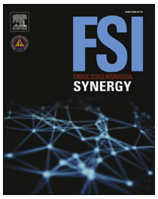
Contents lists available at ScienceDirect

Forensic Science International: Synergy

journal homepage: https://www.journals.elsevier.com/forensic-science-international-synergy/



An overview of the digital forensic investigation infrastructure of Ghana

Richard Apau [a, *], Felix N. Koranteng [b]

[a] Department of Computer Science, Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, UPO PMB, Ghana
[b] Department of Information Technology Education, University of Education Winneba, P.O. Box 1277, Kumasi, Ghana

ARTICLE INFO

Article history:
Received 10 June 2020
Received in revised form
8 October 2020
Accepted 13 October 2020
Available online 21 October 2020

Keywords:
Digital forensic
Cybercrime investigation
Digital evidence
National critical infrastructure
Electronic legislation
Ghana

ABSTRACT

Cybercrime incidents continue to plague economic development in the African region. Prior research indicates that millions of dollars are lost annually due to this menace. The prospects of Digital Forensics Investigation (DFI) as evident in developed countries provide hope for defeating cybercriminals. The paper assesses the effectiveness of legal infrastructure, technical mechanisms, the availability of capacity building programs, organisational infrastructure as well as the existence of cooperation mechanisms among relevant institutions in Ghana. The paper contends to the existence of legislation and mandated institutions. It concludes that, though the sector has recorded advancements over the years, the progress has been very slow leaving DFI still at an infant stage. Existing legislations are scattered and cumbersome whereas mandated institutions lack the requisite capacity. There is a need to streamline existing laws into a comprehensively harmonized legal framework. Furthermore, heavy investments must be deployed to boost the capacities of relevant institutions.

1. Introduction

Digital Forensic Investigation (DFI) has become a recognised profession and research field, due to the continuous and increased proliferation of cyber and digital crimes across the globe [2]. Whilst the field of digital forensics is now well established, its research community can be considered relatively emerging in comparison to the associated areas of traditional forensic and computer sciences [3]. DFI comprises different digital investigation processes, including identification, preservation, analyses, documentation and presentation of digital evidence [4]. These processes must be conducted in a robust and legally accepted manner in order to stand the test of legal scrutiny in the courts of law. Globally, many institutions are relying on digital media for the storage of information [5]. Information is now being processed, stored and exchanged through these media. As the use of digital media for information storage expands rapidly, there is a corresponding growth in computer crimes and cyber fraud [6]. This growth has compounded the challenges faced by law enforcement organizations and security forces across the world.

DFI is defined as the use of scientifically proven methods to obtain digital evidence from digital media sources like a computer, mobile phone, server, or network which can be used by the court of law [7]. These processes are often for the facilitation of or in furtherance of reconstructing events found to be criminal or anticipating unauthorised actions perceived to be disruptive to planned operations. It is, therefore, a broad concept encompassing many computer activities. This suggests that DFI is not limited to personal computers but other digital devices such as cell phones, Personal Digital Assistants (PDAs), network traffics, among many others. The various types of digital forensics include disk forensics, network forensics, wireless forensics, server forensics, database forensics, malware forensics, email forensics, memory forensics, mobile phone forensics [8] and more recently dashboard camera (dashcam) forensics [9]. Digital forensics aims to establish comprehensive knowledge and develop appropriate methodologies that can be adopted to defeat digital criminals and cyber fraudsters.

Due to the advantages it enables, DFI continues to gain tremendous recognition as an academic and professional discipline in many developed countries such as the United Kingdom (UK) and United States of America (USA) [4,10]. Indeed, there is evidence of abundant higher educational courses in these areas. For instance, in the UK and USA, digital forensic degree programs or forensic science and cyber security degree programs with concentration in

[*] Corresponding author.
E-mail addresses: Rich4u34@yahoo.com (R. Apau), felixnkoranteng@gmail.com (F.N. Koranteng).

https://doi.org/10.1016/j.fsisyn.2020.10.002

digital forensic have become ubiquitous [11]. In addition, well defined, well-structured and accepted professional digital forensic infrastructure that support cybercrime and computer fraud investigations by law enforcement agencies as well as the private sector, are readily available [12]. The UK National Cyber Security Centre (NCSC) hosted by the Government Communication Headquarters (GCHQ), the Computer Emergency Response Team (CERT) run by the US Department of Homeland Security, Computer Analysis and Response Team (CART) of the Federal Bureau of Investigations (FBI) and the National Computer Forensics Institute (NCFI) to mention a few, are well-established institutions equipped and mandated with relevant legislation to deal with computer crimes [13]. This presupposes that digital forensic processes are well-grounded in these countries, making the investigation and prosecution of cybercriminals an established procedure with well-defined approaches.

Yet issues regarding DFIs are rarely given attention in developing communities particularly, Africa [14]. in a review of relevant literature contends that scholarly works in the area of DFI predominantly originate from developed countries. In Ghana, reliable information on the state of digital forensics is very limited. This leads [11] to question the capacity of forensic science institutions in Ghana. Cybercrime issues across many economies are increasing at a faster rate [15]. The rapid diffusion and penetration of the internet, as well as the processes of digitisation of economic activities, have been the major catalyst [16]. However, cybercrime issues in Africa seem to be worse [17,18]. Amidst the staggering activities such as human trafficking, financing of terrorism, money laundering, incidents such as credit card fraud, SIM-box fraud and false identification have surged considerably [6].

In 2018, the Bank of Ghana banking cyber fraud report revealed that cyber fraudsters steal or attempted to steal 325.9 million Ghana Cedis (61.5 million US Dollars) from financial institutions operating in the country [1]. Cybercrime, therefore, hinders the smooth development of the country's economy [16]. This study is aimed at exploring the digital forensic investigation infrastructure of Ghana, with the view of identifying legal, technical, organisational, capacity building and international collaborative structures available for digital investigation. There is presently little or no studies that have previously investigated the digital forensic investigation infrastructure. The study will provide the academic community with the opportunity to develop higher education courses in cyber security and digital forensics as well encourage researchers in US, UK and other developed countries to strengthen research collaboration with overseas institutions such as those in Ghana. For industry practitioners, it offers the opportunity to foster stronger international partnership in fighting against borderless cyber fraud activities. The paper also provides an empirical foundation for policy decision-makers in Ghana to develop appropriate comprehensive structures for digital forensics investigation. In summary, the study will explore areas of digital forensics investigation infrastructure of Ghana such as legislation, institutional capacity, research and development, mechanisms, and technical capabilities to deal with cybercrime investigation. The study adopted archival research method (secondary data analysis). The main sources of data for the study were government reports, previous studies, reports by international and local institutions on digital crime and digital forensics in Ghana as well as presentations by governmental organizations. The next section discusses the digital forensic infrastructure through the lens of the International Telecommunication Union framework for cyber security preparedness.

2. Conceptual framework

The investigation of the digital forensic infrastructure of Ghana will be done around five main pillars. The pillars are adopted from the International Telecommunication Union's framework for multi-stakeholder cooperation in cybersecurity to build synergies between current and future initiatives as contained in the 2018 Global Cybersecurity Index [20]. These pillars are legal infrastructures, technical infrastructures, organisational, capacity building and cooperation. These five pillars form the basis of the investigation because they shape the inherent building blocks of digital investigation in every country. Digital forensics cut across almost all industries and sectors. Fig. 1 shows detailed information of the five pillars of the digital forensic investigation infrastructure.

To ensure that digital forensic capabilities and capacities are developed at the national level, efforts have to be put in place by political, economic and social forces within the country's administrative landscape. This could be broadly achieved through justice and judicial mechanisms, law enforcement, academic institutions, Ministries, Departments and Agencies (MDAs), technology developers, operators of the private sector, building Public-Private Partnerships (PPAs), intra-state cooperation and inter-agency cooperation with the aim of increasing efforts to adopt and

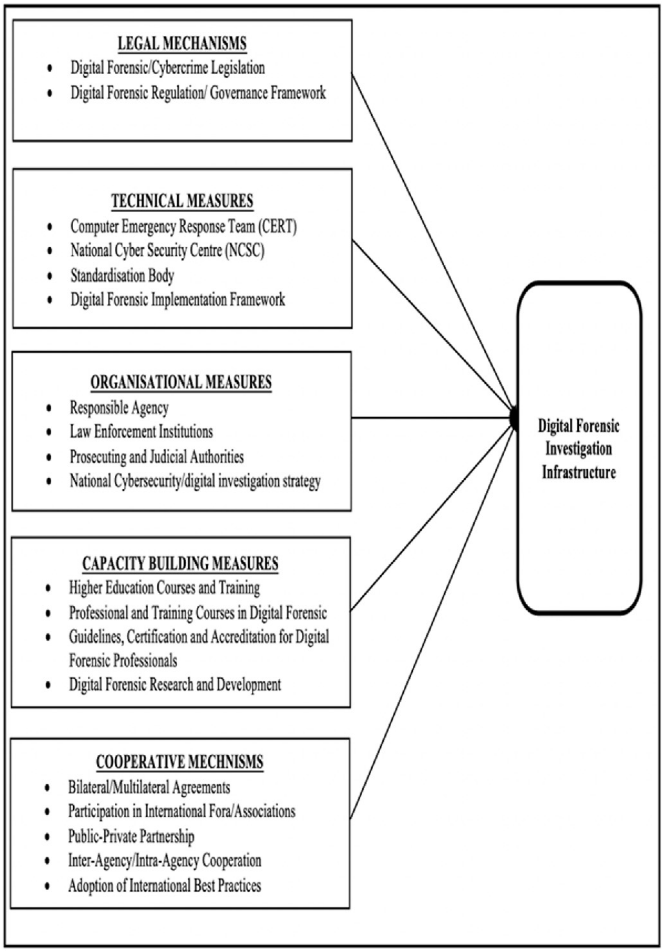

LEGAL MECHANISMS
• Digital Forensic/Cybercrime Legislation
• Digital Forensic Regulation/ Governance Framework
TECHNICAL MEASURES
• Computer Emergency Response Team (CERT)
• National Cyber Security Centre (NCSC)
• Standardisation Body
• Digital Forensic Implementation Framework
ORGANISATIONAL MEASURES
• Responsible Agency
• Law Enforcement Institutions
• Prosecuting and Judicial Authorities
• National Cybersecurity/digital investigation strategy
CAPACITY BUILDING MEASURES
• Higher Education Courses and Training
• Professional and Training Courses in Digital Forensic
• Guidelines, Certification and Accreditation for Digital Forensic Professionals
• Digital Forensic Research and Development
COOPERATIVE MECHNISMS
• Bilateral/Multilateral Agreements
• Participation in International Fora/Associations
• Public-Private Partnership
• Inter-Agency/Intra-Agency Cooperation
• Adoption of International Best Practices
Digital Forensic Investigation Infrastructure

Fig. 1. Digital forensic investigation infrastructure source: Authors' construct, 2020.

integrate digital forensic on a large scale. Each pillar adopted in this study will focus on a specific sector of the digital infrastructure needs. Pillar one will deal with legal issues taking into account the existence of legal frameworks and institutions to deal with digital forensic investigation and cybercrime. Pillar two which focuses on the technical aspect will examine the availability of technical institutions, including standardization bodies to deal with digital forensics. Pillar three considers the organisational measures for policy coordination and development of digital forensics strategies at the national level. Pillar four tackles capacity building including educational degree courses, research and development as well as professional development certifications. Finally, pillar five covers the measures that are in existence to foster international cooperation and partnership for continuous advancement of digital forensics in Ghana.

3. Existing legal infrastructure

Legal frameworks, thus legislation and regulations provide authorisation to the nation to set up the necessary response mechanisms through investigation and prosecution of cybercrimes. The primary objective is to have adequate legislation to deal with the evolution of cybercrimes.

3.1. Legislation

The use of digital forensic evidence is recognised and accepted by the justice system of Ghana. Like in many countries, law enforcement agencies draw their investigative and intelligence function from the existence of legislation mandating their work. In Ghana, the 1992 Constitution of the Republic of Ghana is considered the supreme and the fundamental law from which all other laws originate [11]. For instance, Article (19) of Ghana's constitution provides law enforcement agencies with the authority for the management and disclosure of evidence during trial of criminal cases. What this means is that the collection, preservation and presentation of evidence, including digital evidence must be legal, and transparent in a manner that does not cause miscarriage of justice.

Apart from the constitution, specific laws are also in existence to provide the law enforcement agencies additional powers to gather evidence and present the evidence in a way that is admissible in court. One of such laws for the arrest, detention and treatment of suspected individuals is the Criminal Offenses Act (Criminal Code) 1960, known as Act 29 (Act 29, 1960). Aside the 1992 constitution of Ghana, which serves as primary reference for criminal and civil prosecution, the Act 29 is the most comprehensive law which contains criminal offenses envisaged by the Act. Offenses listed in the Act include attempt to commit criminal offence, abetment and conspiracy, criminal harm to a person, sexual assault, libel, unlawful entry, forgery, counterfeit, obscenity among many others. In 2012, Act 29 was amended to include more offenses which have become prevalent such as organised crime groups and racketeering. The coverage of Act 29, therefore, presupposes that it is used in the prosecution of all manner of offenses including digital crimes.

There is also the Criminal and Other Offenses (Procedure) [21]; known as Act 30 (Act 30, 1960). The Act mandates law enforcement agencies to search and seize evidence where necessary, including digital evidence for investigation and prosecution of an offence. Section 121 of Act 30 gives specification on the evidence that may be admitted in court, which includes scientific reports. However, the Act only allows the court to admit reports from scientific analysts recognised by the Ministry of Justice, in which information of these analysts are supposed to be published in the Gazette.

The Evidence Act 1975 is another important legislation for the investigation and prosecution of offenses. sections 51 and 52 of the Evidence Act 1975 gives the court discretion to accept evidence including digital evidence in prosecution. For instance, section 51(2) of the Evidence Act says that all pieces of evidence are admissible except otherwise provided by law. The Evidence Act, specifically, sections 67, and 112-155, also makes provision for a court expert to be called upon to provide expert opinion on matters within their expertise. The expert witness is to assist the court to determine the authenticity of evidence when it lacks the technical expertise. This practice is common and consistent with other jurisdictions such as England and Wales, where the common law of assistance is used [22]. In purely technical fields there are always challenges regarding the understanding of the evidence before the courts [23], hence expert witnesses are key in this regard. As per the Evidence Act, an expert does not need to declare the basis of his opinion, neither must his expert opinion be necessarily admissible in court. This provision, however, is a contradiction of the impartiality and evidentiary reliability in the common law assistance of England and Wales [24].

Another crucial Act, perhaps most related to the investigation and prosecution of digital crime is the Electronic Transaction [25]; Act 772. Section 98 of Act 772 creates what is known as "*Cyber Inspectors*". The section empowers the law enforcement officers to arrest suspected cybercriminals, search and seize evidence in accordance with the law. The Act basically brings to fore the criminalisation of cyber offenses, admissibility of electronic evidence and provide an avenue for promoting legal certainty within the cyber ecosystem of Ghana [26]. The Act categorically mentions certain materials that may be seized as part of the investigation of digital or cybercrime [27]. Section 98(2) states that a law enforcement officer may seize any computer, electronic record, program, information, document, or a thing in the execution of a warrant if the officer believes reasonably that an offence under the act is committed or may be committed [25]). Also, sections 107-140 list all offenses that are considered cybercrime under Act 772. Example of these offenses includes electronic trafficking, denial of service, child pornography among others. For instance, section 136 (1c) states: "*a person who intentionally possesses child pornography in a computer system or on a computer or electronic record storage medium commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both".*

The Electronic Communication Act, 2008 known as Act 775 [28] also mandates law enforcement agencies to arrest and prosecute individuals who commit offenses related to the electronic media. Section 73 of Act 775 specifically spells out the offenses that may call for digital investigation and evidence. The offenses include giving false information on electronic platforms, damaging electronic equipment including computers and network devices, confidentiality and disclosure of personal information on electronic medium, re-programming mobile phones and possession or supply of device for the re-programming purposes. For instance, section 77 (b) of Act 775 states: "*a person who recklessly, intentionally or negligently interferes with, causes damage to, or accesses without authorisation a computer, switch or other facility used in connection with the operation or provision of electronic communications network or service, commits an offence, and is liable on summary conviction to a fine of not more than three thousand penalty units or to a term of imprisonment of not more than five years or both*". This Act is, therefore, relevant in the prosecution of digital crimes committed on the electronic medium including social networking sites (SNS) like Facebook, Twitter and Instagram.

Furthermore, the Data Protection Act, 2012 known as Act 843 [29] is legislation created for the protection of individual data and privacy and prescribes punishment for offenders. Just like the coming into force of General Data Protection Regulations (GDPR) for countries of the European Union (EU) in 2018, the Data Protection Act of Ghana provides mechanism to safeguard individuals' privacy, risk and security and further protect them from unlawful usage of their private data. Act 843 has brought strict controls and compliance to privacy measures and institutions that fail to comply are faced with prospects of heavy fines and sanctions. The Act also establishes the Data Protection Commission (DPC) charged with the responsibility to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters. The role of the DPC is, therefore, paramount in protecting individuals against digital crimes. The concept of the DPC in Ghana is similar to the Information Commissioner's Office (ICO) in UK, which ensures that companies and individual comply with the GDPR and the UK data protection laws.

In addition to these laws and acts mentioned, other Acts that also provide legislation backing for the investigation and prosecution of cyber offenses leading to the gathering of digital evidence include Mutual Legal Assistance [30] (Act 807) and Criminal Offenses (Amendment) [31] (Act 849). Although there appears to be a robust legislative framework in place to deal with cyber offenses, the various provisions are scattered in many legislations making it difficult to have a one-stop-shop for all cyber offenses and prosecution. There is presently no legislation or law in Ghana, that specifically deals with cybercrime and its associated DFI. There is the need to harmonise all existing legislation into a comprehensive digital forensic legal framework to aid in the investigation and prosecution of cyber offenses. Table 1 shows a summary of existing legislation for digital forensics investigation arranged in chronological order.

3.2. Regulation/governance framework

Presently, there is no regulation of digital forensic investigation in Ghana. Even though digital evidence is admissible within the courts of Ghana as per the legislations mentioned, the conduct of digital forensic investigation is not formally regulated by anybody. In Ghana, the Cyber Crime Unit of the Criminal Investigations Department (CID)-Ghana Police Service (GPS), is the major provider of digital forensic evidence in the law courts. As the forensic investigation profession is not well-grounded in the country, the participation of the private sector in forensic investigation is very limited. The E-Crime Bureau is a private entity that performs some private digital forensic investigation [34]. There is no specific regulation or policy framework from the Ministry of Justice that regulates the Ghana Police Service regarding the conduct of digital forensic investigations in order to produce digital evidence that could be relied upon in the court. It could, therefore, be said that the entire DFI of the country is a police-led system. This situation raises prosecution bias and may cause greater adverse effects on the application of digital forensic evidence in the criminal justice system [35].

Internationally, objectivity of digital forensic evidence has been recognised as a key component in DFI [36]. In most jurisdictions, there is a separate authority for regulating forensic investigation, different from the body responsible for prosecution using forensic evidence thereby ensuring autonomy and independence of digital evidence [37]. The UK for example provides a clear governance framework for forensic investigation and regulation [38]. The Association of Chief Police Officers (ACPO) 'Good Practice Guide for Computer-Based Electronic Evidence' guidelines (referred to hereon simply as 'the ACPO guidelines' or 'the ACPO principles') is a framework which ensures that digital forensic report in the UK conforms to international standard of digital forensics investigation, industry standard tools, techniques and procedures for evidence acquisition, processing, and analysis of exhibit retrieved [39]. The ACPO guidelines consist of a set of four principles and then the detailed guidelines, they are aimed specifically at 'police officers, police staff, and private sector investigators working in conjunction with law enforcement' [39]. The ACPO guidelines is considered the standard principles for UK based digital investigation [38]. According [40]; ACPO offers a means of ensuring the investigation is conducted in a professionally accepted manner. In Scotland, the Scottish Police Authority is an independent state regulator of forensics, which is different from the Scottish Police Service (Scottish Police Authority, 2018). This practice results in a DFI that is more independent and impartial [41]. A similar system also exists in England and Wales. There exists an independent forensic science regulator in England and Wales that provide some level of transparency and independence and also provide guidelines on quality forensic services [42]. Even though the DFI landscape in England and Wales are mixed with both the public and private sector, the Forensic Science Regulators try to ensure consistency in service and provision of high level digital forensic evidence [43]. Perhaps, a similar system and governance framework should suffice for Ghana, which will take the biases likely to arise from a police forensic investigation and prosecution. Already, there is a high level of mistrust between the Ghana Police Service and the public [44],

Table 1
Summary of existing legislations.

No	Legislation/Law	Summary
1	Criminal Offenses [32] (Act 29, 1960)	An act that empowers law enforcement agencies to arrest and prosecute individuals as per laid down procedure
2	Criminal and Other Offenses (Procedure) 1960 (Act 30, 1960)	Mandates law enforcement agencies to search and seize evidence where necessary, including digital evidence for investigation and prosecution of an offence.
3	The Evidence Act 1975 [33]	Makes provision for a court expert to be called upon to provide expert opinion on matters within their expertise.
4	The 1992 Constitution of Republic of Ghana (Ghana Republican Constitution, 1992)	Provides law enforcement agencies with the authority to manage evidence during trial of criminal cases.
5	Electronic Transaction [25] (Act 772, 2008)	Creates "*Cyber Inspectors* and empowers law enforcement officers to arrest, search and seize evidence in accordance with law.
6	Electronic Communication [28] (Act 775, 2008)	Mandates law enforcement agencies to arrest and prosecute individuals who commit offenses related to the electronic media
7	Mutual Legal Assistance [30] (Act 807, 2010)	Allows Ghana to provide assistance to external entities to locate and identify persons who have committed an offence.
8	Data Protection [29] (Act 843, 2012)	Legislation created for the protection of individual data and privacy and prescribes punishment for offenders
9	Criminal Offenses (Amendment) [31] (Act 849, 2012)	Criminalises the participation in organised crime groups, racketeering and other related crimes

Source: Authors' Compilation, 2020.

primarily due to the public perception that the police are a corrupt institution. An independent public body could be established to regulate digital forensic investigation in Ghana.

It is also recommended to the Government of Ghana to establish and set up National Computer Forensic Institute under the National Security Council Secretariat. This institute when established could help standardise, provide relevant digital forensic investigation guidelines, and regulate provision of digital forensic services. The institute could also provide state and local law enforcement, legal and judicial professionals a free, comprehensive education on current cybercrime trends, investigative methods, and prosecutorial and judicial challenges. Additionally, the institute could also provide training and capacity building programmes for both private and public digital forensic services providers. The US has a national computer forensic institute (NCFI). The US NCFI is a federally funded training centre dedicated to instructing state and local officials in digital evidence and cybercrime investigations. The modus operandi could be adopted and modified to suit Ghana's proposed institute.

4. Technical infrastructure

Key to the successful implementation of DFI infrastructure will be the ability of the nation to rapidly respond to cyber threats and provide mitigation response to avoid loss of property. The primary frontier for defence against cyber threat is technology (International Telecommunication Union (ITU), 2018). In order to properly defend against cyber threats, there should be in existence computer emergency or incident response teams, technical mechanisms and capabilities deployed for the investigation and detection of digital fraud. It is also imperative to put in place frameworks for the effective coordination of technical incidence response [45]. A country that has no suitable technical skills to detect and respond to cyber-attacks will continue to remain vulnerable to cybercriminals. There should be in existence a national body responsible for cyber incident response to effectively prevent the occurrence of digital fraud.

At present, Ghana has no national Computer Analysis Response Team (CART) to deal decisively with the technical detection and investigation of potential digital fraud. This has resulted in many state organizations that maintain critical national cyber-physical infrastructure to rely on internal IT teams to protect their assets. For instance, following the increase in cybercrime activities in the financial sector, the Bank of Ghana set up an internal cyber response team to monitor and reduce the incidence of cyber-fraud [1]. In 2017, the President of Ghana, H.E. Nana Addo Danquah Akufo-Addo announced the intention of the government to establish a National Cybersecurity Centre to be charged with the responsibility of drafting and implementing national cybersecurity strategy with relevant security institutions [46]. It must be noted that, Ghana drafted its first National Cyber Security Policy and Strategy in 2014 and made provisions for the establishment of National Cyber Security Centre to deal decisively with cyber security issues and policy directions. The National Cyber Security Centre was also to have a Computer Emergency Response Team (CERT) to deal with cyber-related crimes. Subsequently, the Government of Ghana established the National Cyber Security Centre (NCSC) in 2018 [47]), and appointed Dr Albert Antwi-Boasiako, a cybersecurity expert of the Council of Europe's Global Action on Cybercrime Extended to be in charge of the centre [48]. The NCSC established under the Ministry of Communications is responsible for Ghana's cybersecurity development including cybersecurity incidents response coordination within government and with the private sector. The NCSC is responsible for Awareness Creation & Capacity Building, Cybersecurity Incident Coordination & Response (CIRT), Critical National Information Infrastructure Protection (CNIIP), Child Online Protection (COP) and International Cooperation, among others. The NCSC is also responsible for the development and implementation of Ghana's National Cybersecurity Policy & Strategy. The NCSC works closely with the National Cyber Security Technical Working Group (NCSTWG) in the implementation of cybersecurity initiatives across government and non-governmental sectors [47]).

The concept of the NCSC of Ghana is similar to the GCHQ's NCSC of UK, the US Department of Homeland Security's CERT and the CART established by the FBI in the US. The GCHQ, the US's CERT and the FBI's CART have remained strategic and prevented many cyberattacks, assisted police institutions to trace and track criminal elements who perpetrated crime though the internet. The capability of Ghana's NCSC to have an appropriate CERT with the requisite knowledge and technical skills to prevent cyber fraud and assist law enforcement organizations will be crucial. Prior to the establishment of Ghana's NCSC in 2018, the Ghana National Computer Emergency Response Team was formed by the Ministry of Communication in 2014 [47]). More recently, sectoral CERTs have been established at the National Communications Authority (NCA), Central Bank of Ghana (BoG) and the Ghana Police Service (GPS). These are to help deal with digital crimes at the specific mentioned sectors, since they maintain critical national information infrastructure. At present, it thus appears Ghana's NCSC lacks the necessary capabilities to carry out these works as compared to its counterparts in the US and UK. As part of measures to adequately resource the NCSC to have the necessary technical, financial and human resources to conduct, investigate and assist in digital forensic investigation, the Ministry of Communication of Ghana increased its Communication Service Tax to fund the activities of the NCSC [49]. It is aimed that this measure will improve the NCSC's capacity to effectively deliver on its mandates.

There is the need to consider rearrangement, realignment and restructuring of Ghana's NCSC. Crimes committed in the digital space is a national security issue. In these days, cyber security has become a national security concern, because it is about protecting the sovereignty of the nation in the cyber space. The location of the NCSC at the Ministry of Communication presents issues of policy incoherence. The NCSC does not have prosecutorial or investigative power. Digital Forensic investigation and prosecution are done by the security agencies. Therefore, locating the NCSC at the national security secretariat will be more appropriate in line with international best practice. The structuring of the UK GCHQ, UK NCSC, the US FBI CART and the US Homeland security CERT could serve as a guide.

5. Organisational infrastructure/responsible agency

Organisational Infrastructures are measures put in place for the investigation of digital forensic cases. These include agencies responsible for the investigation of cybercrimes as well as national bodies responsible for prosecuting offenders of cyber and computer crimes. Without a clear national strategy and supervisory bodies, efforts in different agencies and departments become conflicted thereby preventing effective harmonization of digital forensic investigation processes [50]. The organisational infrastructures are discussed based on the existence of institutions involved in digital forensic investigation and prosecution at the national level.

5.1. Law enforcement institutions

At the national level, four national agencies are mandated with the investigation of cybercrimes leading to the prosecution of offenses. The Criminal Investigation Department (CID) of the Ghana

Police Service, Economic and Organized Crime Office (EOCO), Bureau of National Investigation (BNI) and the National Security Council Secretariat (NSCS). These institutions are charged with the requisite legal mandate of investigating offenses relating to digital and computer fraud. The CID of the Ghana Police Service has a cybercrime unit responsible for forensic investigation including digital forensics. Through their activities, the cybercrime unit of the CID has become the largest provider of forensic investigation services in Ghana. The forensic science lab of the cybercrime unit of the CID was established in 1948 [51]. Over the years of its existence, the cybercrime unit has grown in both infrastructure and capabilities offering forensic investigation in areas such as chemistry and drug analysis, ballistics and firearms, document examination, photography and DNA analysis [11]. If properly resourced, the forensic lab of the CID'S cybercrime unit will become a centre of excellence for digital forensic investigation with the capacity to provide quality forensic services for Ghanaian public and private institutions as well as other countries in Africa. Over the years, many organizations both home and abroad have contributed to the resourcing of the cyber forensic lab of the Ghana Police Service. For instance, the European Union in 2011, provided 3 million euros for the refurbishment of the forensic lab under international cooperation agreement [34]. However, more needs to be done to elevate the status of the lab to internationally acceptable standard. Government should make a conscious effort towards the provision of appropriate resources to enable the lab function adequately.

The Bureau of National Investigation (BNI) is the internal intelligence agency of Ghana. The BNI is a creature of the Security and Intelligence Agencies [52] (Act 526). Its equivalent is the Federal Bureau of Investigation (FBI) in the US and MI5 of the UK. The set-up of the BNI makes it an integral part of the National Security Council of Ghana with the responsibility of overseeing counterintelligence and internal security of Ghana. The BNI has investigative powers and authority to arrest and interrogate on a wide range of criminal offenses [53]. The BNI however, require cybersecurity and digital forensic capacity and capability to be effective in investigating cyber and digital crimes.

The Economic and Organized Crime Office was established by Act 804 in 2010 [54]. The EOCO is a reengineering of the former office called Serious Crime Office [55]. Like the BNI, EOCO requires capacity in cybersecurity and digital forensics to effectively investigate cyber related crimes. Finally, the National Security Council Secretariat as a national body for the coordination of security matters of Ghana has established various units to deal with specific matters of national interest [56]. Following the proliferation of cybercrimes in Ghana, the secretariat has become active in cyber and digital investigation in support of other security agencies such as the CID, BNI and EOCO. It must be indicated that, all responsible law enforcement institutions need cyber intelligence operation and cybercrime investigation capacity to effectively respond to the threats posed by cybercriminals. The ability of law enforcement institutions to trace the source of internet crimes in order to arrest and prosecute has always been indicated as a challenge confronting the fight against cybercrime in Ghana [57], as the capacity to do so is limited.

5.2. Prosecuting and judicial authorities

In Ghana, the prosecutorial powers of the country are vested in the Attorney General [58]. This is an office established under the 1992 constitution of Ghana. The Attorney General (AG) prosecutes all crime offenders on behalf of the Republic. Practically, the prosecution division of the Ministry of Justice and Attorney General's Department has been charged with the responsibility of prosecuting offenders [59]. All investigations by the various law enforcement agencies, thus CID, BNI, EOCO ends up with the Attorney General who offers legal advice on the next step to take. Due to the volume of work, some of the law enforcement agencies have been given fiats and powers to prosecute if they reasonably believe a prima facie case is established. This means that evidence pertaining to offenses, including digital evidence arising out of DFIs will be handed over to the AG. EOCO is such an agency that has a fiat to prosecute. The Ghana Police Service prosecutors are also trained to prosecute cases at the circuit courts. In terms of the judiciary, under the supervision of the Chief Justice, all cyber-related crimes can be prosecuted at the high courts and the lower courts. The Chief Justice of Ghana has set up a financial division of the high court to adjudicate cybercrime cases. The court is manned by judges that have been trained on the admissibility of electronic and digital evidence. Capacity building of judges and lawyers to fully understand the scope of digital forensic investigation and evidence will facilitate cybercrime offence prosecution. Table 2 provides a summary of the responsible agencies in charge of cybercrime investigation and prosecution.

It is important to recognize that digital crimes are often complex and sophisticated, thereby requiring tact and capacity to investigate and prosecute. Considering the upsurge in digital crimes and the paucity of police digital forensic investigators in Ghana, there is the urgent need to build the capacity of law enforcement agencies, particularly the Ghana Police Service, BNI, EOCO and National Security operatives. The police administration could identify police officers with requisite technical and computer crime knowledge to undergo digital forensic investigation training. This will help build the capability of the police service in conducting effective digital forensic investigation. The central government could also make scholarship schemes available to the security agencies to take up academic degree courses in countries where digital forensic investigation and cyber security are well grounded. State prosecutors and judges must continually be trained on how to effectively adjudicate cases involving digital evidence. In this case also, there could be a collaborative program among commonwealth countries on capacity building that provides judges the opportunity to efficiently understand the crimes committed in the cyber space and how to effectively adjudicate same to avoid miscarriage of justice.

6. Capacity building infrastructure

Although investigations into cybercrime are tackled from a technological perspective, there exist numerous socio-economic and political implications. To this end, building institutional and human capacity to effectively carry out DFI is crucial in promoting the development of qualified digital forensics professionals. Capacity building, therefore, takes a look at the existence of availability of guideline to guide digital forensic investigators, the existence of certification and accreditation of digital forensic professionals, professional training courses in digital forensics, educational programs or academic curricula and the opportunity for research and development [60]. These are critical in effectively producing the necessary manpower required for digital forensic investigation at all level of the national development.

6.1. Higher education courses and training

Ghana practices a complex educational system as compared to that of the US and UK. The National Council for Tertiary Education (NCTE) is responsible for ensuring the standard and quality of all tertiary education in Ghana, both public and private. Whiles, the NTCE is responsible for the administration of tertiary education, the National Accreditation Board (NAB) grants accreditation to all tertiary institutions to run higher education courses. Therefore, the

Table 2
Responsible national agencies.

No	Agency	Responsibility
1	Criminal Investigations Department, Ghana Police Service	Conducts criminal investigation and prosecutes offenders. Has established forensic science lab under its cybercrime unit (Ghana Republican Constitution, 1992).
2	Economic and Organized Crime Office	Investigates criminal offenses particularly those relating to organized crimes including cyber fraud and money laundering (Act 804, 2010)
3	Bureau of National Investigation	An internal intelligence agency that gathers intelligence information for the investigation, arrest, and prosecution of offenders (Act 526, 1996)
4	National Security Council Secretariat	Has established a special unit that assists various security agencies in investigating various crimes (Ghana Republican Constitution, 1992)
5	Prosecution Division, Attorney General's Department	In charge of prosecuting all categories of offenders in Ghana. Issues fiats to allow other security agencies prosecute offenders (Ghana Republican Constitution, 1992).
6	The Judiciary (lower and high courts)	Have the adjudicating powers over all matters brought before it by law enforcement and prosecuting authorities. Has also set up specialized courts and trained judges to deal with cybercrimes issues (Ghana Republican Constitution, 1992)

Source: Authors' Compilation, 2020.

inspection of quality of academic faculty, infrastructure and the supervision of quality academic degree courses are the responsibilities of the NAB [61]. Public institutions are educational institutions that receive funding from the central government, whereas private universities are privately funded. Unlike the UK where there is the existence of Universities and College Admission Service (UCAS) that facilitates a centralized admission system, in which courses of universities could be searched and identified online, the same system is not practiced in Ghana. Each university in Ghana, both public and private advertises and publishes degree courses information on their website. A thorough search and review was conducted on the internet of universities to review their courses.

Forensic science education has become common in the educational system of most countries [62]. For instance, there are currently over 150 universities in the USA that run over 417 forensic science courses [63]), over 68 accredited institutions in the UK run over 337 forensic science courses (UCAS, 2020), whereas Australia has accredited over 17 Universities [64] that run over 43 forensic science courses [65]). Forensic Science Infrastructure under the Ghana police service has existed since 1948 [11]. Although the Ghana Police Service forensic lab has existed for a very long time, the concept of digital forensic is not very well established in Ghana. Perhaps, this is a reflection of a few prominent universities running higher education courses in forensic science.

At present, there are only five forensic/digital forensic and cybersecurity degree courses accredited by the NAB and run in Ghana. One course at the undergraduate level and four courses at the postgraduate level. In Ghana, the University of Cape-Coast is the only accredited university offering an undergraduate degree course in forensic science in the Department of Forensic Science [66]. In fact, in the whole of the West African sub-region (comprising Benin, Burkina Faso, Cape Verde, Cote D'Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo), it is the only undergraduate degree course in forensic science [11]. In 2013, the university received accreditation and begun enrolment in the 2015/2016 academic year. Also, all four postgraduate level courses in forensic/cybersecurity are run at the Kwame Nkrumah University of Science and Technology (KNUST). These courses are MPhil/PhD Human Anatomy and Forensic Science at the School of Medical Sciences (SMS), MPhil/MSc Forensic Science at the Department of Biochemistry, MPhil/MSc Cyber Security and Digital Forensic at the Department of Computer Science, and MSc Cyber Security Intelligence and Management at the Institute of Distance Learning [67]. Whilst forensic science and human anatomy began around 2013, the cybersecurity and digital forensic and cybersecurity intelligence and management all enrolled their first students in September 2018. Although, there are opportunities for employment of graduates of these courses, the existence of infrastructure for these courses are limited. The key focus of every university degree programme is not only for competence or expertise. Availability of jobs for graduate of university programmes are also crucial. In the case of digital forensic, many organizations including the Ghana Police Service, Ghana National Fire Service, the Military Intelligence as well as other security agencies have all expressed the need for forensic/digital forensic experts and cyber security professionals. The limited infrastructure will hamper effective training and prevent many students from pursuing forensic/digital forensics courses and those that will have the opportunity will not be adequately trained to meet the demand of the job market. Whilst the KNUST rely on the existing central forensic lab and recently established digital forensic lab in collaboration with the Ghana Police Service, the UCC is at the stage of building a multi-purpose forensic lab for its degree program and currently relies on the faculty of agriculture and natural resources lab. Fig. 2 compares forensic courses in Ghana with other countries.

6.2. Professional and training courses in digital forensics

Just like the higher educational courses, the existence of capacity building digital forensic courses for professionals is limited. The complexities and technical nature of DFI and prosecution demand professional training courses. In this regard, law enforcement

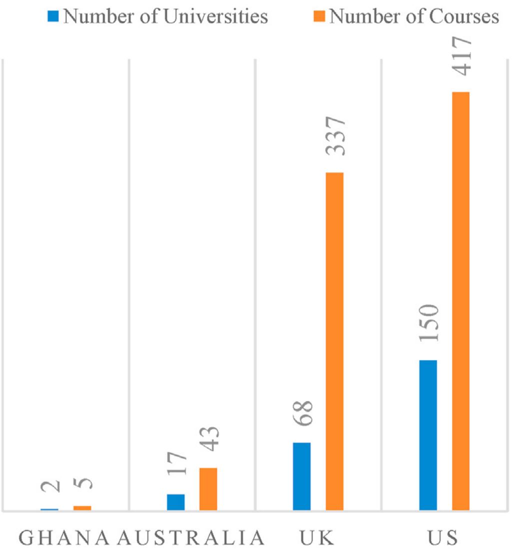


Fig. 2. Forensic science courses.

agencies, political decision-makers, the judiciary and practicing digital forensic professionals require regular training programs in digital forensics to be abreast with the happenings in the discipline. Although the police and other law enforcement agencies have received training in cybercrime investigations from the UN and Interpol in the past, such courses are often limited in Ghana. Occasionally, the Kofi Annan International Peacekeeping Training Centre (KAIPTC) in collaboration with E-Crime Bureau, a private cybersecurity company run certificate course in Cyber Security for the law enforcement agencies, researchers, lawmakers, investigators and digital forensic professionals [68]. The Advanced Information Technology Institute - Ghana India Kofi Annan Centre of Excellence in ICT (AITI-KACE) also runs a one-month certificate course in Cyber Security for working professionals [69]. The National Institute of Information Technology (NIIT), an Indian based IT firm accredited in Ghana offers a certificate course in Cyber Security [70]. As part of efforts to raise awareness of cybersecurity in Ghana, the National Cyber Security Centre under the auspices of the Ministry of Communication on regular basis organize refresher courses for the law enforcement, journalists and other security professionals. Table 3 summarizes both academic and professional courses.

6.3. Guidelines, certification and accreditation for digital forensic professionals

It must be recognised that the courts in which forensic evidence is presented for the successful prosecution of digital crimes have zero-tolerance for the least error since such error can results in miscarriage of justice [72]. Any errors in digital forensic investigation leading to the wrongful prosecution of a person can cause public mistrust of the concept. As such, there is the need for guideline, accreditation, and standardization of digital forensic procedure in order to guarantee quality of forensic services. In the UK and the US, the ACPO and the National Institute of Standards and Technology (NIST) principles form the basis of digital forensic investigation respectively [38]. Ghana has no equivalent of such guidelines. This means that the cybercrime unit of the Ghana Police service, which provide most of the forensic services has no developed guidelines. As already mentioned, the various legislations mandate law enforcement to search and seize electronic equipment to aid in investigations. Without proper guidelines and principles to guide such investigation, there will be inconsistencies in DFIs across the country. Given that, the ACPO guidelines is robust and well accepted as the framework for digital forensic investigation in the UK, the Ghana Police Service, National Security Council Secretariat, Economic and Organized Crime Office and the Bureau of National Investigation could collaboratively adopt and modify the ACPO guidelines for digital forensic investigation in Ghana. This help provide standard and serve as professional guidelines for both public and private digital forensic practitioners. There is also no accreditation procedure for the establishment of digital forensic labs for both public and private organizations offering forensic services. Similarly, the NIST which is the standard framework cybersecurity protection also provide guidelines on how to retrieve, process, analyze and present digital evidence. The law enforcement agencies could engage the services of experts to comprehensively examine the NIST, and possibly adopt it to investigate cyber and digital crimes in Ghana. There should be in existence a national body charged with the responsibility of accrediting digital forensic labs. In the interim, the Ghana Standard Authority can play this role. Certification of digital forensic professionals is another issue that deserves mention. There is the need for the certification of all persons providing digital forensic services to ensure quality of standard and service. At present, there exists an informal Association of Cyber Security Practitioners (ACSP) and Forensic Science Society of Ghana (FSSGH). However, all these bodies exist as informal without any certification. The Information Technology Association of Ghana (ITAG) was formed by the National Information Technology Authority (NITA), the regulator of information technology services and ICT policy unit of the government. Perhaps, the NITA could begin formalizing the existing association and come up with professional certification for Cyber Security and Digital Forensic Experts as the GCHQ does for cybersecurity practitioners in the UK.

6.4. Research and development

In most developed countries, particularly, the US and the UK, many of the national scientific decisions are often backed by research and empirical study. These have made academic institutions and research organizations very relevant in the discourse of national debate. In Ghana, research and development, both in academia and industry on the development of DFIs are very limited. Evidence has shown that there is a gap in research on technological development, foundation and leadership and oversight functions [73]). Even in the UK, where forensic science has existed for long, demand for research aimed at improving the quality of the services has heightened [74]. While this paper elucidates and highlights the research gap in digital forensic investigation in Ghana, it calls for the urgent need to have a concerted effort towards DFI research to aid in the numerous prosecutions of cybercrimes in the courts of Ghana. Often, national policy decisions on cyber security and digital forensics have been based on anecdotal evidences rather than empirical proofs. Research forms the building block of scientific decision making, as such its importance in the planning of DFI in Ghana cannot be over-emphasized. In general, unlike many developed nations, funding allocations for research and development in Ghana is woefully inadequate. At present, research in higher institutions forms only 0.3% of the country's GDP, although there is a proposal for this to be increased to 1% of GDP [75]. For instance, in 2017, the total research and development expenditure of the UK stood at 1.69% of GDP [76]. Similarly, in the US, France and Germany research and development expenditure as a percentage of

Table 3
Forensics science, digital forensics and cybersecurity courses available in Ghana.

No	Institution	Course Type	Course Name
1	KNUST	MPhil/PhD	Human Anatomy and Forensic Science [67]
2	KNUST	MPhil/MSc	Forensic Science [67]
3	KNUST	MPhil/MSc	Cyber Security and Digital Forensics [67]
4	KNUST	MPhil/MSc	Cyber Security Intelligence and Management [67]
5	UCC	BSc	Forensic Science [71]
6	KAIPTC, NIIT, AITI-KACE	Certificate	Cyber Security [68]
7	National Cyber Security Centre	Professional Development Course	Cyber Security Awareness [47])

Source: Authors' Compilation, 2020.

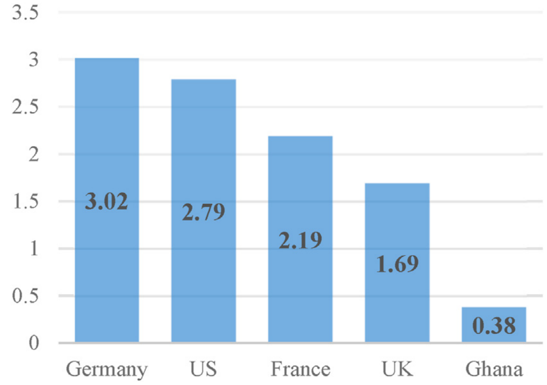


Fig. 3. Research development expenditure.

GPD in 2017 stood at 2.79%, 2.19% and 3.02% respectively [77]. In addition to creating National CERT at the NCSC, there is the need to consider establishing a national research centre at the NCSC for digital forensics and cyber security cutting edge innovations. Fig. 3 demonstrates research and development of expenditure of some selected developed countries as a percentage of GDP.

7. Existence of cooperative mechanisms

Cybercrime has become a global issue and is not restricted to national borders or any sectoral distinctions [20]. This presupposes that DFI aimed at tackling cybercrime requires concerted stakeholders' approach. All sectors and disciplines must be involved in the issues of digital forensic investigation of crimes perpetrated in the virtual space. This could be achieved through participation in international forums and associations, inter-state cooperation, inter-agency cooperation, bilateral and multilateral agreements, public-private partnership as well as learning of best practices from those advanced in the digital forensics. The existence of cooperative mechanisms will facilitate the building of stronger digital forensics capabilities in order to curtail persistent online attacks and enable better investigation, apprehension and prosecution of malicious agents. In evaluating national and international cooperative mechanisms, there is the need to reemphasise partnerships, cooperative framework and information sharing channels.

Internationally, Ghana has been very active in the issues of cybersecurity and the need to make the internet safe for its citizens. As part of these efforts, Ghana is a signatory to a number of international conventions that seek to bring the problem of cybercrime to its minimum level. In 2018, the Government of Ghana signed the Budapest Convention, becoming the third African country to have signed the convention since its adoption by the United Nations [78]. The signing of the Budapest convention on cybercrime affords the country the opportunity to pursue a common criminal policy aimed at protecting the Ghanaian society against the threats of cybercrime and also facilitates the adoption of appropriate legislation and foster international cooperation. In the same year, Ghana also signed the African Union Convention on Cyber Security and Personal Data Protection that was adopted by the Assembly in 2014 in Malabo, Equatorial Guinea. The convention is also aimed at providing inter-state cooperation among Africa states. Ghana is a member of the International Telecommunication Union and has oftentimes participated in the union's cybersecurity forums and conferences.

Many other international, continental and regional institutions have cooperated, or partnered with the government of Ghana for capacity building programs. The World Bank, European Union, the United Nations Office of Drug and Crime (UNODC) are all institutions that have either funded or provided training for government and law enforcement officers on cybercrime investigation. The Economic Community of West African States (ECOWAS), the Inter-Governmental Action Group Against Money Laundering in West Africa and other ECOWAS member states have also collaborated with Ghana to organize sub-regional capacity building in the fight against cross-border cybercrimes. Whilst these cooperation's have been mainly executed at the national level, the higher educational institutions have also enjoyed significant cooperation from the international academic community. The Gujarat Forensic Science University of India, The University of Lincoln of the UK and the University of Cordoba of Spain have all provided support to the Forensic Science Department of UCC to ensure students are trained in forensic science to meet international standard [11]. Internally, both the UCC and KNUST have been granted access to the Forensic Science Lab of the Ghana Police Services for student learning activities. Law enforcement institutions within the country, however, have to improve on their inter-agency cooperation to avoid duplication of digital forensic investigation and prosecutions. Universities and Institutions within the country could also collaborate in sharing resources including manpower and equipment to help train expertise for Ghana on multiple fronts.

8. Conclusion and recommendation

Digital Forensic Investigation (DFI) has become an emerging technology and research issue due to the rise in cybercrime activities globally. Although Ghana faces cyber threats from multiple fronts, the development of DFI infrastructure is at its infancy. The paper examined the various aspects of digital forensic investigation in Ghana. Areas of infrastructure covered in this study include the existence of legal infrastructure, the availability of technical mechanisms and capacity, organisational infrastructure and responsible national agencies, capacity building programs and cooperation mechanism. The overarching aim of the study was to identify key sectors of the digital forensic landscape in the country, with a view of identifying policy issues and proffer recommendations based on international best practices and principles. Key issues identified in the study and the corresponding policy recommendations are provided to guide digital forensics in Ghana. Recommendations are as follows:

Legal Infrastructure: Although there is a plethora of legislation on cybercrime investigation and prosecution of cyber offenses, these legislations are scattered in various acts and laws making its cumbersome for law enforcement agencies to apply during digital forensic investigation. Harmonization of the existing legislation into one-stop-shop comprehensive law for digital forensic investigation and prosecution of cybercrime is therefore advocated. The Government of Ghana should set up a Cyber Law Review Committee to bring all stakeholders together in order to identify issues in the cyber landscape and propose a comprehensive legal framework that deals specifically on cyber related crime and prosecution.

Effective governance structure is crucial in ensuring the sustainability of digital forensics and cyber security activities. Government should therefore set up cyber security institutions and also put in place the necessary governance structure for existing agencies including National Cyber Security Council, National Cyber Security Centre, National Computer Security Incidence Response Team, and National Cyber Security Policy Working Group as envisaged by the 2014 National Cyber Security Policy and Strategy.

Technical Infrastructure: The National Computer Emergency and Response Team (CERT) established under the newly launched National Cyber Security Centre is at its capacity development stage. As such Ghana lacks the effective capability and capacity to respond appropriately to cybercrime incidents. Building the necessary requisite cyber security capacity is essential to safeguard Ghana's cyber space. Therefore, the Government through the Ministry of Communication should increase resource allocations to the country's CERT and NCSC to set up the needed infrastructure to mitigate the increasing cyber threats. Also, due to the fact that crime perpetrated on the internet are borderless, advanced countries with superior technology could assist Ghana build its expertise to investigate crime. The National Cyber Security Centre of the GCHQ UK, the CERT of US Department of Homeland Security and the Computer Analysis and Response Team (CART) of the FBI US may assist Ghana in this regard bearing in mind the borderless nature of cybercrimes.

Organisational Infrastructure/Responsible Agency: The investigative role of the law enforcement institutions appears to be overlapping. Appropriate mapping and assessing of the capacity of each law enforcement institution will help avoid duplications of roles. Effective mobilisation of resources for these agencies are more crucial now than before. The capacity of the Cyber Crime Unit's Forensic Lab of the Ghana Police Service must be efficiently resourced. More digital forensic investigation laboratories equipped with the necessary tools must be vigorously pursued by state authorities.

Capacity Building: There is the need for the redevelopment of the national agencies responsible for digital forensic investigation and prosecution. Unlike the UK and the US where ACPO and NIST provide a comprehensive guideline for investigators respectively, Ghana lacks such guidelines. The ACPO and the NIST could be adopted and modified to suit Ghana's legal regime in order to serve as a guideline on digital forensic investigation for both public and private digital forensics providers. The capacity of digital forensic law enforcement investigators needs to be appropriately enhanced. The lack of existence of regulation, accreditation and certification of digital forensic services in Ghana is a major concern. This could potentially lead to miscarriage of justice as results of low-quality forensic services. The proposal to establish a National Cyber Security Council charged with the responsibility of overseeing all issues of cybersecurity, cybercrime and digital forensic investigation and regulations is therefore laudable and must be quickened.

In the interim, the Ghana Standard Authority (GSA) and the National Information Technology Authority could be asked to provide oversight responsibility and supervision of digital forensic investigations to avoid the provision of quackery services. In times of escalating cybercrime activities, the government must increase its research funding to higher educational institutions to provide cutting edge research that could lead to the formulation of national policy on digital forensics and cybersecurity.

Cooperative Mechanism: Finally, there is an opportunity for increased collaboration between the international community particularly the UK, US and other countries with advanced digital forensics investigation infrastructure to help develop and strengthen digital forensic in Ghana. Academic institutions and research professionals could also enhance research collaborations and exchange of ideas on digital forensic technologies. Universities that run digital forensics courses could also begin an exchange program with oversee institutions aimed at facilitating learning opportunities for students. This will go a long way to contribute significantly to training of students.

Declaration of competing interest

The authors declare no conflict of interest. The research was funded from the researcher's own resources with no financial contribution from any source. There is also no information either work or affiliation that suggest conflicts of interest on the part of the authors.

References

[1] R.A. Abbey, Cyber fraudsters attempt stealing GH'329.7mn from banks — new BoG report – citi Business News. Citibusinessnews, Available at: URL, 2019. (Accessed 6 June 2020), https://citibusinessnews.com/cyber-fraudsters-attempt-stealing-gh&cent;329-7m-from-banks-bog-report/.

[2] Act 29, Criminal offenses act 1960, Available at: https://www.wipo.int/edocs/lexdocs/laws/en/gh/gh010en.pdf, 1960. (Accessed 7 October 2020).

[3] Act 30, Criminal procedure Code (Act 30). Available at: URL, https://www.wipo.int/edocs/lexdocs/laws/en/gh/gh011en.pdf, 1960. (Accessed 6 June 2020).

[4] Act 526, The security and intelligence agencies act 1996, Available at: https://acts.ghanajustice.com/actsofparliament/security-and-intelligence-agencies-act-1996-act-526/, 1996. (Accessed 7 October 2020).

[5] Act 772, Electronic transaction act 2008, Available at: https://moc.gov.gh/sites/default/files/downloads/Electronic%20Transactions%20Act%20772.pdf, 2008. (Accessed 7 October 2020).

[6] Act 775, Electronic communication act 2008, Available at: https://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf, 2008. (Accessed 7 October 2020).

[7] Act 804, Economic and organised crime act 2010, Available at: http://www.eoco.org.gh/wp-content/uploads/2015/03/Economic-and-organized-crime-Ac.pdf, 2010. (Accessed 7 October 2020).

[8] Act 807, Mutual legal assistance act 2010, Available at: https://www.unodc.org/res/cld/document/gha/2010/mutual-legal-assistance-act_html/Mutual_Legal_Assistance_Act.pdf, 2010. (Accessed 7 October 2020).

[9] Act 843, Data protection act 2012, Available at: https://www.dataprotection.org.gh/index.php/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843, 2012 (Accessed: 07/10/2020).

[10] Act 849, Criminal offenses (amendment) act 2012, Available at: https://www.refworld.org/pdfid/44bf823a4.pdf, 2012. (Accessed 7 October 2020).

[11] I.O. Ademu, C.O. Imafidon, D.S. Preston, A new approach of digital forensic model for digital forensic investigation, Int. J. Adv. Comput. Sci. Appl. 2 (2011) 175–178.

[12] K.K. Adu, E. Adjei, The phenomenon of data loss and cyber security issues in Ghana, Foresight 20 (2) (2018) 150–161, https://doi.org/10.1108/FS-08-2017-0043.

[13] A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta, Systematic digital forensic investigation model, Int. J. Comput. Sci. Secur. 5 (2011) 118–131.

[14] Aiti-KACE, Cyber security | AITI-KACE [WWW Document]. URL, https://www.aiti-kace.com.gh/course/cyber-security, 2019 (accessed 4.5.20).

[15] A. Amankwaa, History of forensic science in Ghana-overview, Sci. e-mag 1 (2016) 1–10.

[16] A.O. Amankwaa, E.N. Amoako, D.O.M. Bonsu, M. Banyeh, Forensic science in Ghana: a review, Forensic Sci. Int. Synerg. 1 (2019) 151–160.

[17] America Academy of Forensic Science, College and university listings [WWW Document]. URL, https://www.aafs.org/aafs/Resources/Students/College—Univerisity-Listings/AAFS/Resources/College-and-University.aspx?hkey=3244fe90-9143-4401-8270-789e579e8d85, 2019 (accessed 4.5.20).

[18] M.A.B.K. Amidu, The qualification and the constitutional position of the attorney-general, Rev. Ghana Law 17 (1989) 95.

[20] R. Apau, F.N. Koranteng, Impact of cybercrime and trust on the use of E-commerce Technologies : an application of the theory of planned behavior, Int. J. Cyber Criminol. 13 (2019) 228–254, https://doi.org/10.5281/zenodo.3697886.

[21] R. Apau, F.N. Koranteng, S. Adu, Cyber-crime and its effects on E-commerce technologies, J. Inf. 5 (2019) 39–59, https://doi.org/10.18488/journal.104.2019.51.39.59.

[22] Association of Chief Police Officers (ACPO), Good practice guide for computer based electronic evidence, Available at: https://www.digital-detective.net/digital-forensicsdocuments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, 2012. (Accessed 25 August 2020).

[23] D. Barrett, Cloud based evidence acquisitions in digital forensic education, Inf. Syst. Electron. J. 18 (6) (2020) 46–56.

[24] C. Baylon, A. Antwi-Boasiako, Increasing internet connectivity while combatting cybercrime: Ghana as a case study, Available at: https://www.cigionline.org/publications/increasing-internet-connectivity-while-combatting-cybercrime-ghana-case-study, 2016. (Accessed 6 June 2020).

[25] W.S. Becker, W.M. Dale, E.J. Pavur Jr., Forensic science in transition: critical leadership challenges, Forensic Sci. Pol. Manag. 1 (2010) 214–223.

[26] F.D. Boateng, I.N. Darko, Our past: the effect of colonialism on policing in Ghana, Int. J. Police Sci. Manag. 18 (2016) 13–20.

[27] R. Boateng, R.S. Isabalija, J. Budu, Sakawa -cybercrime and criminality in Ghana, JITI J. Inf. Technol. Impact 11 (2011) 85–100.

[28] K. Cashman, T. Henning, Lawyers and DNA: issues in understanding and challenging the evidence, Curr. Issues Crim. Justice 24 (2012) 69–83.

[29] H. Chi, F. Dix-Richardson, D. Evans, Designing a computer forensics concentration for cross-disciplinary undergraduate students, in: 2010 Information Security Curriculum Development Conference, 2010, pp. 52–57.

[30] D.S. Dolliver, C. Collins, B. Sams, Hybrid approaches to digital forensic investigations: a comparative analysis in an institutional context, Digit. Invest. 23 (2017) 124–137.

[31] D. Ennin, R.O. Mensah, Cybercrime in Ghana and the reaction of the law, JL Pol'y Glob. 84 (2019) 36.

[32] EOCO, About EOCO | economic and organised crime office [WWW Document]. URL, http://eoco.org.gh/about/about-eoco/, 2019 (accessed 4.5.20).

[33] J. Fraser, A. Ludwig, Forensic science and policing in Scotland, in: Policing in Scotland, 2010, pp. 375–398. Willan.

[34] Ghana News Agency, Cape coast university to introduce new programme | Ghana news agency (GNA), Available at: https://www.gna.org.gh/home, 2014. (Accessed 6 June 2020).

[35] Ghana Police, Forensic science laboratory – FSL – Ghana police service [WWW Document]. URL, https://police.gov.gh/en/index.php/forensic-science-laboratory-fsl/, 2019 (accessed 4.5.20).

[36] Ghanaweb, Telcos begin charging 9% communication service Tax today [WWW Document]. URL, https://www.ghanaweb.com/GhanaHomePage/business/Telcos-begin-charging-9-Communication-Service-Tax-today-785206, 2019a (accessed 4.5.20).

[37] Ghanaweb, Government to increase research funding for tertiary teachers [WWW Document]. URL, https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Government-to-increase-research-funding-for-tertiary-teachers-755217, 2019b. accessed 4.5.20).

[38] Ghanaweb, Ghana to establish national cyber security centre [WWW Document]. URL, https://www.ghanaweb.com/GhanaHomePage/business/Ghana-to-establish-National-Cyber-Security-Centre-593389, 2017 (accessed 4.5.20).

[39] Graphiconline, Communications Ministry appoints cyber security advisor, Graphic Online [WWW Document]. URL, https://www.graphic.com.gh/news/general-news/communications-ministry-appoints-cyber-security-advisor.html, 2017 (accessed 4.5.20).

[40] M. Grobler, J.J. van Vuuren, Broadband broadens scope for cybercrime in Africa, in: 2010 Information Security For South Africa, IEEE, 2010, pp. 1–8.

[41] G. Horsman, M.A.B. Mammen, A glance at digital forensic academic research demographics, Sci. Justice (2020), https://doi.org/10.1016/j.scijus.2020.06.003.

[42] E. Hutchful, Military policy and reform in Ghana, J. Mod. Afr. Stud. 35 (1997) 251–278.

[43] International Education Specialist, 40 Forensics courses in Australia | IDP Australia [WWW Document]. URL, https://www.idp.com/australia/search/forensics/all/aus/, 2020 (accessed 4.5.20).

[44] International Telecommunication Union (ITU), Global cybersecurity Index (GCI) 2018 ITU publications studies & research, Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, 2018. (Accessed 6 June 2020).

[45] KAIPTC, Certificate programme in cyber security – KAIPTC [WWW Document]. URL, https://www.kaiptc.org/academic-programmes/short-courses/certificate-programme-in-cyber-security/, 2019 (accessed 4.5.20).

[46] A. Kershaw, Professional standards, public protection and the administration of justice, in: Handbook of Forensic Science, 2013, pp. 580–605. Willan.

[47] KNUST, Admission to higher degree or research programmes 2020/2021, Academic Year | School of Graduate Studies [WWW Document]. URL, https://sgs.knust.edu.gh/node/314, 2020 (accessed 4.5.20).

[48] H. Kobus, M. Liddy, University forensic science programs: a student attraction strategy or a value-adding partnership with industry? Forensic Sci. Pol. Manag. 1 (2009) 125–129.

[49] N. Kshetri, Cybercrime and cybersecurity in Africa, J. Global Inf. Technol. Manag. 22 (2) (2019) 77–81.

[50] H.S. Lallie, An overview of the digital forensic investigation infrastructure of India, Digit. Invest. 9 (2012) 3–7.

[51] H.S. Lallie, Dashcam forensics: a preliminary analysis of 7 dashcam devices, Forensic Sci. Int.: Digit. Invest. 33 (2020), 200910, https://doi.org/10.1016/j.fsidi.2020.200910.

[52] H.S. Lallie, L. Pimlott, Applying the ACPO principles in public cloud forensic investigations, J. Digital Forensics. Secur. Law 7 (1) (2012) 5.

[53] S.S. Mir, U. Shoaib, M.S. Sarfraz, Analysis of digital forensic investigation models, Int. J. Comput. Sci. Inf. Secur. 14 (2016) 292.

[54] Myjoyonline, Parliament to ratify budapest convention on cybercrime, MyJoyOnline.com [WWW Document]. URL, https://www.myjoyonline.com/business/parliament-to-ratify-budapest-convention-on-cybercrime/, 2018 (accessed 4.8.20).

[55] NAB, National accreditation board - national accreditation board, About Us [WWW Document]. URL, http://nab.gov.gh/about-us, 2019 (accessed 4.5.20).

[56] National Cyber Security Centre – Ghana (NCSC-Gh), Establishment and information, Available at: https://cybersecurity.gov.gh/about, 2020. (Accessed 23 August 2020).

[57] NRCD 323, The evidence act 1975. https://acts.ghanajustice.com/actsofparliament/evidence-act-1975-n-r-c-d-323/, 1975. (Accessed 7 October 2020).

[58] NIIT, NIIT programs offered [WWW Document]. URL, https://niitghana.com/course info/?id=50&amp;loc=Accra, 2019 (accessed 4.5.20).

[59] Y.A. Obuobisa, Challenges faced regarding cyber crime and the rule of law in cyberspace from the perspective of a prosecutor in Ghana, Available at: https://rm.coe.int/16806be179, 2016. (Accessed 7 June 2020).

[60] Office for National Statistics, Gross domestic expenditure on research and development, UK - office for National Statistics, Available at: https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure, 2019. (Accessed 6 September 2020).

[61] Ti Osafo-Affum, Globalization and state security: the case of Ghana, University Of Ghana, Legon, 2015. Available at: https://pdfs.semanticscholar.org/1f08/51e841405dd3cb84bc024efe1910758de19d.pdf. (Accessed 6 June 2020).

[62] P. Owen, P. Thomas, An analysis of digital forensic examinations: mobile devices versus hard disk drives utilising ACPO & NIST guidelines, Digit. Invest. 8 (2) (2011) 135–140.

[63] G. Peterson, S. Shenoi, in: Advances in Digital Forensics XV: 15th IFIP WG 11.9 International Conference, Springer International Publishing, 2019. Orlando, FL, USA, January 28-29, 2019, Revised Selected Papers.

[64] A. Samarji, Forensic science education: inquiry into current tertiary forensic science courses, Forensic Sci. Policy Manag. An Int. J. 3 (2012) 24–36.

[65] Science and Technology Committee, Forensic science and the criminal justice system: a blueprint for change, Available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf, 2019 (15/05/2020).

[66] N. Scheidt, M. Adda, Framework of confidence values during digital forensic investigation processes, WSEAS Trans. Syst. Control 15 (2020) 228–234.

[67] G.F. Shi, P. Huang, N.G. Liu, X.T. Yu, H. Zhang, S.Y. Li, S.N. Wu, W.T. Wang, C.T. Li, Analysis of forensic sciences literature in SCIE from 2008 to 2017, Fa Yi Xue Za Zhi 35 (2019) 30–38.

[68] P. Sommer, Accrediting digital forensics: what are the choices? Digit. Invest. 25 (2018) 116–120, https://doi.org/10.1016/j.diin.2018.04.004.

[69] P. Sommer, Certification, registration and assessment of digital forensic experts: the UK experience, Digit. Invest. 8 (2011) 98–105.

[70] M. Stockdale, A. Jackson, Expert evidence in criminal proceedings: current challenges and opportunities, J. Crim. Law 80 (2016) 344–363.

[71] G. Tully, Forensic science in England & Wales, a commentary, Forensic Sci. Int. 290 (2018) e29–e31.

[72] G. Tully, Forensic science and forensic pathology: quality standards and risks, Med. Leg. J. 85 (2017) 117–129.

[73] UCC, Forensic science department at the university of Cape coast, Available at: https://ucc.edu.gh/about-colleges/forensic-sciences-department, 2020. (Accessed 7 October 2020).

[74] A. Valjarevic, H.S. Venter, Harmonised digital forensic investigation process model, in: 2012 Information Security for South Africa, 2012, pp. 1–10.

[75] Y.M. Wara, D. Singh, A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN), Afr. J. Comput. ICTs 8 (2015) 1–8.

[76] G. Whitman, R. Koppl, Rational bias in forensic science, Law Probab. Risk 9 (2010) 69–90.

[77] P. Wiles, Commissioner for the retention and use of biometric material publishes annual report 2019, Available at: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019, 2019. (Accessed 20 May 2020).

[78] World Bank, Research and development expenditure (% of GDP), Data [WWW Document]. URL, https://data.worldbank.org/indicator/gb.xpd.rsdv.gd.zs, 2019 (accessed 4.5.20).