# A SYSTEMATIC PERFORMANCE REVIEW OF SECURITY METHODS FOR THE CYBERWORLD


## ABSTRACT

Governments and organisations globally increasingly recognise the importance of cybersecurity as a critical measure against cyber threats in our highly interconnected society. Establishing robust security measures has become paramount in safeguarding sensitive information and infrastructure. Biometric systems have emerged as critical components in various sectors, including industry, civilian applications, and rhetoric, to enhance security measures.This paper provides an overview of diverse security approaches in the cyber world and examines several research works, highlighting their strengths and weaknesses in implementation. We critically analyse existing methodologies and address potential shortcomings, aiming to improve the effectiveness of security measures. Additionally, we explore emerging trends and novel research directions in the field of biometric and rhetorical security.The study delves into contemporary biometric toolkits, examining their functionalities and applications across domains. Furthermore, we discuss digital ornamental models, evaluating their efficacy in enhancing cybersecurity measures. Through comparative analysis, we identify key differences and areas for improvement in existing security frameworks.In conclusion, this paper proposes a generic computer security model tailored to address the evolving challenges of cybersecurity. We highlight potential applications of this model in society, emphasising the importance of proactive measures to mitigate cyber threats effectively. Through comprehensive analysis and innovative approaches, we aim to contribute to advancing cybersecurity practices in contemporary society.



Keywords: Cybersecurity, Cyber Threats, Cyber Space, Cyber World, Safeguarding, Biometric.


## 1.0 INTRODUCTION

The fast development of information and Communication Technologies (ICTs) over the last decades has contributed heaps to the progress of society. The presence of recent technologies in each facet of human life has extended to such a degree that major public sector industries, like National Security, Education, Government, Health, and Public Safety, yet as sectors like Nutrition, Energy, social science and Transportation & Communication, square measure closely associated with, if not addicted to new ICTs.

“Security is a widespread and growing concern affecting all facets of society: business, domestic, financial, government, and so on. The data society is progressively addicted to many networks

and systems whose mission is vital, like traffic management systems, monetary systems, or public health systems" (Simson and Garfenkel, 2010).

Cybersecurity protects computers, networks, programs, and information from unauthorised access, amendment, or destruction. The vital question is: what quantity should a corporation invest in cybersecurity to reduce losses thanks to cyber-attacks? (ISO/IEC, 2011). The reality is that each investment in security measures and the loss sustained by the organisation thanks to cyber-attacks square measure prices to the organisation. Nonetheless, within the planet, there's no definitive answer on how these prices may be balanced or listed off. The lack of effective dealing with cyberattacks, though they represent an immediate threat to a state's ICTs, stems from various things. This study thus seeks to judge and analyse the impact of security techniqueson the cyberworld

## 2.0 OVERVIEW OF LITERATURE ON SECURITY

Cyber, as a prefix, denotes electronic and computer-based technologies. Cyber-space is an active area. Additionally, to the normal land, air, and ocean environments, new environments like space and cyberspace became operational domains for states in their negotiation (Hayden, 2016).Because of the environment within which state military actions are conducted, operational domains could also be distinguished, supported by the various technologies needed to work within. For example, military service ships work in maritime surroundings, and aircraft work in aerospace. Cyberspace could also be outlined as an indefinite place where people interact and communicate. It's the place between places (Dunn & Myriam, 2012).

Created with the web at its core, some crucial options of computer networks aren't congruent with a state-centric system. Computer networks' thinness, presence, and obscurity are already reshaping speculation, policy, and their usage in international relations. Choucri (2012) describes seven key options of cyberspace: temporality, disposition, permeation, fluidity, participation, attribution, and responsibility.

"Cybersecurity involves protective info and information systems (networks, computers, databases, information centres, and applications) with applicable procedural and technological security measures. Firewalls, antivirus programs, and different technological solutions for safeguarding personal knowledge and PC networks are essential; however, they are not spare to ensure security. Cyber Security plays a crucial role in the development of information technology and internet services". (Atul et al., 2013).

Current Approaches to IT – Security

The national security approach to cybersecurity is also outlined collectively and is frozen within the notion of cyber sovereignty, which needs states to grade national security and, by extension, protect important national infrastructure from cyber-attacks. Important national infrastructure, as utilised in the study, refers to the physical-digital infrastructures of a state, like its transportation, communication, info and utility systems, and computer networks. On the other hand, the human

security approach to cybersecurity is also outlined as a comprehensive approach that acknowledges the multiple sources of insecurity across many dimensions and addresses them consequently. It works towards guaranteeing cybersecurity at the individual level by making the person the referent object of security.

Gorodnichy (2009) argues that “biometric systems have evolved considerably over the past years”. “For instance, biometric systems vary from one sample-controlled verification intermediator to a large range of multiple samples multi-modal full machine-driven person recognition systems operating in diverse environments and behaviours at liberty. Various biometric characteristics are used for various applications” (Wayman et al., 2005). Every biometric attribute has its strengths and weaknesses, so the selection depends on how it is applied. No single biometric is predicted to effectively meet all applications' necessities (e.g., accuracy, utility, and cost) (e.g., DRM, access management, and welfare distribution). In other words, no biometric is “ideal,” though various area units are “allowable.”

Ruibin, et al., (2005) outlined“digital rhetorical investigation as a method of "identifying, preserving, analysing, and presenting digital proof in such a way that's lawfully acceptable through the appliance of computer technology to the investigation of computer-based mostly crime”. “Coincidently, whereas computers became further networked, digital forensics evolved into a term for the post-incident analysis of computers that are ill-used by intrusion or malicious code” (Ruibin et al., 2005). “As a result, individuals would usually describe the previous hacking instance, whereby network traffic has been captured and analysed as network forensics” (Kent et al., 2006). Since 2008, digital rhetoric has gone international, and it's reliable as it has left the science laboratory into a TV (TV) screen. Consequently, digital forensics has historically been employed in crime investigations, casualty identification, medical exterminations, network intrusion detection, forensic professional testimony, repositories, consulting services, analysis, and developments.

## 2.1 MODELS IN SECURITY FOR THE CYBERWORLD

Predictive models for estimating the incidence of cyber-attacks are urgently required to counteract the growing threat of a cyber act of terrorism. Sadly, except to a restricted degree, there's no real info on attacks, vulnerabilities, consequences, and risks for model development and validation. There are different kinds of cybersecurity: vital infrastructure security, application security, network security, cloud security, and Internet of Things (IoT) security.

## 2.2 PROBLEM SPECIFICATION AND SCOPE

“Analyses covering the IT atmosphere of organisations inside Ghana’s general public and private sectors have known major cyber threat areas targeting the IT landscape. More analysis suggests existing internal and external management measures are inadequate to sight and stop these technology-driven attacks. Various crime cases are reported across different sectors. Several of these attacks include internet attacks, IT-based network attacks, knowledge breaches, Malware

attacks, E-mail attacks, Distributed Denial of Service (DDoS) incidents, Man-in Middle (MITM) attacks, business executive-connected IT fraud, and Phishing attacks, among others. Network intrusions ensuing from system and application vulnerabilities, weak internal security controls, and non-compliance with IT procurance and usage of best practices are reported". (MFWA, 2017)

"A cyber-attack involving the "WannaCry" Ransomware affected several notable organisations globally in May 2017. Specialists rate this attack as the world's biggest single cyberattack incident in terms of the number of nations affected. The attack targeted a minimum of one hundred fifty countries and shut down two hundred 000 computers and databases of organisations. Analysis of Ghana's cyber atmosphere suggests such attacks are likely to affect Ghana's IT systems and networks. This is due to specific vulnerabilities, as well as a lack of a culture of cybersecurity awareness and important usage of unaccredited (cracked) operational systems across varied sectors". (MFWA, 2017)

This study focuses on cyberspace security. This survey is meant to spot methodologies, and tools of cybersecurity best observe approaches for the analysis of secure cyber world victimisation analysis works. Wherever possible, this report describes and analyses the strengths, weaknesses, and ways to overcome these weaknesses of security approaches to the cyber world. The study once more discusses future security strategies and their benefits.

## 3.0 METHODS

Mode of operation of the biometric security approach

Biometric technology nowadays depends on two central instruments as in the past. These are authentication and identification.

Authentication Systems

The general method for authentication systems is shown in Figure 1. The authentication method starts with, for example, a person inserting a smart or magnetic card into a reader (The user keys in his or her usernameinstead of a card). If it's a smart card, the reader reads a biometric example from the cardboard. If not, the reader reads the username, and then his/her live biometric data is captured and compared with the sample either scanned from the smart card or obtained from the database. The system then grants the person access if his/her identity is verified. Else. The person is denied access. Whereas the authentication method sounds like today's common security systems, biometric systems take issue in many respects.

1. An individual's biometric details captured when using the card help to verify the person to whom the card was issued.
2. People tend to forget PIN, but that's not so with biometric data.
3. Each person's biometric detail is unique.

The figure below shows the logic of a typical biometric authentication algorithm:

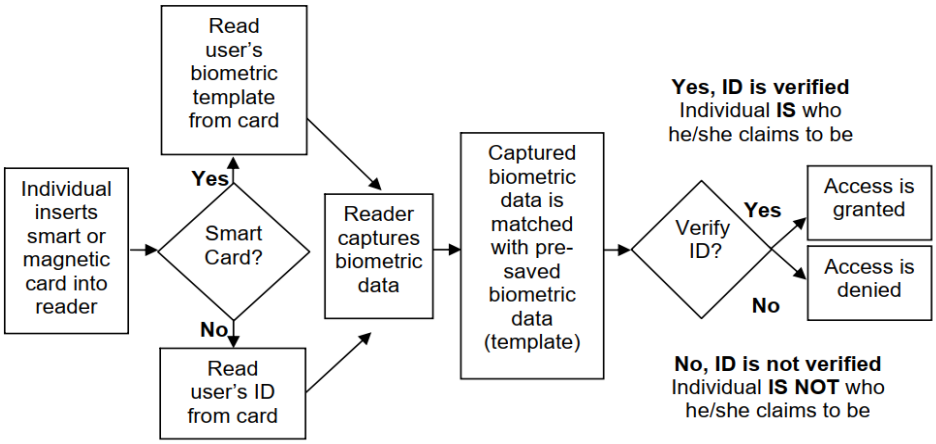



Figure 1. Biometric Authentication Algorithm

Identification Systems

Identification systems are either active or inactive to the individual. That is to say, they can be used without the user's knowledge or require that the individual provide biometric data, i.e. requiring active cooperation from the user.

For an active identification system, an iris recognition system installed near the entrance to an airport is a hypothetical example. Passengers entering may be asked to look into an iris recognition device. The iris image is likened to iris images in a database that contains iris images of people with a criminal record or people whose background shows a disposition to extremism. A person identified as such is then subjected to thorough search procedures before the person boards a plane. This is an example of an active identification system, as criminals are made aware of the identification system by being asked for their cooperation. The figure below shows the conceptual procedure behind an identification system.

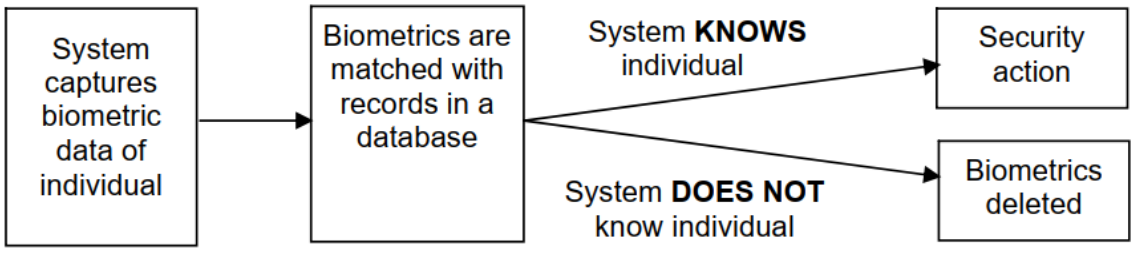



Figure 2: Biometric Identification Algorithm

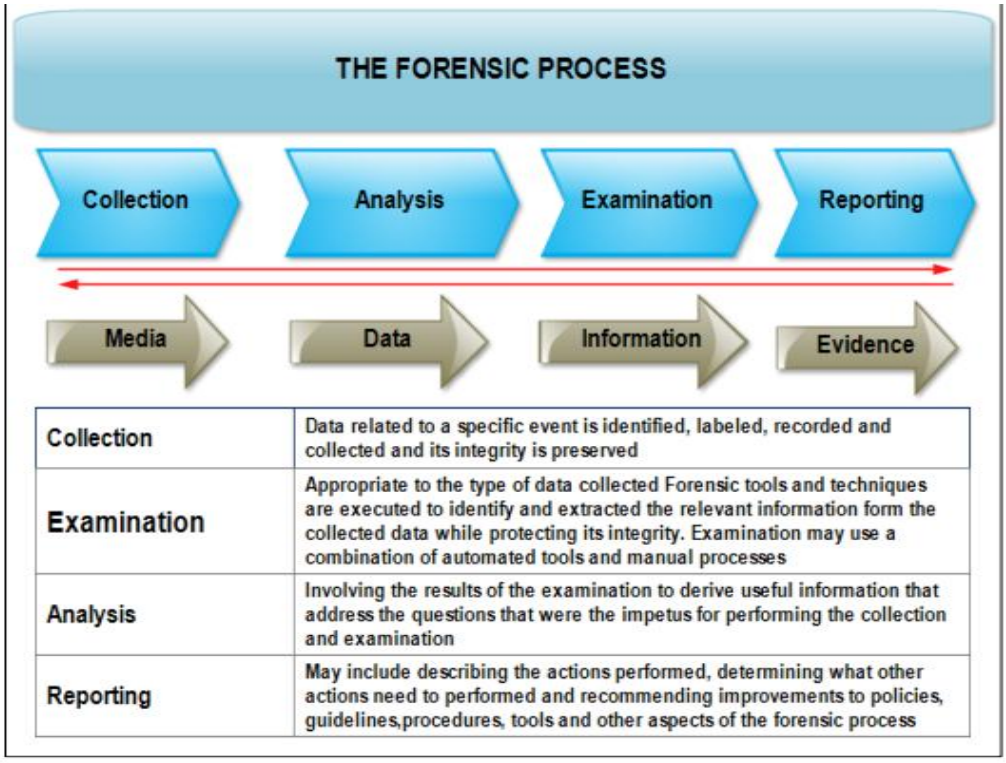
Further down the identification procedures, the individual does not take any deliberate actions to be identified. The system automatically captures the biometric data without the person's active involvement. Using thedatabase, the system verifies the identity of the individual. “The database can comprise biometric data of people who may bea potential public threat (e.g. criminals, terrorists, violent sports fans). The system’s main task is to try to match the biometric data obtained from the individual with numerous biometric templates stored in the database. For this purpose, the identification method is also known as a “one-to-many” comparison” (Ashbourn, 2000). If this type of individual is identified by the system, then the action is taken (e.g. the police is notified by the system about the presence of the individual). Otherwise, the taken biometric data is erased.

Mode of operation of the forensic security approach

Several efforts have been contributed towards a flexible and uniform digital forensic model that can offer full evidence concerning files, operating systems, network traffic, and applications. This has been donein line with the events that have occurred within digital forensic systems and networks. Below is a description of some early computer (digital) forensic models and applications.

According to Carrier & Spafford (2003), the basic forensic process, as defined by the Department of Justice (DOJ) and the National Institute of Standards and Technology (NIST), is based on four modules, including Collection, Analysis, Examination, and Reporting as demonstrated and explained in the figure below.

Fig .3 Forensic process




| | |
|---|---|
| Collection | Data related to a specific event is identified, labeled, recorded and collected and its integrity is preserved |
| Examination | Appropriate to the type of data collected Forensic tools and techniques are executed to identify and extracted the relevant information form the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes |
| Analysis | Involving the results of the examination to derive useful information that address the questions that were the impetus for performing the collection and examination |
| Reporting | May include describing the actions performed, determining what other actions need to performed and recommending improvements to policies, guidelines,procedures, tools and other aspects of the forensic process |

3.1 For an article to be incorporated in the review, the study has to be perfect in cybersecurity with adefinite scope of the study or any related model relative to the study. Any other article outside the above-specified scope, including literature in other dialects, except English, was omitted.

## 4. RESULT

Biometric System Performance

Technical Outlook

“Computer-powered biometrics is still a technology under development. Since computer-enabled biometrics is not fully developed, it is essential for organisations that may consider using this technology to evaluate its performance before implementation. The performance of a biometric security system can be assessed in terms of its precision, storage requirements, and speediness” (Jain et al., 2000).

FNR and FMR

“Errors may occur in the use of biometric systems. The system can reject a valid individual (a false no match) or accept an impersonator as a valid individual (a false match)”, according to Jain et al. (2000). “These mistakes give two important variables for rating the performance of the system i.e. False No Match Rate (FNR) and False Match Rate (FMR). The variables are negatively correlated. When a system is intended to function at a high level of accuracy, a slight

interference (such as dust or light conditions) in its operation may yield an error in its result. On the other hand, a system operating at lower levels of accuracy is more vulnerable to intrusion because it may accept an imposter as an authorised individual. This restraint necessitates seeking balance in the accuracy level along the Receiver OperatingCharacteristics (ROC) line. The ROC signifies an estimate for systemaccuracy in a given test environment"(Jain et al., 2000).

FTE

Failure to Enroll Rate (FTE) is another measure of the performance of biometric systems (Navati etal., 2002). FTE is "the likelihood that a given individual will be incapableof being enrolled ina biometric system" (Navati et al., 2002). Thereare two key reasons for FTE which are:

1. The biometric details of an individual may not be adequately distinct or can be replicated. Forinstance, grownup people or manual labour workers may have more "blurry" fingerprints, making it difficult for the system to enrol them.
2. A biometric system design (e.g. ergonomics) may pose difficulty in enrolling certaingroups of people. A study by UKPS (2005) revealed that biometric data (face, iris, and fingerprint) from younger/healthy individuals give more accurate authentication when likened to the biometric detailsofelderly or disabledindividuals. The study further revealed thatthose aged 55 and above had more difficulty positioning themselvesfor fingerprint enrollment than the 18-54 age group.

## 5.0 DISCUSSION

Cybersecurity guards the veracity of internet-connected systems, hardware, software, and computer data from cyber-attacks. Without any security plan, personal information, your customer's information, your business intel, and much more can be accessed by hackers and distorted. Today's world depends on the internet and computers for entertainment, communication, carriage, medicine, shopping, etc. Businesses are run online by banks.

Nations and large organisations globally are gradually implementing biometric data for Personal Identification and Recognition. Persons of all walks of life will, therefore, become holders of biometric E-Passports, Visa and Credit cards, and other biometric identification documents.The complex technical and disjointed settings of governmental systemsare a problem for society's general lay and non-technical members. Thereception of biometric technology and its dispersal within organisations andcountries are other possiblyrich avenues for research. Even the most dependable, effective, andproductive technology can't do much for an organisation,hence the need to adopt the technology.The use of biometric technology may be affected by both objective (e.g. how rapidlybiometric devices authorise an individual) and subjective factors (e.g. attitudes and insightstowards the new technology).

How does one report a hacking incident? Projected below is a Forensic Model that provides easy 'do it yourself' directives for laypeople without a technical background in organisations or homes.Thus, those who use computers or possess any form of a legal identification document in case of a potential breach of the law. The forensic examination mechanisms include all probable tasks carried out during each model phase. The three Phasesof the model include:

1. The Basic Phase - indicates thecommencement of the forensic investigationapproach once the user realises that he/shehas been hacked.
2. The Advanced Phase– denotesamore detailed examination of evidencerelatingto a moreurbane computerand skilled staff.
3. The Specialist Phase - refers to acomprehensive investigation and live demonstration ofpieces of evidence by the Forensic ScientificLaboratory Team with dedicatedequipment.

Applications for Non-TechnicalLay Members of Society.

1. The Basic Phase– An individual suspecting that any of his or herIdentification Documents have beenhacked may require conductingan in-house investigation using the informalflexible digital forensic investigationmechanisms, which include gathering, probing, reporting, presenting, and preserving the information. Making changes in the documents is discouraged.
2. The Advanced Phase – Incidents as such are to be reported immediately to any of the community non-profit organisations such as the Community Law Centre or Citizens Advice Bureau, call local police, or seek the assistance of experienced friends with the forensic processes. The innovative level staff will then properly refer to the Professional Level.
3. The Specialist Phase - will conduct the forensic investigation, examination, and presentation of shreds of evidence in a court of law.

## 5.1 CHALLENGES OF THE STATE-OF-THE-ART SECURITY MODELS FOR THE CYBERWORLD

There exist several reasons for the defective accuracy in biometric system performance. Various stimulating analysis glitches in biometric matcher design must be addressed before the performance gap is closed efficiently. At the very best level, the failure modes of a biometric system can be classified into two classes: intrinsic failure and failure thanks to an attack by an adversary. Intrinsic failures occur due to inherent limitations within the sensing, feature extraction, or matching technologies, additionally because of the restricted discriminability of the precise biometric attribute. In adversary attacks, an explicit hacker (or probably an organised group) attempts to bypass the biometric system for private gains. We tend to classify the opposer attacks into three sorts of supported factors that enable the opposer to compromise the system's security. These factors embody system administration, non-secure infrastructure, and biometric overtness.

"Given the importance of finding crimes quickly and, therefore, the want for automation to help rhetorical specialists, using biometric algorithms in enforcement and forensic applications can profit society. Further, the outcomes supported by most forensic proof (e.g. fingermarks, tool marks, etc.) haven't been scientifically validated. The 2009 National Academy of Sciences (NAS) report on the present state of forensic science within the US clearly articulates this defect, viz., that regularly created claims in forensic science are supported by less rigorous analysis than

may have been expected. The report points out: ‘Except DNA analysis, no forensic technique has been strictly shown to own the capability to systematically, and with a high degree of certainty, demonstrate an association between proof and a selected individual or source. In several cases, the long expertise of a forensic professional is assumed to be a substitute for scientifically gleaned empirical proof. Whereas experiential learning is very important once practising forensic science, it should essentially be foreign into a scientific framework that balances ‘domain knowledge’ with ‘empirical data’. Such a quest culture is usually missing from forensic science, and empirical information from rigorous studies that justify forensic scientists’ opinions arerare. Instead, the non-DNA forensic sciences (e.g. hair and bite marks Eckholm E. (2014)) have shown a worrisome tendency to treat oft recurrent opinions as scientific facts that are therefore well-accepted at intervals the field that the absence of supporting information is considered unimportant” (Mnookin JL et al., 2011). William Thornton & Peterson (2002) compactly propose: ‘Ironically, those areas of forensic science that have real underlying information supply reduced statements of discrimination, whereas those restricted to subjective or impressionistic information create the strongest statements, typically of absolute certainty. Thus, there's a chance for biometric researchers to collaborate with forensic specialists and statisticians in grouping giant forensic datasets (e.g. finger marks) and analysing the dependability and validity of forensic procedures by automatic strategies.

## 6.0 CONCLUSION

Cybersecurity is vitalinoverseeing the behaviours and manners of interacting with computer systems from waryconduct. Cybercriminals have endless opportunities to cause pandemoniumbecause we live in a world where even our kitchen appliances and cars are connected to the internet. IT security specialists, whose main focus is securing our data, must increase their knowledge because hackers continue to adapt to progressing technology.

Biometrics depend on a form of knowledge established over periods. Biometrics has been brought to a higher level of effectiveness due to theadvancements in computer technology. This has allowed its use in a variety of security applications. Biometrics is more consistent than traditional security approaches in a lot of ways. Nevertheless, manyuncertain issues (such as privacy concerns and the expensive nature of large-scale biometric solutions) have made biometrics a less attractive alternative to traditional security measures. Developments in computing technology and associated areas of studyare progressivelycontributing to theimprovements in biometric information processing. Biometrics should become a major security technology in the years ahead as businesses gradually gain more experience in deploying biometric security measures.

Whereas forensic investigation of documents isbeneficialin guiding and supporting criminal investigations and border regulatory activities, they can also generatevaluable data on the means of faking documents. Forensic examination and analyses may be performed on fraudulent identity documents, security documents, and non-security documents to Detect fake documents (both altered and forged documents), Examinethe authenticity of security structures; Determine

the authenticity of documents comparedto known standards; Determine the author of signatures; Outlineapproaches used to modify documents and to produce forged documents; Make available intelligence data; Offerguidance for the expansion of new security features for identity and security documents; Deliver other appropriateevidence related to the content of the document.

REFERENCE


Ashbourn, J. (2000) Biometrics: *Advanced Identity Verification*, London, UK: Springer-Verlag

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence*, 2(2), 1-20.

Choucri, Nazli, and Clark, David D. 2012. "Integrating Cyberspace and International Relations: The Co-Evolution". Massachusetts Institute of Technology, Political Science Department, Working Paper No. 2012-29. Accessed January 3, 2017. http://ssrn.com/abstract=2178586

Dunn C., Myriam. "The militarisation of cyber security as a source of global tension." STRATEGIC TRENDS ANALYSIS, Zurich, Möckli, Daniel, Wenger, Andreas, eds., Center for Security Studies (2012).

Gorodnichy, D. O. (2009). Evolution and evaluation of biometric systems. In *Computational Intelligence for Security and Defense Applications*, 2009. CISDA 2009. IEEE Symposium on (pp. 1-8). IEEE.

"Hayden: Hackers Force Internet Users to Learn Self-Defense". *PBS NewsHour*. N.p., 2011. Web. 13 July 2016.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43(2), 90-98.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-86.

MWFA, 2017. Cyber security in Ghana key issues and challenges. Policy brief.

Nanavati, S., M. Thieme, and R. Nanavati (2002) Biometrics: *Identity Verification in a Networked World*, New York, NY: John Wiley & Sons, Inc.

Ruibin, G., Yun, T., & Gaertner, M. (2005). Case-relevance information investigation: binding computer intelligence to the current computer forensic framework. *International Journal of Digital Evidence*, 4(1), 1-13.

United Kingdom Passport Service (UKPS) (2005) “Biometric Enrollment Trial”, http://www.homeoffice.gov.uk/docs4/UKPS_Biometrics_Enrolment_summary.pdf (current Sept. 24, 2004).