Global Trends in Cyber Security

Frankline Makokha

University of Nairobi

ABSTRACT

With the growth of Internet of Things (IoT) technology, a lot of devices are being connected and exchange information using the Internet. This increases the number of devices susceptible to cyber crimes or themselves posing as cyber attack vectors. This poses a challenge to current cyber security systems, which rely on human intervention for them to work effectively in deterring cyber crimes. This paper recommends integration of Artificial Intelligence techniques in cyber security measures both at prevention level and at investigations level.

Keywords: Internet of Things; Cyber Security; Critical Infrastructure; Cyber Infrastracture; Computer Forensics; Aritifical Intelligence.

Classification: D.4.6

Language: English

London Journals Press

LJP Copyright ID: 975722
Print ISSN: 2514-863X
Online ISSN: 2514-8648

London Journal of Research in Computer Science and Technology

Volume 19 | Issue 1 | Compilation 1.0

Global Trends in Cyber Security

Frankline Makokha

ABSTRACT

With the growth of Internet of Things (IoT) technology, a lot of devices are being connected and exchange information using the Internet. This increases the number of devices susceptible to cyber crimes or themselves posing as cyber attack vectors. This poses a challenge to current cyber security systems, which rely on human intervention for them to work effectively in deterring cyber crimes. This paper recommends integration of Artificial Intelligence techniques in cyber security measures both at prevention level and at investigations level.

Keywords: Internet of Things; Cyber Security; Critical Infrastructure; Cyber Infrastracture; Computer Forensics; Aritifical Intelligence.

Author: University of Nairobi, School of Computing and Informatics Nairobi, Kenya.

I. INTRODUCTION

Cyber infrastructure has become one of the critical infrastructures for any economy to prosper. This is due to reliance on ICTs by all sectors of the economy.

Critical infrastructure is a collection of systems and assets both tangible and non-tangible that provide critical services to the nation [1]. Cyber infrastructure refers to computational systems, data and information management, advanced instruments, visualization environments, and people, all linked together by software and advanced networks to improve scholarly productivity and enable knowledge breakthroughs and discoveries not otherwise possible [2].

Other definitions of cyber infrastructure include: the constellation of ICT that support communication, coordination, collaboration, and collection, storage, analysis and dissemination of data for distributed groups of researchers [3]; The comprehensive hardware for computing, data and networks, digitally-enabled sensors, observatories and experimental facilities, and an interoperable suite of software and middle- ware services and tools needed to capitalize on dramatic advances in information technology[4];.

From these definitions, cyber infrastructure can be defined as a collection of electronic and computing systems, configured to provide specific services via computer networks.

Due to the value derived from cyber infrastructure and the level of investments in them, cyber infrastructures have become a target from malicious persons out to vent their anger on regimes or persons utilizing the cyber infrastructures.

This has necessitated the development of measures to protect cyber infrastructures, called cyber security. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets [5].

The measures that have been put in place to mitigate against or deter the occurrence of cyber crimes are collectively referred to as cyber security.

Cyber crimes refers to computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks [6].

Other definitions of cyber crime include: crimes in which computer networks are the target or a substantial tool [7]; acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime [8].

Investigation of cyber crime requires acquisition of evidence from digital devices through Computer Forensics. Computer Forensics is the use of specialized techniques for the preservation, identification, extraction, authentication, examination, analysis, interpretation and documentation of digital information, while Forensics is the application of investigative and analytical techniques that conform to evidentiary standards used in or appropriate for a court of law or other legal context [9].

Computer forensics could also be referred to as: the science that is concerned with the identification, collection, examination and analysis of data during an investigation [10]; The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools , repeatability and possible expert presentation [11].

II. FORMS OF CYBER CRIME

Cyber crime takes three mains forms depending on the target, namely: cyber crime against persons/entity; cyber crime against institution; and cyber crime against computers and its associated infrastructures [11].

Cyber crimes could also be classified into four classes as: offences against the confidentiality, integrity and availability of computer data and systems; Computer-related offences; Content-related offences; and Copyright-related offences [12].

2.1 Cyber crime against persons

These are the most common forms of cyber crime and include: cyber stalking/bulling, cyber defamation, email spoofing, identity theft, Phishing, password sniffing.

2.2 Cyber crime against institutions

These are criminal activities targeted at certain institution e.g. financial institutions, academic institution or government bodies. They include compromising the Confidentiality, Integrity and Accessibility of the information held by those institutions e.g. systems hacking, intellectual property (software piracy, copyright infringement, trademark violations, theft of computer code) and Distributed Denial of Service (sabotage).

2.3 Cyber crime against Computers and associated Infrastructure

These are criminal activities targeted at computer infrastructures in general without targeting any specific person, entity or computing systems. They include computer virus creation, cyber vandalism.

III. MOTIVATIONS FOR CYBER CRIME

The motivation for cyber crime can be understood through analysis of the groups of persons engaged in the cyber crime.

The persons involved in cyber crime could be categorized as: the idealist, the greed motivated (criminals) and the cyber terrorist [11].

The idealists are normally teenagers, seeking social recognition and pleasure by deriving satisfaction in successfully challenging existing cyber security measures in place.

The greed motivated, the typical cyber criminals, are money motivated persons, ready to sabotage cyber security measures for monetary gains.

The cyber terrorists are usually a group of individuals out to sabotage cyber security measures for purposes of supporting a given cause they defend or due to disgruntlement with

government policies. It is also called cyber warfare.

VI. TRENDS IN CYBER CRIME

Computer crimes date back in the 1960s [13]. Computer crimes in this era involved physical damage to computer systems and subversion of the long-distance telephone networks crimes.

The crimes later evolved to sabotage of computer systems in the 1970s. This took the forms of intentional power systems shutdown and cable cuts. The Late 1970s saw the emergence of impersonation after credentials stealing from social engineering tactics like dumpster diving amongst other tactics. This later transformed to credit card frauds in the 1990s.

Technological advancements in the 1990s led to the emergence of hacking as a computer crime. The main target of this crime was banks where client money could be transferred without their consent and knowledge. This evolved to Salami Attacks, where money in small negligible and not easily detectable was moved from bank accounts.

The 1990s and early 2000s saw the prevalent of malwares from viruses, logic bombs, Trojan horses and worms. This could be used for various vices including confidential information gathering, alteration, destruction, spamming and denial of service.

The mid 2000s saw the emergence of malicious botnets. A bot is a script or sets of scripts designed to perform a predefined function in an automated fashion [14]. The same author defines a botnet as networks of infected end- hosts, called bots that are under the control of a human operator commonly known as a bot master/ bot herder.

The botnets are used for various cyber crimes namely launching Distributed Denial of Service (DDoS) attacks, spamming, sending Trojan and phishing emails, illegally distributing pirated media and software, force distribution, stealing information and computing resource, e-business extortion, performing click fraud, and identity theft for financial gain [15,16].

By 2013, Cyber crime had taken the form of ransomware. Ransomware is a type of malware that stops or limits users from accessing their system, either by securing the system's screen or by locking the users' files unless a ransom is paid [17].

Examples of common Ransomwares include Cryptolocker, Crypotwall, Locky and TeslaCrypt. The ransom is normally paid in form of bitcoin [17].

The latest cyber crime model is cybercrime as a service (CaaS). This refers to provision of services to others to facilitate their commission of cyber-crimes [18].

The various services available on CaaS platforms include: Research as a Service (Legal or illegal collection of information on victims); Infrastructure-as-a-service (Hosting of malware on secure networks, Rental of established botnets for Distributed Denial-of-Services, Cloud-based computing power for operations; Crimeware-as-a-service (Design and delivery of customized crime solutions); Hacking-as-a-service (Outsourcing of a complete cyber-enabled attack and Technical support for cybercrime activities) [19].

These development of a “as-a-service” innovations have accelerated the evolution of the cybercrime ecosystem and the growth of the cybercrime business, reconstructing into a specialization, commercialize, and cooperation system [20].

A summary of the trends in cyber crime is as shown in figure 1.

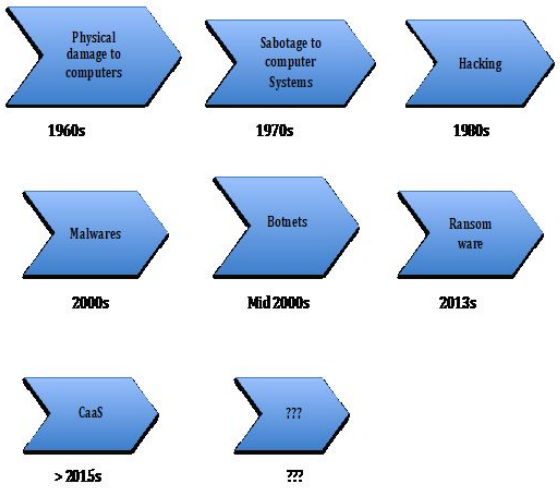

Figure 1: Trends in Cyber crime

V. MEASURES IN PLACE TO COUNTER CYBER CRIME

The advancements in cyber crime have evolved hand in hand with measures of fighting cyber crime. These measures can be categorised as: physical measures, technological measures and collaborative frameworks.

The physical measures aim to address access to cyber infrastructure by implanting access control features ranging from physical barriers to unauthorised access, biometrics and human guards.

Technological measures include rapid development of Anti virus, Firewalls, Intrusion detection systems and Intrusion Prevention systems.

Collaborative frameworks in fighting cyber crimes involve setting up of computer emergency response teams that liaise with other teams globally in alerting and educating each other on latest attack vectors.

Whereas these measures have helped mitigate cyber crimes, they have limitations which impact on their effectiveness in combating cyber rime.

5.1 Limitations of Anti Virus and Intrusion Detection/Prevention Systems

Antivirus and Intrusion detection/Prevention systems, if not designed with care can turn from defense mechanisms to instruments of attacks [21]. Further, since most anti virus operate based on known virus signatures, unknown threats for which no signatures exist can easily bypass the detection.

Several vulnerabilities have been sported in various anti virus softwares e.g. Kaspersky [22], AVG [23], FireEye [24] and EST [25].

Anti viruses use byte patterns, hash sums and heuristics during virus signature mapping [21].

Anti virus assisted attacks are launched using malicious markers, which do not rely on exploiting vulnerabilities but is based on the weak design of pattern-based signatures [21].

The main vulnerabilities identifiable in anti virus software are Local privilege escalation, Active –X related, Engine based and management interface related [26].

Intrusion Prevention and Detections systems can be classified based on detection methods, namely Anomaly Detection Systems, signature based detection and Decision Making Techniques [27].

These system have limitations in terms of gathering a set of static criteria of normal behaviors, how to identify new attacks with no signatures in the database and how or who makes the decisions, respectively [27].

Firewalls suffer from various limitations too, including inability to protect systems against malicious insiders and inability to protect against completely new threats [28].

5.2 Limitations of collaborative frameworks

Collaborative frameworks suffer from lack of secure channels to exchange cyber crime information. This raises the possibility of risk of

the exchanged information falling into the wrong hands.

Cyber crimes spread at alarmingly fast rates hence delays in sharing cyber crime information renders the shared information less effective especially if the information is received after the attack has occurred.

Legal constraints that prevent sharing of experiences on going legal proceedings against cyber crime mean that law enforcement authorities are not at liberty to divulge all the facts and elements of an on going case [29].

Other major limitations include: issues surrounding trust and control of incident response; questions about obligations regarding disclosure and exposure; the evolving liability and regulatory landscape; challenges faced in the cross-border investigation of cybercrime; and cross-border data transfer restrictions that impede the ability of companies to respond nimbly to cyber threats and incidents [30].

VI. TOOLS USED IN DIGITAL FORENSICS

Some of the tools used in digital evidence gathering include: Encase developed by Guidance Software of USA; Forensic Toolkit (FTK) by AccessData of USA; SANS SIFT Workstation of USA; Helix3 Pro of the USA; Automated Image and Restore (AIR) developed by Steve Gibson, founder of Gibson Research Corporation [31].

Additional forensics tools include: X-Ways Forensics developed by X-ways of Germany; Virtual Forensics Computing (VFC) developed by the MD5 of the UK [33].

Others include ProDiscover by Technology Pathways of the USA; and SMART by ASR Data of the USA [34]; Belkasoft Evidence Centre by Belkasoft of the USA; Computer Aided Investigative Environment (CAINE) created by the digital forensics project of Italy; Foremost created by Special Agents Kris Kendall and Jesse Kornblum of the United States Air Force Office of Special Investigations; MemGator created by the E5h Forensic Solutions of the UK; and OSForensics from PassMark of the US [35].

Whereas several tools have been developed to aid in digital forensics they suffer from various limitations, namely: limitations in terms of the operating systems on which they can operate, limitation on the file formats they can read, limitation of the area of focus for the tool (e.g. hard disk, browser, operating systems files etc.), their effectiveness on ability to process encrypted files and ability to recover overwritten files.

Further, most tools were designed for usage on traditional computing platforms, namely desktop or laptop. In cases where the forensics are to be carried on other computing platforms, like cloud computing, edge computing, Fog Computing, mist computing, etc, then the tools will be limited if not rendered unusable.

The proliferation of big data poses a challenge to current tools since they are not optimized to analyze big data, which is varied, and moving at high velocity. The overall efficiency of current forensics tools is limited to employment of simple hashing and indexing algorithms [36].

Digital investigations are also hindered by the limited processing capabilities of human analysts, since the tools as currently designed present data to the analysts who have to evaluate it and present in report form. With big data, this becomes a challenge in terms of man hours required to evaluate and analyze the large data sets.

This limitation can be overcome by integration of artificial intelligence techniques in the tools used for digital forensics.

VII. ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Due to the proliferation of devices connected on the internet, combined with an uptake of Internet of Things (IoT) technologies, the number of devices vulnerable to attacks or used in cyber crimes will surge, posing a challenge to existing means of fighting cyber crimes.

The rate at which new threats are being created now far exceeds the financial resource or human capability required to manually analyze or create rules for each and every new piece of malware code [37].

To cope with the high rate at which new malwares are spawned, Artificial Intelligence will come in handy. Artificial Intelligence (AI) is a field of study concerned with development of computers that are able to engage in human-like thought processes such as learning, reasoning, and self-correction [38].

Other definitions of AI are: A discipline devoted to developing and applying computational approaches to intelligent behavior [39]; machines that are capable of performing tasks that, if performed by a human, would be said to require intelligence [40]; is a subfield of computer science aimed at the development of computers capable of doing things that are normally done by people — in particular, things associated with people acting intelligently [41]

AI therefore is a paradigm for studying, development and application of computational systems capable of perceiving and learning from their usage context, and independently applying the gained knowledge in a way a human being would apply.

7.1 AI Techniques

The various AI techniques include Intelligent Agents, Neural Networks and Expert Systems [42].

1) Intelligent Agents

These are software components with features of intelligent behavior such as (at a minimum) pro-activeness, the ability to communicate, and reactivity (in other words the ability to make some decisions and to act) [43].

They have also been defined, as a piece of software that is situated within a given environment, where it acts autonomously, responds to changes in its environment including self recovery from failure, as it pursues its goals by assessing multiple ways of achieving the goals as it interacts with other agents [44].

Other definitions include: pieces of software that act based on information which is gathered from dynamic environment and achieve the goals successfully [44]; software entities that carry out some set of operations on behalf of a user or another program with some degree of independence or autonomy, and in so doing, employ some knowledge or representation of the user's goals or desires [45].

Intelligent agents which are able to detect unusual and malicious activities could be incorporated in Intrusion Prevention and Detection systems, in Operating systems, in Anti virus. Based on their heuristics knowledge, the agents will be able to decide on whether to terminate or allow the activity.

A typical conceptual architecture for the integration of an intelligent agent in a host environment is as shown if figure 1.

Figure 2: High Level Conceptual Architecture of an Intelligent Agent in A host Environment

A zoomed view of the figure 1 is as shown in figure 2.

From the diagram, the agent learns the state of the environment and updates its knowledge base. Anew requested state is compared with the learned states in the knowledge base and the Beliefs (known Information about the environment), Desires (objectives to be

accomplished by the agent) and Intentions (current chosen course of action) (BDIs), of the agent.

Depending on the chosen course of action, the knowledge base and the BDIs are updated accordingly. The learning process is continuous and the decisions are dynamic depending on the requested state and the BDIs

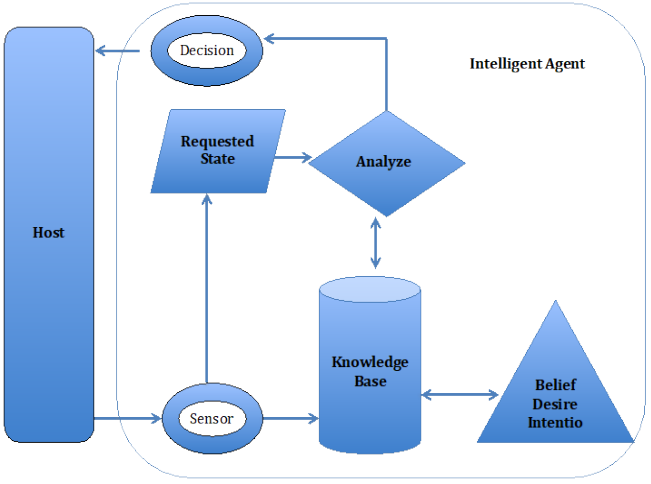

Figure 3: A zoomed High Level Architecture Diagram of An Intelligent Agent and Host Environment

2) Artificial Neural Networks (ANN)

ANN is a system simulating the work of the neurons in the human brain [46].

It consists of a collection of iterations to transform a set of inputs to a set of desired outputs, through a set of simple processing units, or nodes and connections between them. Subsets of the units in the iteration are input nodes, output nodes, and nodes between input and output form hidden layers; the connection between two units assigned some weight, used to determine how much one unit will affect the other. [47].

Due to the generalization feature of ANN, they are able to work with imprecise and incomplete data, meaning that they can recognize patterns not presented during a learning phase [46]. This feature is very vital in signature based detection systems.

Based on this relationship, an ANN can be used in pattern recognition and thus identify anomalies in the various computing platforms. This capability can be implemented in Intrusion Detection /Prevention Systems.

A high level architectural representation of the concept of an ANN in an IDS is shown in figure 3.

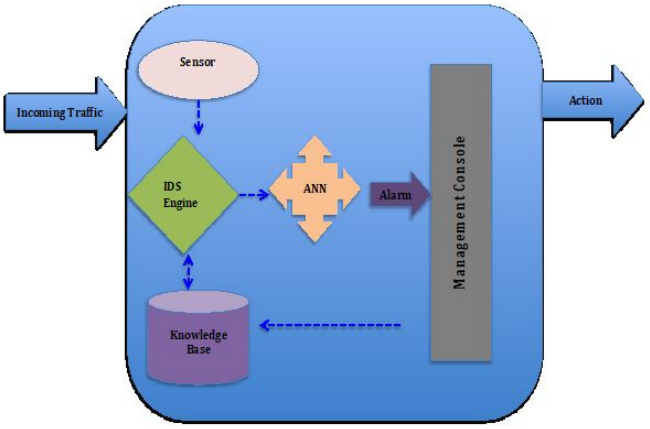

Figure 4: A high Level Architectural representation of an ANN in an IDS

From figure 3, all traffic is detected by the IDS sensor, and passed to the IDS engine, which analyses it based on the rules in the Knowledge base.

After analysis, the result is passed to the ANN, which uses that information for learning purposes. With time, the ANN will have learnt the patterns presented to it from the IDS engine, which it uses for future decision-making.

This lowers the chances of false alarms and zero days attacks from intrusions not yet configured in the knowledge base since the ANN can detect them.

Neural networks can also be extended to data encryption and used to construct an efficient encryption system by using a permanently changing key.

3) Expert Systems

This is a computer system that mimics the decision making of a human being [48]. They are composed of the Knowledge base which

represents illustrations and assertions about the real world and the Inference Engine, which is the reasoning system.

Expert systems can take the form of Associate skilled system, which is software system for locating answers to queries in some application domain bestowed either by a user or by another software system [49].

The knowledge base could be composed of items like malicious IP addresses, known malwares, expected end system state and allowed applications.

The inference engine on the other hand could contain information on application usage patterns, geographical location of certain IP addresses.

The Inference Engine reads the current state (Knowledge) of the knowledge base, applies the rules relevant to that and asserts new knowledge in to it.

Incase a new state is required which is not contained in the Knowledge Base, the inference engine executes a set of algorithms (rules) which predict the desired state. A decision is made depending on the predicted state.

A high level architectural depiction of the expert system concept is as in figure 4.

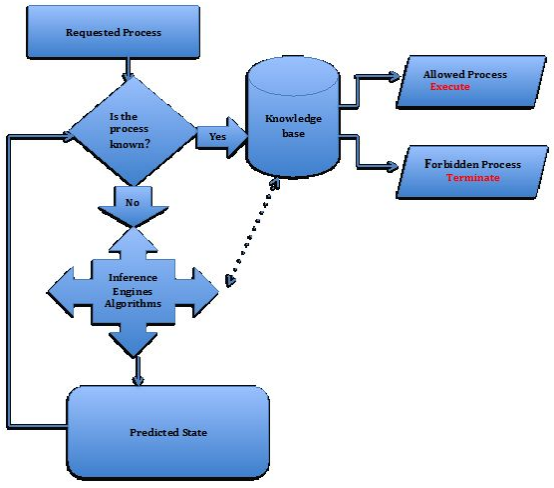

Figure 5: High Level Architecture of an Expert System Function

From figure 4, the requested process is passed through an expert system to determine whether it is a know process. If the process is known it is analyzed against the knowledge base to determine whether it is whitelisted or blacklisted.
If the requested process or state is not known, the inference engine analyzes it to determine its potential state or outcome. Depending on the outcome and system objectives, the Knowledge base is updated and the process loops back through the knowledge base for either termination or execution.

VIII. CONCLUSION

Whereas the use of Artificial Intelligence techniques in cyber security is currently on an upward trend, there is a possibility of cyber criminals using similar Artificial Intelligence tactics to counter the fight against cyber crime.

To prevent this, this paper recommends direct integration of Artificial Intelligence techniques directly into user applications, system software as well as embedded systems. The integration will also eliminate the need for third party tools downloaded by users to fight cyber crime , which could turn out to be malicious.

Further, from the analyzed literature, AI techniques have only been used in preventing or detecting cyber crimes. AI techniques have not been used in post cyber crime activities like investigations. This paper therefore recommends explorations of ways in which AI can be applied in cyber crime investigations to reduce the reliance on human intervention in view of the proliferation of IoT devices.

REFERENCES

1. Saadawi, T. and Colwell, J. D. Jr.(Eds) (2017) Cyber Infrastructure Protection Volume III. U.S. Army War College Press: Pennsylvania.
2. Stewart, A. C., Simmis, S., Plale, B., Link, M., Hancock, D., and Fox, C., G.(2010) What is cyberinfrastructure. In SIGUCCS '10 Proceedings of the 38th annual ACM

SIGUCCS fall conference: navigation and discovery. Norfolk, Virginia, USA.
3. Kim, Y. and Crowston, K. (2012) Technology Adoption and Use Theory Review for Studying Scientists' Continued Use of Cyber-Infrastructure. Proceedings of the American Society for Information Science and Technology. Volume 48, Issue 1. John Wiley & Sons, Inc. :New Jersy.
4. National Science Foundation(2007) Cyber Infrastructure Vision fo 21st Century Discovery.
5. International Telecommunications Union (2009) Understanding Cyber Crime: A Guide for Developing Countries. ICT Applications and Cybersecurity Division (CYB): Geneva.
6. Lakshmi, M. P. and Ishwarya, T. S. K (2015) Cyber Crime: Prevention & Detection. International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3.
7. Koops, E. J. (2010). The Internet and its Opportunities for Cybercrime. In M. Herzog-Evans (Ed.), Transnational Criminology Manual (pp. 735-754). Nijmegen: Wolf Legal Publishers (WLP)
8. United Nations Office on Drugs and Crime, UNODC (2013) Comprehensive Study on Cyber Crime. United Nations , New York.
9. Cartel Working Group(2010) Anti Cartel Enforcement Manual: Digital Evidence Gathering. International Competition Network (ICN).
10. Palmer, G. (2001). A Road Map for Digital Forensic Research. Proceedings of the First Digital Forensic Research Workshop,Utica, New York.
11. Ayofe, A. N. and Oluwaseyifunmi tan, O. (2009) Towards Ameliorating Cybercrime And Cybersecurity. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1.
12. Council of Europe (2001) Convention on Cybercrime: European Treaty Series - No. 185
13. Bosworth, S., M. E. Kabay and E. Whyne (2009), eds. Computer Security Handbook, 5th Edition, Volume I. New York: Wiley.
14. Tyagi , A. K. and Aghila, G.(2011) A Wide Scale Survey on Botnet. International Journal of Computer Applications (0975 – 8887). Volume 34– No.9, November 2011
15. Massi, J., Panda,S., Rajappa, G., Selvaraj, S. and Revankar, S.(2010) Botnet Detection and Mitigation, presented on *Proceedings of Student- Faculty Research Day, CSIS, Pace University* , May 7th, 2010.
16. Feily, M., Shahrestani, A. (2009) A Survey of Botnet and Botnet Detection, *3rd International Conference on Emerging Security Information, Systems and Technologies*, 2009. Athens, Glyfada, Greece.
17. Fasheem, S. M., Kanimozhi, P. and 3AkoraMurthy, B. (2017) Detection and Avoidance of Ransomware. *International Journal of Engineering Development and Research,* Volume 5 Issue 1.
18. Zheng, Y., Chaudhry, A. (online) Cyber crime as a Service. CaaS Analysis Report. https://www.eecs.yorku.ca/course_archive/2016-17/W/3482/Team15_CrimeAsService.pdf (accessed on 03rd July 2018).
19. Standard Chartered Bank(online) Cyber Crime as a Service. https://www.sc.com/fightingfinancialcrime/av/SCB_Fighting_Financial_Crime_Deep_dive_Cybercrime_as_a_Service_August_2017.pdf (accessed on 4th July 2018).
20. Huang, K., Siegel, M. and Madnick, S.(2017) Cybercrime-as-a-Service: Identifying Control Points to Disrupt. *MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity*, MIT-(IC)3. Vol. 1, No. 1, Article 1, November 2017.
21. Wressnegger, C., Freeman, K. , Yamaguchi, F. and Rieck, K. (2016) From Malware Signatures to Anti Virus Assisted Attacks. Computer Science Report No.2016-03, Institute of System Security, Technische Universität Braunschweig.
22. Ormandy, T. (2015) Kaspersky: Mo unpackers, mo problems. http://google

projectzero.blogspot.de/2015/09/kaspersky-mo-unpackers-mo-problems.html, 2015 (accessed on 10th July 2018)
23. Ormandy. T.(2015) AVG: "Web TuneUP" extension multiple critical vulnerabilities. https://code.google.com/p/google-securityresearch/ issues / detail?id=675, 2015. (Accessed on 11th July 2018)
24. Ormandy. T(2015) Fireeye exploitation: Project zero's vulnerability of the beast. http://googleprojectzero.blogspot.de/2015/12/fireeye-exploitation-project-zeros.html, 2015. (accessed on 11th July 2018).
25. T. Ormandy. Analysis and exploitation of an ESET vulnerability. http://googleprojectzero.blogspot.de/2015/06/analysis-and-exploitation-of-eset.html, 2015. (Accessed on 11th July 2018)
26. Xue, F.(Online) Nevis Netwroks inc. : Attackig Antivirus. http://www.blackhat.com/presentations/bh-europe-08/Feng-Xue/Presentation/bh-eu-08-xue.pdf [accessed on 13th July 2018]
27. Jadidoleslamy, J. (2012) Weaknesses, Vulnerabilities and Elusion Strategies against Intrusion Detection Systems. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.4, August 2012.
28. Archana D wankhade,D. A. and Chatur, P. N (2014) Comparison of Firewall and Intrusion Detection System. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 674-678.
29. World Economic Forum(2017) Recommendations for Public-Private Partnership against Cybercrime. REF 040117. Geneva.
30. Hermano, J. H.(2016, online) Cybersecurity Partnerships: A New Era of Public-Private Collaboration. http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf [accessed on 21st July 2018].
31. Cusack, B. and Liang, J. (2011). Comparing the performance of three digital forensic tools. *Journal of Applied Computing and Information Technology*, Volume 15 Issue 1.
32. Simon, T, 2012, Discussion on the Challenges and Opportunities of Cloud Forensics, *Multidisciplinary Research and Practice for Information Systems*, Vol. 9, no.1
33. Almulla, Sameera; Iraqi, Youssef; and Jones, Andrew (2014) "A State-Of-The-Art Review of Cloud Forensics," Journal of Digital Forensics, Security and Law: Vol. 9 : No. 4 , Article 2. DOI: https://doi.org/10.15394/jdfsl.2014.1190; Available at: https://commons.erau.edu/jdfsl/vol9/iss4/2
34. Carrier, B.(2005) File Systems Forensics Analysis. Addison Wesley professional, Boston.
35. Rana, N., G Sansanwal, G., Khatter, K and v Singh, S. (online) Taxonomy of Digital Forensics: Investigation Tools and Challenges. https://arxiv.org/pdf/1709.06529.pdf [accessed on 30th July 2018].
36. Beebe, N and Clark , J.(2005) Dealing with terabyte data sets in digital investigations. In: Pollit, M. and Shenon, S. (Eds) Advances in digital forensics: IFIP international conference on digital forensics. Orlando, Florida Feb 13–16, 2005, Proceedings. Springer: New york, USA.
37. Avira(Online) The Application of AI to Cybersecurity |:A n Avira White Paper Link (accesed on 3rd August 2018).
38. Kok, J. N., Boers, E. J. W., Kosters, W. A. , van der Putten, P. and Poel , P. (Onlie) Encyclopedia of Life Support Systems (EOLSS) : ARTIFICIAL INTELLIGENCE – Artificial Intelligence: Definition, Trends, Techniques and Cases. http://www.eolss.net/sample-chapters/c15/e6-44.pdf [accessed on 15th August 2018].
39. Gevarter, W. B (1983) Nasa Technical memorandum 85836 : An Overview of Artificial Intelligence and Robotics Volume I -- Artificial Intelligence
40. Scherer, M. U. (2016) Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, And Strategies. Harvard

Journal of Law & Technology Volume 29, Number 2 Spring 2016.
41. Hammod, K (2015) Practical Artificial Intelligence For Dummies, Narrative Science Edition. John Wiley & Sons, Inc. Hoboken, New Jersey
42. Anwar, M. and Hassan, S. I(2017) Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. *International Journal of Computational Intelligence Research* ISSN 0973-1873 Volume 13, Number 5 (2017), pp. 883-889
43. Tyugu, E. (2012) Command and Control of Cyber Weapons. *4th International Conference on Cyber Conflict*. Tallinn, Estonia.
44. Padgham, L. and Winikoff, M (2004) Developing Intelligent Agent Systems :A practical guide. John Wiley & Sons Ltd, England.
45. Rhem, A. J. & Associates, Inc (online) The Role of Intelligent Agents in the Information Infrastructure. http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.126.5461 [accessed on 7th August 2018]
46. Kukiełka, P and Kotulski, Z.(2008) Analysis of Different Architectures of Neural Networks for Application in Intrusion Detection Systems. In Proceedings of the International Multiconference on Computer Science and Information Technology. Wisla, Poland. Volume 3.
47. Parveen, J. R (2017) Neural Networks in Cyber Security. *International Research Journal of Computer Science* (IRJCS) Issue 09, Volume 4 .
48. Arockia, P. S, Giri, P. U and Khan, S. K. (2018) Aritificail Intelligence Techniques for Cyber Security. *International Journal of Engineering and Technology*, Volume 5, Issue 3.
49. Patil, P. (2016) Aritifical Intelligence in Cyber Security. Internationl Journal of reseacrh in Computer Applications and reseacrh. Vol 4, Issue 5.

This page is intentionally left blank