The Impact of Artificial Intelligence on the Human Aspects of Information and Cybersecurity

M. Malatji[1], A. Marnewick[1] and S. von Solms[2]

[1]Postgraduate School of Engineering Management, University of Johannesburg
[2]Department of Electrical and Electronic Engineering, University of Johannesburg
e-mail: masikem@gmail.com; amarnewick@uj.ac.za; svonsolms@uj.ac.za

Abstract

This paper presents the results of a literature survey on the impact of artificial intelligence on the human aspects of information and cybersecurity. Artificial intelligence and its two subfields, machine learning and deep learning, are briefly described though much emphasis is placed on the impact of their applications to the human aspects of information and cybersecurity. In addition, the paper presents arguments by those in favour of autonomous artificial intelligence designs that do not require human interventions as well as counter-arguments by those opposed to the idea for ethical and other reasons. The current and future security trends of the human-artificial intelligence integration are explored. The findings reveal that artificial intelligence is currently utilised only for augmenting human capacity in information and cybersecurity activities whereas the future trends are unknown. The study proposes the socio-technical systems approach for attaining the optimal security results through the human-artificial intelligence integration.

Keywords

Artificial intelligence, cybersecurity, human aspect, information security, machine learning, socio-technical system

1 Introduction

Information and cybersecurity incidents have grown rapidly both in scale and number (Fang *et al.*, 2018). Organisations are battling to keep pace with the proliferation of such incidents (U.S. Newswire, 2017). With 20 years of investigating and analysing cyber-incidents, Antuit (2018) consider the rapid expansion and sophistication of the recent cyber-attacks as unprecedented. There is also complete anticipation by security professionals that the cyber-threats will progressively become challenging and complex (Cisco, 2018). This has compelled many organisations to introduce somewhat unpredictable and chaotic processes (CyberSaint, 2017). What is information and cybersecurity though? Buczak and Guven (2016) consider it a set of technologies and processes responsible for protecting computer networks, associated software and data from unauthorised access, alteration, or destruction. Protection of these computer system networks has careened into a danger zone over the last decade (Greengard, 2016).

It is Buczak and Guven's (2016) position that each of the computer network security systems should have, at a minimum, an intrusion detection system (IDS), antivirus software, and firewalls. However, Greengard (2016) is adamant that firewalls have effectively become unreliable as application programming interfaces and cloud computing string together data across different enterprises. In the context of big data from the cloud cybersecurity has become a critical challenge and poses greater risk (Sabar *et al.*, 2018). This is exacerbated by a lack of human capacity to screen big volumes of data for proper threat analysis (Talwar and Koury, 2017). This prompted practitioners and researchers to look for new and better information and cybersecurity approaches (Greengard, 2016). Consequently, researchers have begun developing security solutions that employ artificial intelligence (AI). AI encompasses both machine learning and deep learning (Pumin, 2016). As the core AI subfield, machine learning is about effective simulation of human activities as applied to speech and pattern recognition, image processing, cybersecurity, and even decision-making (Greengard, 2016; Liu *et al.*, 2018). Essentially, AI is about machines that simulate intelligent human behaviour such as learning, thinking, and reasoning (Dragomir, 2017).

However, what are the current and future trends on the impact of AI to the human information and cybersecurity activities? To answer this question, the literature review study purpose has three objectives: (1) Examine the AI trends in information and cybersecurity; (2) Describe how the AI trends impact the human aspects of information and cybersecurity; and (3) Propose how the new ‘people-technology’ security integration could be achieved for optimal results. To examine the trends, a literature review protocol is proposed. The methods section describes the protocol in detail. The layout of this paper begins with the introduction section outlining the research purpose. Section 2 outlines the research approach and the execution of the approach is described in Section 3. Section 3 further reviews the AI trends in information and cybersecurity. The results of the literature survey are discussed in Section 4. The paper concludes with Section 5 where future research is also suggested. The adopted methodology to study the current and future trends on the impact of AI to the human information and cybersecurity activities is described in the next section.

2 Methodology

2.1 Literature Review Approach

The aim of the literature review process of this study is to (Silic and Back, 2014):

- Compile and classify articles according to themes devoted to AI trends in information and cybersecurity and their impact on human security aspects
- Analyse, understand, and show how the compiled literature addresses the research purpose stated in the introductory section
- Given the impact of AI on the human aspects of information and cybersecurity, propose how to accomplish the new AI-human integration for optimal results

In order to attain valid results for this type of research, a rigorous stand-alone literature review approach is followed.

According to Fink (2005), a stand-alone literature review approach must be systematic in following a methodological technique, explicit in explaining the procedures by which it was conducted, comprehensive in its scope of including all relevant material, and hence reproducible by others who would follow the same approach in reviewing the topic. A four-stage approach, each consisting of two steps, is adopted as summarised in Figure 1.

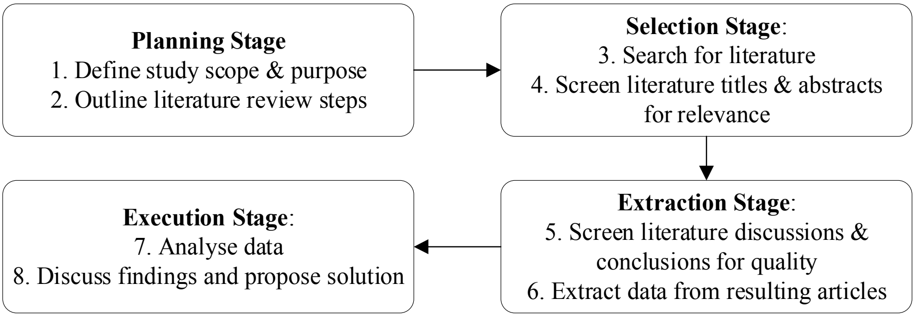
Planning Stage
1. Define study scope & purpose
2. Outline literature review steps
Selection Stage:
3. Search for literature
4. Screen literature titles & abstracts for relevance
Extraction Stage:
5. Screen literature discussions & conclusions for quality
6. Extract data from resulting articles
Execution Stage:
7. Analyse data
8. Discuss findings and propose solution

Figure 1: Systematic literature review process, derived from Okoli and Schabram (2010)

With reference to Figure 1, the four-stage systematic literature review protocol consists of the planning stage, selection stage, extraction stage, and execution (Okoli and Schabram, 2010). The planning stage is essentially Figure 1 as it outlines the literature review steps. The selection stage of the systematic literature review process is outlined in the next subsection.

2.2 Research Material Selection Scope

The study limited the review articles search to between January 2008 and May 2018 and a maximum number of 12 articles per journal. Levy and Ellis (2006) recommend that when repeated searches result in the same references, and with no new results from the same keywords, then the search is exhaustive. This is the search rule the researchers adopted. In addition, non-peer reviewed sources such as theses and dissertations, reports, conference papers, industry publications, and popular media were sought (Ridley, 2008). It is important to further augment the literature search in order to provide assurance that as many sources have been identified (Okoli and Schabram, 2010). According to Levy and Ellis (2006), this is achieved by further studying the reference sections of the relevant articles and performing both backward and forward searches. Backward search refers to references cited by the primary articles resulting from the researchers' keyword searches, and forward search relates to other publications citing articles compiled by the researchers. The following keywords were used to search for the literature and Table 1 shows the final results.

Database name	***Initial search results***	***Excluded no. of articles***	***Total no. of articles reviewed***
EBSCO – Academic Search complete	11	9	2
Access Engineering	541	541	0
Access Science	109	109	0
ACM Digital Library	409 773	409 773	0
Emerald	17	17	0
IEEE Xplore	390	385	5
JSTOR	87	87	0
OECD iLibrary	0	0	0
ProQuest Central	12 425	12 415	10
Sage Journals Online	58	57	1
ScienceDirect	259	257	2
SpringerLink	912	912	0
UJ Library Catalogue	5	5	0
Wiley Online Library	121	121	0
Google Scholar	19 800	19 792	8
Backward/forward search	0	0	3
TOTAL	444 508	444 476	**32**

Table 1: Total number of articles reviewed

The literature search conducted on May 18, 2018 was confined to 14 scholarly databases. Combined, these databases contain thousands of journals. In addition, the Google scholar search results of May 24, 2018 were included. The first top 20 Google scholar search results were screened. Only 8 were found to be relevant and of good quality. The screening of articles from the initial search results was based only on the titles and abstracts. Where the maximum of 12 relevant articles per database was not reached, the search results were augmented through backward and forward searches as recommended by Levy and Ellis (2006). Consequently, an additional 2 articles were identified through the EBSCO – Academic Search Complete database and 1 through ProQuest Central. At this stage, duplicates were also manually screened and eliminated. Table 1 was finalised with a total of 32 AI trends in information and cybersecurity articles. The systematic literature review relating to the AI trends in information and cybersecurity is described in the next section.

3 Related Work

With reference to the adopted literature review approach in Figure 1, the extraction stage is executed in this section. That is, the 32 articles in Table 2 are reviewed and the data as it relates to the research purpose are extracted and analysed.

3.1 AI Trends in Information and Cybersecurity

The main aim of information and cybersecurity is to minimise, or completely eradicate, the frequency of successful cyber-attacks (Yampolskiy and Spellchecker, 2015). It was previously mentioned that cyber-threats have become increasingly challenging to detect and respond to (Craig, 2018). This might be indicating that new information and cybersecurity measures are required (Dhananjay and Pandey, 2018). Dragomir (2017) has noticed that some of the new measures include the application of AI that is growing in adoption. The growth is attributed to perception by industry that AI has a quicker turnaround time to detection and reaction (Patil, 2016).

This is quite significant, especially, where traditional methods are too slow and insufficient to react (Wirkuttis and Klein, 2017). With its ability to recognise patterns of behaviour through massive datasets, AI could help detect a broad spectrum of cyber-threats and make intelligent decisions (Dilek *et al.*, 2015). The biggest threat from AI, however, is its potential for weaponisation (Carriço, 2018). This is because attackers will also leverage on AI's ability to learn from experiences and start developing AI-powered malware that traditional security systems will hardly be prepared for (Brundage *et al.,* 2018). Adding to this threat is the growing prevalence of polymorphous malware (malicious software with the ability to change its code) and zero-day attacks (type of attacks that strike and spread immediately), and viruses that can obfuscate for months or even years (Greengard, 2016).

With that in mind, the information and cybersecurity communities need to prepare for a future where AI-powered cyber-attacks will be autonomous (Hobbs, 2018). To prepare for this future, attention must also be paid to the security of AI applications themselves before they are deployed to other areas. Liu and Yu (2018) posit that as the usage of machine learning techniques gradually become widely accepted protecting its security at both the data learning and inference nodes becomes crucial. This is because a system may fail, either through design flaw or vulnerability exploitations on the nodes, to learn what the humans intended for it to and instead absorb malicious lessons (Yampolskiy and Spellchecker, 2015). Brundage *et al.* (2018) agree that AI systems are indeed susceptible to various security vulnerabilities distinct from traditional software's. Such vulnerabilities could also be exploited to automate cyber-attacks (Tadjdeh, 2018). If this happens, it could prove far-reaching and very dangerous for us all (Hobbs, 2018). Perhaps the danger comes from the fact that, if fully exploited, AI systems can attack targets much quicker than humans can (Brundage *et al.*, 2018). To this end, the literature has revealed that while AI-powered systems clearly surpass human performance in many ways, they are also vulnerable to attack in ways that humans never would (Brundage *et al.*, 2018). As described in the next subsection, human capabilities can significantly be augmented by AI when addressing organisational complexities (Jarrahi, 2018).

3.2 AI Trends Relating to Human Aspects of Security

Qualified personnel in information and cybersecurity are so scarce that organisations are turning to AI to fill the gaps (Fazzini, 2017). To shoulder the workload, it is expected that organisations will spend more on AI and machine learning to help improve security defences (Cisco, 2018). Although an ideal cyber-defense is to provide complete protection to users, we are still quite far from this scenario (Morel, 2011). In fact, Yampolskiy and Spellchecker (2015) argue that a 100% secure system does not exist because every security system eventually fails. Complete protection to users, therefore, is unlikely to ever be provided (Morel, 2016). In 2016 alone, the United States needed to fill 200 000 cybersecurity vacancies (Roberts, 2016). This shows that organisations wanting to deploy AI to bolster information and cybersecurity are not yet ready to remove the human from the entire process (Jack, 2016). Further, the application of AI to information and cybersecurity is not a tool in its own right; rather, AI still requires some level of human interaction for continuous improvement and, for example, to learn to understand new methods of attack and avoid false positive alarms (Maher, 2017).

False positive alarms can occur through the anomaly-based IDS technique where legitimate but previously unseen system behaviors are categorised as anomalies (Buczak and Guven, 2016). Practical examples of these include spear-phishing (when covertly malicious email is purported to be coming from a familiar source), application spoofing (when malware is masquerading as familiar and trusted software application), multimedia masquerading and other semantic social engineering attacks (Heartfield *et al.*, 2017). It would seem that no matter the levels of AI sophistication, humans will likely remain at the security controls and actively involved (Fazzini, 2017). It could be that humans still remain better positioned to render a more intuitive and holistic approach to decision making (Jarrahi, 2018). However, Pissanetzky (2016) holds a different view. According to the researcher, the Internet will ultimately be automated and secure without human intervention.

Whatever the future of AI holds, humans currently perform better cognitive functions of detecting, identifying and responding to cyber-attacks (Roberts, 2016). In a number of information and cybersecurity scenarios, Heartfield *et al.* (2017) observed that humans currently detect threats better than technical security checkpoints. However, the researchers qualify this assertion by stating that this is particularly the case, especially, when the threat is based on social engineering rather than exploitation of a specific technical flaw. Wirkuttis and Klein (2017) offer a different view. The researchers think that the current human and AI security capabilities are even. Moreover, they argue that since neither the human nor AI has individually proven total success in information and cybersecurity an organisational holistic view of the cyber-environment is therefore required in which AI is combined with human insight. Pissanetzky (2016) disagrees with the notion of integrating the human with AI applications to security. This researcher argues that human interventions should rather be reduced or completely eliminated as they introduce flaws and delays in response. In most cases, argue Rajbanshi *et al.* (2017), a delay in response time is usually caused by the sheer size and volume of cyber-incidents data, which is sometimes impossible for humans to analyse without automation.

Greengard's (2016) argument complements Pissanetzky's (2016) that the objective, quite simply, is to identify suspicious behaviour and patterns better, and build autonomous security frameworks that are more adaptable and resilient. Some experts take it further that the autonomy will inevitably be accomplished when the increasingly complex cybersecurity tasks are taken over by AI (Roberts, 2016). As matters currently stand though, cybersecurity techniques are desperately in need for change (Patil, 2016). Regardless of advances in AI and cybersecurity, Greengard (2016) is adamant that we will never be able to completely do away with the need for human interactions with machines. Landwehr (2008) is of the same view that even if we do succeed in developing what may seem like perfect AI security applications, attackers will continue to find creative ways to exploit social engineering approaches to trick users. As long as there are people, argues Greengard (2016), cybersecurity risks will never completely disappear. Whatever the case might be, the future of AI to the information and cybersecurity domain will depend on defining what humans and machines are each best suited at (Fazzini, 2017). Perhaps even the ethics of defining and delegating decision-making activities between humans and machines need to be looked at (Ramchurn *et al.*, 2012).

4 Results, Analysis, and Discussions

With reference to Figure 1, the final and execution stage of the systematic literature review is performed in this section and the findings are also presented.

4.1 AI Trends in Information and Cybersecurity

Generally, the intrusion detection system approach for identifying and responding to cyber-attacks utilises three techniques: signature-based, anomaly-based, and hybrid of the two. Most traditional information and cybersecurity solutions utilise the hybrid technique. The technique is usually adopted to increase the detection rates of known cyber-intrusions and reduce false positive alarm rates for unknown incidents (Buczak and Guven, 2016)). With increasing volumes of datasets resulting from the proliferation of the Internet of Things, cloud computing and edge devices, it has become difficult for traditional IDS methods to be effective. The literature reveals that with its ability to recognise patterns of behaviour through massive datasets AI could help detect a broad spectrum of cyber-threats and make intelligent decisions. Thus, it is safe to infer that AI has already surpassed the human intelligence when it comes to cyber-analytics of huge volumes of data. The literature further shows that AI systems are themselves also susceptible to various security vulnerabilities. Such vulnerabilities could be exploited to automate cyber-attacks. In this regard, the biggest threat from AI is its potential for autonomous weapons because attackers also have, access to and, the ability to leverage on AI advances. Society should therefore anticipate a possibility for a future replete with AI-powered weapons and malware that conventional IDS will be ill-prepared for. Put differently, the information and cybersecurity communities should prepare for a future where the impact of AI-powered cyber-attacks will be autonomous.

4.2 AI Impact to Human Aspects of Information and Cybersecurity

With organisations generating huge volumes of data on a daily basis, the literature revealed that it is impractical for any human to analyse such quantities of data. As a consequence, the application of AI has become increasingly more effective at analysing and identifying new data patterns and anomalies (Talwar and Koury, 2017). However, the application of AI to information and cybersecurity is currently used for bolstering security personnel. Although interest in deploying AI for human augmentation for cybersecurity purposes has also increased, it is still a long way off from making humans redundant. It is therefore generally accepted that organisations are not yet ready to remove the human from the entire security process. Furthermore, because the application of AI to cybersecurity is currently at an embryonic stage, it is argued that humans still perform cognitive functions better in terms of detecting, identifying and responding to new cyber-attacks. However, as time passes AI will learn enough from the data to start performing autonomous functions without human intervention; at least, this is what some researchers claim. This claim is at the heart of the argument by those who believe and those who do not believe that AI will, or should, completely replace human interaction. This question remains open for debate and further research.

4.3 Proposed Human-AI Security Symbiosis

The literature has shown that some are advocating for complete automation of AI and others not. It is therefore quite difficult to predict which way this may go. However, approaching AI as a panacea would be myopic because decades of research have shown that organisations are complex socio-technical systems (see Figure 2) and that any technological advances prove more powerful only if integrated into the social dimension of organisations (Sawyer and Jarrahi, 2014).

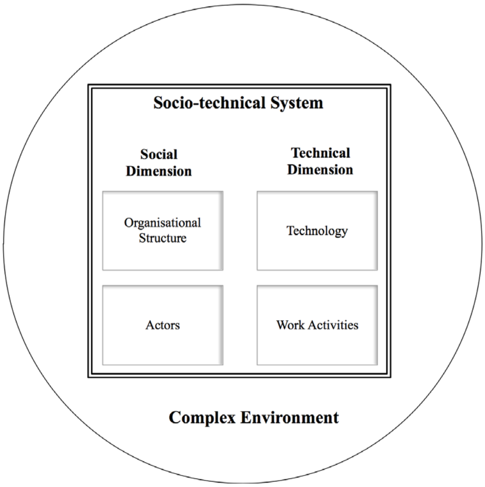

Figure 2: Socio-technical system, derived from Bostrom and Heinen (1977), Wu *et al.* (2015) and Oosthuizen and Pretorius (2016)

In this regard, the researchers propose the approach in Figure 3. This approach states that an optimal AI-human integration for information and cybersecurity can only be achieved if the social, technical, and environmental dimensions of an organisation are equally emphasised. The three dimensions are mutually interconnected.

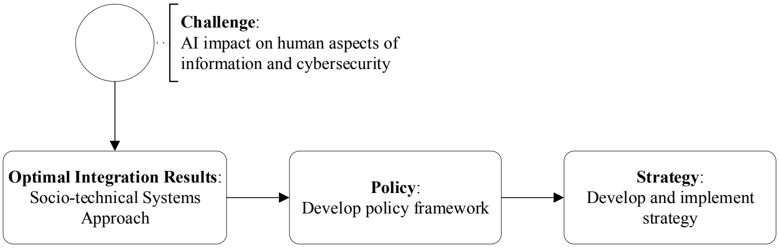
Challenge:
AI impact on human aspects of information and cybersecurity
Optimal Integration Results:
Socio-technical Systems Approach
Policy:
Develop policy framework
Strategy:
Develop and implement strategy

Figure 3: Socio-technical systems approach

5 Conclusion

With increasing volumes of data generated by systems, traditional intrusion detection systems have become less effective. Consequently, artificial intelligence applications have become widespread although currently for human augmentation. This is because humans are believed to currently perform cognitive functions much better than AI in terms of detecting, identifying and responding to new cyber-threats. There is a concern, however, that AI tools themselves may not be secure and attackers may produce AI-powered weapons soon. This is an area of research that requires further attention. The impact of AI to the human aspects of information and cybersecurity is therefore summarised in terms of the current and future scenarios. In the current scenario, the impact of AI is for bolstering human capacity. In the future scenario, however, the impact can go either way; that is, humans may become completely replaced by autonomous AI applications or humans and AI might mutually complement each other for optimal results. The researchers go with the latter where a socio-technical systems approach is recommended as a solution and requires further research in this regard. There is recognition of some limitations of the study and two are worth noting. On the one hand, there are various AI journals not screened. However, these journals are restricted in scope to contribute positively to our study as they focus mainly on the technical aspects of AI. On the other hand, a different combination of keywords would have yielded different but relevant search results. Researchers are therefore encouraged to explore this topic further.

6 References

Antuit (2018), “Artificial intelligence; Antuit launches cyfirma, a cybersecurity division delivering AI-driven threat intelligence”, Journal of robotics & machine learning, pp. 7. ISSN 1944-1851.

Bostrom, R.P. and Heinen, J.S. (1977), “MIS problems and failures: A socio-technical perspective; part I: the causes”, MIS Quarterly, Vol. 1 No. 3, pp. 17-32.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … Filar, B. (2018), “The malicious use of artificial intelligence: Forecasting, prevention, and mitigation”. ArXiv Preprint ArXiv:1802.07228.

Buczak, A.L. and Guven, E. (2016), “A survey of data mining and machine learning methods for cyber security intrusion detection”, IEEE communications surveys & tutorials , Vol. 18 No. 2, pp. 1153-1176.

Carriço, G. (2018), “The EU and artificial intelligence: A human-centred perspective”, European view, Vol. 17 No. 1, pp. 29-36.

Cisco (2018), “2018 annual cybersecurity report: Discover security insights, key findings, and the latest threat intelligence”, available at: https://www.cisco.com/c/en/us/products/security/security-reports.html?CCID=cc000160&DTID=esootr000875&OID=anrsc005983&_ga=2.257988170.1599669543.1526832714-2121005692.1526832714 (accessed 19 May 2018).

Craig, J. (2018), “Cybersecurity research – essential to a successful digital future”, Engineering, Vol. 4, pp. 9-10.

CyberSaint (2017), “CyberSaint, Inc.; CyberSaint[Registered trade-mark] security releases breakthrough AI powered cybersecurity management platform”, Journal of engineering, pp. 427. ISSN 1945-8711.

Dilek, S., Çakır, H. and Aydın, M. (2015), “Applications of artificial intelligence techniques to combating cyber crimes: A review”, International journal of artificial intelligence and applications, Vol. 6 No. 1, pp. 21-39.

Dhananjay and Pandey, M. (2018), “Artificial intelligence in cybersecurity”, Proceedings of the 7th national conference on emerging trends in information technology, New Delhi, India.

Dragomir, F. (2017), “Artificial intelligence techniques cybersecurity”, Proceedings of the 12th international scientific conference strategies XXI, Bucharest, Romania, Vol. 3, pp. 147.

Fang, B., Ren, K. and Jia, Y. (2018), “The new frontiers of cybersecurity”, Engineering, Vol. 4, pp. 1-2.

Fink, A. (2005). Conducting research literature reviews: From the internet to paper (2nd ed.). Thousand oaks, California: Sage publications.

Greengard, S. (2016), “Cybersecurity gets smart”, Communication of the ACM, Vol. 59 No. 5, pp. 29-31.

Heartfield, R., Loukas, G. and Gan, D. (2017), “An eye for deception: A case study in utilizing the human-as-a-service-sensor paradigm to detect zero-day semantic social engineering attacks”, IEEE computer society, pp. 371-378.

Hobbs, J. (2018), “AI enters the cyber attack realm”, Signal, Vol. 72 No. 7, pp. 38-39.

Jack, D. (2016), “Will artificial intelligence revolutionize cybersecurity”, The Christian science monitor. ISSN 08827729.

Jarrahi, M.H. (2018), “Artificial intelligence and the future of work: Human-AI symbiosis in organisational decision making”, Business horizons, Vol. 61 No. 4, pp. 577-586.

Levy, Y. and Ellis, T.J. (2006), “A systems approach to conduct an effective literature review in support of information systems research”, Informing science: International journal of an emerging transdiscipline, Vol. 9 No. 1, pp. 181-212.

Liu, Q. and Yu, S. (2018), “Survey on security threats and defensive techniques of machine learning: A data driven view”, IEEE access, Vol. 6, pp. 12103-12117.

Maher, D. (2017), “Can artificial intelligence help in the war on cybercrime?”, Computer fraud & security, pp. 7-9.

Morel, B. (2011), “Artificial intelligence and the future of cybersecurity”, Proceedings of the 4th ACM workshop on security and artificial intelligence, Chicago, Illinois, United States, pp. 93-98.

Okoli, C. and Schabram, K. (2010), “A guide to conducting a systematic literature review of information systems research”, SSRN electronic journal. 10. 10.2139/ssrn.1954824.

Oosthuizen, R. and Pretorius, L. (2016), “Assessing the impact of new technology on complex socio-technical systems”, South african journal of industrial engineering, Vol. 27 No. 2, pp. 15-29.

Parry, K., Cohen, M., and Bhattacharya, S. (2016), “Rise of the machines: A critical consideration of automated leadership decision making in organizations”, Group and organization management, Vol. 41 No. 5, pp. 571-594.

Patil, P. (2016), “Artificial intelligence in cyber security”, International journal of research in computer applications and robots, Vol. 4 No. 5, pp. 1-5.

Pumin, Y. (2016), “When machines become men”, Proceedings of the 3rd world internet congress, Wuzhen, China.

Pissanetzky, S. (2016), “On the future of information: Reunification, computability, adaptation, cybersecurity, semantics”, IEEE access, Vol. 4, pp. 1117-1140.

Rajbanshi, A., Bhimrajka, S. and Raina, C.K (2017), “Artificial intelligence in cyber security”, International journal of scientific research in computer science, engineering and information technology, Vol. 2 No. 3, pp. 2456-3307.

Ramchurn, S.D., Vytelingum, P., Rogers, A. and Jennings, N.R. (2012), “Putting the “smarts” into the smart grid: A grand challenge for artificial intelligence”, Communications of the ACM, Vol. 55 No. 4, pp. 86-97.

Ridley, D. (2008). The literature review: A step-by-step guide for students. Sage publications Ltd.

Roberts, P.F. (2016), “Cybersecurity's artificial intelligence future”, The Christian science monitor. ISSN 08827729.

Sawyer, S. and Jarrahi, M.H. (2014), “Sociotechnical approaches to the study of information systems. In A. Tucker and H. Topi (Eds.), Computing handbook, 3rd edition”, Information systems and information technology, pp. 5.1—5.27. Boca Raton, FL: Chapman and Hall/CRC.

Sabar, N.R., Yi, X. and Song, A. (2018), “A bi-objective hyper-heuristic support vector machines for big data cyber-security”, IEEE access, Vol. 6, pp. 10421-10431.

Silic, M and Back, A. (2014), “Information security: Critical review and future directions for research”, Information management & computer security, Vol. 22 No. 3, pp. 279-308.

Tadjdeh, Y. (2018), “AI: A tool for good and bad”, National defense, Vol. 102, pp. 774.

Talwar, R and Koury, A. (2017), “Artificial intelligence – the next frontier in IT security”, Network security, pp. 14-17.

U.S Newswire (2017), “With global cyber attacks on the rise, Zenedge says artificial intelligence holds the answer”, available at: https://search.proquest.com/docview/1922897220?accountid=13425 (accessed 19 May 2018).

Wirkuttis, N. and Klein, H. (2017), “Artificial intelligence in cybersecurity”, Cyber, intelligence, and security, Vol. 1 No. 1, pp. 103-119.

Wu, P.P., Fookes, C., Pitchforth, J. and Mengersen, K. (2015), “A framework for model integration and holistic modelling of socio-technical systems”, Decision support systems, Vol. 71, pp. 14-27.

Yampolskiy, R. and Spellchecker, M. (2016), “Artificial intelligence safety and cybersecurity: A timeline of AI failures”, available at: Google scholar (accessed 29 May 2018).