. *Information Management*, Volume 12, Pages 13-23.
- Redmond, M. and Baveja, A. (2002). Computing, Artificial Intelligence and Information Technology. A data-driven software tool for enabling cooperative information sharing among police departments. *European Journal of Operational Research*, Volume 141, Pages 660–678.
- Reed, M. (2018). The Classification of Artificial Intelligence as “ Social Actors”.
- Rigano, C. (2019). Using artificial intelligence to address criminal justice needs. *National Institute of Justice Journal*, 280, 1-10.
- Rogers, E. M., Singhal, A., & Quinlan, M. M. (2019). Diffusion of innovations 1. In *An integrated approach to communication theory and research* (pp. 415-434). Routledge.
- Schmidhuber, J. (2007). 2006: Celebrating 75 years of AI- History and Outlook: the Next 25 Years. <http://arxiv.org/abs/0708.4311v1v>.
- Schwab, K.M. (2016). *The Fourth Industrial Revolution*. World Economic Forum, Geneva, Switzerland.
- Townsley, M., and Johnson, S. (2008). The Need for Systematic Replication and Tests of Validity in Simulation. Ch1 In Liu, L. & Eck, J. *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*. Premier Reference Source. USA.
- Zelevnikow, J., Oatley, G., and Leary, R. (2005). A Methodology for Constructing Decision Support Systems for Crime Detection. R. Khosla et al. (Eds.): KESLNAI, 3684, Pages 823-829.
- Zuev, A. and Fedyanin, D. (2012). Models of Opinion Control for Agents in Social Networks. *ProblemyUpravleniya*, Volume 2, Pages 37–45.