Partners in National Cyber Security Strategy?

An analysis of Cyber Security strategies of Ministry of Defence and Police in UK

Authored and Submitted

by

Onugha Chikaodi Viola

MPhil in Policing, Security and Community Safety

London Metropolitan University

March 2018

Formal Declaration

I, Onugha Chikaodi Viola hereby certify that this dissertation has been compiled by me. In presenting this work I also confirm that this has been compiled by me and has not formed any part of any previous degree application.

This submission was conducted in support of my Master of Philosophy in Policing, Security and Community Safety under the academic supervision of Dr. Nick Ridley and Dr Svetlana Stephenson.

Signature of candidate:-

Date: - 30 March 2018

Acknowledgements

I am thankful to Dr Nick Ridley and Dr Svetlana Stephenson for their advice and patience with me through this journey. Also my thanks go to Dr. Robert Lambert, Dr Robin Bhairam and the academic staff at London Metropolitan University for their support. Ultimately I would like to offer my thanks to my husband, Okechukwu Onugha and my children, Kenna, Kamsi, Chizaram and Ugomma who patiently endured my disruption and encouraged me throughout the journey. And my eternal thanks to God whose mercy and grace kept me alive and strong to complete this study.

Abstract

This research dissertation analyses and compares the Ministry of Defence (MOD) Cyber Security Strategy and Police Cyber Security Strategy in the UK. The research employed qualitative and quantitative methods to investigate issues in the partnership by focusing on the police force and the MOD represented by the Armed Forces.

The research objectives were: identifying challenges in police-military partnership and collaboration in cyber security; examine personnel understanding of the cyber partnership and pluralisation of policing in a cyber context and also propose means of facilitating participation and understanding of cyber issues. Questionnaires and telephone interviews were used to gather information on personnel understanding of cyber security strategy and the nature of the partnership that exists between the two forces – military and police. Research findings reveal that despite efforts by Government and the MOD to streamline Cyber into defence and policing, the workforce has not been educated in the whole concept of cyber defence, thereby undermining the implementation of the strategy. The research reveals that to effectively prevent, investigate and prosecute cybercrime in the UK, policing techniques and strategy that will meet the challenges of current crime environment will need to be put in place by the both forces. The research also found that the Cyber Security Strategy is mainly state centric while policing is human centric in approach, this accounts for the challenges in bringing the policing cyber strategy in line with the National cyber strategy. The research concludes that an increase in education and expertise of both forces will help enhance bi-lateral and multi-lateral partnerships in the race to make the UK cyberspace safe.

Table of Contents

Chapter One

Introduction

The thesis investigates partnership in National cyber security strategy and the role of the police force and the Military as stakeholders in the partnership. The research strategy began with a review of policy documents from both forces. Defence policies reviewed are those related to technological changes from the twentieth century that have a big impact in the way defence conducts its business. The lessons learnt from these events were compared to the unfolding cyber state to shed more light of the research topic. The research also involved interviews with members of the two forces to gain a current view on cyber security practice on a day by day basis.

This chapter examines different definitions of cybercrime and how varying definition affects approaches to dealing with the crime. The chapter considers the different arguments as to what constitutes cybercrime from the perspective of United Kingdom and other developed world.

Chapter two looks at cyber governance and how the stages in adopting a cyber-strategy in United Kingdom unfolded. The definition and scope of cybercrime lies in the layout of cyberspace. This is explored in the chapter and offers reasons why cyberspace requires a strategy to defend and govern it. The chapter raises salient points from the 2009 UK Cyber Policy and Strategy, when the first UK cyber security strategy was released and post 2011 when it can be argued that UK adopted a cyber-security strategy that reflects the importance of cyber security on the ladder of the national security agenda. The cyber strategy of the United Kingdom identifies roles and responsibilities for both the Ministry of Defence and the police force amongst other partners.

The research methodology employed in the thesis is presented on chapter three. It details the use of mixed methods of questionnaire and semi structured interview; leaning on the guidance of the mixed method proponents. While presenting the ethical and reflective experiences of the researcher; the chapter shows the difficulties in conducting research within the Armed forces and the police force.

Chapter four presents the analysis of the data from questionnaires and the semi structured interview. The salient observations from the data are further elaborated alongside current issues arising within the cyber security environment.

Chapter five discusses the findings and themes especially in Pluralization of policing which is also evident in cyberspace and different models of pluralized policing employed in combating Cyber Crime are explored in chapter five. The chapter explores the plural policing bodies that currently exist and how interactions between them keep cyberspace monitored.

To achieve cyber security and resilience, partnership has been proposed as the best option in combating cybercrime and achieving the objective of the National cyber security strategy. The thesis

seeks for ways through which military and law enforcement strategies have to find a meeting point in order to work together to meet the challenges that cyberspace poses; challenges that transcend national boundaries.

Chapter six focuses on the two forces that are involved in policing cyberspace namely the police force (policing by government) and the Armed Forces (policing inside government).

The NSS and CSS have set out their objectives which challenge the established responsibilities of law enforcement and the Armed forces such as jurisdictions, law of arms conflict and issues of security. The police forces amidst the challenges of cyberspace are still responsible for law and order. What are the features of a police Cyber Strategy that is required in the wider scope of Policing in 21st Century? Is the police force in the United Kingdom an adaptable force or does it muddle through organisational change that 21st century imposes.

The research looks at how the personnel of both forces interpret and understand the cyber security strategy and means to achieve the objectives and the role they have to play towards its success.

Chapter seven concludes the thesis. It reflects and evaluates the whole thesis, the research field, limitations and advantages and suggests areas of further research.

Survey Questionnaires were sent to personnel from the two forces to gauge their understanding of the cyber strategy and their role; also key personnel from the Armed forces were interviewed to elicit how organisational culture have evolved within their workforce from a cyber-security perspective. The Armed forces and the police force are known for their secrecy and rank structured access to information. While cyber Security permeates all level and rank of the work force, the research will inform whether there is openness in informing and educating the work force on cyber issues. The thesis does not delve into the technical and technological development in the national security strategy.

Research context

There has been scholarly research in cyber strategy in recent years across the developing world. From the 1993 book by Arquilla and Ronfeldt, titled ‘Cyberwar is Coming’ where they comment that war has shifted from the traditional ‘attritional warfare by massive armies’ borne from industrialisation, to the digital war whose victor is the entity that can deploy superior networks over the other, a shift from ‘mass and mobility’ to computer network manoeuvres which will demand a huge change in military strategy and conduct of war.

‘As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare […] just as critical to military operations as land, sea, air, and space’ (Arquilla and Ronfeldt, 1993).

This notion of cyber war gained traction and in 2005, the US National Defence Strategy formally recognised cyberspace as a war domain (National Strategy of The United States, 2005).

There ensued books, media announcements, reports, research and commentary speculating on the newly declared domain. Nations started recognising the threat that cyberspace poses, and cyberspace became a regular lexicon in military and national defence policies (Weimann, 2004; Nissenbaum, 2005; Eriksson; Kramer; Starr, 2009; Rid, 2012). Countries in Europe started publishing their national cyber strategies following the attack on Estonia by Russia in 2007 (Arquilla and Ronfeldt, 1993). Finland and Slovakia published theirs in 2008, with the Czech Republic, France, Germany, Lithuania, Luxembourg, the Netherlands and the UK following in 2011.

The UK cyber security strategy was published soon after the 2010 National Security Strategy (NSS), and Strategic Defence and Security Review (SDSR). Its publication was welcomed and also criticised as lacking depth. ‘While widely acknowledged as a “good start”, most security industry representatives felt the strategy did not provide enough detail on how its goals can be achieved, how success will be measured, and what the deadlines are for many of the initiatives’ (Arquilla and Ronfeldt). Peter Sommer in his column in The Guardian (Sommer, 2011) raises the question of command and control namely; who will authorise offensive cyber weapon capability - the MoD or the Government, what are the rules of engagement and who is in charge of cyber incident monitoring? These questions are directly linked to the role of the military as laid down by law. With the vagueness of the strategy, it also follows that there will be unfolding readjustments and additions to the strategy through reviews.

This is not the first time that a government strategy has been criticised as being off the mark. Some of the UK’s military strategy in operations have been criticised and often accused of being unfit for purpose, due to its inability to articulate a sustainable strategy given the UK’s failure in recent operations abroad (Johnson et al., 2011).

Concentrating on the 2010 National Security Strategy (NSS), the Strategic Defence and Security Review (SDSR), the 2011 Cyber Security Strategy (CSS) and the Serious and Organised Crime Strategy (2013), the thesis looks at how the military and the police have been influenced by these strategies. For the military, an overhaul of the whole concept of defence has gradually changed as cyber security is streamlined into defence policy coupled with economic influence and globalisation. ‘In the military, information and intelligence operations, routine administrative functions, and a wide

array of everyday jobs have been increasingly developed and transformed with the support of interconnected electro-electronic devices'(Cepik, Canabarro and Ferreira, 2015, p2).

Defence policy and military strategy go hand in hand and defence policy is guided by the budget of the present government and since the UK economy was in recession in 2008 prior to the release of the CSS, the question of funding becomes unavoidable. Both the Armed Forces and the police budgets were cut during the coalition government budget statement. Amid the reduced budget, the MoD will follow the route of research and development to develop, test and evaluate their cyber warfare capabilities leaving the police force lagging behind due to their organisational structure.

From 2011 to 2015, the Armed Forces commenced changes that reflect the then current economic and technological state nationally and internationally and which included reducing the workforce through four tranches of redundancy and the formulation of a new employment model (Army Technology, 2016). The number of trained regular soldiers will be reduced from 102,000 to 82,000, while increasing the number of reservists from 19,000 to approximately 30,000 by 2020. This will generate a savings of £10.6bn (ITV News, 2014).

Although the thesis does not take this line of enquiry but instead concentrates on the partnership with the police force, it is worth noting that the relationship that exists in this partnership as recognised by the new doctrine will reflect how the current regular force will view their role in future.

With this reduction, the MoD released a Joint Doctrine Publication 0-01 (JDP 0-01) (5th Edition), dated November 2014 that 'draws on the lessons of history, upon original thinking and from experiences gained from training and operations (UK Defence Doctrine, 2014). It sets out the fundamental principles of the future military force which is depleted from what it used to be. The new doctrine takes into consideration the following strategies; International Defence Engagement Strategy (Ministry of Defence, 2014), New Operating Model: How Defence Works (Ministry of Defence, 2014), and DCDC's Global Strategic Trends Programme (Ministry of Defence, 2014).

The policy is steeped in utilising the present budget dispensation and optimising efficiency of the workforce and recognition that many essential defence skills are in the private sector rather than the Armed Forces, and promotes partnership with the private sector and industry. The theme of partnership that runs across the cyber security strategy for the first time in military doctrine is the basis for a whole new defence doctrine that spans from now to 2020 and beyond.

The national cyber security strategy (Cabinet Office, 2011) involves partnership across different institutions which predictably will involve an overlap of responsibilities. The two forces are both public entities. There are many studies on public private partnership but not much on public to public

partnership which, like the public private partnership has components of feasibility, legality, scalability and accountability. The proposed partnership across the public sector has limitations which will be investigated in relation to the Cyber Security Strategy.

The distinction between the police force and the military both strategically and operationally according to Friesendorf (2012), highlights the complexity of such partnership.

The Internet has redefined national security and an emerging strategic perspective is challenging the functional and fundamental role of both forces. What is the state of the UK cyber capability maintained and sustained by both forces? Both forces are empowered to fulfil specific roles. How is the power shared within the same role: the National Cyber Security Strategy? Is there military cyber defence capability convergence with police cyber security capability?

In situating the institutions in their roles within the national cyber strategy at the end of the research, it will be evident to identify a practical approach to harness the benefit of each institution's expertise within the CSS.
The partnership proposed in the NSS involves the private sector, the MoD and the police in a common goal to protect society, the economy and the critical national infrastructure. These stakeholders have different management systems and organisational culture which is likely to affect the collaboration between them.

The MoD is tasked with defending its own network and mainstreaming cyber into its operations. The Defence Cyber Protection Partnership (DCPP) will identify and implement actions that have a real impact on the cyber defences of its members and the UK defence sector as a whole (MoD, 2013). The research will explore the extent of the above statement among members of the Armed Forces.

The police strategy stems from the role of the National Crime Agency (NCA) (National Crime Agency, 2013). The NCA's responsibilities are to prevent cybercrime and make the UK a safer place to do businesses.

Cybercrime: Definitions and Scope

In this section, issues concerning the definitions and scope of cybercrime will be discussed so as to put the research into context. The section starts by bringing together all the definitions of cybercrime across the United Kingdom and other states that have recognised the threat that cyberspace poses. It explores how this awareness has been incorporated in the legal systems of these states.

The United Kingdom's National Security Strategy (NSS) together with the Strategic Defence and Security Review (SDSR) raised cyber security to a Tier One risk to national security, with the former

launched to deal with policing cybercrime (HM Government, 2010). The strategy recognises the role of partnership in cyber security. It also recognises that the relationship between the law and the policing of cybercrime is a crucial part of the UK's evolving cyber strategy. These strategies and policies inform law making and law enforcement in the UK, but cybercrime is also an international crime and the role of law enforcement agencies is not restricted to within the UK only. There are a global perspective of strategies on cybercrime and how law enforcement should develop in dealing with cybercrime, especially in the empowerment of the police and partner agencies in fighting, investigating and the prosecution of cybercrime and in future international partnership.

'The changing nature of transnational threats has made it imperative that we achieve greater cooperation at many levels — national and local, national and international, military and law enforcement, private and public' (Pumphrey, 2000).

Computer crimes have been in existence since the invention of computers and their worldwide application since the 1970s (Staff, 2017). While these incidents were localised, the advent of the Internet transported computer crime to a global status. Majid Yar defined computer crime based on the computer as the object of the crime (Yar, 2006). Cross and Shinder (2008) distinguish between types of crime according to the level of violence involved: cybercrime is either classed as violent crime, potentially violent crime and non-violent crime, while Wall (2007) defines cybercrime as "the transformation of criminal or harmful behaviour by networked technology," other authors have defined cybercrime as new wine in an old wine skin but however it is defined, the effect of computerization and cyberspace gave rise either to new crimes or enhanced the commission of old crimes. Wall's classification reflects the United Nations' definition of cybercrime. He classified cybercrime under three categories, namely 'crime involving the integrity and good working order of computer systems (hacking); crime making use of cyberspace (encrypted communications among criminals, the sale of counterfeit pharmaceuticals); and crime involving computerized information contents (theft of secrets, dissemination of harmful contents)'. The United Nations definition groups cybercrime under three broad headings as follows-

Crimes against the Machine: This includes offences such as hacking, denial of service, deception, spying and interception of computer data. Cybercrimes are those crimes that prevent the confidentiality, integrity and availability of the computer system.

Crimes using the Machine: This category of crime are old crimes that have been facilitated by the computer, they include forgery, fraud and defamation.

Crimes in the Machine: Content-related crime such as copyright offence, piracy and website defacement (Wall, 2014).

There is no universally accepted definition of what constitutes cybercrime and terminologies such as cybercrime, high tech crime, computer crime, technology crime, digital crime and IT crime seem to connote the same thing.

The United Kingdom approaches the classification of computer-related crime from two perspectives. The country's adaptation of existing laws by way of inclusion of definitions and references to electronic modes of communication and commission means that there will not be exclusive laws to deal with cybercrime. The actual criminal acts of cybercrime are similar to traditional offences, therefore existing laws will be sufficient in dealing with cybercrime and where there is insufficient coverage, and a modification of the existing law with new definitions relative to cybercrime will be enacted. Chik (2006), in his seminal work, summarised the difference between computer crime and cybercrime as follows -

'Computer Crime encompasses crimes committed against the computer, the materials contained therein such as software and data, and its uses as a processing tool. These include hacking, denial of service attacks, unauthorized use of services and cyber vandalism. 'Cyber Crime' describes criminal activities committed through the use of electronic communications media. One of the greatest concerns is with regard to cyber-fraud and identity theft through such methods as phishing, pharming, spoofing and through the abuse of online surveillance technology. There are also many other forms of criminal behaviour perpetrated through the use of information technology such as harassment, defamation, pornography, cyber terrorism, industrial espionage and some regulatory offences' (Chik, 2006).

The above extract makes a distinction between cybercrime and computer crime, a distinction that mimics that of crimes against the machine and crime through the machine; a summary unlike the Council of Europe treaty which does not go into minute details but offers definitions from previous existing laws and open to varying interpretations across European nations.

The Council of Europe on Cybercrime Convention, also referred to as the Budapest Convention on Cybercrime, is a criminal justice treaty that has established criminal law measures based on rule of law and human rights principles (Council of Europe, 2004). The treaty has not made a distinction between computer crimes and cybercrimes but defined cybercrime as any offence targeting computer data and systems. This definition encompasses all offences that involve computers without restricting the offences that have existed before the Internet but which have acquired a momentum and proliferation through the Internet. These are old offences like fraud, intellectual property rights violations. Offences against computer data and systems are classified as offences against the "confidentiality, integrity and availability" (C-I-A offences) of computers, such as illegal access, data

and system interference and others. In addition to these "c-i-a" offences, it also addresses offences that have been given coverage by procedural law.

The three prescribed guidelines in dealing with cybercrime by the Convention on Cybercrime are: harmonisation of Substantive Criminal Law, harmonisation of Procedural Law, and enactment of the rules of International Judicial Cooperation. The first section of the second chapter of the Convention refers to the Substantive law provisions and includes the following categories of criminal activity: Crimes against the Confidentiality, Integrity and Availability of Computer Data and Systems. These are expounded in articles 2-6 and Computer-related offences within articles 7-8. The whole of article 9 deals with Content-related offences, and Offences related to infringements of Copyright and Related Rights come under article 10. There are other notable treaties and conventions initiated by states and union of states, all focused on dealing with the threat of cybercrime. Below are a few:

ORGANISATION	CYBER CRIME STRATEGY
UNITED NATIONS	UN Convention on the Rights of the Child, Optional Protocol to the Convention on the Rights of the child, Tenth United Nations Congress on the Prevention of Prostitution and Child Pornography. UN General Assembly Resolution 45/121; 56/121; 55/63; 64/211.
The Commonwealth	Commonwealth Model Law on Computer and Computer-related Crime.
European Union	The EU Directive on Electronic Commerce European Union Council Framework Decision on combating fraud (2001) European Union Council Framework Decision on attacks against information systems (2005) Data Retention Directive (2005) Amendment of the European Union Council Framework Decision on combating terrorism (2007) Draft Directive on attacks against information systems strengthens the 2005 directive with two extra articles; 6 and 7
Organisation for Economic Co-operation and Development	The Information, Computer and Communications Policy (ICCP) Committee OECD Guidelines for the Security of Information. Report on the legislative treatment of "cyber terror" in the Domestic law of individual states.
Asia-Pacific Economic	Statement on fighting terrorism (2002) and Conference on

Cooperation	cybercrime legislation (2005)
The Group of Eight (G8)	Subcommittee on High-tech Crimes (Reviewed from 1997 to 2011)

Computer-related crime comes under the Computer Misuse Act (Cap. 50A) (CMA) in the United Kingdom and cybercrime is dealt with under the provisions of the Penal Code (Cap. 224) and a host of other legislation. Despite these treaties and conventions, there is no unified stance on cybercrime globally and this can be directly linked to the differences in the definition of what constitutes crime and cybercrime, and differences in the legal systems of various nations. The differences in definition are because of the fundamentals of traditional criminal law. In criminal law, there are two important elements that must be present. It is a common test of criminality expressed in this Latin phrase: 'actus non facit reum nisi mens sit rea', which means "the act is not culpable unless the mind is guilty". The onus is to prove that there is an actus reus, or "guilty act", and a corresponding mens rea present before there is a conclusion that a crime has been committed. It also follows that a person acting in a mental fault cannot sustain criminal liability. Relating this legal principle to cybercrime (the computer as an object is personified as the offender), the computer must be proved to have the knowledge or intention to commit a crime either by its use or content. Furthermore, both must be viewed as property (content and usage) that should be protected under the law. The content of a computer is inert until it is used in the commission of a crime; however, the objectivity of a computer in legal liability infers treating it as human and with no mental faults. It is quite complex and difficult to prove culpability in cybercrime, especially in the case of fraud where the computer's connectivity via the Internet is used or where an accountant alters a database for fraudulent gains. Cases are thus different; in the first instance, the computer can be used as a 'BOTNET' and in the second case, the computer is not connected to the Internet or other computers but its content. Therefore in both cases the extent that the computer is used as a tool or instrument to commit a crime determines the proof of culpability. The actus reus of the computer crime is its content. Relating this to cybercrimes lies in the communication means through which the crime was committed, that is; the Internet and the connectivity of computers. Therefore, the crime committed through the use of the Internet connectivity, primarily qualifies the offence as if the offence concerned relates to tangible property. The definition of what constitutes a computer crime varies from country to country. There is no universally accepted definition. In practice, the two similar categories of crime have been treated as two separate forms of crime. Some Commonwealth countries follow the United Kingdom in legislating new laws to deal with computer crime and existing laws to deal with cybercrime, and modifying the existing law to accommodate the ever-evolving technological development and appropriate enforcement mechanisms. The modification of existing laws does not always occur at the same rate as the technology that facilitates the crime, thus leading to 'a lost in translation phenomenon' making the new law either antiquated or inadequate for the crime for which it was initially modified to deal with. Justin Hughes, in his article 'The internet and the Persistence of Law', identifies three possible

approaches to cyber law, namely: Internet law as a translation of existing law, the no-law Internet and the Internet law as a separate jurisdiction (Hughes, 2003). To view the Internet law as a translation of existing law creates a loophole that is often exploited by cyber criminals and when prosecuted may result to inadequate and unsuitable punishment for the crime in question. This leads to a deficiency in social policy objectives in punishment, crime prevention, and offender rehabilitation.

The UK Data Protection Act 1998 is one of the laws that were modified to protect individuals' rights regarding their personal information held by others. The law also imposes greater control over individuals or organizations that hold and process personal information. In modifying existing laws, the new fraud bill carries a maximum of a 10-year jail sentence and has eased the prosecution process; the main feature of the bill is that it defines that new offences exist through false representation, by failure to disclose information or by abuse of position. This covers offences such as phishing and potentially can be used to deal with Internet fraudsters, financial crimes and services.

There are countries whose cyber law and regulation is restrictive and certain instances of cybercrime are treated differently, such as China's cyber policy which upholds that the use of the Internet must directly benefit the state. China's cyber policy has led to laws that segregate, control and monitor telecommunications; the laws also empower the blocking of access to any Internet content that does not promote the national interest (Chang, 2014). In the Commonwealth nations, Europe and the other western countries the penal code and the common law are generally similar in nature and hence are susceptible to equal and similar laws and punishments. Differential treatment exists in different jurisdictions due to the social and cultural make-up of the country and the political dispensation. In jurisdictions where the distinction of what constitutes cybercrime or computer crime overlaps, judicial discretion takes precedence; however, these similar approaches to cyber policy and law have not yet been built upon in effectively combating cybercrimes. The reason may be political rather than legal.

Cyber fraud, phishing, pharming, identity theft and other related cybercrime have not received the same enforcing effect in every jurisdiction; these crimes demand a consistent treatment under existing law, both in its criminalization and punitive sentencing. This will require extending existing laws and enacting new ones to cover all intricacies of the crime. Yet there are regional differences on interpretations, definitions, applicability and scope of criminal liability. The debate on whether to criminalise illegal access to a computer network is an example of variance in the scope of a criminal act. Illegal access to a computer system is always the first step in subsequent crimes. It is the first step in modifying or obtaining stored data which by law has violated the integrity and confidentiality of the data. Some countries criminalise mere access, while others limit criminalization only to offences where the accessed system is protected by security measures such as a password or encryption keys (an example is the German Criminal Code before it was amended in 2007) or where the perpetrator

has harmful intentions, or where data were obtained, modified or damaged, whilst other countries do not criminalize the access itself, but only subsequent offences (Kadir, 2010).

Most existing laws were in force long before the advent of the Internet. Although they may cover the same crime in the same principle with cyber fraud, their interpretations may not fully apply to the Internet technology and its fast changing environment. The recent 'cloud computing' poses an ongoing contention on ownership and intellectual property. Also, the electronic form of transacting and banking falls into the two categories of crimes which can be dealt with under the penal code, such an offence as cheating should apply to acts of phishing, fraud and crimes in banking and financial institutions, companies and business. It is not enough to have a prescriptive judicial stance in criminalizing acts of cybercrime, without a criminal legal procedure to bring offenders to justice. The future establishment of a global legal system to govern cyberspace will eliminate variations in regional legal systems.

The enforcement of the law in countries affected by the same cybercrime should be a provision in a cyber treaty. This will ensure that criminals do not seek protection in jurisdictions where the law is either lax or non-existent. An adjudicatory and enforcing jurisdiction will also facilitate extradition of offenders, a common biding law dealing with the offence but most importantly the recognition of the decision of the court where the case is tried irrespective of the nationality of the offender or victim or location of the crime's asset. Some countries do not recognise the sovereignty of other countries and the adoption of cyber threat in these countries are yet to be realised. For example, Iran does not recognise Israel, and there is the issue of South Korea and North Korea, to mention a few. A cyber treaty appears to be the only way out of these political stalemates.

Crime fighting is traditionally associated with nation states and their police force but when the crime and its victim is located in a particular state while the criminal is situated across the globe, fighting such crime will no longer be the sole responsibility of one of the nation states linked to the crime. This is usually the nature of cybercrime.

Cybercrime's profile often spans across countries with judicial disparity. This makes investigation and prosecution difficult except between countries that have an established relationship and cooperate in trans-border crime investigations. In cybercrime cases that span across countries with legal disparity, where the case does not have the same priority rating in the countries it will not get the same level of investigation or conviction. In countries that have no specific law dealing with a particular crime which in a different country has an established legal definition, it poses a problem to prosecute the same crime and obtaining similar conviction. That is if the alleged crime is recognised as a crime in the first place; nullum crimen (No Crime, No Offence). An example is the United States V. Elcomsoft (Whyte, 2017), where Elcomsoft, a Russian company, was indicted for offering

advanced eBook processor software that exposes the weakness in Adobe software. The law's enforcement in the United States is not consistent with the traditions of the international system, as its application to a foreign corporation for activities that occurred in cyberspace would conflict with the laws of Russia. Russian law permits the development and sale of the AEBPR [Advanced eBook Processor) program. The case was dismissed because of its violation of section 1201 of title 17 of the United States Code, which prohibits subjecting Elcomsoft to a law that conflicts with the regulations of sovereignty.

The current judicial procedure safeguards the traditional law enforcement which fights crime by investigating and prosecuting physical crime. The police are vested with the sole right of investigating crime. Cybercrime tends to follow a different style of investigation due to its very nature of mostly not being a physical crime; it thus becomes inadequate for the police force to investigate cybercrime with the same method for localised crime. Apart from technical competence in computer technology, an administrative cooperation and legal assistance and cooperation in investigations between countries affected by the same cybercrime will facilitate the enforcement of a cyber treaty by law enforcement agents. Interpol currently has a legal recognition internationally. Such legal infrastructures are paramount to successfully investigate, capture, prosecute and convict cyber criminals.

The police have been constrained by the law, institutional structure and protocol and international regulations and this has extended to their efficiency in fighting cybercrime, but a central specialized policing authority open to consenting countries' signatory to a legal cyber treaty is a step closer (Seth, 2010).

Internet Service Providers also play a crucial role in the investigation of cybercrime. Most cybercrime investigation is often traced back to the provider of the service as in the Canadian legal case of R v Kerr, and then linked to the culprit through log files maintained by the ISP (Kerr and Gilbert, 2004). It is thus difficult to prosecute a culprit who is thousands of miles away without the cooperation of the ISPs. The very nature of the web architecture places the ISPs with access to the entry point of all cybercrimes. While the law enforcement agencies are legitimate enforcers of the law, the role of the ISP in fighting cybercrime cannot be viewed in the same light.

The provision of a legislative mandate to private agencies such as ISPs with regards to their role in cybercrime will give them the legal authority that is extended to the police.
This will define their responsibilities, power and limits. The onus of the matter then becomes how to bring the two bodies to work together effectively within judicial and legal bounds without each of them diluting or losing their primary role.

This will also prescribe their obligation in procedural law. In support of the above recommendation is the 2007 Council of Europe project on cybercrime, as contained in the Global Interface Conference in Strasburg of April 2008.

The applicability of substantive laws to electronic transactions, both tangible and transient digital assets, has limited coverage in deterring offenders or preventing the cybercrimes. There is no legal sanction applied for intention to commit such crime. In some decided cases the punishments have been found to be grossly ridiculous compared to the effect of the crime committed; this calls for either specific stand-alone legislation for all cybercrime or, at best, extension of existing laws with new definitions specific to cybercrime. Still, on the extension and amendment of existing laws, procedural laws that cover the investigation of crimes are also insufficient in facilitating the gathering of evidence and investigation of computer-related crimes. Apart from the technical competence of law enforcement agencies in computer forensics, the volatile nature of computer data requires expedited procedure in gathering of digital evidence while protecting human rights yet not sacrificing evidence at the expense of data protection acts. In other words, procedural law should be succinct in drawing a line where investigation supersedes data protection, especially in cases of national security. The current procedural law cannot keep up with the speed of technological developments. The need for a technologically neutral law is needed. The composition of such laws should guarantee their applicability to changing technology and techniques used by cyber criminals. The downside of non-specific open ended laws is that their application will be down to interpretation, making such laws difficult to be applied and, at most, useless. Except where provisions are made for reactive amendment to existing laws to deal with an emergent trend of technological crime, this is the current situation (Malby et al., 2013).

The law should create a credible and effective deterrent effect and sufficient punishment to suit the nature and severity of the offence. Also where relevant, provisions allowing for rehabilitation could be useful, particularly if previous offenders, with their expertise, knowledge and connections, can be inducted into the system to aid and assist in future investigations and in the development of computer forensics. Chapter II, Section 1, Title 5, Article 13 of the Cybercrime Convention, states that each party "…shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty…[and] shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions". The sanctions within this Convention are prescriptive without going into detail of its relationship to existing law.

Britain as a key member of the European Union has had its criminal justice system influenced by the Standards set out by the Council of Europe. United Kingdom was a signatory state of the Council of Europe (CoE) in its Cybercrime Convention. Although the Cybercrime Convention provides for both computer crime and cybercrime under one instrument, the United Kingdom has implemented the provisions under the Convention alongside other European Union countries; however, a two tract approach was adopted by the United Kingdom. As previously mentioned, the United Kingdom's Computer Misuse Act of 1990 (CMA) and its amendments deals with computer crimes while cybercrime or computer-enabled crime resembling traditional offences are to be dealt with under existing criminal legislation. The amendments to traditional criminal laws are to accommodate the new breed of criminal acts and actors, means and modes of crime commission and digital information and products from the Internet technology. The amendments take into consideration issues arising from definition, interpretation and the scope of Internet crimes.

The amendment affects legislations pertaining to fraud and theft, pornography and intellectual property offences. The fraud bill proposed to modernise the definition of fraud which has been in existence in its original wording since 1968, and will cover cases of phishing and other Internet enabled fraudulent activities. This will close up the loophole in the law that has seen criminals escape prosecution due to the limitations of the provisions of The Theft Act of 2006 in covering such crimes. The new bill will cover offences of fraud which can be committed in one of three ways:

"Fraud by false representation" is defined by Section 2 of the Act as a case where a person knowingly (makes a representation that is false and misleading) "any representation as to fact or law".

"Fraud by failing to disclose information" is defined by Section 3 of the Act. A person legally bound to disclose information by virtue of the relationship to another party, fails to do so.

"Fraud by abuse of position" is defined by Section 4 of the Act as a case where a person is expected to safeguard the financial interests of another person by virtue of his position, and abuses that position; either by omission or intentionally.

The scope of the Act encompasses scenarios that can arise in cybercrimes (Fraud Act, 2006). In spite of the enhanced Fraud Act 2006, the UK Government was involved in the creation of two treaties on the prevention of cybercrime, under the CoE and the EU, both of which originated in Europe and both of which calls for international coordination to tackle abuses of computer systems. They are the Cybercrime Convention of 2001 and the E.U. Council Framework Decision on Attacks Against Information Systems (OJ L 069, 16 March 2005), which was proposed on 19 April 2002, adopted on 24 February 2005 and required to be transposed into national law by 16 March 2007 by member states. The UK opted out of the framework decision in December 2014.

Cybercrime has given rise to new concepts in criminal activities that traditional law does not cover. One of the legal challenges in fighting cybercrime, as mentioned before, is definition of concepts. Definitions are a very important aspect and a common element of the judicial framework both nationally and internationally. But why are definitions so important? It is because they differentiate functions. There are two main definitions in law, namely descriptive and statutory definitions. Statutory definition provides meaning of words within certain context while descriptive definition defines concepts by removing ambiguity where features could lead to confusion. The concept of both definitions is challenged in the quantitative aspect of cyber law. The Convention on Cybercrime has been criticised for not being computer-specific; it contains only five definitions of cybercrime, with four definitions included in Art. 1 and an additional provision was included in Art. 9 of the Council of Europe Convention on Cybercrime.

Convention on Cybercrime does not define child but only child pornography; child pornography is a new concept within cyber law that requires new definition.
There is a significant difference to the definition of child pornography provided in the Optional Protocol and the definition in the Council of Europe Convention on Cybercrime. The later focuses on visual depiction; however, child pornography comes in various forms such as pictures or movies, and audio files. Audio files are not visual and therefore not provided in Article 9 which refers to “material that visually depicts” a child.

The fight against cybercrime is global and involves multi stakeholders. The launch of the Global Cyber security Agenda (GCA) on 17 May 2007 was one of many international efforts to resolve the legal, technical and institutional challenges of cyber security. The GCA aims to coordinate international cooperation in five areas; Legal measures, Technical and procedural measures, Organizational structures, Capacity building and International cooperation. The legal measures and international cooperation involves both national and international legislation. As mentioned before, the provision of national criminal codes are not fully adequate to deal with criminal acts committed over the Internet; there are lacunas in current national laws and substantive criminal law. These laws need to be critically enhanced to empower law enforcement agencies to investigate cybercrime on a global platform.
Law enforcement is another area of focus of the global cyber security agenda. The success of cybercrime investigations depends on cooperation between the countries affected by the crime. Much improvement is needed in harmonising the current legal assistance between law enforcement agencies globally, which is frosted with complex protocol and procedures. The concept of dual criminality investigation is limited to cybercrimes that are criminalised by the participating countries; however, the cybercrimes that have regional differences in definition do not meet the same level of

investigatory cooperation. This is where harmonised global law enforcement will play a vital role to ensure quick procedures and response to incidents.

To fight cybercrime there needs to be a global legal framework, with globally efficient and empowered law enforcement agencies. Over the last decade, improvements have been made in educating law enforcement agencies especially with regards to hi-tech crimes and cyber forensics to facilitate joint policing operations across national borders. To investigate cybercrime, law enforcement agents require change in procedural law to empower them in investigating crime. Brown Cameron, associate investigator of Australian National University notes that the identification of offenders, preservation of evidence and actual prosecution of offenders for traditional crime is different from cybercrimes (Brown, 2015). The evidence in cybercrime is digital and often outside the jurisdiction of the state. The provision of procedural law that will make way for the peculiarities of digital evidence is crucial. The provisions of the data misuse act, computer misuse act and human rights act hinders access to cyber investigation. It is in areas like this that a procedural law specific to cyber forensics is needed.

Professional law enforcement is a reactive system that is centralised within a set geographical boundary, which operates by deterring crime, investigating and aiding the prosecution of crime (Balkin, 2007). By its definable geographic position, the current judicial model is limited in its applicability in cybercrime prosecution within traditional law enforcement.

Cyberspace, which literally means extra-terrestrial, has no geographic boundaries but transcends geographical boundaries. This unique nature of cyberspace demands a different judicial approach which is outside the scope of this research. However, close to the research objective is the need to differentiate cybercrime from other traditional criminal acts because there is a marked difference between the nature of crime and cybercrime within the scope of criminal opportunity. While physical crime deals with tangible concepts, is symmetric and cited within a physical time frame and boundaries, cybercrime on the other hand is asymmetric, intangible and cannot be cited within a fixed time and physical location.

Similar to physical crime is the different levels of criminal activity associated with cybercrime. The levels of activity/victims are; criminal activities that affect personal security, corporate/organisational security and national/international security. The legal approach in prosecution and punishment of cybercrime hence will have to be structured according to this form, because each requires a different form of investigation and deals with different stakeholders. However, it is difficult to propose a judicial process that will not have an international recognition as is the case with localised crimes and law enforcement agencies. The disparity in the definition of computer-related crime by different countries also has a great effect on the prosecution of the crimes.

The burden on the Criminal Justice Authorities is the need for a unified legal empowerment that is universally accepted in dealing with cybercrime in a way that meets the international divergence of cybercrime. There exists currently two courts with international reach; the International court of Justice so far is the principal organ established by the United Nations that presides over legal disputes submitted by its member states and gives judicial advise. On other hand, the International Criminal Court (ICC) is the first ever permanent, treaty-based, fully independent international criminal court. It was established to promote the rule of law and the trial and punishment of the gravest international crimes. Its jurisdiction complements national criminal jurisdictions. There is a parallel need for the establishment of an international court or tribunal for dealing with the most serious cybercrimes of global dimension; cases where the crime spans across the globe and across different judicial systems. Global cyber-attacks in recent years have been either poorly investigated or prosecuted because there is yet to be a global treaty on cybercrime to facilitate investigation and prosecution before an international criminal court or tribunal.

However, without a universal cybercrime convention, cross-jurisdictional conflict of criminal laws raises the unavoidable dilemma of "what law should be applied to determine the legal effect of a person's conduct when he does an act in one state which produces harmful effects in another" (Brown, 2015). The 2010 WikiLeaks activity is a typical example, till date no state has been able to successfully prosecute Julian Assange and he is currently living at the Embassy of Ecuador in London (Alexander, 2015). The delay in such a binding legal common ground has been influenced by the definition and differentiation of criminal concepts relevant to cybercrime.

The collection and presentation of evidence is a vital part of the legal process. Digital evidence arising from the use of the Internet becomes a new source of evidence in not just cyber prosecution but in traditional crime. The use of digital evidence found in mobile phones and emails is now being used in traditional crime investigation and prosecution. The United Kingdom Police and Criminal Evidence Code (currently reviewed by the Serious Organised Crime and Police Act 2005) defines digital evidence as "all information contained in a computer". The definition of computer here covers a broad spectrum electronic appliances. A definition of computer in the 2002 Commonwealth Model Law on Computer and Computer-related Crime defines a "Computer system" as a device or a group of interconnected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.

The admissibility of electronic or digital evidence in court differs from traditional evidence; although both traditional evidence and digital evidence undergo two stages, namely the investigation stage and the presentation stage. Traditional evidence exists in a physical state but digital evidence needs to undergo certain processes before it can be extracted and presented in a physical state. This process of extraction means that the digital evidence has technically been altered and as such rendered

inadmissible under traditional law, and therefore the likelihood of admissibility of digital evidence in court is slim.

A cybercrime can be committed in the United Kingdom using cloud computing, with the victims being in Japan and France. Or the cybercriminal can be in Nigeria, using a computer server in South Africa. These scenarios present a typical transnational crime that involves different jurisdictions. It raises the questions of which country's criminal law is applied, which of the countries has jurisdiction and which country should investigate? To deal with cybercrime's global dimension the principle of jurisdiction has to be addressed. In the principles of public international law, the authority of a sovereign state to apply its domestic law in a criminal matter implies that such a state has "jurisdiction" over other affected states. There are different principles of jurisdiction in the legal process. Below are some of the issues of jurisdiction in cybercrime.

The most common basis of jurisdiction is the principle of territoriality. It defines jurisdiction by virtue of a state's geographical location and boundary. It is applicable if an offence is committed within the geographical boundary of a sovereign state irrespective of the nationality of the offender or victim. Article 22 paragraph 1.a of the Council of Europe Convention on Cybercrime stipulates a state's jurisdiction to include its geographical territory, a ship flying the flag of the state, an aircraft registered under the law of the state or a citizen of the state if the crime is punishable in another state where the crime is committed. In traditional law, a crime is committed when the offender and the victim were physically present within the state's boundary when the offender illegally accessed the victim's computer system. The application of this principle in cybercrime raises a problem when we apply the previous cloud computing scenario.

The International Court of Justice expressed in the "Lotus" case the "principle of objective territoriality" that extends the definition of territoriality but considers a scenario where both the offender and victim are not located within the country, but that instead the crime is committed via a server in an entirely different country albeit the effect of the crime is huge in another country entirely unrelated to the country of the victim, criminal and infrastructure.

The principle of nationality refers to jurisdiction exercised by a state over their citizens that are located abroad. It reinforces the right of the state over its citizen. Without due consideration of the location of the citizen or its law, a state can try its citizen in absence and enforce its judgment. This poses a problem where countries act as havens for criminals avoiding prosecution in their country.

The principle of passive nationality is jurisdiction based on the nationality of the victim. For cybercrime, its relevance is when a citizen of the state becomes a victim. For example, Section 7 of the German Penal Code recognises the application of German criminal law to offences committed abroad where a German is the victim of the offence, 'if the act is a criminal offence at the locality of

its commission or if that locality is not subject to any criminal jurisdiction'. It appears that the German law does not recognise the jurisdiction of any other associated state.

The principle of universality establishes jurisdiction in relation to specific crimes that are in the interest of the international community, such as serious crimes such as crimes against humanity and war crimes. Again the German Penal Code, in section 6(6), stipulates that where 'offences committed abroad against internationally protected legal interests; German criminal law shall further apply, regardless of the law of the locality where they are committed'. The list of crimes or offences covered in this section of the penal code includes cybercrimes and computer crimes such as child pornography, human trafficking and acts of terrorism. Once more Germany may exercise jurisdiction even if the victims are not German nationals and the operator of the website or the infrastructure are not located in Germany.

The 2008 training course of The United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) listed countries and the offences that they have criminalised according to the Council of Europe's convention on cybercrime. Fighting cybercrime has been a challenge to most countries. The establishment of appropriate strategies and policy to deal with these crimes involves a multifaceted and interdisciplinary process. It includes, but is not limited to, areas such as substantive law, procedural law, International Corporation, stakeholder's empowerment and technical regulations. There is no 'one cap fits all' solution to the problem.

Some countries have a separate legal system dealing with cybercrime, while others such as the UK have modified and extended existing structures to deal with cybercrime. In the Explanatory
Report to the Council of Europe Convention on Cybercrime, the drafters reiterated the importance of substantive criminal law, procedural law and investigative technique to be robust enough to deal with emerging new techniques in cybercrime. They should be pre-emptive in dealing with new technology. This is desirable but not easily achieved. It is not simple to prescribe legal concepts to deal with technology that has not been developed, rather it is the need for nation states to expedite law making process to deal with variants of emerging cybercrime as the need arises. This involves three stages; extending existing laws to cover the new cybercrime, identification of gaps in the penal code that cyber criminals will take advantage of and avoid prosecution, and the drafting of new legislation where the last two approaches will not suffice.

As advancement in Internet technology has given rise to new cybercrime and criminal technique, so also must it to new investigatory technique. The fight against cybercrime will be facilitated by the provision of cyber/computer forensic training for law enforcement and establishment of specialist

units to deal with cybercrime, as was the case of the defunct UK's Serious Organised Crime Agency (SOCA).

The need for collaboration is unavoidable in the fight against cybercrime. One of the advantages of collaboration is learning from other partners' experience, both in dealing with certain kinds of crime and sharing of resources to deal with specific criminal acts.

This chapter has put cybercrime in a context that is neither in respect of air, land, sea or space. The next chapter will discuss the concept of cyberspace and why it needs a strategy. Because of the threats and challenges in cyberspace, an attempt is made in the chapter to expunge the need for a strategy for dealing with these threats and challenges. It also looks at the history of the UK's cyber strategy and the role that partnership plays across private and public organisations in the United Kingdom. This directly links to the research objectives.

Chapter Two

Literature review of cyberspace

What is cyberspace and why does it require a strategy to govern it?

Cyberspace is described in the UK Government's National Cyber Security Strategy (NCSS) as "encompassing all forms of networked digital activity" (NCSS, 2011). This is a blanket definition which agrees with the DCAF Horizon 2015 working paper by Fred Schreier which also named cyberspace the 5th space of warfare: 'Cyberspace, the novel 5th space of warfare after land, sea, air, and space, is all of the computer networks in the world and everything they connect and control via cable, Fiber-optics or wireless. It is not just the Internet – the open network of networks' (Schreier, 2015, p10).

This definition encompasses the Internet, extranet, transactional networks, Supervisory Control and Data Acquisition (SCADA) systems and many other networks that are designed for purposes other than the obvious Internet usage, such as: GPS, ACARS, SWIFT, GSM Cellular. Other definitions of the cyberspace looks at the different levels or components that make up cyberspace causing the definition of cyberspace to be diverse to a point that there is no unified definition but instead the very concept of cyberspace varying from country to country, organisation to organisation and even from academics to academics. Some definitions of cyberspace appear to portray it as insubstantial. The definition by Wingfield (2000) is an example of such definitions. He notes that 'cyberspace is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, IT systems, and telecommunication infrastructures commonly referred to as the World Wide Web'(Wingfield, 2000, p17). This definition is ambiguous as it suggests to alienate the physical connectivity that exists to make communication in cyberspace possible.

Kuehl offered a table of definitions of cyberspace as detailed below. He then defined cyberspace as 'an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infra-structures' (Kuehl, 2009, pp26-28).

Table 1. Definitions of Cyberspace

• Greece: kybernetes (the steersman) or cybernetics, the study of control processes, which was the basis for Tom Rona's concept (1976) of "information warfare".
• William Gibson, Neuromancer (1984): "a consensual hallucination".
• Edward Waltz, Information Warfare: Principles and Operations (1998): The "cyberspace dimension" refers to the middle layer—the information infrastructure—of the three realms of the information warfare battle- space. These three realms are the physical (facilities, nodes), the information infrastructure, and the perceptual.
• Google: "The electronic medium of computer networks, in which online communication takes place. . . . a metaphor for the non-physical terrain created by computer systems. . . . the impression of space and community formed by computers, computer networks, and their users. . . . the place where a telephone conversation appears to occur. . . . the place between the phones."
• Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (1994): "That intangible place between computers where information momentarily exists on its route from one end of the global network to the other. . . . the ethereal reality, infinity of electrons speeding down copper or glass fibers at the speed of light. . . . Cyberspace is borderless . . . [but also] think of cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world."
• Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (2d ed., 1996): "[National] cyberspace is distinct entities, with clearly defined electronic borders. . . . Small-C cyberspaces consist of personal, corporate or organizational spaces. . . . Big-C cyberspace is the National Information Infrastructure. . . . add [both] and then tie it all up with threads of connectivity and you have all of cyberspace."
• Oxford English Dictionary (1997): "The notional environment within which electronic communication occurs."
• Walter Gary Sharp, Cyberspace and the Use of Force (1999): "The environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web."
• Dorothy Denning, Information Warfare and Security (1999): "The information space consisting of the sum total of all computer networks."
• Gregory Rattray, Strategic Warfare in Cyberspace (2001): "A physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place. . . . Cyberspace is a man-made environment for the creation, transmittal, and use of information in a variety of formats. . . . Cyberspace consists of electronically powered hardware, networks, operating systems and transmission standards."

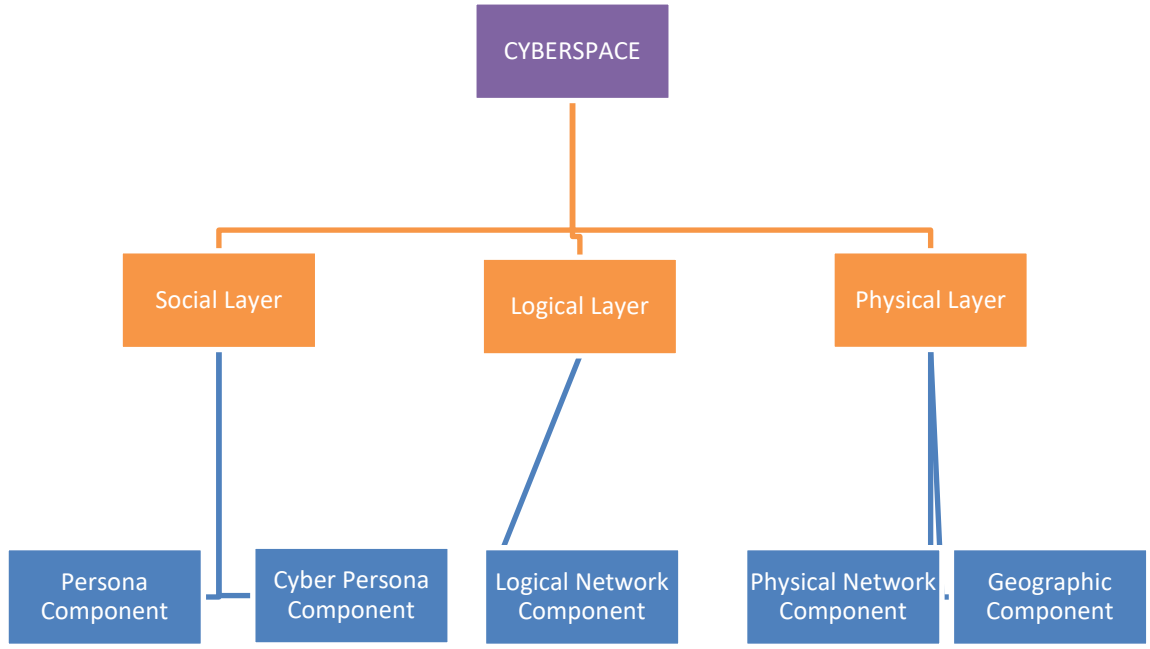
• Merriam-Webster Third New International Dictionary (2002): “The on-line world of computer networks.”

• National Military Strategy for Cyberspace Operations (2006): “A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures.”

• National Security Presidential Directive 54 (2008): “The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.”

• Deputy Secretary of Defence Gordon England (2008): “A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

Drawing from the various definitions above, cyberspace can be seen to operate at different layers. Kuehl offers ‘three separate but related and synergistic dimensions’ or levels, namely: connectivity, content, and cognition. These levels of connectivity are similar to the US Army’s layered approach to defining cyberspace. The US Department of Defence defined cyberspace as comprising of ‘three layers (physical, logical, and social) made up of five components geographic, physical network, logical network, cyber persona, and persona’.



.

Figure 0-1

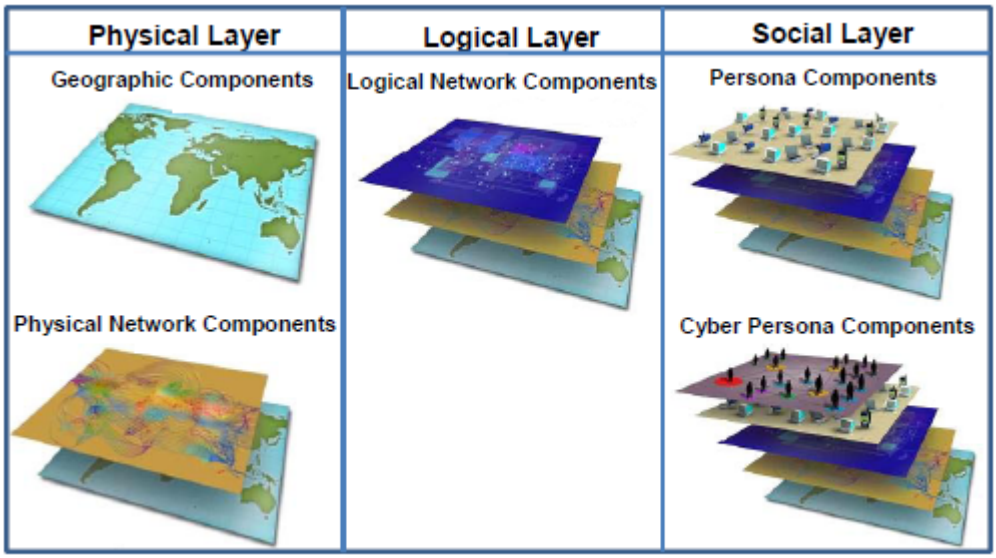


Figure 0-2 - Pictorial depiction of the three layers of cyberspace (AcqNotes, 2015)

The three layers of cyberspace, namely; physical, logical and social have five subsets of layers. The physical layer subsets are the geographic and the physical network layers. While the geographic layer is the physical location of the network hardwares or structures, the physical layer is the actual hardware and structures.

The logical layer is made up of all the logical connections that exist between networks and connected nodes. This layer includes the routing system, connectors, nodes, and other devices that interact within the network and the programme that controls the interoperability of the components. While this aspect of the cyberspace make-up is outside the scope of this research, its relevance to the need for a cyber strategy will become obvious as the thesis develops.

The social layer comprises the human and cognitive elements that use the network. It consists of the cyber persona component and the persona component. The cyber persona component relates to all the identifiable features of a user of the network such as the user's profile: username, e-mail address, computer IP address and phone numbers. The persona component consists of the users that are actually on the network at a given time. A user can have more than one profile within a particular geographic network and a group of users can have one cyber persona, for example two research students can have one email address which they use collaboratively. At any given time that both users are on the Internet at the same time (multiple users), their persona is still single.

The dependence of the 21st century on telecommunication technology leads to both vulnerabilities and strengths (NCSS, 2011). Prior to the financial crisis of 2007 and successive cyber security attacks on Estonia in 2007, there have been other attacks but what made Estonia different is that the western world suddenly took notice of the potential harm and the costly effect of cyber-attack on national

infrastructure (European Parliament, 2011). Other cyber-attacks recorded include cyber-attacks between India and Pakistan which commenced in the 1990s. India and Pakistan were engaged in a long-term dispute over Kashmir which escalated to cyberspace (BBC 2009). There have been instances where state sponsored hackers from both countries repeatedly attacked each other's computing database system. The statistics recorded 45 in 1999, increased to 133 in 2000 and to 275 by the end of August 2001 (Prichard and MacDonald, 2004).
In 2000, cyber-attack between Israel and Palestine witnessed the launch of DOS attacks on computers owned by Palestinian resistance organizations (Hamas) and Lebanese resistance organizations (Hezbollah) by Israel. Israel's action attracted reprisals from anti-Israel hackers who crashed several Israeli websites by flooding them with bogus traffic (Cllifi, 2014).

The Lovegate attack on Ministry of Defence Computer systems in April 2003 did not destabilise operations but took four weeks to be cleared at an estimated cost of £10 million (Computer Weekly, 2004). This attack came during the early months of the US-led invasion of Iraq in which UK forces were involved. The Titan Rain attacks of 2007 on UK Foreign and Commonwealth office systems were alleged to have originated from China and also attacked US governmental agencies (Norton-Taylor, 2007).

The BBC reported the July 2009 cyber-attacks against South Korea and the United States (BBC News Online, 2009). The attacks involved the activation of a botnet against major government, news media, and financial websites of these two countries. More attacks directed at the UK government were countered; amongst the list is the Zeus attack on government systems in December 2010. In February 2011, news sources revealed that the Government of Canada suffered cyber-attacks by foreign hackers using IP addresses from China (McMillan and Kan, 2011). Over the years up until now, cyber threat escalation has speedily increased across the globe.

The Fire Eye advanced threat report of 2013 recorded 5,000 APT attacks where the use of distinct TTPs appeared to have been carried out directly or indirectly by a nation state, or a professional criminal organization, for the purposes of cyber espionage and subversion of target computer networks (Fire Eye Lab, 2014). From these attacks, 160 malware families associated with APT activity featured initial CnC infrastructure within 206 national top-level domains (TLDs). Cyberspace has been argued as strategic importance to both the military and the police in the 21st century. A NATO review of member state Information Operation Documents cites the evolution of war from the traditional warfare to the information warfare (NATO, 2010). The current international strategic environment suggests that modern conflict and warfare is characterised by advanced information technologies and asymmetric threats, a notable shift away from military tactics to non-military tactics that are affecting the social, political, economic and traditional military battle space. Although specifically referring to Information Operations Strategy, it features in the broader spectrum of cyber

strategy because Information Operations are intrinsically linked to computer networks. The Review proposed that the provision of security through prevention, defence and management of threats and conflicts globally will be the strategic issues of the 21st century.

Threat in cyberspace can come from any of the layers mentioned in the previous pages, therefore to manage these threats, a multi-layered approach is required. Public / private organisations control the entry point of the cyberspace and therefore have a flexible continuum of monitoring and preventing crime than the physical law enforcement agent (police). The big question is who is responsible for the Internet and how can cyberspace be governed. With responsibility is the connotation of ownership and governance.

Cornish, Hughes and Livingstone (2009) came up with the notion of the 'Village Commons'. According to them, cyberspace belongs to everyone and should be safeguarded by everyone ranging from individuals to states and nations. It is the 'global technological common' based on how its users perceive it. Using cyber espionage as an example, these authors propose two approaches; deterrence by interdependence and deterrence by association. Relating deterrence by interdependency to other cyber threats, behaviour and norm building of the users (both individuals and state nations) becomes the basis for counteracting cyber threats.

On the other hand, Nielsen in 2012 described security in cyberspace as risk management comprising of threat; vulnerability and consequences (Nielsen, 2012). Cyber threat is a product of the intention and capability of the attacker. Vulnerability is the characteristic of the target (cyber persona) that enables the probability of a successful attack, while consequences are the cost of a successful attack. Vulnerability applies to both the user and the network.
This opinion is further narrowed down by Deibert and Rohozinski (2010), whose conceptualizations of cyberspace security is classified into two dimensions of 'risk': 'risks to the physical realm of computer and communication technologies (risks to cyberspace); and risks that arise from cyberspace and are facilitated or generated by its technologies, but do not directly target the infrastructures per se (risks through cyberspace)'. How can vulnerability be minimised to reduce threat or risk? The need for a guideline on behaviour in cyberspace is called for.

Why does cyberspace need a strategy?

The Internet is made up of areas controlled by private organisations and areas under public governance. The Internet Engineering Task Force (IETF) controls the internet protocol, while the domain name system is controlled by the Internet Cooperation for Assigned Names and Numbers (ICANN). Different governments have control over copyright, intellectual property and cybercrime as expressed in their national policies. And the United Nations and the International

Telecommunications Union have all set down norms on how to behave in cyberspace; yet the threat posed by both state and non-state actors in cyberspace is proof that not everyone is bound by the protocols established by the aforementioned entities, nor is there a unified framework that they all agree and adhere to; an opinion that resonates in Deibert and Rohozinski's article. State actors can form alliance as evidenced in previous technological innovations such as the nuclear and the industrial revolutions but unlike these past inventions, cyber technology also empowers non-state actors. The options available in order to maintain safety and security and mitigate threats include collaboration amongst government and the non-governmental sector. To attain this, nations need to set out rules on their behaviour in cyberspace and how to counter or operate against rules established by other state actors. How these rules will translate to accommodate non-state actors is yet to evolve. However, the need for a cyber strategy is born.

Strategy has its origin in the military. Callahan, quoting Paul Nitze, notes that 'the notion of strategy implies an organised authority capable of sustained action along the lines of policy' (Callahan, 1990).

Three aspects of strategy emerge here: that strategy is organised authority, it is sustainable, and it follows the line of policy. Policy according to the Oxford English dictionary is the course of action adopted and pursued by a government. Policy therefore is a political goal of a government for the collective benefit of its nation. If policy is 'what needs to be done', then strategy is 'how to achieve what needs to be done'. Strategy is the means to achieve policy. It is therefore the precise objectives and resources that are to be applied to meet the goals of a policy.

"…In other words, strategy is the interface which provides governmental policy with its ways and means (or its capability), and which gives activity – military or other – its ends (or its purpose) (House of Commons, 2010). The USA's Joint Publication 1-02, Department of Defence Dictionary of Military and Associated Terms, defines strategy as 'A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theatre, national, and/or multinational objectives' (Thomas, 2014).

Applying this definition to cyber strategy falls short in covering the basic components that make up cyberspace. The 'instruments of national power' are diplomatic, information, military, and economic (DIME). Although cyber encompasses these instruments, there are other instruments which have emerged since this definition and must be considered. More so, the definition was applicable to definite geographic terrain, while cyber encompasses these terrains and much more. Cyberspace is interconnected and constantly changing.

History of UK Cyber Strategy

Military strategy has been expanding since technology began to emerge before the 18th century. The concept of warfare exists over two levels: strategy and tactics. In modern military leadership, the separation of military and political leadership led to two levels of strategy: grand strategy and military strategy. Grand strategy is the government's strategy. It sets out the government's policy on war and peace at a national level. Liddell Hart wrote that grand strategy coordinates and directs all the resources of the nation(s) to the attainment of the political objective of war (Liddell Hart, 1991). The British defence doctrine of 2008 published the hierarchy of command, establishing four levels of strategy, namely;

Grand Strategy – Is the national political aim in peace and war for Her Majesty's government.

The Military Strategy – The strategy of the Ministry of Defence stems from their responsibility within the grand strategy in developing, sustaining and assigning military forces and assets to support government policy and achieve the goals of the grand strategy. It operates on two levels, namely the Operational Strategy which is the Permanent Joint Headquarters (PJHQ) strategy guiding the use of military forces to achieve the objective of the MoD, and Tactical which is the field commanders' directive for Land, Sea and Air in achieving the Operational goals. The grand strategy was renamed the National Strategy but its definition remains as 'Co-Ordinated application of the instruments of national power in pursuit of national aspiration'.

Boyd's strategy for cyberspace, for both national and international, defined strategy as:

'A mental tapestry of changing intentions for harmonizing and focusing our efforts as a basis for realizing some aim or purpose in an unfolding and often unforeseen world of many bewildering events and many contending interests' (Boyd, 2017, p58) .

Cyber strategy has also been described as "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational realms, to achieve or support the achievement of objectives across the elements of national power" (Kuehl, 2009).

It explores the intricate influence of politics on policy and national objectives and goals. To achieve goals and objectives, nations will have a means of employing the resources at their disposal, translating this to cyber strategy, with cyber resources and cyber protocols being combined in a systematic way to achieve the objective of the nation towards its security, economic or social objectives. This also echoes Nielsen's views on risk management because national cyber strategy should focus on how nations employ their cyber capability to achieve their aims and objectives by employing their cyber power, and the risk associated with it (Nielsen, 2012).

Cyber power therefore extends to the larger military, political, economic, diplomatic, and national security objectives of a nation. As mentioned before, the United kingdom, New Zealand, Luxemburg, France, Germany, Spain and the Netherlands all produced their national cyber security strategy in 2011, the US and Australia in 2009 and Canada in 2010. Asian countries have also published editions of cyber security strategy and true to the definition of strategy as continually changing, most countries have reviewed and published versions of their cyber security strategy as the world of technology changes or releases new cyber threats (Sabillona et al., 2016). Prior to the official publication of the UK's NCSS, threats posed by the Internet have been on the agenda of the UK government and actions to mitigate against these threats were in place but not in such a wide scale and coordinated means as now. Below is a chronological list of offices set up to tackle these threats:

1999 - NISCC

The National Infrastructure Security Co-ordination Centre (NISCC) was set up in 1999 to minimise the risk to the Critical National Infrastructure (CNI) from electronic attack. The NISCC provided advice and information on computer network defence and other information assurance issues across different sectors of the CNI. NISCC existed for eight years and in 2007, it merged with the National Security Advice Centre (NSAC) to form the Centre for the Protection of National Infrastructure (CPNI).

2007 - CPNI

Under the mandate of the security service act of 2008, the Centre for the Protection of National Infrastructure (CPNI) was formed to bridge the gap between the role of the NISCC and the requirement to integrate the non-governmental organisations and UK business sector. It provides integrated security advice to businesses and organisations by providing security information and educating personnel. Its responsibility is to reduce the vulnerability to terrorism and other threats to the CNI. The CPNI is a part of MI5 and accountable to the Director General of the Security Service, and exempt from the Freedom of Information Act.

2009 - OCS & CSOC

The UK's first Cyber Security Strategy (CSS) was produced by the Labour government in June 2009. The publication of the CSS led to the formation of the Office of Cyber Security (OCS) and the Cyber Security Operations Centre (CSOC) in the same year. The CSOC was renamed the Office of Cyber Security and Information Assurance (OCSIA) in 2010. OCS was located in the Cabinet Office and responsible for running cyber security programmes such as the allocation of the National Cyber Security Programme funding, while CSOC is housed with the Government Communications Headquarters (GCHQ) and is responsible for cyberspace monitoring and analysis, including threat and advice to government and businesses.

The lifespan of the CSS was short when a change in government led to the apparent jettison of the CSS and the publication in 2010 of the NSS and SDSR by the Coalition government.

2010 - NSS and SDSR

The National Security Risk Assessment (NSRA) and the Comprehensive Spending Review were the guide behind the drafting of the National Security Strategy (NSS) and the Strategic Defence and Security Review (SDSR). This was during the peak of the UK economic recession. The NSS was to ensure a secure UK resilient to cyber-attacks. The protection of the national economy and critical infrastructure against threats was the main purpose of the strategy, and cyber security was given a multi-dimensional approach in the new UK security strategy split into three main stages.

The end result is national security, and the SDSR was the framework through which the aims of the NSS will be achieved. The timeline contains a series of maturity milestones in achieving the goals for national security set at 2020. The National Cyber-Security Programme was allocated £650 million over four years to deliver the goals of the NSS.
The National Security Strategy concentrated on the high possibility of cyber-attack on the UK's critical infrastructure, and past attacks on the UK highlights the cost of such attack on the UK economy. A holistic approach was used in the drafting of the NSS. Cyber-security, defence, intelligence, security and resilience (ISR), international relations and development were contributing factors. This led to the establishment of the Defence Cyber Operations Group (DCOG) which was responsible for defence-wide cyber-security, as at this time the role of the military was yet to be defined, especially within the protection of the critical national infrastructure. The Defence Cyber Operations Group (DCOG) has the responsibility of developing, testing and validating more efficient military cyber capabilities.

2011 and 2016 - CSS

Finally, in 2011 the Cyber Security Strategy was published with an increasing budget of £860 million and with the following objectives:

To make the UK public safe online and……one of the most secure places in the world to do business in cyberspace. A UK that will……be more resilient to cyber-attack and better able to protect our interests in cyberspace and a UK to have helped shape an open, vibrant and stable cyberspace that supports open societies; a UK that will…have the cross-cutting knowledge, skills and capability……to underpin……cyber security objectives.

The 2011 CSS highlight is mainly on the Government and private sector relationship in tackling cyber-attacks. Both the NSS and the CSS identify only three types of actors, namely; criminals,

terrorists and foreign states (HM Government, 2011). The CSS has omitted the individual cyber attacker who is not linked to any state but in some cases is motivated by political aspirations or financial goals. The focus is on groups, organisations and state actors. Such oversight creates a problem, bearing in mind that individuals acting alone can cause the same damage as states or organisations. 2015 saw the launch of a new strategy, building upon the success of the one of 2011 and increasing the budget to £1.9 billion which will be channelled to protecting the UK from cyber-attack and developing the UK's sovereign capabilities in cyberspace.

The chapter has built from chapter one an understanding of the concept called cyberspace and how it is viewed as the emergent operational environment of the century. As an environment, it requires a code of conduct, a strategy by linking the layers of cyberspace to the type of attack that can originate from these layers. It continued to trace the history and origin of strategy from a military perspective to a national agenda. The history of cyber strategy in the UK paints a picture of reactive continuum as cyber threats emerge and the system finds out that it has not prepared for the next challenge. By recognising the role of the Armed Forces and the police force, the next chapter details the research method employed to explore the application of the cyber strategy in the Armed Forces and the police.

Chapter Three

Research Methods

This chapter discusses the methodology and stages that the research underwent. It narrates the issues encountered in the course of researching in predominantly male organisations by a female researcher who is of ethnic minority, and also junior ranked personnel in the Armed Forces. The author of the thesis had her studies significantly disrupted and was significantly hampered by injuries for 17months. The chapter commences with the current affairs of the period and goes on to the fieldwork of accessing, sampling and interviewing police and military personnel and the ethical considerations that appeared at different stages of the research.

`

From 2011 to 2015, the Cyber Security Strategy (CSS) was released and reviewed, containing objectives that the Armed Forces and the police force are to fulfil. These objectives were rolled out in policies and courses across public establishments in the country. The research aimed to investigate a disparity between the policies and objectives and the practices within the units and during this period consideration was given to whether the same practice existed in the police force. The research explored the differences between the policies; their interpretation and challenges in application and this led to the interest in researching cyber security within the Armed Forces and the police. Although both forces have different responsibilities within the CSS, the thesis was scoped to investigate the means of achieving the objectives of the CSS within both forces, especially in the partnership that exists within the diverse governmental, public and private bodies that have a role to play in the CSS.

The research objectives were:

1. To identify the role of the Future force *(Armed Forces and police) in cyber security.
2. Explore Plural Policing in cyber security.
3. Study Public Private Partnership within the CSS and the relationship between the police and the Armed Forces.
4. Identify the level of awareness within members of the two forces of cyber security policies and their role.

Achievement of this aim lies in the answer to these research questions:

1. What is the role of the MoD and the police force with regards to the Cyber Security Strategy? How does it work?

2. What framework is employed for categorizing cyber incidents and allocating response?
3. What are the rules for escalation of cyber incidents and what agencies are involved?
4. What is the nature of the police-military relationship in the Cyber Security Strategy?

The research questions emerged from data condensed from open source publications, defence publications and books and research on policing and lesson notes from London Metropolitan University. The research questions covered three areas:

• General awareness of roles within the National Security Strategy for Cyberspace.

• Cyber security in the workplace.

• Partnership and Multi-disciplinary governance for cybercrime in the UK.

From the onset of the research, the researcher was in direct contact with the military participants and discussed the issue of cyber security and the SDSR freely; however, the change in response was noticeable whenever the topic of carrying out a research for a degree in the same field was mentioned. Issues that were freely discussed and critiqued did not receive many comments and often the individual would indicate that they did not wish to discuss the issues again.

This response was predominant across ranks but higher from officers than Non-Commissioned Officers. 70% of the officers were willing and interested in discussing cyber security but refused to participate in the research, citing the Official Secrets Act, while 50% of junior rank personnel were unwilling to discuss or participate in the research for reasons that ranged from absence of an officer ordering them to participate to their view that their opinion and that of the researcher, a fellow JNCO, does not matter in the bigger scheme of things. On the policing side, the researcher had no direct contact with any police establishment and discussed the issue of cyber security and policing with course mates who are in the police force. At this point there was a re-basing move of British forces in Germany where the researcher was based and some of the respondents were also posted out from their current location. The strategy to carry out the research was being formulated and looking at past research in the field of policing and security; the use of qualitative and quantitative methodologies and mixed methodology was considered suitable for the research due to their merits and demerits and the aim and objectives of the researcher.

Choosing a research strategy and methodology

Focus groups and semi-structured interviews were the two qualitative methods considered for this research. Semi-structured interview has the flexibility and style that fits the aim of the research because the conversational style helps both the interviewer and participant to be unrestricted in the flow of the interview. Opinions expressed during the interview can open related issues that were not initially on the list and this can also reveal the wealth of experience and knowledge of the participant unknown to the researcher but pertinent in uncovering useful research data. However, the constant relocation of potential respondents resulted in a small number of respondents from both forces being available for interview. The small sample sizes were matched and within these sample sizes were respondents who would not commit to the whole research process for various reasons; recurring reasons were that the researcher is not of the correct rank associated with such a level of study and did not have the direct mandate from the MOD or police to study to this level. It is not common for junior non-commissioned officers (JNCO) in the British Army to be studying at post graduate level. These misgivings about the person and rank of the researcher ruled out the use of a focus group as a form of qualitative approach because the time constraint and lack of practicality and affordability. Interview method was considered to bridge the logistics of time and affordability compared to using focus groups, despite interviews being time-consuming in terms of analysis.

Semi-structured interviews do not pose the same challenges that a focus group entails and offers the flexibility that is absent when using questionnaires. It links directly to the context and the personal view of the respondent (Barbour and Schostak, 2005). Barbour and Schostak proposed that qualitative research aims to produce data that is in depth, flexible and focused on the topic in real time.

To achieve the research objectives, certain aspects of the research require the use of questionnaires. As a quantitative method, it was considered as it will give a statistical basis that captures more participants across the police and Armed Forces and also lends to greater reliability of the data, and the structured nature of the questions will eliminate personal bias that may arise from using semi-structured interviews only; more so when considering the constant mobility of the participants in the Armed Forces who were constantly moving from one location to another.

It is worth mentioning that the researcher encountered a number of comments that were biased and aimed at the researcher being of ethnic minority; bias often creeps in when male respondents express their opinion that the researcher should be concerned in areas that are easier for women of black origin than in policing and security, or that the topic is suitable for commanders and not a female JNCO. These biases were dealt with in a way that reassured the respondents of the focus of the research rather than the personal characteristics of the researcher.

Structured questionnaires made it easier to collect primary data, while the key informant semi-structured interviews provided means for further exploration of pertinent points that were raised from the questionnaire response.

Mixed Methods

For this research, a mixed method aptly suited the successful completion of the research. Using a mixed method offers the advantage of the two methods stated above, without the limitations that the use of just one method will present.

In the 1990s and up to the present time, the term 'mixed methods' has become more acceptable as a research methodology in the behavioural, social, business, and health sciences (Creswell and Plano Clark, 2006). The combination of qualitative and quantitative methods as a recognised methodology is the fundamental principle of 'mixed methods', and using two separate methods of qualitative and quantitative has given rise to the diverse definition of mixed methods across various fields and schools of thought.

Another definition is by (Johnson 2007) who summarised mixed method research as

> 'The type of research in which a researcher or team of researchers combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the broad purposes of breadth and depth of understanding and corroboration' (Johnson 2007 p.118).

Johnson et al. (2014) identified various definitions of mixed method research by leaders in the field and the definition that represents the purpose of this research is that by Creswell (2013) in Johnson et al. (2014).

'John Creswell: Mixed methods research is a research design (or methodology) in which the researcher collects, analyses, and mixes (integrates or connects) both quantitative and qualitative data in a single study or a multiphase program of inquiry.' Johnson et al. (2014) p. 51

Mixed methods combines the strength of both qualitative and quantitative methodology, eliminating the shortfall of both, and it is also opined that mixed methods offers a more comprehensive understanding of the research data (Tashakkori and Teddlie, 2010).

The need for a framework to categorise different aspects of mixed methodology is met in Johnson, Onwuegbuzie and Turner's (2007) three classification of mixed methods research. They proposed three distinctions of mixed methodology, namely: quantitatively driven approaches/designs, qualitatively driven approaches/designs, and interactive or equal status designs.

This research follows the quantitative approach which Johnson et al. (2014) describes as:

> ‘The quantitatively driven approach is a quantitative study augmented with a qualitative data/method to supplement and improve the quantitative study by providing an added value and deeper, wider, and fuller or more complex answers to research questions’ (Johnson and Christensen, 2014, p311)

This framework reflects the approach adopted throughout this research and resonates with the complexity of researching in the police and military establishments.

This approach is suitable because in this research the questions that emerged from the application of cyber security policies were directly correlated to the research questions and vice versa. For example, the role of the future force (Army 2020) links directly to what is the role of the MoD and police force within the Cyber Security Strategy; resultantly the answer to the question of what are the rules for escalation of cyber incidents and what agencies are involved, links to the exploration of plural policing and its limitations in cyber security.

The process of matching the research method with the identified issues in cyber security policy and practices was rigorous, the research topic was continuously in a modification mode as the cyber strategy unfolds nationally; published books and articles with in-depth analysis of the subject matter and responses from study subjects/respondents suggested a developing and volatile research field.

The widening understanding of the subject matter shaped the choice of the wording of the thesis title and with Government and academia in a better understanding and agreement on the role of partnership in cyber security, I began thinking of the area of cyber security that will suit my current job profile and be relevant to academia at the same time. Selecting the topic required a lot of soul searching, consideration of career prospects and the rigorous task of fieldwork.

I decided that the strategy for developing and administering my research instruments (questionnaire and (structured and semi structured) interview) in order to obtain a statistically valid sample size will be the use of the mixed method.

Sampling

The initial stage of the fieldwork was to identify the sample population to contact; the research purpose indicates that cyber security within the police and military cuts across all ranks, therefore the general population is the entire membership of the two forces. Sampling was made for both the qualitative and quantitative phase of the research. The initial stage in the sample planning was to decide which phase of data collection should come first, what Onwuegbuzie and Collins (2007) refer to as ‘time orientation dimension’.

> ‘Time orientation refers to whether the qualitative and quantitative phases of the study occur at approximately the same point in time such that they are independent of one another (i.e., concurrent) or whether these two components occur one after the other such that the latter phase is dependent, to some degree, on the former phase (i.e., sequential)’ (Onwuegbuzie and Collins, 2007, p290).

The researcher decided on a two-phase sequential explanatory mixed method research to collect statistical quantitative data and follow up with a few qualitative interviews to further explain the cyber security strategy within the police and Armed Forces.

The quantitative phase sampling

A list of units with cyber related roles was selected across the two forces. For the Armed Forces, the DII (Defence Information Infrastructure) profile was used to select those with security roles. Out of this initial list, another sample was created of those with a system security role or information security officer roles. These personnel have a cyber security responsibility and are required to comply with cyber security policies in daily routines. A total of 200 email profiles were finally selected and were sent the questionnaire for completion. For the police force, lists of police units with a cyber department were contacted across England, Scotland and Northern Ireland. The units can only offer cyber security advice and were unable to involve themselves in any research. The communication with the units informed the choice of units with an established cybercrime department and willingness to complete the questionnaires. 200 questionnaires were sent to selected police units in England, Scotland and Northern Ireland respectively.

For the police, initial telephone calls were made to the contact numbers for reporting cybercrime and the researcher explained the reason for the call. Further advice was given with the detail of the officers to contact, some police departments requested that the questionnaire be emailed to the head of the cyber team. Other police units requested that the questionnaire be sent via post and addressed to the head of the cyber department. Questionnaires for the police force in Northern Ireland and police units in Scotland were sent via email although completed questionnaires were returned by post.

Purposive sampling was used for the qualitative phase. This is a non-probability sampling technique based on the role of the officers interviewed within the chain of command of both forces. The qualitative stage concentrated on key personnel that have a direct role in cyber security policy formulation within units. Eight people were interviewed, five from the armed forces and three from

the police force. The researcher conducted two face to face interviews, while the rest were conducted over the telephone. All interviews were recorded and later transcribed to paper.

This choice of sampling is supported by Morse (1994, p228), in that respondents are selected from those "who have the knowledge and experience the researcher requires, have the ability to reflect, to articulate, the time to be interviewed and is willing to participate in the study".

Connection

The researcher was confident at the initial stage of the research fieldwork that gaining access to the research population will be easy because she considered herself as part of one of the organisations. However, access to the police was almost non-existent in the interview stage. The lack of access to high ranking police officers was so pertinent to the result of the research that the researcher had to seek the assistance of the John Grieve Centre colleagues to facilitate access to relevant police establishments. Such was the difficulty in gaining access to the policing establishment that despite the reference from the John Grieves colleagues only three out of the five high ranked police officers responded and were eventually interviewed. Nevertheless, the questionnaire stage received a good response. There was a better outcome within the Armed Forces on both the questionnaire and interview stages because the researcher had an easier access to the Armed Forces research population compared to the police population, as not having pre-existing relationships with the police posed problems (Duke, 2002). Also, the researcher could be classified as what Brown (1996) describes as an "outsider outsider" within the police force and at a certain level in the military because despite being a serving member of the latter, she was still unable to gain free access with some officers who felt that she was not educated enough and being a junior ranked soldier was consider proof of this. In some cases she was asked what 'relevance will her research have as any findings cannot be taken seriously due to the way the system works'.

The dilemma of the researcher being presented as an ordinary researcher or revealing her links to the military was constantly played out throughout the research fieldwork. In most cases, the researcher often had to go through higher ranked military officers to forward questionnaires and then be linked up to willing participants. As for the police force, as mentioned elsewhere, academics from the university who had trusted links with the police force connected the researcher to potential participants. This was the indirect way in that she was vetted and considered to be good enough and acceptable in the eyes of some of the research population.

Ethics

The research was given consideration and approval by the London Metropolitan University Ethics Committee. During the course of the research, other ethical considerations came up and were mostly dealt with in accordance with the guideline laid down by the UK Research Integrity Office, to ensure that the research adhered to and was conducted within the established standards such as:

Informed consent

Gaining informed consent of the participants was covered in the introductory part of the questionnaire and the email. Those who responded were made to understand their right to freely volunteer and what their role was, as well as the choice to refuse further involvement. The majority of the participants were voluntary and a few that may have been asked by their superior officers were encouraged to make their own decision and some took the choice of refusing to complete the questionnaire.

With the interview, two participants who were asked to participate kept changing the schedule until one was posted to another job and informed the researcher that he could not represent the views of the department as he does not work there anymore, while the second participant was relieved from participating in the interview because of his reluctance to answer questions during the interview. His body language was interpreted as indifferent as though he was taking part in obedience to an order from a superior officer. It was apparent that being in the military, they are expected to obey orders; however, respecting the ethical consideration that the participant's willingness to freely consent to the research, both of them did not want to take part in the research.

Confidentiality

Measures were taken to ensure confidentiality during and after the fieldwork. The interview transcripts and field notes held no information that can personally identify the participant and this was maintained throughout the analysis and writing up stages to ensure anonymity. Although emails were used to communicate with the respondents, the attached questionnaires were printed off, the emails deleted and the responses were manually entered into the Survey Monkey tool.

Stage 1: The questionnaires were designed for the army and police/law enforcement. Qualitative data from open-source literature and defence-related publications were used to inform the formulation of the questions and link the questions to current cyber issues. The questionnaire is pre-coded using the Likert scale, and which enables an easier grading of the responses. As mentioned earlier, the questionnaire contained 10 questions, two of which have no pre-coded options; they are free text responses to allow the respondent to confer their opinion freely.

Stage 2: 200 questionnaires were then sent out to respondents. The aim was to explore the level of involvement and awareness of the cyber security strategy. The research focused on the workforce within defence and the police who have a cyber security role so as to identify the hierarchy of cyber strategy participation.

Stage 3: Responses from the questionnaire were then used to formulate the interview questions for the qualitative stage involving head of departments. This stage involved 8 participants because their level of involvement directly linked into the daily implementation and realisation of the cyber strategy goal.

Stage 4. The analysis of the questionnaire survey and the interview.

Data from the questionnaire were analysed with the online tool Survey Monkey.

Qualitative Stage - Interview Data Analysis

Several methods were considered for the analysis of the interview stage of the research: Thematic Analysis (TA), Grounded Theory (GT), and Interpretative Phenomenological Analysis (IPA).

The Grounded Theory approach utilises trends and codes prominent in sets of data to formulate a theory (Sigel and Leiper, 2004; Charmaz and Bryant, 2010). The validity of the collected data is directly proportional to the validity of the resultant theory; therefore the data must be of a quantity representing a high percentage of the participants. 'The data are analysed using coding and theoretical sampling procedures. A set of interpretative procedure are then used to assist in the construction of theory that emerges from, and is grounded in, the data (Haig, 2010).

This interview stage involved subject expert specialists (SEP) in cyber security in the police and Armed Forces and GT would have been suitable because their account of the research subject fits into the objective of GT; however, the small number of participants made it unsuitable to use GT as it requires a higher number of participants (Richardson, 1996; Sigel and Leiper, 2004).

With the number of participants in this interview stage, Interpretative Phenomenological Analysis would have been a suitable approach, as it focuses on the account given by a small homogenous number of participants to find similarities and differences in their experience of a particular event in their life. However, it was not used because there was not enough homogenous attributes shared by the participants to justify its use (Smith et al., 2009).

Thematic Analysis is popularly used in qualitative research (Braun and Clarke, 2006; Holstin and Gubrium, 1994). TA looks at themes that emerge across the data, and these themes are patterns contained in the data sets that describe a phenomenon in the research area which can be associated to a specific research question. Braun et al. note that 'a theme captures something important about the

data in relation to the research question, and represents some level of patterned response or meaning within the data set' (Braun et al., 2006).

These themes will be categories under which the data analysis can be headed. Guest (2012) wrote that thematic analyses "move beyond counting explicit words and phrases and focuses on identifying and describing both implicit and explicit ideas within the data" (Guest, 2012, p10). Braun and Clarke (2006) developed a six-phased process for developing meaningful patterns. These phases are: familiarization with data, generating initial codes, searching for themes among codes, reviewing themes, defining and naming themes, and producing the final report. Thematic Analysis using the Braun and Clarke (2006) Model can use either an inductive or deductive approach, or both. According to Braun and Clarke (2006), the researcher remains open-minded towards the themes that might emerge in an inductive or 'bottom up' approach, while in a deductive approach or top down approach the emerging themes may not relate to the interview questions but are uniform across the experiences of the participant (Gray, 2009). Both inductive and deductive approaches were used in this interview analysis because themes that came out of the data contained both approaches.

The researcher will not deny a certain degree of interest in the emergence of the themes in the initial stage of formulating the themes because cyber security was and still is a major topic, both in the media and in the Armed Forces. This does not negate the value of the themes from the data set, as the interpretation of the data was not biased. Furthermore, TA provides a flexible tool which enables a detailed analysis of the data (Braun and Clarke, 2006)

PHASE	DESCRIPTION OF THE PROCESS	OUTCOME
1.Familiarization with data	This stage involved a lot of rereading of the interview transcripts and cross-referencing it with the research questions. Rereading facilitated familiarisation with the data. The interviews with the Armed Forces participants were conducted first and were brief in detail compared to the interviews from the police participants. The initial interviews were transcribed in a	Appendix 2 Appendix 3

	tabular format. (See Appendix 2 for an example of the transcribed data.) The interviews with the police, although less in number, contained more detail. The codes identified in the transcripts from the Armed Forces also reoccurred in the police transcript. (See Appendix 3.) Critical and repeated readings of the interview transcripts led to the identification of a list of recurrent phrases which were later used to formulate codes. *(Braun and Clarke, (2006)...* (see Appendix 4 for an example.)	Appendix 4
2.Generating initial codes	"A code in qualitative inquiry is most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and / or evocative attribute for a portion of language-based or visual data...In qualitative data analysis, a code is a researcher-generated construct that symbolizes and thus attributes interpreted meaning to each individual datum for later purposes of pattern detection, categorization, theory building, and other analytic processes" (Saldaña, 2013, pp3-4). The sorting of initial codes from data was carried out in this stage.	Appendix 5 Appendix 6

	Clusters of data were collected and grouped alphabetically. (See Appendix 5.) Emerging themes were extracted with references to keep track of the research questions that they related to. Then the themes were reviewed to identify patterns that were recurring. As many codes as were relevant were compiled (Boyatzis, (1998); Braun and Clarke (2006). (See Appendix 6.) Divergences in the data were noted and, where further scrutiny was desirable, were revisited later in the course of the analysis.	
3.Searching for themes among codes	This stage was predominantly reiterative. It follows a broader view of the codes as the themes form. Themes were identified and codes were assigned then arranged in a tabular format, which made it easier to identify "The relationship between codes, between themes and subthemes" (Braun and Clarke, 2006, p89). Themes were approached at both semantic and latent levels (Boyatzis, 1998). Semantic themes were taken literally while latent themes were explored further to uncover possible meanings.	Armed Forces extract: The MoD has the task of defending the UK in the event of any threat **(role/responsibility**). We will work with other government bodies such as the police in the event of a cyber-attack. However, I would argue that the military, police, government companies and individuals all have a role to play. (**partnership/corporate responsibility).** Cyberspace does not have physical boundaries so you cannot defend it in a traditional military way. (complexity/**difference in approach**). All have a responsibility to defend cyberspace where they interact and use it **(corporate responsibility).** Police extract: The police as well as their primary role are one of the key stakeholders in the NCSS.**(role/other responsibility)** The role of investigating cybercrime with partner agencies and safe guarding the police computer system is their main remit. **(Role/responsibility**). The police force has a labyrinth of partners

		of which the MoD is one. (**partnership)**
4.Reviewing themes	INITIAL REVIEW. Here the themes were generated from codes depending on: relationship between codes, frequency (see Appendix 7a and 7b) and underlying meaning. Firstly, by checking that there is a correlation in meaning across collated extracts under each theme, each theme, code and extract were extracted and reviewed. The purpose of the review was also to check whether the extract represented the code and in turn the over-arching. In the second phase, themes were reviewed in relation to the entire data set. This process showed that that the themes accurately reflected the meaning evident in the whole data set and made it easy to identify possible divergent themes or any data omitted during earlier phases that could be explored further. This phase led to a thematic table. (See Appendix 8 for extract.)	
5.Defining and naming themes	In this phase the thematic table of the data was used as a guide to determine the scope and content of each theme. Final titles for the final analysis were selected out of the emerged titles.	
6.Producing the	The final analysis and report of	

final report	findings began. Throughout the report, extracts from the data were used to support the argument of the data in relation to the research questions posed.	

Research Evaluation

The research is not entirely a comparative study (law enforcement vs military) of like vs like due to the differing roles and priorities of the two forces within the Cyber Security Strategy. The military see the principal danger from cyberspace as sabotage or disruption of equipment and systems, whilst law enforcement have a wider remit of cybercrime in terms of leakage or victims; financial information, the virtual dimension as an extension of perpetrating fraud, use of the Internet and a virtual domain for sexual exploitation, and as a prelude to the process of luring victims of human trafficking.

During the initial stages, actual information on the application of policies on the cyber strategy across the MoD and the police were unavailable on open sources and in libraries. Most importantly, cybercrime was not included in the police crime data report until 2015 when the first estimate of cybercrime was reported:

‘2015 saw the Office of National Statistics trial the inclusion of cybercrime in the annual Crime Survey for England and Wales for the first time. The ONS estimated that there were 2.46 million cyber incidents and 2.11 million victims of cybercrime in the UK in 2015. These figures highlight the clear shortfall in established reporting, with only 16,349 cyber dependent and approximately 700,000 cyber-enabled incidents reported to Action Fraud over the same period’ (NCA: Cyber Crime Assessment 2016).

As a starting point, the research needed data that indicates the framework for the implementation of the Cyber Security Strategy and collaboration across government establishment and public bodies. Without these secondary data, the research would have limited grounds for evaluation. A Freedom of Information request was sent. There was no response on the initial request and so a second one was sent and the response is attached at Appendix 1. The absence of real time police and military data on collaborative fieldwork in cyber security along with the withheld data from the Freedom of Information request made by the researcher did not help the research and could have steered it to a wide scope or coverage.

The research concentrated on the three arms (Army, Navy and Air force) and the police force. The focus was restricted to the police military exchange, and only the police force was used from amongst the members of the law enforcement agencies as the police force is facing greater radical pluralization than other law enforcement agencies, and policing as a concept is dominant in the realization of goals of the Cyber Security Strategy. Out of 200 questionnaires distributed, 13 were chosen for being properly completed. 60 questionnaires were completed with only the neutral option, with the remainder of the questionnaires not being returned despite repeated reminders. The result of the survey might have been different if a higher number of questionnaires had been properly completed. Subsequent email reminders did not yield any further returns.

Furthermore, this reflects one of the critiques of mixed method research, where the exclusion of responses presents a dilemma and the researcher has to be careful in justifying the choices made against the validity of the overall result; this situation is also concurred in Curtis et al. (2000).

A research commissioned or sponsored by the MoD or Police would have had a wider access to restricted data, and personnel would be more agreeable to be interviewed because such authority will bridge the negative effect of the organisational culture and the political sensitivity behind the research topic. The limited number of respondents did not give a wider reflection of the whole forces. However, judging the research on its merits, its contribution is beneficial. One of the merits of the research is that it gave a glimpse of the infancy of the cyber strategy as both forces attempt to unravel their specific roles, it also shows the views of both forces regarding policing roles in cyberspace. While the police are aware of the pluralization of policing functions, the impressions expressed by the Armed Forces regarding plural policing were vague.

Validity

In this thesis, the validity of the research refers to the credibility of three issues: the case study; the data/evidence and the conclusions drawn from the data. Tashakkori et al (2003) offers advice on answering the question of validity by answering the question: ―did we indeed capture the phenomenon or attribute that we intended to (or we believe we captured) (Tashakkori and Teddlie, 2003, 694). The onus of the research is to capture and present authentically the lived experiences of people being researched. In this thesis both the qualitative and quantitative case study and data are authentic; however the number of participants and the resulting data collected restricts the conclusions drawn to be generalised. This issue reflects the difficulty of researching into the Armed forces and the police force (Gravelle and Rogers,(2014) and (Punch, 1989) . Similar experiences found in these two books while relating the difficulties of reaching the research group also encourages the conducting of such researches because these researches collectively present insightful information about the police force and similar institutions. The inferences and interpretation of data in this thesis are indicative and relevant not definitive.

Chapter Four

Questionnaire and Interview Analysis

The joint public and private sector initiative 'Cyber Security Challenge UK' launched a new framework to enable people to move into cyber security mid-career. The government delivered 'Protecting Information' levels 1 to 3 and 'Fraud and Corruption' e-learning packages for the wider public sector. Cyber security training for the civil service, law enforcement and the military was rolled out.

The National Audit Office 2014 report on the progress of the Cyber Security Strategy mentioned the Armed Forces only once and nil occasions in its 2015 report (National Audit Office, 2014). The above objective implies that the Armed Forces and the police have received education on cyber security. It is the back drop of this claim that the field research was carried out.

The first question in the questionnaire, that 'The policing of cyber space lies more with the police than with the MoD and private agencies', elicited the perceived stance of each force's suitability for the role. Responses of the participants from the police force shows that none of the participants strongly disagree while 15% of them disagree, 15% strongly agree, 38% agree and 31% are neutral. Inference from these responses suggests that although the responders from the police force recognise the need of partnership, they will prefer the ultimate control of cyber policing to be led by the police, a stance that stands short of the expectation and resources needed compared to police capability. On the other hand, the respondents from the military responded with 35% disagreeing that 'The policing of cyber space lies more with the MOD than with Police and private agencies'. 29% are neutral and 18% agree and with the same percentage strongly agreeing.

The role of the Armed forces is to defend Britain and its overseas and crown dependant territories, a task that is defined within a set geographical dimension. The notion of waging cyberwar irrespective of cyberspace identity as the fifth domain of war is still novel to majority of servicemen and women (The Economist, 2010).

The police encounter crime more often than the Armed Forces due to the nature of their job, and so it is not surprising that 77% of respondents from the police agree to the question that 'I am aware of the specific strategy or policy giving guidance on the role of the police regarding cyberspace within the work place'. 8% strongly agree and 8% were neutral and unaware respectively. This differs to the responses from the military where 15% were neutral and 35% disagree and very strongly disagree

were 5%. 40% are aware and 5% very aware of the policy and strategy. Policy and strategy in most Armed Forces units is the remit of commanders rather than the wider ranks.

Since 2011, the police forces across the UK have had a specific strategy for cybercrime. The strategic framework and good practice guidelines for forensic investigation of e-crimes is contained in the National Association of Chief Police Officers (formerly ACPO) Core Investigative Doctrine. However, specialist training is still required for investigating cybercrime due to its fragility and stringent prosecutorial requirement. Building on this, the 'Think Digital' Framework was introduced in 2015 to map police grassroots investigatory guideline on cybercrime.

The review of cybercrime report conducted by the computer security firm Norton estimated that the annual number of UK victims of cybercrime is more than 12.5m people, which is 34,246 cases daily (NORTON, 2012), a figure higher than the 2.5millin reported by the National Crime Agency (NCA 2006).

Compared to the Armed Forces, the investigation of cybercrime is outside the military, Naval or Air Force police personnel and there is nil or few requirements for the wider members of the Armed Forces to investigate cybercrime. However, being users of technology both in private and at work, the necessity to be cyber aware is high and a specific strategy should be in place for guidance. Judging by the responses, if there is one, it is classified or not widely published.

The police forces across the UK are working hard to keep up with the increase in cybercrime. The respondents were asked if 'Policing across the United Kingdom should focus more on cybercrime'. The question was asked to capture attitudes towards the recent criticism levelled against the police force over failures to adequately investigate and deal with cybercrime as, reported in the SC Magazine UK edition of July 2015 (Drinkwater, 2015). The former Scotland Yard's Computer Crime Unit Detective, Adrian Culley told SCMagazineUK.com that a 'digital society requires digital policing' (Drinkwater, 2015).

"It is as fundamental now for all police officers to be trained in cyber-crime, as it was in previously for them to be able to read and write. Every police service in the world is currently addressing this challenge." The response from the questionnaire presents a marginal value of 46% agreeing and 38% neutral while 8% strongly agree and disagree respectively. While the opinion that the police should focus on cyber security received a 46% score for agree, 69% agreed that reactive and proactive actions should be extended to policing. Presently, such a role is reserved for Special Forces outside the core police force, and there was no indecisive response expressed in respect of this question (Corera, 2012). With strongly disagree and disagree scores at 8% each, a total sum of 74% agree/strongly agree that the police should have a reactive role to play in their future expectation of cyber roles. At present, cybercrime is transnational in nature and the constraints imposed on the police

force by virtue of the area of jurisdiction poses a big problem. Law enforcement is restricted to dealing with domestic security while the military deals with national security.

One of the Armed Forces-specific questions on the questionnaire was whether cyber strategy and tactics were included in recent military courses or presentations that they attended in the past 12 months. The period covered in this questionnaire was from September 2014 to August 2015. By this time, cyber security had been proposed to permeate every aspect of defence and this includes the Armed Forces.

The Defence Cyber Security Programme (DCSP) responsibilities include improvement and transformation of MoD Cyber Operations via four major work streams (Publications.parliament.uk, 2012). One of these streams covers the wider employees of the MoD; the Armed Forces. 'Mainstreaming Cyber' seeks to establish cyber operations as part of the mainstream of departmental planning and operations through appropriate training, education and awareness. The research responses reflect the Armed Forces' notable practice of high secrecy, although the responses cannot be attributed to lack of awareness or refusal to divulge classified information. 5% jointly agree / strongly agree while 15% disagree and 5% strongly disagree. Furthermore, a high number of respondents (70%) were neutral about receiving any training in cyber security in the past year.

'Military strategy links political aspiration, expressed in Government policy, and military feasibility. It is derived from national strategy and determines how the Armed Forces should be configured and employed, in conjunction with other instruments of national power, to achieve favourable outcomes' (Chin, 2009).

The response of participants from the Armed Forces does not agree with the 'political aspiration' leading to the previous report from the UK Parliament's select committee Committee's Sixth Report of Session 2012–13. Furthermore, the responses indicate that one of the aims of the UK Defence Cyber Operations Group (DCOG) to 'plan, train, exercise and operate in a way which integrates our activities in both cyber and physical space' is yet to be achieved (HM Government, 2010).

Both forces have a wide list of cyber courses on offer. For the Armed Forces, courses are available for all levels and ranks, but which cannot be mentioned in this thesis as this falls within the remit of the Official Secrets Act. However, its publicity and awareness across the ranks is very low. The Army is still operating on the 'Cold war needs to know' basis of information dissemination. Such an approach may be redundant in the present environment because cyber awareness should be widely known and cascaded down the chain of command to the lowest ranks, but the reverse is the case based on the interviews responses. From the questionnaire responses, the need for the two forces to engage more in cyber security knowledge is clear and both forces have introduced cyber courses. The MoD has not released publicly the number of its personnel that are cyber trained; while citing national security as

the reason behind non-disclosure, it is difficult to estimate the level of awareness across the three Arms.

The UK Cyber Security Strategy Report on progress and forward plans – December 2014, reports that 'The College of Policing has designed four e-learning modules on cybercrime aimed at police officers and staff, which give an introduction to cyber, digital and social media (Cabinet Office, 2014). Since they were rolled out in 2013, over 120,000 of these modules have been completed. The College and police forces have also been delivering a classroom-based course to police investigators which gives them understanding of how to exploit intelligence and evidential opportunities offered by technology, social networking and communications data'.

The question of 'To increase resilience to cyber-attacks, cyber tactics should be included in policing courses' was asked to find out how cyber security courses have been applied to current modules offered to police staff.

Figures obtained by Veracode under the Freedom of Information Act reveal that 'Nineteen police forces across the country revealed how 3,888 police officers have undertaken specific cyber security training in 2015, a near 100 times increase from five years ago' (Veracode, 2015).

Respondents from both forces were asked in the questionnaire 'if cyber security strategy/policy regarding actions in the event of an attack is published and understood within the workplace'.

Despite the availability of cyber-related courses or the number of personnel who have undertaken specific training in cyber security, a high percentage of personnel on both forces do not understand or have access to strategy/policy regarding actions in the event of an attack. There is also lack of a clear reporting chain in the event of a cyber incident. Although such directive exists and is enshrined in the day to day practice of the two forces, the interpretation of the responses suggests either a lack of understanding of the reasons behind the security practices or a carefree view of security measures; an attitude that permeates the lower ranks more and is almost non-existent with high ranking personnel. None of the respondents expressed having actual knowledge of reading such guidelines. This was more in respect of the responses from the Army than the Navy or RAF, and less on the police response.

The responses of participants from the Armed Forces was; strongly agree 10%, agree 30%, neutral 5%, disagree 50%, strongly disagree 5%.

The role of the MoD in cyber defence is contained in the Strategic Defence and Security Review 2010 (SDSR) which required the MoD to establish 'a cadre of experts to support (its) own and allied cyber operations to secure our vital networks and to guide the development of new cyber capabilities' (HM Government, 2010). This responsibility is part of a transformative cross-government approach; bringing in other governmental agencies in joint collaboration.

The answer to the question above affirms a different perspective, because cyber security awareness is not specifically prominent both in the 2011 National Strategy for Defence and the MoD Defence Plan 2010-2014 (Ministry of Defence, 2010). Both documents did not place Cyber security and associated threat on the same par as did the National Security Strategy (NSS); despite the MoD being named as the governments lead to ensure that the UK has the capability to protect our interests in cyberspace (HM Government, 2010).

The UK Parliament's select committee Committee's Sixth Report of Session 2012–13 highlighted the lack of transparency and coordination, especially in the internal structure and division of responsibilities for cyber security in the MoD and the Armed Forces;

'Good cyber-security practice needs to permeate the whole of the MoD and the Armed Forces. It would be a cause for concern if different units were to compete for particular roles and resources, if lines of accountability were to be unclear, if they were to operate in silos that would obstruct the best use of skills across the organisation, or if policy were to become fragmented' (House of Commons Defence Committee, 2012).

A similar question on the MOD questionnaire 'The relationship between the MoD and partner agencies is reflected in the Cyber Strategy' also reflects the same level of response from participants from the police.

The question of 'The legal role of the military, for both offensive and defensive actions should be reviewed regularly to reflect changes in cyberspace' was asked to weigh the respondent's grasp of the fast changing cyber environment. Most MoD defence instruction notices have a lifespan of one year or whenever superseded by a new notice. It is not uncommon to have an event in cyberspace that will have high strategic and operational effect occur with rapid succession with zero time for contingency plans to be effective. To that end, the resilience of the two forces to cyber-attack will depend to a great extent on their grasp of technological progress that is likely to impact on their network. 70% of the Armed Forces' respondents strongly agreed and 20% agreed. None disagreed or strongly disagreed, while 10% were neutral. The police respondents answering a similar question had 38% agree and 15% strongly agree. The sum total of those that disagree and strongly disagree was 31% while 15% were neutral.

The question of 'The structural governance suitable to cyber defence should be jointly controlled by the police and the Armed Forces' aimed to test the understanding of partnership within the cyber strategy. The existence of other stakeholders is not reflected in the responses. The nature of cyberspace demands a cross spectrum of participants in its defence. Although 23% disagreed and 8% strongly disagreed, the 38% that strongly agreed and the 15% that agreed constitute more than half of

the responses. The role of academia, the private sector and industry is as important as the joint role of the two forces. More education is needed to highlight the joint defence that partnership offers.

The pluralisation of policing involves diverse organisations involved in policing both the Internet and other traditional crimes. However, knowledge of the relationships and vital roles of these organisation is not reflected in the responses.

46% of the police were neutral to the question 'The relationship between the police and partner agencies is reflected in the policing Cyber Strategy'. A response that is worrying and reflective of the problem the police faces in combating cybercrime. The response also concurs with the criticism on the policing of cybercrime across the UK by the media. On 21 March 2014, Charlie McMurdie - senior crime adviser with PricewaterhouseCoopers (PwC) and former head of the Met Police Central e-Crime - told SC UK (SC Magazine UK, 2014):

"We are moving in the right direction, building national capability to provide a response around cyber-crime. But time and time again, what we are really missing and where we need to focus more effort is better intelligence, both strategic and tactical intelligence exchange with industry."

She comments on the lack of cooperation between the police and partner agencies which includes the MoD and the private sector.

"We keep using the 'partnership' word but it is still frustratingly difficult for industry to identify who to speak to (in the police) and how to actually become part of that intelligence exchange. There's a wealth of knowledge and expertise in industry that needs to be capitalised on."

The MoD is not the only partner in this case. In the 2013 Waking Shark II Desktop Cyber Exercise: Report to participants, participants received a stimulated cyber-attack exercise across the wholesale banking sector, including investment banks and key financial market infrastructure to rehearse their cyber response mechanism and communication. Throughout the successful exercise, there was a notable absence of the police and law enforcement agents (Keeling, 2013).

'The participants did not engage directly with law enforcement during the exercise in reporting the cyber-attack, primarily because there were no law enforcement representatives present. It is possible that participants considered that law enforcement agencies were aware through the extensive media coverage, or assumed incorrectly that reporting via the CISP platform constituted advising law enforcement.'

The response from the military on the same question yielded 25% agree and 5% strongly agree, 30% are neutral and 40% disagree.

Cyber-attacks, threat and vulnerability information released to the public and partner agencies does not reflect reality. In April 2014, the United Kingdom's government published a new classification standard. The Government Security Classifications Policy (GSCP) uses three levels of classification: OFFICIAL, SECRET and TOP SECRET.

The act of classifying, safeguarding, and declassifying is balanced against the expectations of the citizens of any democratic country. It is for the protection of the citizen and the state and it is behind this backdrop that various nations have a system of classifying information. Balancing the need for transparency and security of sensitive information has always been a challenge for any administration.

Against this classification lies the declassification of information that is previously classified. Protecting information critical to a nation's security requires strict adherence to these standards and elicits outrage when such information is released to the public without proper authorisation or even leaked for whatever altruistic reasons.

The question 'cyber-attacks, threats and vulnerability information released to the public and partner agencies does not reflect reality' had very high scores on agree and strongly agree. A sum of 77% of participants from the police force agreed, while 23% remained neutral.

The effect of releasing the wrong kind of information to the public is typified by the Snowden disclosures from the National Security Agency in 2013 (Lanchester, 2013), which has been argued by some as a threat to freedom and for some was 'treacherous betrayal' (Coughlin, 2014). Although, it can be argued that Article 8 of the Human Rights Act which safeguards the freedom being referred to above can be violated or breached by the state if it is: "In the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (Equalityhumanrights.com, 2015).

Interviews Analysis

The interview stage involved eight participants; five from the armed forces and three from the police force. These participants are top management in their respective forces in a cyber security capacity. The interview analysis was based on the research objectives and incorporated answers to the research question as presented in the interview transcripts. The first objective was to identify the role of the Future force (Armed Forces and police) in cyber security.

Both the police force and the Armed forces are convinced in their current and future roles in cybersecurity despite the uncertainty in the nature of the threats that cyberspace will present in future. From the interviews, similar responses to the question of role were made by the three participants from the armed forces. They responded that 'The MOD has the task of defending the UK in the event of any threat. We will work with other government bodies like the police in the event of a cyber-attack' while first armed forces participant concluded that he ' will argue that the military, police, government companies and individuals all have a role to play. Cyberspace doesn't have physical boundaries so you can't defend it in a traditional military matter. All have a responsibility to defend cyberspace where they interact and use it' and second armed forces participant agreed that cyber security is larger than the military can contain and acknowledged the contribution of other governmental and non-governmental bodies. Second armed forces participant also noted that the armed forces are not the lead department.

The police responses also point to the established role of the police force as incorporating cyberspace but acknowledged that the 'The police as well as their primary role are one of the key stakeholders in the NCSS. The role of investigating cybercrime with partner agencies and safe guarding the police computer system is our main remit'. First Police participant noted that' currently there is no specialist department in this force. Cybercrime is referred to CERT UK or resolved through the ACTPOOL. The force has collaborated with MOD, as well as other organisations on issues of personal protection, infrastructure protection, and public crime'. This brings to fore that plural policing is also present in cyber security and is further explored in the net chapter. From the responses, the future force; both military and police, still have significant roles within the cyber security strategy, roles that are bound to evolve in the future as threats evolve.

Exploring Plural Policing in cyber security within the United Kingdom recognises that crimes and the notion of security reflect policing in the physical state. The presence of partner agencies in cyber security is mentioned by all the participants however; the level of involvement, roles and area of expertise is vague. In answer to the second research objective, the question 'What frame work is employed for categorizing cyber incidents? was asked in order to elicit the levels of involvement of the participants in cyber security and cyber policing and also the category of the cyber incidents. The

research data points to varying understanding of how the interaction with other agencies works. The four Armed forces participants mentioned 'The National Cyber Incident Management Plan (NCIMP). The three police participants have different answers varying from the first police participant who stated that there is no specific framework: 'There is no framework that we strictly adhere to. Local cybercrime are dealt with locally while crimes that have a national scope are delegated to a higher authority'

The second police participant stated that 'Currently in place is a tiered system starting with the local, national and international levels. There are also specialist units that work across these tiers.

As a developing area of study, uniformity is hard to define due to the autonomy of each force but the framework exists. How it is adhered to is up to respective forces and the nature of the crime. Overlaps will always exist' while the third participant stated that 'There is a consistent framework in use which is restricted. The breakdown is a 3321 tier. Tier 1. Highest, global and National Cyber Security. Tier 2 Dealt with by NCA and Tier 3 is the remit of Local police forces. There is a grey area of overlap but progress is being made to fine tune this'

The responses from the armed forces regarding the framework within which partners operate shows lesser awareness compared to the police responses. The National Cyber Incident Management Plan (NCIMP) held by OCSIA in Cabinet Office defines the framework, reporting and escalation process

The security behind the NCIMP held by OCSIA is highly restricted and confidential that the document is not available through the freedom of information request. Compare to the NCIMP of United States of America, which is electronically available on open sources. Although the framework exists; adherence to it or in-depth knowledge of its guidelines appears vague and no insight is further given to the question:' 'What are the rules for escalation of cyber incidents and what agencies are involved'? The response across the armed forces participants was: 'All contained in the NCIMP'. No further information was given and questions relating to the framework were ignored or discouraged during the interview.

The first police participant responded with these words' The force works with NCA and MI5. Officers will link up with regional cyber unit and partners with full collaboration on both side' and the second participant stated that 'fighting and policing cybercrime is a joint role involving other agencies. Global and national incidents are dealt by GCHQ, NCA and MOD' and finally the third participant response was that' depending on the scale. GCHQ, NCA and MOD deal with Tier 1'.

With varying answers to the framework question; further responses reveal a level of critique of the current National Security Strategy especially in the question:' Is the strategy comprehensive or are there areas that need more work'? The Armed forces responses conveyed a mixture of technical terms

that was not elaborated on. however, these responses are notable. From first Armed forces participant, the response was:

'Areas like the defence of CNI (SCADA, Banking etc.), corporation/info sharing with PAGs and multi-national agencies, what limits sovereignty places on DCO-RA when CNE/A originates overseas. General awareness of vulnerability of C4I systems may be useful. Understood within specialist agencies, but cyber awareness across the military remains poor'.

The second participant stated that:

'There is still more to come. Cyber is a new challenge for many organisations and the MOD is not exempt. The relationship between military mission critical assets and the network. The value of information within the MOD. The value and subsequent criticality of applications and networked enabled platforms'

The third participant noted that:

Any strategy needs to have a clear, deliverable 'end-state', with balanced 'ways' and 'means' to achieve. Sadly most strategies are high on ambition, and delusional on 'ways' and 'means'. So my focus would be on achieving something that is actually deliverable and not just a pipe-dream.

Cyber defence must take priority over offensive cyber in particular funding of capability.

The strategy must highlight who is responsible for what – too many 2*(two star generals) think they own the issue which is creating friction and empire building.
The need for better doctrine – the JDP isn't well written'

The fourth response was:

'National vulnerability impact assessment to assure appropriate proportional effort is expended on defence (thus denying adversary's easy access through national weak points, regardless of ownership)'

The fifth response was: 'Provision of an integrated National Capability CONOPs (Concept of operations) for delivery of tactical cyber effects in a JOA (Joint Operational Area.) Authorities to execute cyber missions at the tactical level. The industrial base needed to provide the enduring national and tactical capabilities.

These responses from the armed forces participants compared to the response from the police participants below show that the Cyber Security Strategy is short of expectation. These responses are

also centred within the Armed forces and do not mentions other partner agencies like the police force and the law enforcement agents.

Responses from the three police participants refer to other partner agencies operating in the Cyber security partnership. The first police participant noted that:

'Media collaboration, victim support group. Legislation on cyber forensics such as removal of malicious data online' are areas that need to be incorporated in the Strategy but were absent or sparingly explored. The second participant mentioned areas like: 'more funding, issues of human rights, etc. Existing barriers to collaboration… Time and tier pose a few barriers' and the third participant stated that the:

' key thing here is that the strategy should be all inclusive down to the citizens on the street. Priority should be reassessed. Funding made available. Other issue is the commercial interest and capitalist base in the cyber industry should be addressed. There are disparate areas that make up cyber security strategy in need of harmonisation'.

These responses bring to the fore the different angles that the two forces approach the Cyber security Strategy. They responses also show that the strategy is awash with shortfalls that undermine its success at least within the two forces. The interview also delved into the Public Private Partnership within the CSS and the relationship between the police and the Armed Forces. Public private partnership is dealt in depth in one of the chapters however the present relationship between the police and the armed forces with regards to cyber security strategy is limited and almost non-existent. There is no depth to show that both forces are working together.

The question 'What is the nature of Police military relationship in cyber strategy (if any)'? led to the following response from the first Armed Forces participant:

'There is a network of relationships among agencies including the police and the NCIMP is the umbrella that connects all relevant agencies'.

The second participant stated that:' there is a relationship that exists among agencies not only the police and the NCIMP is the umbrella that connects all relevant partners'

Similar responses were given by subsequent participants accompanied by gestures that dismiss further questions or elaboration. The citing of the NCIMP, a document that is classified and unavailable can be construed that either the participants are evasive or have no clue as to the content of the NCIMP or the police military collaboration in cyber security.

The police response on the other hand elicits some form of relationship. The first police participant's comment was that: 'MI5 provides liaisons in areas of collaboration, infrastructure and equipment

sharing'. The second participant stated that: 'There is no strict or restricted role for both forces however military police partnership exists in many operations such as peace keeping and when and if a need to work together in cyber related incident, both forces are by law expected to collaborate. Areas like infrastructure and equipment sharing'; while the third participant noted that there is 'Very limited due to difference in roles. Areas of collaboration include, infrastructure and equipment sharing. Note that the MOD does not have operational independence. Collaboration is possible were the need arises'

There is an absence of a collaborative relationship between the armed forces and the police force going by the responses above which can be attributed to the diversity of the cyber spectrum however the need for partnership is critical to the success of the strategy and the wider partners. The interview aimed to gauge the level of awareness within members of the two forces on cyber security policies and their role. During the interview, participants from the Armed forces were reluctant to answer questions about specific cyber security courses available to the members of the armed forces while the police force participants were open to questions in this regard. The question 'What percentage of your workforce received or attended cyber security courses in the past six months? How many are qualified cyber forensic. Is cyber course mandatory to all staff?' received the following responses:

First Police participant: 'Current policy and training has been given on personal protection'. The second participant went on to say that 'Currently the figures are not consolidated but it depends on what aspect of cyber security. Cyber security is now a mandatory course for new intakes. As we speak, courses are running across the country' and the third participant said that 'There is no priority for a specialist course as the need is met through partner agencies; there is ongoing training in specialist areas especially in capability to conduct core role without much recourse to private organisations. Training is tailored to need due to limited funding. Mandatory training is not popular with the force; funding dictates training.

The findings of the study are a revelation of the influence of current practice over proposed practice. For example, most of the participants exhibited a degree of indifference to cyber security and were willing to adhere to policy only because there will be disciplinary consequences otherwise. The next chapter will delve more into the themes and sub themes from the interviews and how the themes are reflected in current practice, especially in regards to the research questions and objectives. Pluralization of policing is very central to the cyber security strategy and is discussed in detail.

Chapter Five Discussion of Findings and Themes

The overarching themes from the interview data are Plural policing and partnership. They are central to all the main themes and their sub themes like: Collaborative Governance, Partnership, Levels or Responsibility and diversity of the police force.

Pluralisation of Policing and Cyber Security Partnership

Most of the literature on pluralization or fragmentation of policing have omitted cyber policing and instead concentrated on policing within geographical boundaries; yet cyberspace has its share of fragmented policing as reflected in the interview and questionnaire data. This chapter applies the framework and classification offered by these studies to analyse the different means through which cyberspace is policed.

The chapter explores the plural policing bodies that currently exist and how interactions between them keep cyberspace monitored. There is policing by the government carried out by the civil police; policing through government, policing above government, policing beyond government, policing below government and policing inside government, which are forms of policing undertaken by entities other than the civil police. Each form of policing will be described in detail in this chapter.

Cyberspace has introduced non-traditional crimes conversant to the public police; a continuous phenomenon that has left the public police striving to be reactive and adaptive, however not truly winning the war on crime control, as noted by Wall (2010):

‘The relationship between the public police and technology dates back to their origins in the early nineteenth century. Traditionally a responsive organisation designed to counter the dangers produced by urban migration caused by eighteenth-century industrial technology, the police had, by the second half of the nineteenth century, situated themselves as an all-purpose emergency service.’

The policing of cyberspace revolves, to some extent, around received notions that policing is the core responsibility of the police as an instrument of a modern state; a notion that has far-reaching significance in the challenges that face 21st century policing (Etter, 2001). Burton, in his book ‘private policing’, documents the history and development of policing in the United Kingdom and unfolds the public private relationship between the diverse bodies that engage in policing (Burton, 2012). The book lays out a framework that identifies subsets of both private and public policing bodies with varying levels of legitimacy, albeit in a broad spectrum.

Other writers have explored the emergence of policing services other than the services offered by the public police; Johnston (1992) offers four forms of policing: Public Police, Citizen/Self-Policing,

Private Policing and Hybrid Policing. He uses the term 'Hybrid' to further categorise a grey area in policing that is provided by private and public bodies.

A four-fold alternative classification of private policing was offered by Jones and Newburn (1998). Their classification also captures the nuances that have shrouded the development in policing without offering a succinct distinction of these 'other bodies' engaged in policing.

Burton (2012) noted that although Jones and Newburn (1998) rejected Johnson's use of 'Hybrid', they used the term in their classification to describe a new category of space which is neither public nor private. It is safe to suggest that cyberspace fits into this new 'hybrid space', though the definition at the time was focused on territorial policing. Burton further broke down the 'Hybrid' into three distinct categories:

'Central and Decentralised public policing bodies; specialised police organisations and Non-private security private policing bodies' (Burton, 2012).

There are varying reasons given to explain the current state of policing; from the view that policing has devolved over the years as events unfold over time and require different approaches in the systems of policing (Bayley and Shearing, 1996), which has inevitably been formally harmonised through lessons learnt (Jones and Newburn, 2002). Terpstra et al. opines that the changes in policing are a result of complex social, political and economic circumstances and changes (Terpstra et al., 2013a).

A wider view is held on the financial and manpower deficit of the public police and the heightened demand for security in the society (Crawford, 2008; Jones and Newburn, 2006; Terpstra et al., 2013a). Finally, changes in the urban economy and space are also reported to have influenced pluralization (Crawford, 2008; Terpstra et al., 2013a). There is the issue of how private or public is the policing service offered, but which is outside the scope of this chapter.

Irrespective of the views expressed, the provision of policing services by diverse bodies other than the public police have been held a permanent fixture (Burton, 2012) with varying consequences, such as the increasing outsourcing of core policing duties from the public police and the drift from a state-centric policing framework to a multi-platform of policing network (Loader, 2000; Crawford, 2006), a term Loader (2000) defined as plural policing:

'What we might call a shift from police to policing has seen the sovereign state – hitherto considered focal to both provision and accountability in this field – reconfigured as but one node of a broader, more diverse network of power. Sure enough, this network continues to encompass the direct

provision and supervision of *policing by* institutions of national and local government. But it now also extends – as we shall see – to private policing forms secured *through government*; to transnational policing arrangements taking place *above government*; to markets in policing and security services unfolding *beyond government*; and to policing activities engaged in by citizens *below government*. We inhabit a world of plural, networked policing' (Loader, 2000, pp323-324).

Loader's definition contains a framework that can be extended to capture a more compact categorising of the various means; public and private or even hybrid forms through which cyberspace is policed.

Adopted Cyber Policing Framework

Policing by Government

The government plays a significant role in the policing of cyberspace. Despite the nature of cyberspace which negates the concept of geographical boundaries within which a state exercises sovereignty, a percentage of the infrastructure that is part of the connected network of networks that make up cyberspace still falls under the jurisdiction of the state. In the UK, policing by government is carried out by the 43 Home Office police forces in England and Wales, The Police Service of Northern Ireland (PSNI) and Scotland. Some of the trans-force police units also fall within this category such as the National Crime Squad and National Criminal Intelligence Service.

Due to the unique organisational structure of the UK police force, police cyber strategy varies from county to county in the UK, although each regional force operates with the same objective as contained in the UK strategy.

Different policing strategy over the years shows that these strategies have been changing to accommodate different aspects of crime. Since the 1990s, policing and crime analysis have undergone rapid development in approaches to fighting crime, namely; community cohesion policing, neighbourhood policing, problem oriented policing, intelligence led policing, citizen focused policing, knowledge based policing, and reassurance policing, with each approach having consolidated and directly built on the legacy of the other approaches.

Policing is a multi-contextual public service and it follows that different context requires a different policing approach and style and that no particular context fits all. It is also because people and society change and this is followed by policy and perception changes. Law enforcement is both reactive and proactive in many aspects, therefore the specific challenges of policing cybercrime have been explored by different governmental policies, strategies and initiatives. The cyber policing strategy evolved from the challenges from cyberspace on traditional policing.

The National Hi-Tech Crime Unit (NHTCU) is the first actual civil police department that was formed as part of the National Crime Squad (NCS) in 2001. The NCS deals with national and international organised and major crimes such as human and drug trafficking, murder for hire schemes, illegal arms dealing, computer and high tech crimes, money counterfeiting and laundering, extortion, and kidnapping.

NHTCU had a £25 million budget for its operations; a budget that was criticised widely as too low for fighting crime that has cost the UK economy £27 billion (Anderson et al., 2013). The criticism over the commitment of the UK government in tackling cybercrime was reported widely in the media (BBC News, 2013).

The NHTCU was set up to deal with cybercrime due to the specialised nature of the evolving cybercrime. It ceased to operate in April 2006 following the amalgamation of its parent unit, the NCS, with HM Customs National Investigation Service and the National Criminal Intelligence Service to form the Serious and Organised Crime Agency (SOCA) (House of Commons, 2005). SOCA operated till 2013 when it was absorbed to form the non-ministerial National Crime Agency.

The Police Central e-Crime Unit was established as a lead force in the fight against e-crime by the Home Office. The unit was merged with the Computer Crime Unit of the Metropolitan Police Service (MPS) and hosted also by the Met Police.

The Strategic Policing Requirement (SPR) 2012/2014 (Home Office, 2012, 2014) sets out the Home Secretary's perspective with regards to appropriate national policing capabilities to policing the nation during a national threats incident, which includes a large-scale cyber incident. The Home Office Select Committee published a report on the failure of the police in adequately winning the war on cybercrime on 30th July 2013, following a 10 month enquiry. The committee based its report on the increase in cybercrime and the decrease in resources to fight the crime; notably the decrease in 10% of funding of the Child Exploitation and Online Protection Centre. The cut of a quarter of the 800 specialist Internet crime officers by the City of London Police will have enormous effect on cyber policing (Professional Security, 2016).

The National Crime Agency (NCA), was formed in October 2013, merging the Serious Organised Crime Agency (SOCA) and the Police Central e-Crime Unit in the Metropolitan Police Service and with an annual budget of just under £500m. Unlike SOCA, The NCA has a broader mission covering economic crime, border security, child exploitation, cybercrime and organised crime. The NCA has the power to directly task other police forces and therefore is the single, authoritative entity in cybercrime in the police force; an area that is strongly vital to the British National Cyber Security Strategy. Within the same month as the NCA's creation, the new Serious and Organised Crime Strategy was published, which is structured to incorporate four themes of 'pursue, prevent, protect and

prepare' (HM Government, 2013). These themes will later be used to access the progress of the police force in achieving the objectives of the NCSS.

On 10 April 2014, the HMIC found that only three forces (Derbyshire, Lincolnshire and West Midlands) had developed comprehensive cybercrime strategies or plans and only 15 forces had considered cybercrime threats in their Strategic Threat and Risk Assessments (STRA) (HMIC, 2014).

The UK and a number of other nations such as Germany, Canada, the US and France have published editions of their CSS as cyber threats evolve. Although this is a reactive measure and in line with Strategy guidelines, the frequency of cyber threat mutations means that the strategies are a step behind the threats that they are meant to mitigate and often too slow.

Policing Through Government

Loader (2000) defines policing through government as:

'Situations where policing services are enlisted by government, but provided by others (though it might also be extended to encompass the purchase by private concerns –, for example – of additional public police service' (Loader, 2000, p324). The contracting out of policing services by the government to private security firms is opined by Burton as an example.

G4S, a private security company, features prominently in this category. The company has been providing a range of 'police support services' in the UK for a number of years and were awarded the policing duties during the 2012 London Olympics. Policing services are handled by its G4S Policing Solutions department which employs ex-police officers in areas such as fraud investigation. Other parts of its policing portfolio include custody suites, with over 500 cells which they hire out to police forces in the UK (BBC, 2015).

After securing a partnership in 2011 with the Lincolnshire Police Authority (the first of its kind in the UK) to provide core policing functions in a 10-year contract worth £200 million, G4S will be responsible for the operation of the force's control centre, human resources, training, finance and custody. Under the terms of the contract, two-thirds of the force's staff are required to join G4S, further blurring the public private distinction.

Possible comparison in cyber security is the provision of certain services that include a policing function among other benefits. This is evident in the contracting or use of data services provided by a private organisation where the organisation also polices access to the data bank and monitors usage to prevent abuse or breeches that may compromise the security of the data instore (Computer Weekly, Aug 2016).

Levi (2010) notes that ‘Most policing activity in the area of UK public sector fraud is undertaken not by the police but by departmental investigators; most frauds against business come to the attention of the police via corporate actors; while frauds against the public may be reported direct, or via intermediaries like credit card issuers’.

An example of private policing of cyberspace in the financial industry is The UK Payments Administration Ltd (UKPA) which replaced the Association for Payment Clearing Services (APACS), and which manages the systems behind UK payments, such as BACS, CHAPS and the Cheque and Credit Clearing Company. The company has a cyber security department with policing functions for the benefit of its clients among which are the major financial institutions in the United Kingdom. There are numerous organisations like UKPA that represent other infrastructure in the UK, and it is noteworthy to mention that these organisations have international reach due to the nature of the crime prevention and policing that occur in cyberspace.

There are as many benefits as well as risks involved in the growing dependence on private policing through government. Where the risks surpass an unavoidable benefit such as technical expertise and human resources, greater regulation should be imposed on private policing firms to increase public trust.

Policing Inside Government

This ‘Involves organisations employed by the government to police its revenue and expenditure’ (Burton, 2002, p15). Burton added this further classification which is used in this paper to classify state departments that offer some form of policing and cyber security as contained in the National Cyber Strategy.

The Ministry of Defence falls under this category. Although Burton referred to the Ministry of Defence Police under his ‘Specialised Police Category’ (Burton, 2002, pp64-65), it is not in relation to cyber policing but rather in a more broad policing role. Chapter five will go into depth on the role of the MoD within the National Cyber Security Strategy.

Other organisations fall into this category and their formation are as a direct response to the growth of cyberspace from a mere communication tool to a global marketing and communication arena. As opined by Jewkes and Majid (2010), responding to the transformation of cyberspace and within it cyber criminality, gave birth to e-policing and the establishment of several agencies to tackle these waves of crime (Jewkes and Yar, 2010).

It began with the formation of the Internet Watch Foundation in 1996. It was not set up as a typical civil police department but commenced as a charity organisation with a mandate to tackle illegal content online.

The Internet Watch Foundation is empowered by the UK ISPs, Crown Prosecution Service and police (Internet Watch Foundation, 2013). Functions include reporting illegal material either to the police or the ISP. It has become a quasi-public face of Internet regulation in the UK.

The National Cyber Security Centre (NCSC) is a department of the Cabinet Office that focuses on the financial industry. It monitors access to the Internet and assists the police with investigation and prosecution when a crime has been committed (Ncsc.gov.uk, 2015).

In 2008, the National Fraud Authority (NFA) was established to fulfil part of the NSS objective of 'Building the UK's cyber security knowledge, skills and capability'. An agency of the Home Office with a budget of £29 million over a three-year period, it comprised a number of counter-fraud agencies such as; the National Lead Police Force for Fraud, the National Fraud Reporting Centre (NFRC) and the National Fraud Intelligence Bureau (NFIB). It provided support to victims of fraud and promoted information sharing with partner agencies, it created means for educating the public on the consequences of fraud and how to protect themselves from it.

The criticism of the low level of budget allocation toward e-crime agencies paid off and in October 2010, £650 million was allocated to promote cyber security in the UK after The United Kingdom National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) raised cyber security to a Tier One risk to national security. The NSS works alongside The National Fraud Strategy (NFA, 2009) and the Association of Chief Police Officers' E-crime [Policing] Strategy (ACPO, 2009) (Young, 2009).

Get Safe Online launched in October 2005 as a public/private sector campaign to raise awareness of online security. Its objective was to teach the public about Internet safety and privacy. It is sponsored by Government, Microsoft, HSBC, Cable and Wireless, Ofcom, Trend Micro, Gumtree, Verisign, Symantec and PayPal.

The UK Council for Child Internet Safety (UKCCIS) was established in 2010 (Gov.uk, 2010). UKCCIS is working in partnership with over 180 organizations and individuals from government, industry, law enforcement, academia and charities to keep children and young people safe online.

The Centre for the Protection of National Infrastructure (CPNI) is a UK government authority that advises the UK public and private organisations. Its services deal with threats such as espionage, terrorism and other cyber threats that affect British national infrastructure.

Policing Below Government

The users of the electronic/ computing systems

Internet users are the very individuals that use the Internet, these include; family units, small and medium scale businesses that use the Internet in running their business, corporate bodies, and indeed anyone that uses a computer that is linked to the Internet. They have the obligation to protect themselves from cybercrime, either through practical intervention such as installing firewalls and monitoring tools on their computers or in forming interest groups and focus groups whose responsibility will entail monitoring the web to protect their interest.

Burton (2002) calls this voluntary policing engaged by the citizens either ‘responsible’ or ‘autonomous’; quoting Johnson (1992a), responsible policing has the sanction of the state while autonomous citizenship involves individuals or groups of citizens taking out its revenge on alleged offenders, such as vigilantism. This form of policing does not have the sanction of the state.

A corresponding voluntary policing exists in cyberspace, although there is ongoing debate on the definition of cyber vigilantism; scholars have hailed an expansion of Johnson (1999) definition to accommodate a wide range of online behaviour (Smallridge et al., 2016). In addition to voluntary policing, Social Network Supervisors have a policing role over their firms’ domain. They are employed by the owners of social networks to monitor the behaviour of their members and ensure that the users comply with the norms governing the usage of the sites. Actions that are deemed offensive or contravening the set rules are punished either by temporary suspension of access or permanent closure.

In addition to the vested obligatory responsibility to the law, crimes must be reported to law enforcement agencies. An example is the Canadian legal case of R v Kerr (Kerr and Gilbert, 2004).

According to Grabosky and Smith (2001), the security in ‘cyberspace depends on the efforts of a wide range of institutions, as well as on a degree of self-help by potential victims of digital crime’ and it is more likely to depend on a 'mix of law enforcement, technological and market solutions' (Grabosky and Smith, 2001, p29).

Policing Above Government

The existence of complex policing arrangements that transcend state boarders evolved in the fight against transnational crimes (Walker, 2000). Neil Walker, in Newburn's Handbook of Policing, defines transnational policing as 'networks which are relatively autonomous of these states of origin or which owe authority and allegiance to other non-state 'polities'' (Newburn, 2003, p111). The two definitions above infer that these arrangements are complex, transcend geographical boarders and are

autonomous of the forming states. An example is cited in the CCIC (The Cross Channel Intelligence Committee) (Sheptycki 2000), a multilateral collaboration that involved police forces from the UK, France, Belgium and the Netherlands. That these forms of policing have increasingly developed beyond the control of the state governments of the countries that formed them (Sheptycki, 2000) suggests this was not the original vision or status quo.

Before the escalation of cybercrimes, transnational crimes such as terrorism, organised crime, human trafficking, and fraud enforcement have been fought by nations through bilateral and multilateral collaborations. The change introduced by cyberspace has increasingly made these means of dealing with transnational crime more relevant; not just the difficulty in imposing legal mechanism and attribution but in finding a unified platform through which cyberspace can be policed and cybercrime investigated effectively. The investigatory aptitude in cybercrime is one of the deficiencies of the public police as highlighted by (Doig, 2006, 2009), who notes that there are far greater numbers of fraud investigators in non-police governmental and private sectors than in the police force. With the private sector firms, the policing services they offer are customer focused compared to the civil police that is citizen/state-centric.

Williams (2005, p317) observes that 'these firms have positioned themselves as suppliers of a unique and highly specialized form of investigative and quasi-juridical labour geared to the resolution of 'business troubles' ranging from the theft of intellectual property, to the misappropriation of corporate assets, to breaches of financial security'.

Internationally recognised organisations that fall into this category include but are not limited to firms such as: KPMG, Kroll Associates, Ernst & Young, Deloitte and Touche, Price-Waterhouse and Control Risks Group (Williams, 2005), organisations that are experts in insurance, financial and accounting management. One of the international organisations that cybercrime policing services is the Anti Phishing Working Group (APWG) which has more than 1800 institutions worldwide in its membership, ranging from: 'national governments; global governance bodies such as the Commonwealth Parliamentary Association, Organisation for Economic Co-operation and Development, International Telecommunications Union and ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, the G8 High Technology Crime Subgroup, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe, Europol EC3 and the Organization of American States. APWG is a member of the steering group of the Commonwealth Cybercrime Initiative at the Commonwealth of Nations' (APWG, 2016).

The UK is a member of many international policing partnership schemes that collaborate in the fight against cyber and organised crime, working closely with other countries including the US, Australia, Canada and New Zealand. The two partnerships that are directly linked to the UK's cyber security

legal framework are the UN's ITU-IMPACT and the NATO industry cyber partnership. As previously mentioned elsewhere in this thesis, the UK is a member of the UN's Cyber Security partnership 'The International Multilateral Partnership Against Cyber Threats' (IMPACT), which was launched in 2008 and is currently the largest and first comprehensive public-private partnership against cyber threats with a membership of 152 nations (ITU, 2015). 'IMPACT serves as a politically neutral global platform which brings together governments of the world, industry, academia, international organisations, and think tanks to enhance the global community's capabilities in dealing with cyber threats' (Impact-alliance.org, 2015).

UN IMPACT teamed up with ITU in 2008 and both organisations are in partnership with a mandate to fulfil ITU's Global Cybersecurity Agenda (GCA). During the World Summit for Information Society 2011 (WSIS) Forum in Geneva in May 2011, IMPACT became the ITU's lead agency 'with the responsibility to provide ITU's 193 Member States access to expertise, facilities and resources to effectively address cyber threats, as well as assisting, as required, UN's agencies in protecting their ICT infrastructures', and adopted the term of reference ITU-IMPACT (ITU, 2014).

A case file listing the UK's cyber wellness profile shows the cyber security development through partnership with ITU-IMPACT (ITU, 2012). The case file credits the recommendation that global partnership is essential in cyber policing and security, due to the conceptual structure of cyberspace and the global reach of the criminal activities in it.

The NATO Cooperative Cyber Defence Centre of Excellence is one of the partnerships that aim to build cyber capability, cooperation and information sharing in cyber defence. It was formed in 2008 following the 2007 attack on Estonia. Headquartered in Estonia, it was accredited by NATO in the same year and was recognised worldwide as an International Military Organisation on 28 October 2008. The UK is a full member of the NATO Cooperative Cyber Defence Centre of Excellence and hosted the NATO Summit, at which an Enhanced NATO Cyber Policy was endorsed and the NATO Industry Cyber Partnership was launched in 2014.

The UK is a signatory to the formation of The European Criminal Police Office (Europol) from the 1985 Schengen Agreement; other similar transnational organisations exist such as the International Criminal Police Organisation (INTERPOL), United Nations Police (UNPOL), North Atlantic Trading Organisation (NATO), and The European Network and Information Security Agency (ENISA). These organisations and many more have a dedicated cyber division operating beyond the control of the member states and operate under the supervision of international criminal justice organizations.

An example includes the policies or directives from the European Union (EU). Prior to the Brexit vote and until the UK withdraws from the EU, the 2016 EU Network and Information Security Directive (NISD), which has the objective of harmonising the European approach to combating cyber risk, remains valid across EU states.

Policing and Security Services Unfolding Beyond Government

With the dawn of E-commerce in the 1990s, commercial/ corporate organisations have been compelled to set up their own security department to safeguard their website from malicious misuse. They protect their interests by exercising contractual governance over their employees and clients. This is achieved via software solutions and research by their professional cyber security specialist department.

This concurs with Loader's reference (2000) to the existence of an enhanced and expanding commercial market in security systems and policing services, ranging from the employment by public and private concerns of their own 'in-house' security staff, and the purchasing by individuals and businesses of protective hardware ranging from car and burglar alarms to 'integrated security systems'.

While the above policing occurs within the state, there are other forms of policing occurring beyond the government virtually, provided by the Internet Service Providers (ISPs). The ISPs have a rather fluid status because although they are physically located in a particular jurisdiction, they tend to function transnationally (Wall, 2011).

Governors of Internet Services, namely: Network Infrastructure Providers and Internet Service Providers (ISP), render some form of policing and are categorised as follows:

Access providers

ISPs employ a range of technologies to enable consumers to connect to their network via various means such as dial-up, Digital Subscriber Line (DSL), Broadband wireless access, Cable Modem, Integrated Service Digital Network (ADSN), Asynchronous Transfer Mode (ATM) etc. Each means of access is dependent on the need of the user but all perform the same function of connecting the user to the Internet. They operate a multi-tiered structure consisting of ISPs with levels of hosting capacity.

Hosting ISPs

This group of service providers offer email account services, file transfer protocols (FTP), and web-hosting services. Other services include virtual machines, clouds, or entire physical servers where

customers can run their own custom software or services. Hosting ISPs generally, as the name implies, host websites of businesses or individuals for a contractual set time and cost.

Transit ISPs

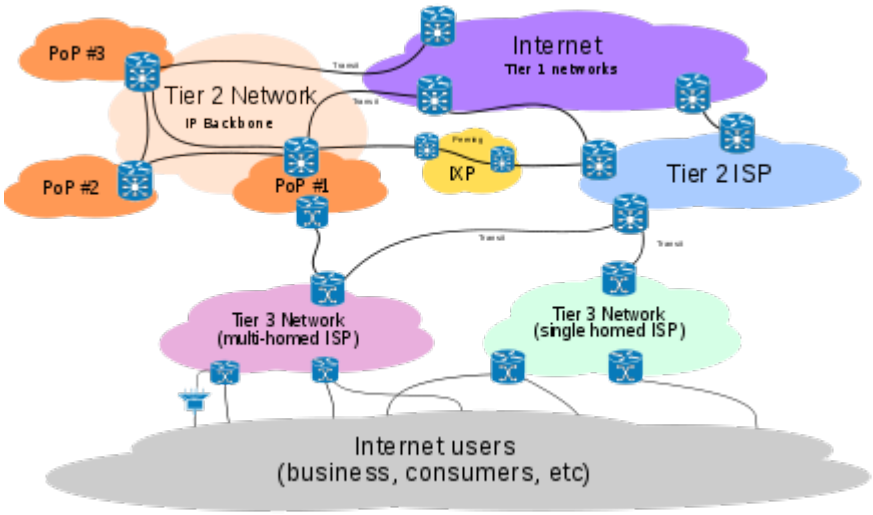
A Transit ISP sits between the Hosting ISP and a larger ISP called an Upstream ISP. Transit ISPs connect to the Upstream ISPs for Internet access and then distributes to the lower Hosting ISP; this connectivity then enables both the Hosting ISP and the Transit ISP to provide access to parts of the Internet that the contracting ISP has no access to on its own.

Technically the ISPs achieve inter-connectivity via more than one point of presence (POP), that the lowest tier on the network is reached. This inter-connectivity leads to peering where multiple networked infrastructures are connected to each other, permitting the routing of data via its nodes. The role of ISPs in policing cybercrime is through contractual agreement both with their clients; the Internet users and the telecommunications providers that are at the supra ordinate ISP Tier.

They can offer effective policing in many ways of which include software solutions to monitor and reduce offending on the Internet such as Spam Filters and other Security systems. They are expected to cooperate with investigations by law enforcement agents as well as adhere to other regulatory demands imposed by the state.

Although ISPs are physically situated in one geographic region, their services are distributed. Therefore, they tend to be governed within distinct geographical jurisdictions. These jurisdictions are further controlled by the law of the countries they are located in. For example, the Internet Service provider Consortium is in the United States of America and the Pan European Internet Service Providers' Association (EURO ISPA) govern the whole of Europe.

Fig 4.1: The Architecture of ISPs (Ferre, 2010)



This thus calls for cooperation across political entities or governments in the countries within these regions and law enforcement agencies and the private sector. Partnerships are already evolving across nations but with increasing involvement of the private sector, it is yet unclear what level of involvement the private sector will be allowed in the criminal justice system.

Indeed there is significant overlapping in Loader‘s categories and this overlap is also evident of the complexity in the UK’s cyber policing. He notes that:

‘These categories are clearly porous ones and no doubt significant overlaps exist between the various policing forms that I have set out. They remain, however, analytically useful in at least two respects. first, to map the contours and component elements of an emerging and loosely coupled ‘network’ of plural policing; They point, secondly, to the diverse problematics of regulation that are brought forth by the advent of plural policing, allowing us in particular to obtain a more adequate grasp of the complex social and institutional dynamics that attend attempts to subject the multiple, differentially powerful bodies that deliver policing to some kind of democratic supervision and control’ (Loader 2000, p328).

With these frameworks it is also possible to bring the decentralised state of the Internet to an eventually less complicated mirage of networks as is being proposed by many scholars, but before this can be achieved, the policing of the Internet with regards to crime will have to follow the nature of the Internet and hence will involve policing across transnational boundaries (Zimmerman, 2014), and the private sector taking up more policing functions. True to the above opinion, cyber policing so far can also be seen to follow the different layers of cyberspace as depicted in Fig 4.2 below.

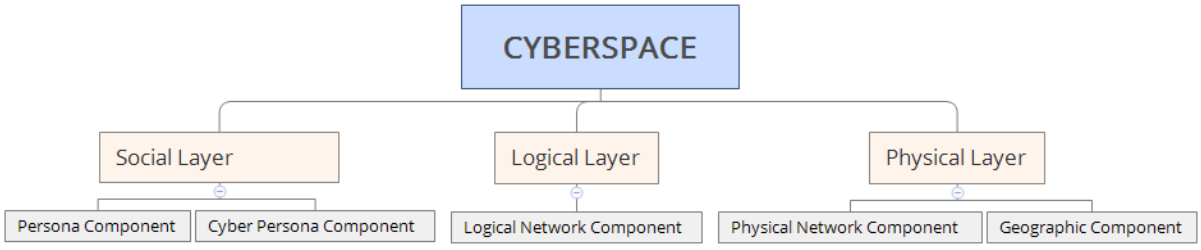
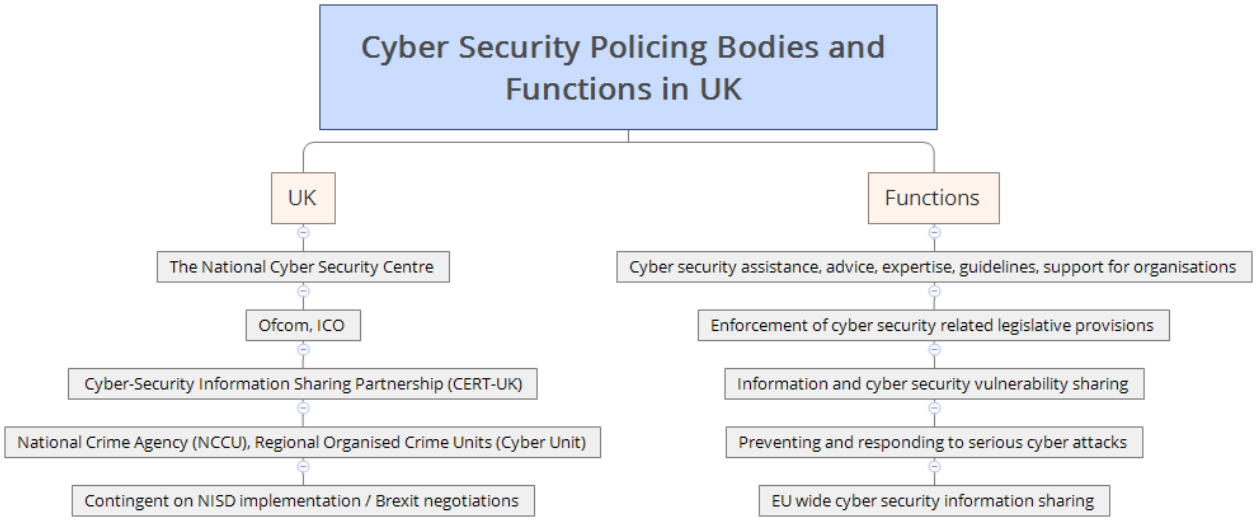


Fig 4.3 shows the different policing bodies, the populations served and sanctions as at 2010 (Wall, 2010, p8). Since this date, significant progress has been made in cyber policing in the UK.

'The Internet's order-maintenance assemblage'

Type (governance providers)	Population served	Sanctions (auspices)
Internet users/user group – including Cyber Angels, Adult sites against Child pornography, spam busters, e-bay	All Internet users within the interest group	Moral censure/cold-shouldering/ lobbying/reporting/activism
Online virtual environment managers and security – for online role playing, game playing, chatrooms, discussion lists, e-auction rooms, cyber worlds	Members of online environments	Removal of access rights, exclusion from the environment when community norms or laws are transgressed
Network infrastructure (ISPs) – Internet Service Providers, ISPs Domain Name Registries	Subscribing users/clients	Withdrawal of Internet service. Introduction of control software such as spam filters or content management
Private (corporate) security- Banks, Telecommunications, Corporate entities	Own private interests/private clients	Withdrawal of services/civil recovery-prosecution
Non-government, non-police hybrids- Internet watch Foundation, CERT, CAUCE	All Internet users	Withdrawal of participation/financial sanctions/reporting to police
Governmental Non-police- Customs excise, Security service, intelligence, Trading standards	All Internet users/business	Financial sanctions/prosecution (civil or criminal)
Government Funded Public police – police forces, national specialist units such as Puce, E-Crime Unit in SOCA (ex-NHTCU), FBI, Local police force cyber capabilities	All Internet users	Criminal prosecution, cautions, warnings (depending on offence)

Fig 4.4 shows the more recent cyber security policing bodies in the UK and their core function (O'Donoghue, 2016). There is realistically an overlap of responsibilities and shows the complex nature of the UK Cyber Security Strategy.



In summary, the chapter has grouped the diverse cyber policing entities involved directly and indirectly with the government to tackle cybercrime using Loader's framework. It appears that core policing duties are gradually being outsourced or taken over by the private policing organisations, and private policing regulation in the UK is not comparable to the regulation imposed on the public police to ensure police accountability. There are criminal justice commissions, independent commissions, police complaints, authorities, royal commissions and internal disciplinary boards or investigative mechanisms and media enquiries undergone on the public police which the private firms are not bound by. Bringing similar control on private policing is highly desirable.

The next chapter looks at partnership in detail. It traces the development of public private partnership (PPP) in the UK. PPP has been adopted in many government projects over the years due to economic constraints. In cyber security, it will be evident that applying PPP while being popularly advocated will be a tricky feat because in previous PPPs, the role of the government in security policy and strategy has been that of the enforcer; with the increasing reliance on the private sector, public private partnership has placed the government in the dual role of enforcer and participant. A delicate balance of this role is ensured in the structure and model of public private partnership adopted. This suggests that there are different models of PPP depending on the participating bodies. In the next chapter, the partnership between the police and the Armed Forces will be explored to draw from lessons learnt and how they can be applied to cyber security strategy where both forces are to work in partnership with other organisations.

Chapter Six

Policing inside, through and by Government

This chapter focuses on the two forces that are involved in policing cyberspace, namely the police force (policing by government) and the Armed Forces (policing inside government). The chapter also delves into different (public to public) partnership that exits between the police and the Armed Forces. From the previous chapter, policing inside government is carried out by state departments employed by the government to police its revenue and expenditure; they offer some form of policing and cyber security as contained in the National Cyber Strategy. Placing the Armed Forces in this category recognises that their role is dictated by the government in power (the incumbent government) and therefore accountable to the government. Their cyber policing role is not as obvious as that of the police force; it is a complex mix, judging by the make-up of the Ministry of Defence and its partners and the relationship with the Government Communication Headquarters (GCHQ).

The police force has from its origin served the citizen and are accountable to the citizens, while the Armed Forces established its civil military co-operation (CIMIC) doctrine in 2003 (Joint Doctrine Publication 3-90 2003). Since then the interaction between the military and civil authorities has grown and expanded with Internet technology.

So how do the Armed Forces police cyberspace and who do they police? A look at the unfolding role of the Armed Forces will help with answering this question.

The initial role of the Armed Forces in the 2011 cyber security strategy was within the role of the MoD, which is:

‘Ensuring that the UK has the capability to protect our interests in cyberspace

- Improving our ability to detect threats in cyberspace
- Expanding our capability to deter and disrupt attacks on the UK’

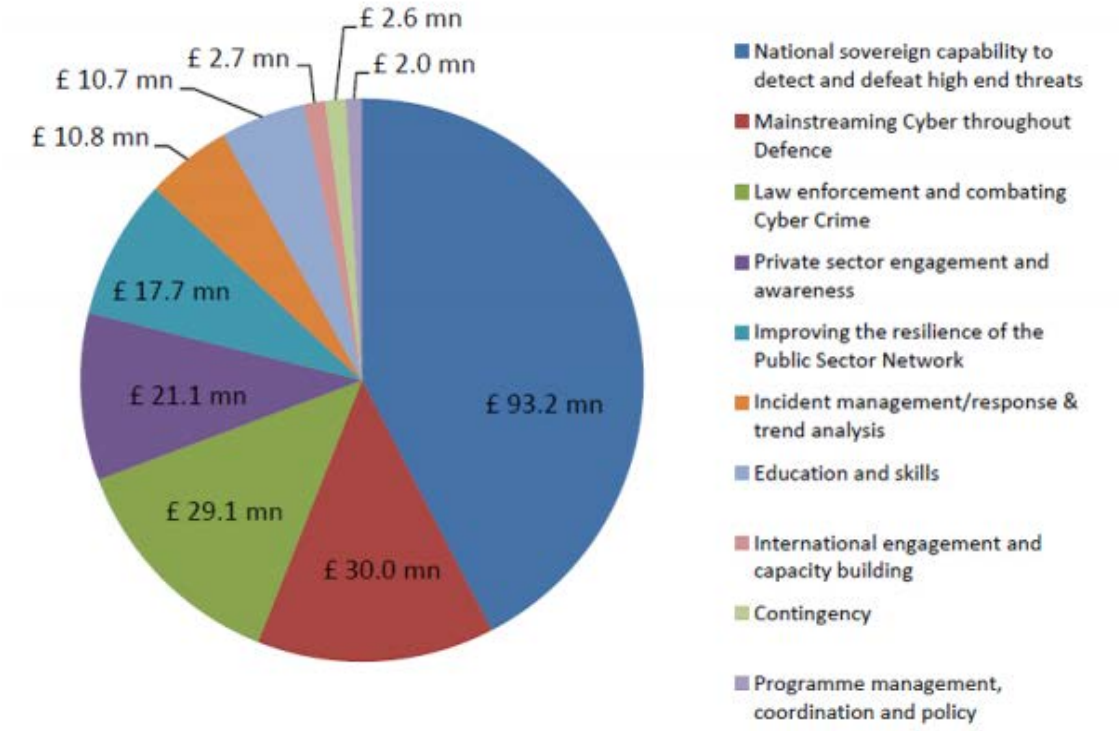
(CSS, 2011, p38)

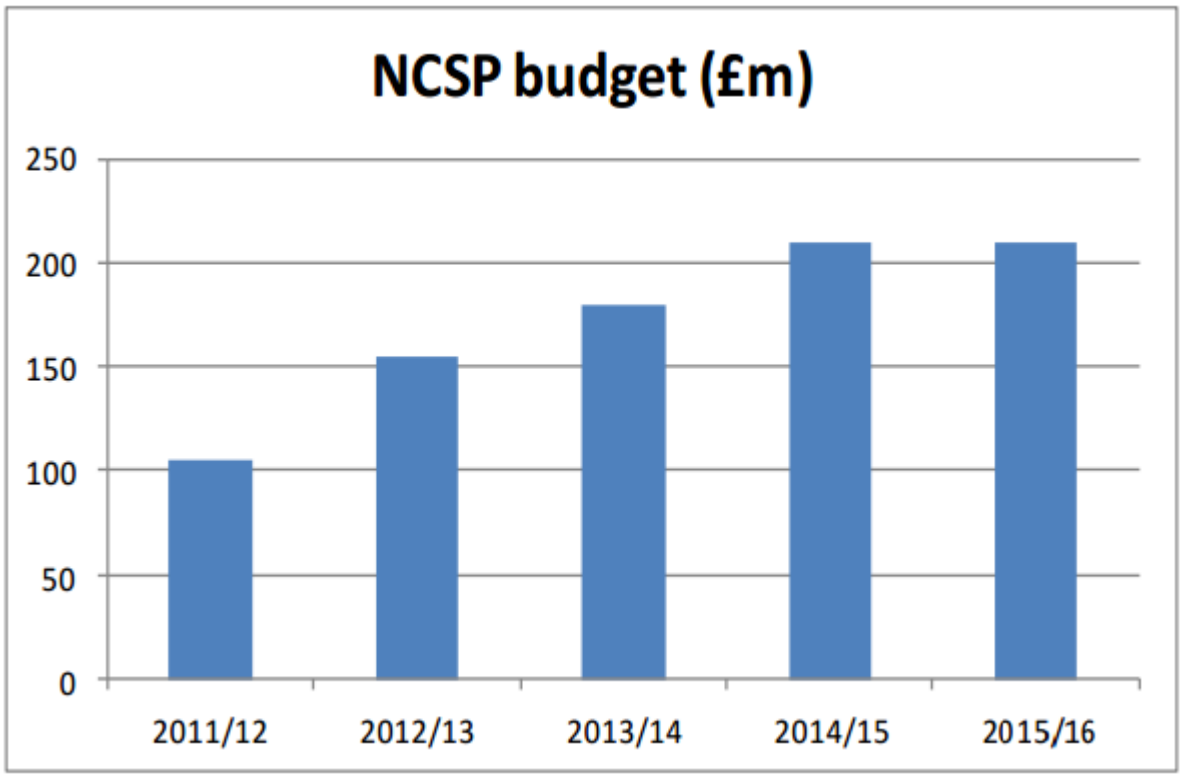
From the above extract, the specific interest or the capability needed for this, or how this can be achieved or which are the lead departments are not mentioned, leading to critics of the strategy labelling it as lacking in conceptual clarity (computerweekly.com, 2011), coupled with a lack of universal consensus on the definition of cyber-weapon or a cyber-attack and what constitutes a cyber-war, the actual role of the Armed Forces remained vague. The House of Commons committee noted that:

‘At present the stated unifying role of the DCOG is more illusory than real, and among its long list of tasks are some which appear to overlap with those of the GOSCC or Information Services and

Systems more generally. We urge the MoD to communicate its cyber-security structures a more comprehensible fashion, setting out strands of work and lines of accountability unambiguously. Only by doing this can we be assured that there is indeed clarity about roles and responsibilities within the MoD and the Armed Forces. We recommend, in particular, that the respective roles of the Chief Information Officer and the Joint Forces Commander are clarified in relation to cyber-security' (House of Common's Sixth Report of Session 2012–13).

It can be assumed that the Armed Forces have a far overriding responsibility in cyberspace than any other state department less GCHQ, and the National Cyber Security Programme (NCSP) budget spending below seems to support this assumption (Cabinet Office, 2014, pp10-11).





Apart from the loosely defined responsibility of the Armed Forces, other sectors that make up the CNI were not explicitly allocated roles, and the strategy for the protection of critical national infrastructure (CNI) became increasingly difficult to analyse as inter-dependency increases between CNI sectors (House of Commons Defence Committee, 2013).

In academia, the role of the military in cyberspace was also being debated and lends affirmation to the earlier assumption. Libicki (2012, p334) brings the debate of the role of the military in defence to encompass every route that threatens the nation including cyberspace, especially in the protection of the nation's critical infrastructure and the defence industrial base. Rid's (2011) article 'Cyber war will not take place' and the counter-argument by Stone (2013) 'Cyber war will take place' both heightened the issue of cyber security and the military perspective.

Also, cyberspace has brought extra meaning to what constitutes the United Kingdom's Critical National Infrastructure (CNI), because prior to the explosion of the Internet, infrastructure are structures and services owned and managed by a country on which its economy relies. But now the core CNI and services are often in the control of foreign investors through the connectivity that links these services to cyberspace, and this makes it difficult for the UK government to have full control of its CNI, making it a more global infrastructure than that of the UK alone. The potential danger of the UK CNI in the hands of foreign and private organisations catalysed the UK authorities to recognise and pronounce the intense high threat level in the second decade of the 21st century, and from 2011 onwards cyber security strategy picked up momentum across the UK's public and private sectors.

It is in the back drop of these teething problems that the MoD tried to forge ahead, and the Defence Cyber Protection Partnership (DCPP) was formed in 2012 with the aim of improving cyber security maturity. The partnership is made up of MoD representatives, 13 prime suppliers and defence industry trade bodies. Prior to the formation of a district defence cyber protection partnership, still in existence are a hybrid of governmental agencies and non-governmental agencies involved in cyber security.

Understanding the organisational issues relating to military cyber-defence capabilities and the role of non-military stakeholders, with emphasis on the interdependence between military cyber-defence and other organisations such as governmental computer emergency response teams, is desirable. Combating cybercrime involves interdependence between the military, the civil police and other private agencies which predictably will involve an overlap of responsibilities. The distinction between the police force and the military both strategically and operationally highlights the complexity of such partnership within the emerging meaning of cyber security from the policing and military perspectives.

Table 5.1 below highlights some of these distinctions:

	MILITARY	POLICE	REMARKS
FUNCTION	Securing the state against external threat through deterrent military action	Controlling crime and maintaining law and order by prevention and apprehension	Except in civil emergencies where both forces work together to restore normalcy
JURISDICTION	EXTERNAL Defends the state against attack from other states	INTERNAL Maintains domestic security and defends and enforces the law within the state's geographical boundaries	Pre-globalisation concept that is now threatened by transnational crime
LEGITIMACY	Legitimacy as dictated by the government in power (the incumbent government)	Legitimacy comes from the people	Gradually democratisation of both forces in the 21st century
ORGANISATIONAL CULTURE	Professional, value-oriented, Rank structured, Collective responsibility	Professional, value-oriented, Rank structured, individual responsibility	

ACCOUNTABILITY	Accountable to the government	Accountable in the law of the state and the people they police	

The MoD has an intelligence doctrine that has been applicable to the three Arms over the years, both in peace time and in conflict (CDS, 2014). The extension of the doctrine to cyberspace or its modification/ new doctrines applicable to cyberspace is gradually becoming the practice. The Law of Armed Conflict is the current doctrine guiding the UK in all cases of conflict that comes under Article 51 of the UN Charter. There is yet to be an internationally contested cyber war, therefore there is no record of any other application of similar doctrine in cyberspace.

'The term 'cyber warfare' is not a legal term or a political concept with a universally agreed definition ... but it may generally be understood to refer to the hostile use of Malware, which is software implemented for the purpose of disrupting the correct operation of computer and network- based systems. There are debates as to when the first 'official' incident of cyber warfare occurred - a Russian pipeline explosion in 1982, allegedly caused by Malware inserted into the pipeline's control software, has been cited as an early example. However, there are doubts as to the veracity of the account' (Chatterjee, 2014).

The police do not have a current doctrine for a similar situation. Analysis of the military and the police reveals certain significant points; both the police and the military have an established chain of command, although the UK police force is decentralised; both forces also have highly sophisticated specialist intelligence personnel, the military are more advanced because of their exposure to international conflict zones outside the UK; the police is restricted to UK geographical boundaries. Also, the military are constantly operating in a continuously changing threat environment, therefore there is a disparity in the level of competencies between the two forces and it is possible that the police internationally will encounter procedures that are different from the practice in their home country, or more so apply procedures that are acceptable in their home country but illegal or different to the country where the cybercrime or offender is located or a national.

Compared to the military, the police force is not deeply rooted in reconnaissance training except for intelligence gathering in the course of a crime investigation, which differs vastly in application to military intelligence and technical ability both in electronic and territorial warfare.

The notion of a multi-talented functional police force in the UK has changed over the years; different policing roles require different capability and accountability to varying authorities. Also, internally in the UK, policing within the constabularies is not uniform. Policing business is conducted differently from one part to another. A notable difference between policing in the UK and other western countries

is the concept of the police as civilians rather than military (Tupman and Tupman, 1999); a concept that is not widely shared across the globe with the majority of nations maintaining a semi-military police force.

'On the whole the notion of the police being civilians in uniform is not one that has been universally accepted by governments on the continent. The police may have had to become civilians in uniforms in many cities, but the distrust governments feel for city populations has led many to maintain a semi-military force as a reserve in the rural areas" (Tupman and Tupman, 1999).

By militarising the police, intervening states may undermine efforts at community policing and send the wrong message to citizens weary of paramilitary forces (Friesendorf, 2012). Pollicising the military holds the risk of degrading war-fighting capabilities.
In Europe, France's Gendarmerie strikes a balance between a civilian police force and a militarised police force. The Gendarmerie blend both extremes of the two forces' characteristics and has been proposed to be more suitable to a globalised society according to Friesendorf (2010), who opines that the hybrid and specialized forces of the Gendarmerie makes them suitable to provide the services which fall within the remit of the traditional police or military. They can be deployed internally and externally in security operations that are usually the domain of the police and the military as separate entities.

The traditional 'police–military divide' has been argued by scholars as blurring in western countries (Campbell and Campbell, 2009). The traditional police-military divide refers to the 'principle of Modern state' (Weber, 1919). The two forces are different in function, accountability, jurisdiction, source of legitimacy, and culture. Andreas and Price (2001, p32) claimed that "one of the most important blurring of traditional boundaries occurring in the post-Cold War era is that between an internally oriented domestic police sphere and an externally oriented military sphere".

As mentioned elsewhere in this paper, globalisation has obscured the distinction between internal and external boundaries. Resultant security issues born out of globalisation include organised crime, terrorism and cybercrime, however the blurring of the police – military divide which has occasioned the police-military partnership which is evident in post-war conflicts where both forces have had to work side by side in peace operations. Rosen (2009, p11) claims that civil military relation is in its third generation, where the differences between military and civil work (police being civilians) have interchanged.

The first and second generation civil-military relations exhibit a divide of 'military' and 'non-military'(civil) status with its attendant characteristics and boundaries. In the face of global disorder or situations that transcend national boundaries such as terrorism, organised crime and cybercrime, the blurring of the divide becomes inevitable.

What is the state of the UK's cyber capability maintained and sustained by both forces? Both forces are empowered to fulfil specific roles but have also found a common ground to work in partnership and consolidate the advantages that each brings. An exploration of the definition and models of public private partnership will shed more light on this complexity (Ziolkowski, 2013), because the success of the national cyber policy advocates close public-private partnership which over the years has assumed different models.

Public to Public Partnership (PPP) – Police and Armed Forces

Civil-military synergies and police–military synergies have a long history in Britain and the US. Early applications in the police-military partnership were in counter-insurgency, peacekeeping and peace building (Mockaitis, 2004; Volker, 2006).

The fight against terrorism is an area that has benefited from partnership between the police and the military, both within the United Kingdom and internationally. NATO, UN and EU peacekeeping forces feature collaboration amongst member states' military and police forces in peacekeeping operations (Nato.int, 2015; Un.org, 2014; European Union, 2015). The Northern Ireland conflict was the setting for one of the UK's peacekeeping operations. The British police and Armed Forces formed the Tasking and Co-ordination Group (TCG) (Charters, 2009). The function of the group was to co-ordinate military and police operational activities in bringing lasting peace and end the conflict at hand. The two forces had to work together for short- and long-term objectives to end the conflict by pooling their resources in a way that maximised the capabilities and resources of both forces.

The UK's revised counter-terrorism strategy (CONTEST) during the 2012 Olympic Games hosted in London was a true test of the success of civil, military and police partnership. The Strategy was revised in 2011 in time for the Olympics. The CONTEST strategy covers all forms of terrorism and is based on four main objectives (Home Office, 2013):

• 'Pursue: to stop terrorist attacks;

• Prevent: to stop people becoming terrorists or supporting terrorism;

• Protect: to strengthen our protection against a terrorist attack; and

• Prepare: to mitigate the impact of a terrorist attack'.

A partnership exists between Avon and Somerset police force and IBM and Lincolnshire police partnership with G4S. The UK police force has an existing ICT policy which the Home Office

Minister Damien Green proposes should be applied to cater for the technological need of each police force in the United Kingdom.

Partnership has also been found in maritime security. The Royal Navy is a key stakeholder in the partnership involving the police, the UK Border Agency, the security service (MI5) and the Department for Transport (DfT) in the 'UK national maritime security programme' (Secretary of State for Defence, 2014).

The partnership is coordinated by the National Maritime Information Centre (NMIC) and the Maritime and Coastguard Agency (MCA). The NMIC is the centre for information communication and based at the military Northwood Headquarters. Other areas where the police have worked in partnership with the military are: crowd control and humanitarian aid.

The National Cyber Strategy offers a joint approach to cyber security involving partnership across different institutions. These institutions are the stakeholders. As previously stated, partnership offers the best possible means of mitigating the risk in cyberspace.

Partnership has been proposed over other means such as Contracting and Out-sourcing. The advantages of these two means abound. Pitched against the current economic downturn and past experiences where each force had worked independently, partnership leverages and reduces cost, creates joint assets and new capabilities and a speedy technological development. Coupled with the fact that most of the infrastructure of cyberspace is owned by private companies, partnership in cyber policing is the best way forward.

There are different models of public private partnership, therefore varying definitions of PPP in the UK.
The Organisation for Economic Co-operation and Development (OECD) of which the UK is a member state, defines PPP as long-term agreements between the government and a private partner whereby the private partner delivers and funds public services using a capital asset, sharing the associated risks (OECD, 2012). PPPs may deliver public services both with regards to infrastructure assets and social assets. OECD principles on PPP guidance does not include projects with rapidly changing technology such as IT of which cyber security aptly fits.

PPP is defined as a contract between the public and private sector to provide services or infrastructure jointly by a mutual and clear specification of responsibilities and risk.

It combines the assets, expertise, risks and responsibilities of both sectors, usually within a legal framework of the country where the partnership is situated along with international law and regulation. The two sectors achieve their goals by maximising the synergy and shared capabilities.

The UK has one of the highest number of public private partnerships and the maturity of the market is evident in its application across a wide-range of sectors such as; the NHS, MoD, education, transport, and housing to mention a few (Parliament of Canada, 2010). It also has its share of failed partnerships and it is the application of lessons learnt over the years that makes current PPP viable across Europe. The application of PPP in policing and law enforcement has proved successful and is still evolving in the cyber area. The success of the PPP market peaked as the barrier to government partnership with the private sector was removed through legislation and economic downtime, making partnership the assured means of project and public service management as opposed to outsourcing or outright contract. A time line of the legislation that transformed PPP in the UK is set out below.

Pre 1992 - Public sector borrowing requirement (PSBR) in the British economy of the early 1990s saw expenditures for the government activities in the public sector of the economy exceed the income, leading to a deficit which the government offsets by borrowing from public funds (Lexicon.ft.com, 2015). This was the favoured means of financing infrastructure by the government. Consequently the government repays the borrowing over the years as the taxes received exceed the amount required for public spending. Either way, the cost of public spending comes only from the government purse.

Maastricht agreement (1992)

Following the United Kingdom's commencement of membership of the European Union in 1973 alongside other European states, further economic integration of the states led to the Maastricht agreement of 1992 (Euro-know.org, 2013). The central feature of the agreement was the incorporation of the European Monetary Union (EMU). The EMU was based on four financial principles of inflation, long-term interest rates, fiscal debt and deficit and exchange rates. The aim of the Union was to harmonise trade and economic relations across member states and as such the EMU imposed restriction on infrastructure investment through strict borrowing limits. As a member state, Britain had to comply with the four criteria despite the pressure it placed on its public borrowing and financing of infrastructure. To meet its social responsibility, the United Kingdom government started the private finance initiative.

1992 - Private finance initiative was the resultant means of financing infrastructure following the Maastricht agreement to reduce public sector borrowing requirement. It was first introduced in the 1992 Autumn Statement by Conservative Chancellor Norman Lamont.

PFI was a means through which the private sector financed major infrastructure projects by lending to the public sector. Operational risk for the infrastructure is passed over to the private sector.

1997 - The Treasury Taskforce

Sir Malcolm Bates reviewed the PFI and made twenty-seven recommendations to streamline and improve delivery of PFI projects (Publications.parliament.uk,). The Treasury Taskforce was one of these recommendations, tasked with restructuring the PFI. There were public services that were viewed to benefit from PFI, and in September 1997 the Taskforce published a series of guidance documents, policy statements, technical notes and case studies to assist government departments to maximise the opportunity that PFI could offer. The lifespan of the task force was two years.

2000 - Partnerships UK (PUK)

In 1999, Sir Malcolm Bates published a second review of PFI and recommended the creation of a permanent organisation that would interface between the government and the private sector. Thus, Partnerships UK (PUK) was formed by the Treasury. PUK was set up as a limited company; the company shares were owned mainly by private companies with interests in PFI, and largely staffed by personnel from financial institutions and management consultancies.
'Partnerships UK (PUK) is a public private partnership which has a unique public sector mission: to support and accelerate the delivery of infrastructure renewal, high quality public services and the efficient use of public assets through better and stronger partnerships between the public and private sectors' (Partnershipsuk.org.uk, 2016).

In March 2001, 51% of PUK was sold to private investors and the remaining 49% was retained by the public sector: 44.6% HM Treasury, 4.4% the Scottish Ministers. The splitting of PUK stakes made it a public private partnership (PPP) (Local Government Chronicle, 2001).
The success of the PPP approach by the UK government lies in the application of a market oriented approach, ensuring that the private public partnership operates according to market principles but under a binding contract within the confines of the law.
Below is the list of private companies involved in providing cyber security services in the UK.

UK Cyber Security Companies (Parker, 2014)

Global Technology Vendors & System Integrators • CSC • IBM • HP • Atos • CGI	Defence Contractors • BAE Systems • Thales • Airbus Defence & Space (Cassidian) • QinetiQ • Raytheon • Lockheed Martin • Northrop Grumman
Major Global Consultancies • KPMG • PWC	Telecoms Operators • BT • EE • Verizon

• Ernst & Young • Deloitte • Gartner	• NTT • Vodafone
Global Technology Vendors • Symantec • McAfee • Check Point • Trend Micro • Kaspersky	University & Administrations • Lancaster University • Royal Holloway University of London • Dstl
IT Security Service Specialists • Regency IT Consulting (Mandiant Partner) • 7SAFE • JustASC • Encryption IT Security & Forensic Services • FireEye	Domestic Technology Vendors • SOPHOS • NEXOR • Intercede • First Cyber Security

The UK government departments concerned with cyber security follow the framework stipulated by the national Cyber Security Strategy. It provides a strategic framework that involves partnership within the UK and internationally. Major government departments, agencies and organisations involved are:

The Office of Cyber Security and Information Assurance (OCSIA), which is a directorate in the Cabinet Office that works collaboratively with the Government's chief information officer and the National Security Council. The directorate provides strategic leadership in UK cyber security issues.

Government Communications Headquarters (GCHQ) works in partnership with government departments such as the MoD, Foreign and Commonwealth Office and law enforcement agencies to protect UK national interests. The Director of GCHQ reports to the Secretary of State for Foreign and Commonwealth Affairs.

CESG, a department within GCHQ, is responsible for the national technical authority for information assurance. It also delivers cyber security advice and support to the UK public sector.

The Centre for the Protection of National Infrastructure (CPNI) works with the security service (MI5) and GCHQ to provide information security advice to business and organisations across the national infrastructure. It aims to reduce the vulnerability through espionage, terrorism and cyber-attack on these organisations in the national infrastructure.

Computer Emergency Response Team UK (CERT UK) is the national-level organisation responsible for cyber response and recovery from attacks across government agencies. It will coordinate and

manage national cyber security incidents, providing a focal point for government departments in the report of and recovery from cyber incidents and be the point of contact for international collaboration. CERT-UK has four main responsibilities within the UK's Cyber Security Strategy (Gov.uk, 2014):

1. National cyber-security incident management
2. Support to critical national infrastructure companies to handle cyber security incidents
3. Promoting cyber-security situational awareness across industry, academia, and the public sector
4. Providing the single international point of contact for co-ordination and collaboration between national CERTs

The Cyber-security Information Sharing Partnership (CiSP) that was formed in 2013 and absorbed into the CERT-UK in 2014, is a collaborative venture between the industry, academia and government to confidentially share cyber threats and vulnerability information. The rationale behind this collaboration is to increase resilience to cyber-attacks, through prevention and application of lessons learnt from previous experiences and also shared capabilities.

The Cyber Security Operations Centre (CSOC) investigates and analyses cyber-attacks on UK networks and provides solutions and means to mitigate future attack. Its job is in cyber forensics and incident response, while the Government Computer Emergency Response Team (GovCERT) deals with the public sector organisations on issues relating to computer security incidents, warnings, alerts, assistance and advice to prevent, reduce, expose and mitigate attacks.

The National Crime Agency was formed in October 2013 to replace the Serious Organised Crime Agency. It also inherited the National Cyber Crime Unit and the Police e-Crime Unit in the fight against organised crime. This is the lead agency in UK law enforcement and works in partnership with other law enforcement agencies in the country.

So far, from the publication of the first cyber strategy through three milestone reviews and up to 2015, the National Cyber Security Strategy should have a high level of standardisation across public and private organisations and government agencies. The question is how comprehensive is the strategy? Are the differing organisations and agencies generally following the strategy faithfully? And does it effectively facilitate international cooperation?

These questions were answered to some extent in the Cybersecurity Capacity Review of the United Kingdom conducted by the Global Cyber Security Capacity Centre. The review found that standardization is yet to be achieved because the strategy has varying metrics across agencies.

‘Another important issue is that differing mandates create a confusion of priorities and it is not clear how to separate responsibilities. As a result, there are different metrics for different aspects of the national security strategy. Additionally, detection of incidents is rather reactive and this is why effective metrics are essential and necessary in order to provide a better understanding of a more proactive capacity’ (Global Cyber Security Capacity Centre, 2016).

The Armed Forces: policing through government

The policing role of the Armed Forces in the National Cyber Strategy is to protect and defend its own systems and networks. Simply put, the Armed Forces in line with the MoD, police the different partner organisations and users of their system through various programmes, partnership, policies and standards which they have to maintain to promote and ensure the security of their system and supply chain. Bearing this responsibility is the Joint Force Command (JFC) which is made up of fourteen organisations including the Defence Cyber Operations Group (DCOG). Its role is to ensure the success of military operations through joint capabilities.

Under the JFC is the office of the Chief of Defence Intelligence (CDI) and which is responsible for defence intelligence, providing defence and its partner agencies with intelligence and assessment. CDI is also responsible for cyber operations.

Also under the office of the JFC is the information systems and services organisation (ISS) which is responsible for cyber defence. ISS is also responsible for strategy, policy and guidance for ICT and information across defence.

The defence cyber security programme

From late 1990s, the Ministry of Defence, which had had a growing dependence on civilian infrastructure whose network security measures and standards are often below that required by defence, began contingent planning to streamline a defence centric network with less dependence on civilian-owned networks. Subsequently, the defence cyber security programme was formulated to integrate cyber into the strategic and operational realms of defence (National Audit Office, 2014). This was to bring the MoD in line with the objectives of the National Cyber Strategy by building a cyber force that is agile and resilient in defence to cyber-attacks while developing and retaining talents.

The MOD is no stranger to private public partnership; starting from the Thatcher administration’s privatisation of the national armament industry (Krahmann, 2010), some of the MoD services have continued to be provided by private companies ranging from equipment, support vehicles, military training (the provision of flying courses to the RAF flight simulators and instructors for the Hawk Synthetic Training Facility in Anglesey in 1998, for instance), to the present evolving cyber security.

A further typical example is the Sponsored Reserves scheme. The Reserved Forces Act of 1996 made provision for the establishment of Sponsored civilians who provide specialist services to the MoD and can be called out to full service to augment the Regular Service forces. Also, their employers enter into contract with the MoD with terms that reflect conditions of employment and release of their employees. Examples are the Mobile Meteorological Unit and the Royal Fleet Auxiliary (RFA). Both are civilian non-fighting components of the Armed Forces and employed by the MoD. Recently, the cyber security specialists are being recruited to form the Cyber Reserved Unit. In 2014, the Unit reached full capability.

PFIs exist under the premise that the private companies retain ownership of the equipment, infrastructure, technical expertise and military service. As a private contract between the MoD and the companies, it cannot be classed as a public responsibility regulated by the government; therefore, the contract is not approved by Parliament.

The European Defence Agency (EDA) is carrying out a study on organisational issues relating to military cyber-defence capabilities and the role of non-military stakeholders, with emphasis on the interdependence between military cyber-defence and other organisations such as governmental computer emergency response teams. It is clear that combating cybercrime will involve interdependence between the Armed Forces, the civil police and other private agencies. The police Corp in the armed forces in combating crime are like any other police force and their role both in the UK and overseas utilize the same concept of partnership in the prevention, reduction and investigation of crime. In fighting cybercrime within the military community, the micro and macro policing element lies with the Military Police and they do not operate in isolation but depend on the partnership of other private agencies.

The Armed Forces Cyber Strategy Stakeholders

The Armed Forces, in order to defend its networks, will mainstream cyber into operations and conduct CAPDEV (Capacity development) in cyber security. The National Cyber Incident Management Plan (NCIMP) held by OCSIA in the Cabinet Office, defines the framework for reporting and escalation of cyber events and all agencies relevant to the nature of the incident are coordinated by COBR if the incident is catastrophic or the potential to be catastrophic.

Defence Cyber Protection Partnership (DCPP)

The Ministry of Defence, GCHQ, and CPNI in partnership with 12 defence contractors form the Cyber Protection Partnership (DCPP) as earlier mentioned. The partnership is part of the requirements towards the UK government’s Cyber Security Strategy. The companies are BAE Systems, BT, Cassidian EADS, CGI, General Dynamics, Hewlett Packard, Lockheed Martin UK, QinetiQ,

Raytheon, Rolls-Royce, Selex ES, and Thales UK. These are prime suppliers of UK defence infrastructure, equipment and services. The partnership will be a forum for the sharing of cyber risks notifications amongst these companies in the supply chain, threat intelligence between and risk-driven approaches to applying cyber security standards.

Part of the government's work towards achieving the goals of the CSS is in developing 'Cyber Essentials', a best practice scheme where defence partners will implement the cyber essentials framework to a high standard and in the process identify a measurements and standards framework and areas of improvement in: 'technical risk assessment; control of removable media; physical security controls; people security (including information security training, roles and responsibilities); compliance with legislation; scanning for vulnerabilities; information security policy; defining information security roles and responsibilities'.

This will culminate in the Cyber Security Model (CSM), a framework that was rolled out to all MOD suppliers from January 2017, with a full launch by April of same year.

DCPP's work will be piloted in selected MoD projects and cascaded across defence.

In summary, partnership in cyber security is both present in national and international levels. The United Kingdom maintains Intra-State and Intra Agency cooperation and cross-border partnerships with ITU -ENISA -TRUSTED Introducer, European CERT Group and NATO. And maintains a national program for sharing cyber security assets within the public sector through OCSIA, as previously mentioned. The next chapter looks at the challenges of policing cybercrime in real time. The police force and the law enforcement agencies are still developing strategies to tackle cybercrime in their day to day affairs. It is important to note that policing cybercrime is just one out of many responsibilities of the police. Policing in the 21st century amid the current financial strain means that resources are scarce and re-training the police force to align strategy, policy and technology becomes a priority.

Chapter Seven Conclusions

Pluralisation of policing as Collaborative Governance

Different theories have emerged in the definition of governance. Public governance involves delivery of government services by private and third sector organizations with a need for collaboration and a community engagement level (Kernaghan, 2009). Rhodes (2009) defined governance as: 'self-organizing, inter organizational networks characterized by interdependence, resource exchange, rules of the game based on trust and significant autonomy from the state' (Rhodes, 1997).

Collaborative governance involves a formal and voluntary engagement between one or more public sectors with a non-public sector or non-state stakeholders in public policy or service.

A collection of definitions of collaborative governance identifies that none of the stakeholders can singularly provide the service or solve the problem (Policyconsensus.org, 2001). Ansell and defined collaborative governance as 'A governing arrangement where one or more public agencies directly engage non-state stakeholders in a collective decision-making process that is formal, consensus-oriented, and deliberative and that aims to make or implement public policy or manage public programs or assets' (Ansell and Gash, 2007).

This fits the analyses from the questionnaire data from a cyber-security partnership context. The applicability and extendibility of the collaborative governance model will find parallels that can be used to harmonise the role of the MoD (Armed Forces) and the police through the eyes of the respondents so that strengths and capabilities are shared and understood.

Analysis of findings with regards to trust

Trust Building – Trust has been defined as "willingness to rely on an exchange partner in whom one has confidence" (Moorman et al., 1993). Morgan and Hunt (1994) felt trust exists "when one party has confidence in an exchange partner's reliability and integrity". Trust, therefore, consists of two components: confidence in ability and intention.

The issue of trust is explored and embedded in the questions on the role of the two stakeholders in the event of an attack and the relationship with partner agencies. Trust, among other factors, affects the willingness of the stakeholders to fully engage in cyber security partnership. The extent of a partner's participation is certifiably a proxy of their perceived trust in the system. This is extended to their overall trust when engaging in cyber security partnership (Lee and Turban, 2001) and therefore their commitment to the partnership.

Trust as a proxy of confidence in the role of the military in the questions ‘Are you aware of specific strategy or policy giving guidance on the role of the military in cyber security strategy’, and ‘The relationship between the military and partner agencies is reflected in the Military Cyber Strategy’, have high score responses in agreement respectively.

Commitment to Partnership in Cyber Strategy

Both the police and the MoD are public organisations with different responsibilities which have been deemed vital in the cyber security strategy. This position places the two organisations in a legitimate opportunity to participate in the partnership without recourse to any alternative differing intention. Ancell and Gash opined that organisations that feel they have a legitimate opportunity to participate are likely to develop a ‘‘commitment to the process’’ (Ansell and Gash, 2007). The level of commitment still varies based on how each entity perceived their role within the NCSS. Both organisations recognise the interdependence of the stakeholder without directly elaborating on the degree of commitment required of other organisations. The police consistently emphasise on the shared ownership of security strategy and an openness and willingness to work with and involve other agencies within the NSS (Greenhalgh, 2015).

Both forces are ambivalent on a joint control of cyber defence. The aim of the question ‘The structural governance suitable to cyber defence should be jointly controlled by the police and MoD’, was to elicit the reaction for the two forces to work jointly on equal par. Drawing from previous joint operations, the lessons learnt and the criticisms that followed suggests that the recommendations to ensure success of joint ventures have not been heeded. Notable is the observation by Gillvary on Military-Police Interaction: the need for specialisation and co-operation in Peace Keeping intelligence. ‘Frequently neither group has sufficient knowledge of the others capacity or capability. This can lead to unrealistic expectations and consequently irritation at the other party’s perceived failure to do something that they were never likely to achieve’ (Gillvray, 2004).

Benefit of the Research

I started this research with the aim to identify the role of the Future force both the Armed Forces and police force in cyber security. This journey has followed the two forces as they unravel the challenges of cyberspace. The police force has set up strategies which are not uniform across the Regional police forces in United Kingdom and depends heavily on the major Cyber units while the Armed Forces concentrate on protecting their own networks. The role of the future force depends heavily on the budget set out by the government for the cyber industry. It appears to be a role that will keep changing within each organisation because cyber security like every other aspect of policing has been influenced by Plural Policing and the overlap of responsibilities makes for the complexities within the National Cyber Security Strategy

The research has some limitations such as funding, number of participants and non availability of restricted materials. however these limitations of the research does not negate its benefit to policing studies as well as personnel studies within the Armed Forces, if cyberspace evolves to be the fifth domain of war in all ramifications. Although the information obtained does not represent the official views of the two forces, the views expressed and inferred from the research data are worth exploring for the future benefit in cyber security studies. Cyber security should be the concern of all, not merely a fraction of specialised forces' members.

Traditionally, police organisations and public prosecution services are well-established organisations with a relatively long life cycle. Like all other organisations, national law enforcement organisations are primarily characterised by stability, continuity and predictability. Their long-term existence is secured by means of a relatively fixed structure, composition and mission. The research will benefit studies in cooperate governance and partnership following the need for partnership and multidisciplinary approaches to the policing of cybercrime. There is a requirement for change across the two forces' organisational culture, perceptions and role. Cybercrime and its policing are so complex that no organisation has sole responsibility or capability to police it.

Future Research

Suggested future research in Cyber Security Strategy are:

Armed Forces future employment model and the feasibility of a cyber-force.

The cost and sustainability of volunteerism in the MoD's cyber-force.

The impact of digital technology on personnel security both in the Armed forces and the police force.

Bilateral collaboration between the Police and the Armed Forces in Cyber security.

The Armed Forces runs different staff feedback mechanisms such as 'Have Your Say' and the 'Armed Forces continuous attitude survey' which all members are encouraged to participate in. These surveys have covered diverse issues of concern in the Armed Forces and can be conducted to analyse cyber issues.

Improved trust relationship between police and the Armed Forces is very vital to building a cyber partnership. The question is how this can be achieved against the organisational culture of the two forces. The Armed Forces should rise above their sense of autonomy in defending the country and its interest and recognise that cyber security has striped this notion away. The police culture in the UK also have an element of autonomy due to its history. The need for a uniformed approach to cyber security is absent, each force conduct their affairs leading to some forces able to embrace the NCSS and some struggling to understand the Strategy. With regards to cyber security, the two forces can be more clear and transparent in their policy and practice across all levels of personnel instead of the notion that Cyber security is for the high ranking officers or specified cyber units.

The evolvement of an actual cyberwar is an interesting dimension for future research in cyber strategy across both forces. Scholars have made a plethora of policing models suitable for cyberspace, but the United Kingdom's police forces are yet to grasp and consolidate a strategy that is standard across the nation, for reasons of organisational structure or capability of personnel. Police forces have started recording and dealing with cybercrimes following the formation of Regional Cybercrime units. Vital statistics from these units can be used to research into the effectiveness of policing, law enforcement and cyber prosecution.

Research in law of armed conflict relevant to a universally accepted cyberwar is yet to emerge. There is still contested stance on cyberwar and Armed Forces deployment in such a war; future research in this area will inform military policy and strategy.

The Armed Forces cites official Secret Acts as the reason for having no publicly available policy or framework on its relationship with other stakeholders in the cyber partnership. A more open approach to cyber security, as the US has, will bring more awareness and understanding to its personnel. The US approach ensures that the general public; including industries and partner agencies all have access to and know the tiers and responsibilities of all participants in the framework. This controlled the overlaps and confusion that was prevalent in the NCSS from the onset and even currently. There is a limited availability of empirical research in this kind of multi-stakeholder partnership. Furthermore,

there is little research into how the Armed Forces and the police collaborate in their roles within the Cyber Security Strategy.

The results of the research have shown, to some extent, the views of members of both forces' personnel on cyber security strategy, and lay a path for future research studies in cyber security partnership. It will also be relevant for both military and police scholars. There is a reason to suggest that the cyber strategy and supporting policies are not clearly understood and appreciated by the respondents, and hence the varying level of comprehension of issues pertaining to the practical application of the strategy. In conclusion, the police and armed forces need a truly transparent platform for partnership in cyber security where their convergence in forward leaning, prevention, reacting to attacks and proactive preparations and measures against attacks are unambiguous and definite.

References

AcqNotes. (2015). Information Technology: Cyberspace. [online] Available at: http://www.acqnotes.com/acqnote/careerfields/cyberspace [Accessed 4 Sep. 2015].

Adair, J. (1983). Effective leadership. Aldershot, Hants, England: Gower.

Alexander, H. (2017). Julian Assange's three-year stay in Ecuadorean embassy has cost taxpayer £11.1m. [online] Telegraph.co.uk. Available at: http://www.telegraph.co.uk/news/worldnews/wikileaks/11685451/Julian-Assanges-three-year-stay-in-Ecuadorean-embassy-has-cost-taxpayer-11.1m.html [Accessed 11 Mar. 2017].

Alimo-Metcalfe, B. and Alban-Metcalfe, R. (2000). Leadership. Heaven can wait. Health Service Journal, 26(9).

Alimo-Metcalfe, B. and Alban-Metcalfe, R. (2001). The development of a new Transformational Leadership Questionnaire. Journal of Occupational and Organizational Psychology, 74(1), pp.1-27.

Alliance, B. (2015). 2015 BSA EU Cybersecurity Dashboard. [online] 2015 BSA EU Cybersecurity

Anderson, R., Dashboard. Available at: http://cybersecurity.bsa.org/countries.html [Accessed 11 Sep. 2015].Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J., Levi, M., Moore, T. and Savage, S., 2013. Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer Berlin Heidelberg.

Ansell, C. and Gash, A. (2007). Collaborative Governance in Theory and Practice. Journal of Public Administration Research and Theory, [online] 18(4), pp.543-571. Available at: http://marphli.pbworks.com/w/file/fetch/55667103/Collaborative_governance_theory.pdf [Accessed 12 Jun. 2015].

Australian Federal Police. (2013). Canada Strategy. [online] Available at: http://www.afp.gov.au/media-centre/speeches/~/media/afp/pdf/l/strategy-canada-02.ashx [Accessed 10 Jun. 2013].

APWG. (2016). *Unifying the Global Response to Cybercrime | APWG*. [online] Available at: http://www.antiphishing.org/ [Accessed 20 Oct. 2016].

Balkin, J. (2007). Cybercrime. New York: New York University Press, p.107.

Bass, B. (1998). Current Developments in Transformational Strategy: Research and Applications. Psychologist Manager Journal. San Francisco

Bayley, D. and Shearing, C. (1996). The Future of Policing. Law & Society Review, 30(3), p.585.

BBC News Online. (2009). | Governments hit by cyber attack. [online] Available at: http://news.bbc.co.uk/1/mobile/technology/8139821.stm [Accessed 7 Aug. 2014].

BBC News. (2013). Cyberbullying law needed, says children's commissioner for Wales - BBC News. [online] Available at: http://www.bbc.com/news/uk-wales-24525491 [Accessed 15 Mar. 2015].

Boels D and Verhage A, (2016) "Plural policing: a State-of-the-Art Review", Policing: An International Journal of Police Strategies & Management, Vol. 39 Issue: 1, pp.2-18

Boyatzis, R, E. (1998) Transforming Qualitative Information: Thematic Analysis and Code development. London: Sage

Boyd, J, (2017). The Strategic Game of ? And ?. [online] Available at: http://www.johnljerz.com/superduper/tlxdownloadsiteMAIN/id934.html [Accessed 12 Mar. 2017].

BBC News. (2013). Is UK doing enough to protect itself from cyber attack? - BBC News. [online] Available at: http://www.bbc.co.uk/news/uk-22338204 [Accessed 9 Aug. 2014].

Brown, B. and Reed Benedict, W. (2002) 'Perceptions of the police', Policing: An International Journal of Police Strategies & Management, 25(3), pp. 543–580. doi: 10.1108/13639510210437032.

Brown, C. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology. [online] K. Jaishankar, pp.Vol. 9 (1). Available at: http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf [Accessed 14 Sep. 2015].

Braun, V and Clarke, V (2006). "Using thematic analysis in psychology". Qualitative Research in Psychology. ***3*** *(2): p93.*

Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology. Qualitative Research in Psychology, 3 (2). pp. 77-101.

Burton, G. (2013). Police prevented from chasing cyber criminals from outside Europe. [online] http://www.computing.co.uk. Available at: http://www.computing.co.uk/ctg/news/2252352/police-prevented-from-chasing-cyber-criminals-from-outside-europe [Accessed 6 Oct. 2014].

Button, M. (2002). Private Policing. Devon: Willan Publishing.

Button, M. (2003). Private security and the policing of quasi-public space. International Journal of the Sociology of Law. 3 1, pp. 22 7-23 7.

Cabinet Office, (2014). The UK Cyber Security Strategy Report on progress – December 2014 Our Forward Plans. London.

Callahan, D. (1990). Dangerous capabilities. New York, NY: HarperCollins.

Cameron, D. (2010). A strong Britain in an age of uncertainty. [Norwich]: Stationery Office.

Campbell, D. and Campbell, K. (2009). Soldiers as Police Officers/ Police Officers as Soldiers: Role Evolution and Revolution in the United States. Armed Forces & Society, 36(2), pp.327-350.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. London: Academic Press.

Castells, M. (2000). The information age. Cambridge, Mass.: Blackwell.

CDS (Chief of Defence Staff) (2014) : http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Organisations/Orgs/DCDC [Accessed 25 Nov. 2016].

Cepik, M., Canabarro, D. and Ferreira, T. (2015). CyberWar Crimes. Computer Law Review International, [online] 16(6), p.2. Available at: http://professor.ufrgs.br/marcocepik/files/cepik__canabarro__borne_-_2015_-_cyberwar.pdf [Accessed 8 Mar. 2017].

Chang, A. (2014). Warring State China's Cybersecurity Strategy. 1st ed. [ebook] Available at: http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf [Accessed 25 Dec. 2015].

Charmaz K and Bryant A (2010). in International Encyclopaedia of Education (Third Edition), Available at: http://www.sciencedirect.com/topics/page/Grounded_theory[Accessed 23 May 2017].

Charmaz, K (2006). Grounded theory: A practical guide through qualitative analysis. Thousand Oaks, California: Sage.

Charters, D. (2009). The Development of British Counter-Insurgency Intelligence. Journal of Conflict Studies, [online] 29. Available at: https://journals.lib.unb.ca/index.php/jcs/article/view/15233/19650 [Accessed 13 Sep. 2015].

Chatterjee, B. (2014). International Law and Cyber Warfare. An agenda for future research. [online] Lancaster: Lancaster University Law School, p.p7. Available at: https://www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/security-lancaster/tallinn_report_final[1].pdf.

Chertoff, M., Lynn, W. and McConnell, M. (2012). China's Cyber Thievery Is National Policy—And Must Be Challenged. [online] The Wall Street Journal. Available at: http://www.wsj.com/articles/SB10001424052970203718504577178832338032176.

Chin, W. (2009). The United Kingdom and the War on Terror: The Breakdown of National and Military Strategy. Contemporary Security Policy, 30(1), pp.125-146.

Clarke, R. (2014). How China Steals Our Secrets. [online] Nytimes.com. Available at: http://www.nytimes.com/2012/04/03/opinion/how-china-steals-our-secrets.html?_r=0 [Accessed 30 Sep. 2015].

Cleveland, H. (1997). Strategy and the Information Revolution. World Academy of Art and Science. Minneapolis, MN.

Cllifi. (2014). Cyber Attacks. [online] Available at: http://cllifi.com/category/cyber/ [Accessed 3 Jun. 2014].

Code of Practice for Research: Promoting Good Practice and Preventing Misconduct – UK Research Integrity Office http://www.ukrio.org/wp-content/uploads/UKRIO-Code-of-Practice-forResearch.pdf (Accessed: 10 May 2016b).

COMPTROLLER AND AUDITOR GENERAL, (2013). The UK cyber security strategy: Landscape review. London: National Audit Office.

Computer Weekly. (2004). Single user costs MoD £10m after allowing worm onto the network. [online] Available at: http://www.computerweekly.com/feature/Single-user-costs-MoD-10m-after-allowing-worm-onto-the-network [Accessed 13 Aug. 2014].

Corera, G. (2012). UK planning 'Cyber Reserve' defence force - BBC News. [online] BBC News. Available at: http://www.bbc.co.uk/news/uk-politics-20578691 [Accessed 19 Oct. 2015].

Cornish, P., Hughes, R. and Livingstone, D. (2009). Cyberspace and the National Security of the United Kingdom - Threats and Responses. A Chatham House Report. [online] Available at: http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0309cyberspace.pdf [Accessed 5 Aug. 2014].

Coughlin, C. (2014). Our enemies are stronger because of Edward Snowden's treacherous betrayal. [online] Telegraph.co.uk. Available at: http://www.telegraph.co.uk/news/uknews/defence/10833862/Our-enemies-are-stronger-because-of-Edward-Snowdens-treacherous-betrayal.html [Accessed 29 Aug. 2015].

Council of Europe, (2004). Organised Crime Situation Report 2004. Focus on the threat of cybercrime. [online] Strasbourg. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf.

Crawford, A. (2006). Networked governance and the post-regulatory state?: Steering, rowing and anchoring the provision of policing and security. *Theoretical Criminology*, 10(4), pp.449-479.

Crawford, A., 'Plural Policing in the UK: Policing Beyond the Police ', in Newburn, T. (ed.) Handbook of Policing (2nd ed.), pp. 147-181, Cullompton: Willan Publishing, 2008.

Crawford, A., 'The Police, Policing and the Future of the "Extended Policing Family"', in J. Brown (ed.) The Future of Policing, pp. 173-190, London: Routledge, 2014.

Creswell, J.W. (2013) Research design: Qualitative, quantitative, and mixed methods approaches. 4th ed. Thousand Oaks: SAGE Publications : SAGE Publications.

Creswell, J.W., Clark, V.P.L. and Vicki Plano-Clark John W Creswell (2006) Designing and conducting mixed methods research. Thousand Oaks, CA: SAGE Publications.

Cross, M. and Shinder, D. (2008). Scene of the cybercrime. Burlington, MA: Syngress Pub.

Cunningham, W.C., Strauchs, J.J. and VanMeter, C.W. (1990) *Private security trends, 1970 to 2000: the Hallcrest report II* (Vol. 2). Boston: Butterworth-Heinemann.

Curtis, S., Gesler, W., Smith, G. and Washburn, S. (2000) 'Approaches to sampling and case selection in qualitative research: Examples in the geography of health', Social Science & Medicine, 50(7-8), pp. 1001–1014. doi: 10.1016/s0277-9536(99)00350-0.

Cybercrime.org.za. (2013). Cybercrime Definition | Cybercrime.org.za | Safety & Security Guide. [online] Available at: https://cybercrime.org.za/definition [Accessed 8 Sep. 2015].

Cybersecurity Policy Making at a Turning Point. (2012). Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. [online] Available at: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [Accessed 1 Dec. 2012].

Deibert, R. and Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. International Political Sociology, 4(1), pp.15-32.

Dobby, J., Anscombe, J. and Tuffin, R., 2004. Police leadership: expectations and impact. London: Home Office.

Doig, A. (2006). Fraud. Cullompton: Willan

Doig, A. and Levi, M. (2009). Inter-agency work and the UK public sector investigation of fraud, 1996–2006: joined-up rhetoric and disjointed reality. Policing and Society, 19(3), pp.199-215.

Dorn, N. and Levi, M. (2007). European Private Security, Corporate Investigation and Military Services: Collective Security, Market Regulation and Structuring the Public Sphere. Policing and Society, 17(3), pp.213-238.

Drinkwater, D. (2015). Met Police chief admits cyber-crime difficulties. [online] SC Magazine UK. Available at: http://www.scmagazineuk.com/met-police-chief-admits-cyber-crime-difficulties/article/424957/ [Accessed 11 Nov. 2015].

Drinkwater, D. (2015). NCCU head: Up-skilling officers on cyber-crime our biggest challenge. [online] SC Magazine UK. Available at: http://www.scmagazineuk.com/nccu-head-up-skilling-officers-on-cyber-crime-our-biggest-challenge/article/427111/ [Accessed 12 Sep. 2015].

DUKE, K. (2002) 'Getting beyond the "official line": Reflections on dilemmas of access, knowledge and power in researching policy networks', Journal of Social Policy, 31(01). doi: 10.1017/s0047279402006505.

Dunlap Jr, C.J. (2005). The thick Green Line: the Growing Involvement of Military Forces in Domestic Law Enforcement, In Tim Newburn (Ed). Policing: Key Readings, (pp786–796). Devon and Portland: Willen Publishing

Dutta, S., 2002. The importance of organizational leadership for creating technology excellence. The Global Information Technology Report 2001–2002.

Electronic Frontier Foundation. (2008). Amicus curiae brief. [online] Available at: https://www.eff.org/node/55467 [Accessed 13 Apr. 2013].

Ellefsen and Van Solms (2010) Home Office, the Local Delivery of Crime Prevention through the Partnership Approach HMSO, London, 1994.

Equalityhumanrights.com. (2015). Article 8: Respect for your private and family life | Equality and Human Rights Commission. [online] Available at: https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life [Accessed 29 Aug. 2015].

Eriksson, J. and Giacomello, G. (2007). International relations and security in the digital age. New York: Routledge.

Etter, B., 2002, February. The challenges of policing cyberspace. In *Proceedings of the NetSafe II Conference*.

Euro-know.org. (2013). A Concise Encyclopaedia of the European Union --M--. [online] Available at: http://www.euro-know.org/europages/dictionary/m.html [Accessed 28 Apr. 2015].

European Parliament. (2011). Defending against cyber attacks. [online] Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611natocyberattacks_/sede150611natocyberattacks_en.pdf [Accessed 14 Oct. 2014].

European Union. (2015). Foreign & Security Policy - European Union website, the official EU website - European Commission. [online] Available at: https://europa.eu/european-union/topics/foreign-security-policy_en [Accessed 13 Sep. 2015].

FireEye Lab, (2017). FireEye Advanced Threat Report: 2013. [online] FireEye. Available at: http://csmres.co.uk/cs.public.upd/article-downloads/fireeye-advanced-threat-report-2013.pdf [Accessed 12 Mar. 2017].

Franke, V., 2006. The peacebuilding dilemma: Civil-military cooperation in stability operations. International Journal of Peace Studies, pp.5-25.

Fraud Act. (2006). [online] p. 35. Available at: http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf [Accessed 26 Sep. 2015].

Friesendorf, C. (2010). The Military and the Fight Against Serious Crime: Lessons from the Balkans. Connections: The Quarterly Journal, 09(3), pp.47-64.

Friesendorf, C. (2012). International Intervention and the Use of Force: Military and Police Roles. SSR, [online] Paper 4. Available at: http://www.dcaf.ch/Publications/International-Intervention-and-the-Use-of-Force-Military-and-Police-Roles.

GARDELS, N. (2010). Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly. New Perspectives Quarterly, [online] 27(2), pp.15-17. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1540-5842.2010.01150.x/full.

Gillvray, M. (2004). Military-Police Interaction: the need for specialisation and co-operation in Peace Keeping intelligence. [online] London. Available at: http://www.oss.net/dynamaster/file_archive/071105/5f76ef27354227c11803b8cbc7e8956e/005 Gillvray UK on Military-Police Interaction.doc [Accessed 21 Jun. 2015].

Gottschalk, P. (2008). Knowledge Management in Policing. New York: Hindawi Pub.

Gov.uk. (2010). UK Council for Child Internet Safety (UKCCIS) - GOV.UK. [online] Available at: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis [Accessed 12 Sep. 2015].

GOV.UK. (2011). The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world. [online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Accessed 24 Sep. 2015].

Gov.uk. (2013). Defence partnership tackles cyber security risks - News stories - GOV.UK. [online] Available at: https://www.gov.uk/government/news/defence-partnership-tackles-cyber-security-risks [Accessed 16 Aug. 2013].

Gov.uk. (2014). UK launches first national CERT - Press releases - GOV.UK. [online] Available at: https://www.gov.uk/government/news/uk-launches-first-national-cert [Accessed 14 Jun. 2014].

Government, H. (2010a) A strong Britain in an age of uncertainty: The national security strategy. London: TSO.

Government, H. (2010b) A strong Britain in an age of uncertainty: The national security strategy. London: TSO.

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles?. Social & Legal Studies, 10(2), pp.243-249.

Gravelle, J. and Rogers, C. (2014). Researching the Police in the 21st Century. Palgrave Macmillan.

Gray, C. (2008). Britain's National Security: Compulsion and Discretion. The RUSI Journal, [online] 153(6). Available at: http://dx.doi.org/10.1080/03071840802670007.

Gray, D (2009) Doing Research in the Real World. (2nd ed.). London: Sage

Greene, J.C., Caracelli, V.J. and Graham, W.F. (1989) 'Toward a conceptual framework for mixed-method evaluation designs', Educational Evaluation And Policy Analysis, 11(3), pp. 255–274. doi: 10.3102/01623737011003255.

Greenhalgh, S. (2015). UK police skill up on cybersecurity to fend off digital crimes. [online] Misco.co.uk. Available at: http://www.misco.co.uk/blog/news/02955/uk-police-skill-up-on-cybersecurity-to-fend-off-digital-crimes [Accessed 18 May 2015].

Grieves, J. (2013). Policing Strategy.

Guest, G (2012). Applied thematic analysis. Thousand Oaks, California: Sage. p. 11

Hall G. (2017) WannaCry: The Role of Government in Cyber-Intrusions. https://www.fairobserver.com/region/europe/wannacry-cybersecurity-uk-news-63110/. Available at (Accessed 20 May 2017)

Haig D. 2010, in International Encyclopaedia of Education (Third Edition), Available at: http://www.sciencedirect.com/topics/page/Grounded_theory[Accessed 23 May 2017].

Hays, J. and Kim, C. (2012). Transforming leadership for the 21st century. [United States]: Xlibris Corporation.

Herrera, G. (2010). International Relations and Security in the Digital Age - Edited by Johan Eriksson and Giampiero Giacomello. Review of Policy Research, 27(1), pp.93-95.

HM Government, (2010). A Strong Britain in an Age of Uncertainty: The National Security Strategy. The Stationery Office, p.Cm 7953.

HM Government, (2010). Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review. [online] Her Majesty's Stationery Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf [Accessed 7 Sep. 2015].

HM Government, (2013). Serious and Organised Crime Strategy. Cm 8715. [online] London: The Stationery Office Limited. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf [Accessed 25 Aug. 2014].

HM Government, (2015). National Security Strategy and Strategic Defence and Security Review 2015. London.

HMIC, (2014). The Strategic Policing Requirement. An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement. [online] London. Available at: http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/2014/04/an-inspection-of-the-arrangements-that-police-forces-have-in-place-to-meet-the-strategic-policing-requirement.pdf [Accessed 25 Aug. 2014].

Home Affairs Committee, (2008). Policing in the 21st Century. London: House of Commons.

Home Office, (2010). Cyber Crime Strategy. London: The Stationery Office.

Home Office, (2012). The Strategic Policing Requirement. London: Home Office.

Home Office, (2013). CONTEST: The United Kingdom's Strategy for Countering Terrorism. LONDON: The Stationery Office.

House of Commons Defence Committee, (2012). Defence and Cyber-Security. [online] London: The Stationery Office. Available at: http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf [Accessed 10 Dec 2016].

House of Commons, (2005). National Crime Squad Annual Report. National Crime Squad. [online] London: The Stationery Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273522/0211.pdf [Accessed 13 Sep. 2014].

House of Commons, (2010). Who does UK National Strategy?. LONDON: The Stationery Office Limited.

http://www.v3.co.uk. (2014). V3 - digital transformation news, analysis and insight. [online] Available at: http://www.v3.co.uk/ [Accessed 15 Jul. 2014].

Hughes, Justin, The Internet and the Persistence of Law. Boston College Law Review, Vol. 43, p. 359, 2003 ; Cardozo Legal Studies Research Paper No. 61. Available at SSRN: https://ssrn.com/abstract=370380 or http://dx.doi.org/10.2139/ssrn.370380

Impact-alliance.org. (2014). Alphabetical List | Countries - IMPACT. [online] Available at: http://impact-alliance.org/home/index.html [Accessed 12 Apr. 2014].

Impact-alliance.org. (2015). Mission & Vision | About Us - IMPACT. [online] Available at: http://impact-alliance.org/aboutus/mission-&-vision.html [Accessed 15 Jul. 2015].

Infosecurity Magazine. (2012). Infosecurity Magazine - Strategy, Insight, Technology. [online] Available at: http://www.infosecurity-magazine.com [Accessed 20 Aug. 2012].

Infosecurity Magazine. (2014). Enterprise Cyber-attacks More than Double in 2013. [online] Available at: http://www.infosecurity-magazine.com/view/37247/enterprise-cyberattacks-more-than-double-in-2013/ [Accessed 18 Aug. 2014].

Internet Watch Foundation. (2013). IWF History. [online] Available at: https://www.iwf.org.uk/about-iwf/iwf-history [Accessed 15 Jan. 2013].

Isper.escwa.un.org. (2014). DRAFT MODEL LAW ON ELECTRONIC EVIDENCE. [online] Available at: http://isper.escwa.un.org/FocusAreas/CyberLegislation/FocusAreas/CyberLegislation/Template/DRAFTMODELLAWONELECTRONICEVIDENCE/tabid/177/language/en-US/Default.aspx [Accessed 29 Sep. 2015].

ITU. (2012). CYBERWELLNESS PROFILE UNITED KINGDOM. [online] Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_Kingdom.pdf [Accessed 12 Sep. 2015].

ITU. (2014). ITU and the UN Agenda. [online] Available at: http://www.itu.int/en/un/Pages/un-agenda.aspx [Accessed 14 Jul. 2015].

ITU. (2015). Overview of ITU's History. [online] Available at: http://www.itu.int/en/history/Pages/ITUsHistory.aspx [Accessed 14 Sep. 2015].

Jewkes, Y. and Yar, M. (2010). Handbook of Internet crime. Cullompton: Willan Publishing.

Johnson, B.R. and Christensen, L.B. (2014) Educational research: Quantitative, qualitative, and mixed approaches. 5th edn. Thousand Oaks, CA: Sage Publications.

Johnson, R.B., Onwuegbuzie, A.J. and Turner, L.A. (2007) 'Toward a definition of mixed methods research', Journal of Mixed Methods Research, 1(2), pp. 112–133. doi: 10.1177/1558689806298224.

Johnston, L. (1992). *The rebirth of private policing*. 1st ed. London: Routledge.

Johnston, L. (1999), 'Private Policing: Uniformity and Diversity', in Mawby, R.I. (end), Policing across the World: Issues for the Twenty first Century, London: UCL Press, 226-238 at 231.

Johnson, A., Chalmers, M., Clarke, M., Codner, M., Fry, R., Omand, D., Rogers, J., Eyal, J., Taylor, T., Louth, J. and Heidenkamp, H. (2011). Wars in peace. 1st ed. London: Royal United Services Institute for Defence Studies.

Jones, T. and Newburn, T. (1998). Private security and public policing. 1st ed. Oxford: Clarendon Press.

Jones, T. and Newburn, T. (2002). The Transformation of Policing? Understanding Current Trends in Policing Systems. British Journal of Criminology, 42(1), pp.129-146.

Jones, T., & Newburn, T. (2006). Understanding plural policing. In T. Jones & T. Newburn (Eds.), Plural

Kadir, R. (2010). The Scope and the Nature of Computer Crimes Statutes - A Critical Comparative Study. [online] German Law Journal. Available at: https://www.germanlawjournal.com/pdfs/Vol11-No6/PDF_Vol_11_No_06_609-632_RM_kadir.pdf [Accessed 8 Sep. 2015].

Kanellis, P. (2006). Digital crime and forensic science in cyberspace. Hershey PA: Idea Group Pub.

Keeling, C. (2013). Waking Shark II. Desktop Cyber Exercise. [online] London. Available at: http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf [Accessed 29 Jun. 2015].

Kernaghan, K. (2009). Moving towards integrated public governance: improving service delivery through community engagement. International Review of Administrative Sciences, 75(2), pp.239-254.

Kerr, I. and Gilbert, D. (2004). INFORMATION ETHICS IN AN ELECTRONIC AGE: CURRENT ISSUES IN AFRICA AND THE WORLD, Thomas Mendina, Johannes Brtiz, eds., McFarland Press, 2004. The Role of ISPs in the Investigation of Cybercrime. [online] p.165. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=907483 [Accessed 18 Sep. 2015].

King, R.D. and Wincup, E. (eds.) (2007a) Doing research on crime and justice. 2nd edn. New York: Oxford University Press.

King, R.D. and Wincup, E. (eds.) (2007b) Doing research on crime and justice. 2nd edn. New York: Oxford University Press.

Kobrin, S. (2001). Territoriality and the Governance of Cyberspace. Journal of International Business Studies, 32(4), pp.687-704.

Koenig, D. (2002). INVESTIGATION OF CYBERCRIME AND TECHNOLOGY-RELATED CRIME. [online] NEIA Associates. Available at: http://www.neiassociates.org/cybercrime-and-technology/.

Krahmann, E. (2010). States, Citizens and the Privatisation of Security. Cambridge: Cambridge University Press, p.73.

Kramer, F., Starr, S. and Wentz, L. (2009). Cyberpower and national security. Washington, D C: Center for Technology and National Security Policy.

Kuehl, D. (2009). The article From Cyberspace to Cyber power: Defining the Problem. Cyberpower and national security, pp.26-28. [online] 1. Available at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf.

Lanchester, J. (2013). The Snowden files: why the British public should be worried about GCHQ. [online] The Guardian. Available at: http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GMGP_UK/G131003L.pdf [Accessed 18 Oct. 2016].

Larned, J. (2012). Becoming More Resilient. [online] FBI. Available at: https://leb.fbi.gov/2012/october/becoming-more-resilient [Accessed 17 Oct. 2014].

Legislation.Gov.UK, (2006). The Fraud Act 2006. London.

Legislation.gov.uk. (1998). Data Protection Act 1998. [online] Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed 8 Sep. 2015].

Leivesley, S. (2016). *Priorities for current policing policy and training: five challenges from cyber space*. [online] Available at: https://www.cifas.org.uk/blogs/leivesleyblog [Accessed 12 Nov. 2016].

Lexicon.ft.com. (2015). Public Sector Borrowing Requirement (PSBR) Definition from Financial Times Lexicon. [online] Available at: http://lexicon.ft.com/Term?term=public-sector-borrowing-requirement--PSBR [Accessed 28 Apr. 2015].

Liddell Hart, B. (1991). Strategy. New York, N.Y., U.S.A.: Meridian.

LLC, P. (2016) TAKING THE NEXT STEP: MIXED METHODS RESEARCH IN ORGANIZATIONAL SYSTEMS. Available at: http://search.proquest.com/openview/9ecbaac0094a59c8bc3a39ea3fb549ef/1?pq-origsite=gscholar (Accessed: 10 May 2016).

Loader, I. (2000). Plural Policing and Democratic Governance. *Social & Legal Studies*, 9(3), pp.323-345.

Local Government Chronicle. (2001). SUCCESSFUL CAPITAL RAISED FOR PARTNERSHIPS UK. [online] Available at: https://www.lgcplus.com/successful-capital-raised-for-partnerships-uk/1345888.article.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S. and Ignatuschtschenko, E. (2013).Comprehensive Study on Cybercrime. [online] UNITED NATIONS OFFICE ON DRUGS AND CRIME. Available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [Accessed 14 Apr. 2015].

Masuda, Y. (1980a). The information society as post-industrial society. Washington, D.C.: World future soc.

Masuda, Y. (1980b). The information society. Tokyo, Japan: Institute for the Information Society.

McConnell International, (2000). Risk E-Business: Seizing the Opportunity of Global E-Readiness. Washington DC: McConnell International.

McCullagh, D. (2011). House panel approves broadened ISP snooping bill. [online] CNET. Available at: https://www.cnet.com/news/house-panel-approves-broadened-isp-snooping-bill/ [Accessed 17 Sep. 2014].

McMillan, R. and Kan, M. (2011). China Denies Role in Reported Government of Canada Hack. [online] PCWorld. Available at: http://www.pcworld.com/article/219906/article.html [Accessed 3 Jun. 2014].

Metropolitan Police (1994): London Drug Forum, Drugs and Community Safety: Promoting a Partnership Approach, Directorate of Public Affairs, London.

Ministry of Defence, (1998). The Strategic Defence Review, Command 3999. London: The Stationary Office.

Ministry of Defence, (2002). The Strategic Defence Review: a New Chapter, Command 5566. London: The Stationary Office.

Ministry of Defence, (2003). Delivering Security in a Changing World: Defence White Paper, Command 6041. London: The Stationary Office.

Ministry of Defence, (2004). Delivering Security in a Changing World: Future Capabilities, Command 6269. London: The Stationary Office.

Ministry of Defence, (2010). Defence Plan 2010 - 2014. London.

Ministry of Defence. (2014). The MOD Private Finance Unit. [online] Available at: https://www.gov.uk/the-mod-private-finance-unit [Accessed 15 Feb. 2015].

Mockaitis, T. (2004). Civil-military cooperation in peace operations: the case of Kosovo. Strategic Studies Institute. [online] Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/pub583.pdf [Accessed 11 Apr. 2012].

Nalla, M. and Newman, G. (1991). Public versus private control: A reassessment. *Journal of Criminal Justice*, 19(6), pp.537-547.

National Audit Office, (2014). Update on the National Cyber Security Programme. [online] London: Comptroller and Auditor General. Available at: https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf [Accessed 2016].

Nationalcrimeagency.gov.uk. (2013). National Crime Agency - Home. [online] Available at: http://www.nationalcrimeagency.gov.uk/ [Accessed 16 Aug. 2013].

Nationalcrimeagency.gov.uk. (2016). National Crime Agency - Home. [online] Available at: / http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file. [Accessed 26 Apr. 2017].

Nato.int. (2015). Operations and missions. [online] Available at: http://www.nato.int/cps/en/natohq/topics_52060.htm [Accessed 15 Jul. 2015].

NATO Bilateral Strategic Command Information Operations Reference Book | Public Intelligence. [online] Available at: https://publicintelligence.net/nato-bi-sc-io-reference/ [Accessed 5 Aug. 2014].

Ncsc.gov.uk. (2015). NCSC Site. [online] Available at: https://www.ncsc.gov.uk/ [Accessed 15 Oct. 2015].

Newburn, T. (2003). Handbook of policing. Cullompton: Willan, p.87.

Newburn, T. (2005). Policing: Key Readings. Cullompton, Devon: Willan Pub., pp.786–796.

News.bbc.co.uk. (2009). BBC NEWS | Asia-Pacific | New 'cyber attacks' hit S Korea. [online] Available at: http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm [Accessed 3 Jun. 2014].

Nielsen, S. (2012). Pursuing Security in Cyberspace: Strategic and Organizational Challenges. Orbis, 56(3), pp.336-356.

Nisbett, C. (2002). New directions in cyber-crime. White Paper. [online] QineticQ. Available at: http://www.qinetiq.com/home/security/information_and_network_security/white_paper_index.Par.0012.File.pdf [Accessed 18 Oct. 2015].

Nissenbaum, H. (2005). Where Computer Security Meets National Security1. Ethics and Information Technology, 7(2), pp.61-73.

NORTON, (2012). 2012 NORTON CYBERCRIME REPORT. [online] Symantec-Norton. Available at: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf [Accessed 6 Jul. 2015].

Norton-Taylor, R. (2007). Titan Rain - how Chinese hackers targeted Whitehall. [online] The Guardian. Available at: http://www.theguardian.com/technology/2007/sep/04/news.internet [Accessed 5 Aug. 2014].

Nye Jr, J.S., 2011. Nuclear lessons for cyber security. AIR UNIV PRESS MAXWELL AFB AL.

Nye, Jr. J. S. (1999). Information Technology and Democratic Governance; democracy.com?: Governance in a Networked World (pp. 1-18). Hollis, New Hampshire: Hollis.

OECD, (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. [online] Available at: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [Accessed 1 Dec. 2012].

OECD, (2012). Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships. [online] Available at: https://www.oecd.org/governance/budgeting/PPP-Recommendation.pdf [Accessed 2016].

Oliver, D.G., Serovich, J.M. and Mason, T.L. (2005) 'Constraints and opportunities with interview transcription: Towards reflection in qualitative research', Social Forces, 84(2), pp. 1273–1289. doi: 10.1353/sof.2006.0023.

Onwuegbuzie, A.J. and Collins, K.M.T. (2007) 'A typology of mixed methods sampling designs in social science research', The Qualitative Report, 12(2), pp. 281–316.

Osinga, F. (2017). Science Strategy War | Theory | History of Wars. [online] Scribd. Available at: https://www.scribd.com/doc/294972409/Science-Strategy-War [Accessed 12 Mar. 2017].

Palmer, D. (2013). Green sets out plans for private sector involvement in more flexible police ICT strategy. [online] http://www.computing.co.uk. Available at: http://www.computing.co.uk/ctg/news/2280267/green-sets-out-plans-for-private-sector-involvement-in-more-flexible-police-ict-strategy [Accessed 6 Oct. 2014].

Parker, J. (2014). UK Cyber Security Business Environment.

Parliament of Canada, (2010). Public-Private Partnerships: why, where, when, and how. Library of parliament research publications.

Partnershipsuk.org.uk. (2016). Partnership. [online] Available at: http://www.partnershipsuk.org.uk.

Pokharel, B. (2006) 'Book review: Bridget Somekh and Cathy Lewin (Eds.) (2005), Research methods in the social Sciences', Economic Journal of Nepal, 29(2). doi: 10.3126/ejon.v29i2.156.

Police Federation. (2015). Review of Policing Final Report. [online] Available at: http:// www.polfed.org/documents/Review_of_Policing_Final_Report.pdf [Accessed 15 Sep. 2015].

Police, M. (2013). Online Crime and Fraud - FALCON - Metropolitan Police Service. [online] Content.met.police.uk. Available at: http://content.met.police.uk/Site/falcon [Accessed 1 Apr. 2013].

Policing: An International Journal of Police Strategies & Management. (1997). American Journal of Police, [online] Volume 1(Issue 3). Available at: http://www.emeraldinsight.com/journals.htm?issn=1363-951X [Accessed 1 Jun. 2014].

Policyconsensus.org. (2001). University Network For Collaborative Governance - Definitions. [online] Available at: http://www.policyconsensus.org/uncg/definitions.html [Accessed 12 Jun. 2015].

Prichard, J. and MacDonald, L. (2004). Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks. Journal of Information Technology Education, 3.

Professional Security. (2016). Cyber crime. [online] Available at: http://www.professionalsecurity.co.uk/news/interviews/cyber-crime-call/ [Accessed 15 Jul. 2014].

Publications.parliament.uk. (2012). Defence and Cyber-security (30th March 2012). [online] Available at: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs01.htm [Accessed 30 Jun. 2015].

Publications.parliament.uk. (n.d.). House of Commons - Treasury - Minutes of Evidence. [online] Available at: http://www.publications.parliament.uk/pa/cm199900/cmselect/cmtreasy/147/0012602.htm.

Pumphrey, C. (2000). TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES. 1st ed. [ebook] p.8. Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/pub224.pdf.

Punch, M. (1989). Researching Police Deviance: A Personal Encounter with the Limitations and Liabilities of Field-Work. The British Journal of Sociology, 40(2), p.177.

Ratcliffe, J. (2008). Intelligence-led policing. Cullompton: Willan.

Recommended Checklist for Researchers – UK Research Integrity Office http://www.ukrio.org/wp-content/uploads/UKRIO-Recommended-Checklistfor-Researchers.pdf (Accessed: 10 May 2016a).

Rhodes, R. (1997). Understanding governance. Buckingham: Open University Press.

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), pp.5-32.

Rid, T. (2013). What War in the Fifth Domain. [online] Available at: Http://kingsofwar.org.uk/2012/08/whatwar-in-the-fifth-domain/ [Accessed 1 Sep. 2014].

Riebling, M. (2006). The New Paradigm: Merging Law Enforcement and Intelligence Strategies. Centre for Policing Terrorism.

Russell, C.K. and Morse, J.M. (1994) 'Critical issues in qualitative research methods', Contemporary Sociology, 23(4), p. 624. doi: 10.2307/2076454.

Sabillon R, Cavaller V and Cano J. 2016. National Cyber Security Strategies: Global Trends in Cyberspace. [ONLINE] Available at: http://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf. [Accessed 10 March 2017].

Saldana, J (2009). The Coding Manual for Qualitative Researchers. Thousand Oaks, California: Sage.

SC Magazine UK. (2014). SC Congress London: Met Police admits cybercrime mistakes. [online] Available at: http://www.scmagazineuk.com/sc-congress-london-met-police-admits-cybercrime-mistakes/article/339316/ [Accessed 23 Mar. 2015].

Schafer, J. (2010). Effective leaders and leadership in policing: traits, assessment, development, and expansion. Policing: An International Journal of Police Strategies & Management, 33(4), pp.644-663.

Schreier, F. (2015). On Cyberwarfare. DCAF HORIZON 2015 WORKING PAPER No.7. [online] Available at: http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf. p10. / [Accessed 23 Dec. 2015].

Schulenberg, J.L. (2007) 'Analysing police Decision-Making: Assessing the application of a Mixed-Method/Mixed-Model research design', International Journal of Social Research Methodology, 10(2), pp. 99–119. doi: 10.1080/13645570701334050.

Secretary of State for Defence, (2014). The UK National Strategy for Maritime Security. London: The Stationary Office.

Secretary of State for the Home Department, (2001). POLICING A NEW CENTURY: A BLUEPRINT FOR REFORM. CM 5326. [online] London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/250905/policing_survey.pdf [Accessed 2 Jun. 2014].

Seth, K. (2010). Evolving Strategies for the enforcement Of Cyberlaws. 1st ed. [ebook] Available at: http://www.karnikaseth.com/evolving-strategies-for-the-enforcement-of-cyberlaws.html [Accessed 1 Aug. 2015].

Shah, S. (2013). Cyber security roundtable: The next steps for government. [online] http://www.computing.co.uk. Available at: http://www.computing.co.uk/ctg/news/2259481/cyber-security-roundtable-the-next-steps-for-government [Accessed 14 Mar. 2014].

Shearing, C. and Stenning, P. (1988). *Private policing*. 1st ed. Newbury Park, Calif.: Sage Publications.

Smith J, Flower P and Larkin M. (2009), Interpretative Phenomenological Analysis: Theory, Method and Research. Sage. Pages 346-347

Sommer, P. (2011). The £650m cyber security blanket | Peter Sommer. [online] the Guardian. Available at: http://www.theguardian.com/global/2011/nov/25/governments-650m-cyber-security-blanket [Accessed 15 Feb. 2012].

South, N. (1988). *Policing for profit*. 1st ed. London: Sage Publications.

Staff, C. (2017). A Brief History of Malware and Cybercrime. [online] CIO. Available at: http://www.cio.com/article/2438631/spyware/a-brief-history-of-malware-and-cybercrime.html [Accessed 8 Mar. 2017].

Strachan, H. (2005). The lost meaning of strategy. Survival, 47(3), pp.33-54.

Strachan, H. (2006). Making strategy: Civil–military relations after Iraq. Survival, 48(3), pp.59-82.

Strachan, H. (2008). Campaign Plans, War Plans and British Defence Policy. The RUSI Journal, 153(6), pp.28-31.

Strachan, H. (2008). Strategy as a Balancing Act. The RUSI Journal, 153(3), pp.6-10.

Strachan, H. (2009). The Strategic Gap in British Defence Policy. Survival, 51(4), pp.49-70.

Sullivan, B. (2004). Police Supervision in the 21st Century: Can Traditional Work Standards and the Contemporary Employee Coexist?. [online] Minnesota. Available at: https://fortress.wa.gov/cjtc/www/administrator/class/692_3.pdf [Accessed 2016].

Sumner, S. (2014). James Brokenshire on the cyber role of the National Crime Agency. [online] http://www.computing.co.uk. Available at: http://www.computing.co.uk/ctg/news/2334335/james-brokenshire-on-the-cyber-role-of-the-national-crime-agency [Accessed 14 Mar. 2014].

Tashakkori, A (2003) Major issues and controversies in the use of mixed methods in the social and behavioral sciences. In: Tashakkori, A, Teddlie, C (eds) Handbook of Mixed Methods in Social & Behavioral Research, Thousand Oaks, CA: SAGE Publications

Tashakkori, A. and Teddlie, C.B. (2010a) Sage handbook of mixed methods in social and behavioral research. Thousand Oaks, CA: SAGE Publications.

Tashakkori, A. and Teddlie, C.B. (2010b) Sage handbook of mixed methods in social and behavioral research. Thousand Oaks, CA: SAGE Publications.

Teddlie, C. and Yu, F. (2007) 'Mixed methods sampling', Journal of Mixed Methods Research, 1(1), pp. 77–100. doi: 10.1177/2345678906292430.

Telegraph.co.uk. (2015). Julian Assange's three-year stay in Ecuadorean embassy has cost taxpayer £11.1m. [online] Available at: http://www.telegraph.co.uk/news/worldnews/wikileaks/11685451/Julian-Assanges-three-year-stay-in-Ecuadorean-embassy-has-cost-taxpayer-11.1m.html [Accessed 20 Jul. 2015].

Terpstra, J.B., Stokkom, B.A.M. and Spreeuwers, R. (2013a) *Who Patrols the Streets?: An International Comparative Study of Plural Policing*. The Hague: Eleven International Publishing.

The Data Protection Act 1998 (Commencement No. 4) Order 2015

The Economist. (2010). War in the fifth domain. [online] Available at: http://www.economist.com/node/16478792 [Accessed 17 Sep. 2015].

The hagueinstituteforglobaljustice.org. (2013). Call for Experts: The Global Governance of Cyberspace – The Hague Institute for Global Justice. [online] Available at: http://www.thehagueinstituteforglobaljustice.org/latest-insights/latest-insights/news-brief/call-for-experts-the-global-governance-of-cyberspace/ [Accessed 14 Oct. 2016].

The White house, (2011). International strategy for cyberspace. Prosperity, Security, and Openness in a Networked World. [online] Washington. Available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf [Accessed 12 Jun. 2013].

The White House. (2010). National cyber incident response plan, [online] Homeland Security. Available at: http://www.federalnewsradio.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf.

Thomas, T. (2014). Creating Cyber Strategists: Escaping the 'DIME' Mnemonic. Defence Studies, [online] 14(4), pp.370-393. Available at: http://dx.doi.org/10.1080/14702436.2014.952522 [Accessed 4 May 2014].

Travis, A. and Williams, Z. (2012). Revealed: government plans for police privatisation. [online] The Guardian. Available at: https://www.theguardian.com/uk/2012/mar/02/police-privatisation-security-firms-crime [Accessed 2 Mar. 2012].

Tupman, B. and Tupman, A. (1999). Policing in Europe. Exeter, England: Intellect.

UK Defence Doctrine, (2014). Joint Doctrine Publication 0-01 (JDP 0-01) (5th Edition). United Kingdom: Ministry of Defence.

Un.org. (2014). Peacekeeping operations. United Nations Peacekeeping. [online] Available at: http://www.un.org/en/peacekeeping/operations [Accessed 13 Sep. 2015].

US Department of Defence, (2011). Department of Defence Strategy for Operating in Cyberspace. [online] Available at: http://archive.defense.gov/news/d20110714cyber.pdf [Accessed 12 Jun. 2013].

US Department of Defence, (2005). Department of Defence Strategy (online) Available at: http://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=2014-06-25-124535-143 [Accessed 12 Jun. 2013].

Veracode. (2015). Is the UK Police Force Keeping up with the Shift to Cybercrime?. [online] Available at: https://www.veracode.com/blog/2015/05/uk-police-force-keeping-shift-cybercrime [Accessed 12 Aug. 2015].

Wall, D. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice and Research, 8(2), pp.183-205.

Wall, D. (2007). Cybercrime. Cambridge: Polity.

Wall, D. (2014). 'High risk' cyber-crime is really a mixed bag of threats. [online] Available at: https://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091[Accessed 12 Aug. 2015].

Wasik, M. (1990). THE COMPUTER MISUSE ACT 1990. CRIMINAL LAW REVIEW, 767-779.

Weber, M. (1919). Politics as a Vocation. [online] Available at: http://anthropos-lab.net/wp/wp-content/uploads/2011/12/Weber-Politics-as-a-Vocation.pdf.

White, J. (2017). U.S. v. Elcom. [online] Digital-law-online.info. Available at: http://digital-law-online.info/cases/62PQ2D1736.htm [Accessed 11 Mar. 2017].

Williamson, T. (2008). The handbook of knowledge-based policing. Chichester, England: John Wiley & Sons.

Wingfield, T.(2000) The Law of Information Conflict: National Security Law in Cyberspace, Aegis Research Corp. p. 17.

Withrow, B.L. (2013) Research methods in crime and justice. New York: Routledge.

Worth, D. (2014). DRIP emergency surveillance bill becomes law but challenges loom. [online] http://www.v3.co.uk. Available at: http://www.v3.co.uk/v3-uk/news/2356058/drip-emergency-surveillance-bill-becomes-law-but-challenges-loom [Accessed 23 Jul. 2014].

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), pp.407-427.

Yar, M. (2006). Cybercrime and society. London: SAGE Publications.

Young, T. (2009). Police chiefs publish first UK e-crime strategy. [online] http://www.computing.co.uk. Available at: http://www.computing.co.uk/ctg/news/1844143/police-chiefs-publish-uk-crime-strategy [Accessed 15 Jul. 2014].

Yukl, G. (1994). Leadership in organizations. Englewood Cliffs, NJ: Prentice Hall.

Zentner, Lynn A. & Klumb, Eric (2003). Donated Resources. Washington, D.C.: U.S. Department of Justice.

Zimmerman, C. (2014). Ten Strategies of a World-Class Cybersecurity Operations Center. MA: The MITRE Corporation.

Ziolkowski, K. (2013). Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. Tallinn: NATO CCD COE.

Online Sources

Adlam, R. and Villiers, P. (2003). Police leadership in the twenty-first century. Philosophy, Doctrine and Developments. Winchester [England]: Waterside Press. Available at:http://www.watersidepress.co.uk/hidden/ss000001.pl?page=search&SS=Robert%20Adlam%20and%20Peter%20Villiers&PR=-1&TB=O&ACTION=Go%21 [Accessed 02 Jul. 2013].

Alkaabi, A., Mohay, G., McCullagh, A. and Chantler, N. (2011). Dealing with the Problem of Cybercrime. Conference Proceedings of 2nd International ICST Conference, on Digital Forensics & Cyber Crime, 4-6 October 2010, Abu Dhabi. [online] Available at: http://eprints.qut.edu.au/38894/1/c38894.pdf.

Amoo, D. and Thomson, N. (2009). *Association of Chief Police Officer of England, Wales & Northern Ireland*. ACPO e-Crime Strategy - Version 1.0. [online] London. Available at: http://www.xact.org.uk/information/downloads/internet/Ecrime_Strategy.pdf [Accessed 17 Sep. 2014].

Army Technology. (2016). UK MoD sets out final tranche of armed forces redundancies. [online] Available at: http://www.army-technology.com/news/newsuk-mod-sets-out-final-tranche-of-armed-forces-redundancies-4293818 [Accessed 2 Nov. 2014].

Arquilla, J. and Ronfeldt, D. (1993). Cyberwar is Coming! | RAND. [online] Rand.org. Available at: http://www.rand.org/pubs/reprints/RP223.html [Accessed 11 Feb. 2012].

BBC News. (2007). BBC NEWS | Europe | Estonia hit by 'Moscow cyber war'. [online] Available at: http://news.bbc.co.uk/1/hi/world/europe/6665145.stm [Accessed 13 Apr. 2013].

Boyd, J. (1987). The Strategic Game of ? and?. [online] Available at: http://www.dnipogo.org/boyd/pdf/strategy.pdf [Accessed 25 May 2014].

Brenner, S. (2007). Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model.Journal of International Commercial Law and Technology, [online] Vol. 2(Issue 2). Available at: http://www.jiclt.com/index.php/jiclt/article/viewDownloadInterstitial/20/19 [Accessed 30 Mar. 2012].

Cabinet Office, (2009). Cyber security strategy of the United Kingdom. safety, security and resilience in cyber space. London: Stationary Office.

Cepik, M., Canabarro, D. and Ferreira, T. (2014). Cyberwar: Clausewitzian Encounters. 1st ed. [ebook] Available at: http://professor.ufrgs.br/marcocepik/files/cepik__canabarro__borne_-_2015_-_cyberwar.pdf [Accessed 12 Sep. 2014].

Chik, W. (2006). Computer Crime, Cyber Crime and Challenges to Criminal Law Making in the New Global Information Society. A Critical Comparative Study of the Adequacies of Computer Crime and Cyber Crime Legislation in the United States, the United Kingdom and Singapore. Paper presented at the VI Computer Law World Conference, Edinburgh, Scotland, and UK. (2006)

Computer Weekly. (2011). UK cybersecurity strategy a bit thin on details, say critics. [online] Available at: http://www.computerweekly.com/news/2240111584/Analysis-UK-Cyber-Security-Strategy-a-bit-thin-on-details-say-critics [Accessed 15 Sep. 2012].

CONVENTION ON CYBERCRIME. (2001). European Treaty Series - No. 185. [online] Budapest: Council of Europe. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 4 Apr. 2013].

Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2011). Cyber Security and the UK's Critical National Infrastructure. A Chatham House Report. London: Chatham House.

Cybercrime. (2013). Action against Cybercrime. [online] Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp [Accessed 30 May. 2013].

Cyber-rights.org. (1997). Cyber-Rights & Cyber-Liberties (UK) Report, Who Watches the Watchmen. [online] Available at: http://www.cyber-rights.org/watchmen.htm [Accessed 26 Oct. 2015].

DETICA, (2011). THE COST OF CYBER CRIME. A DETICA REPORT IN PARTNERSHIP WITH THE OFFICE OF CYBER SECURITY AND INFORMATION ASSURANCE IN THE CABINET OFFICE. [online] London: Cabinet Office. Available at: http://www.iwar.org.uk/ecoespionage/resources/cost-of-cybercrime/full-report.pdf [Accessed 5 Apr. 2013].

Digital-law-online.info. (2002). *U.S. v. Elcom*. [online] Available at: http://digital-law-online.info/cases/62PQ2D1736.htm [Accessed 9 Sep. 2015].

ELITE Group. (2005). Aligning and Sustaining IT Infrastructure for Business Benefit. [online] Available at: http://elite.bcs.org/090605.html [Accessed 6 Feb. 2014].

Enisa.europa.eu. (2015). European Public Private Partnership for Resilience (EP3R) — ENISA. [online] Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r [Accessed 10 Feb. 2015].

Eurim.org.uk. (2015). EURIM - the Information Society Alliance - home page. [online] Available at: http://www.eurim.org.uk [Accessed 31 Jan. 2015].

European CEO. (2012). University College Dublin: Fighting cyber crime. [online] Available at: http://www.europeanceo.com/finance/cyber-threats-and-solutions/ [Accessed 1 Apr. 2013].

Ferre, L. (2010). Internet Connectivity Distribution & Core. [image] Available at: https://commons.wikimedia.org/wiki/File:Internet_Connectivity_Distribution_%26_Core.svg [Accessed 4 Apr. 2012].

Friesendorf, C. (2010). The Military and the Fight Against Serious Crime: Lessons from the Balkans. *Connections: The Quarterly Journal*, 09(3), pp.47-64.

Geist, M. (2003). Cyberlaw 2.0. [online] Lawdigitalcommons.bc.edu. Available at: http://lawdigitalcommons.bc.edu/bclr/vol44/iss2/3 [Accessed 28 Sep. 2015].

Gercke, M. (2008). Council of Europe Guidelines for the Cooperation Between LEAs and ISPs Against Cybercrime. Computer Law Review International, [online] 9(4). Available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf [Accessed 30 May 2013].

Gercke, M. (2008). Council of Europe Guidelines for the Cooperation Between LEAs and ISPs Against Cybercrime. Computer Law Review International, [online] 9(4). Available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf [Accessed 30 May 2013].

Gesetze-im-internet.de. (2013). GERMAN CRIMINAL CODE. [online] Available at: http://www.gesetze-im-internet.de/englisch_stgb/ [Accessed 30 Aug. 2015].

Globalsecurity.org. (2005). The National Defense Strategy of The United States of America. [online] Available at: http://www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm [Accessed 12 Jul. 2012].

Gov.uk. (1995). The 7 principles of public life - GOV.UK. [online] Available at: https://www.gov.uk/government/publications/the-7-principles-of-public-life/the-7-principles-of-public-life--2 [Accessed 1 Jun. 2013].

GOV.UK. (2014). Defence Engagement Strategy. [online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73171/defence_engagement_ strategy.pdf [Accessed 21 Sep. 2015].

Gov.uk. (2014). Global Strategic Trends out to 2045 - Publications - GOV.UK. [online] Available at: https://www.gov.uk/government/publications/global-strategic-trends-out-to-2045 [Accessed 21 Sep. 2015].

GOV.UK. (2014). The Joint Doctrine Publication 0-01 UK Defence Doctrine. [online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf [Accessed 21 Sep. 2015].

Gov.uk. (2015). How defence works: the defence operating model - Publications - GOV.UK. [online] Available at: https://www.gov.uk/government/publications/how-defence-works-the-defence-operating-model [Accessed 21 Sep. 2015].

Home Office, (2010). Cyber Crime Strategy. London: The Stationery Office.Available at:http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf [Accessed on 02 April 2012]

Hughes, J. (2003). The Internet and the Persistence of Law. 1st ed. [ebook] Available at: http://lawdigitalcommons.bc.edu/bclr/vol44/iss2/4/ [Accessed 15 Jul. 2013].

ITU. (2013). Legislation. [online] Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx [Accessed 18 Mar. 2013].

Itu.int. (2003). The WSIS Geneva Plan of Action. [online] Available at: http://www.itu.int/net/wsis/docs/geneva/official/poa.html.

ITV News. (2014). ITV News - 5,300 Army jobs to be cut. [online] Available at: http://www.itv.com/news/story/2013-01-22/ministry-of-defence-to-announce-army-job-cuts/ [Accessed 12 May 2014].

Kaspersen, H. (2009). Cybercrime and internet jurisdiction. Project on Cybercrime. [online] Available at:

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7.

l'Europe, C. (2004). Convention on Cybercrime – Details of treaty No. 185. [online] Bureau des Traités. Available at: http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185 [Accessed 12 Jul. 2013].

McCusker, R. (2007). Transnational organised cyber crime: distinguishing threat from reality. Crime, Law and Social Change, 46(4-5), pp.257-273.

Ministry of Defence, (2012). The MOD Private Finance Unit. Military recruitment, training and operations. [online] Available at: https://www.gov.uk/guidance/the-mod-private-finance-unit [Accessed 15 Feb. 2015].

Mitchell, M. and Casey, J. (2007). Police leadership and management. Annandale, NSW: Federation Press.

OECD. (2005). Task Force on Spam: SPAM ISSUES IN DEVELOPING COUNTRIES. [online] Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf [Accessed 10 Apr. 2013].

Policing: An International Journal of Police Strategies & Management. (1997). American Journal of Police, [online] Volume 1(Issue 3). Available at: http://www.emeraldinsight.com/journals.htm?issn=1363-951X [Accessed 1 Jun. 2014].

Schjolberg, S. (2003). The Legal Framework – Unauthorized access to Computer Systems. Penal Legislation in 44 Countries, 2003. [online] Available at: https://www.mosstingrett.no/info/legal.html

Schjolberg, S. (2010). A Cyberspace Treaty - A United Nations Convention Or Protocol on Cybersecurity and Cybercrime. Twelfth United Nations Congress On Crime Prevention and Criminal Justice. [online] Available at: http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf [Accessed 5 Apr. 2013].

Schreier, F. (2015). On Cyberwarfare. DCAF HORIZON 2015 working paper, No. 7.

Siegel, P., and Leiper, R. (2004) GP views of their management and referral of psychological problems: A qualitative study. Psychology and Psychotherapy 77 (3): 279-295

Sommer, P. (2011). The £650m cyber security blanket | Peter Sommer. [online] The Guardian. Available at: https://www.theguardian.com/global/2011/nov/25/governments-650m-cyber-security-blanket [Accessed 15 Feb. 2012].

Tabansky, L. (2012). Cybercrime: A National Security Issue?. Military and Strategic Affairs, [online] 4(3). Available at: http://www.inss.org.il/uploadImages/systemFiles/MASA4-3Engd_Tabansky.pdf [Accessed 1 April. 2015].

THE WHITE HOUSE, (2011). INTER NATIONA L STR ATEGY FOR CYBERSPACE - Prosperity, Security, and Openness in a Networked World. Washington. Available at:http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf [Accessed 12 June 2013]

US Department of Defence, (2011). Department of Defence Strategy for Operating in Cyberspace. [online] Available at: http://archive.defense.gov/news/d20110714cyber.pdf [Accessed 12 Jun. 2013].

APPENDIXES

London foi.team@cabinet-office.gsi.gov.uk SW1A 2HQ www.cabinet office.gov.uk

Chika Onugha
esiowuchikaodi@hotmail.com

FOI Reference: FOI320570
19/2/2015

Dear Chika Onugha

I refer to your request where you asked:

Under the freedom of information act I am requesting an electronic copy of the following information and documents.

1. For each year, between 2009 and 2013, how many cyber-attacks were made against the police database.

2. And how many were successful.

3. For each year, between 2009 and 2015, how many cyber-attacks made against the MOD.

4. And how many were successful.

5. The role of the MOD under the Cyber Security Strategy.

6. (Capacity development) of cyber report of the MOD from 2010 - 2015.

7. An electronic copy of The National Cyber Incident Management Plan (NCIMP)

Thank you for your email of 25 January 2015 requesting information under the terms of the Freedom of Information Act.

You requested information about how many cyber-attacks were made against the police database and how many were successful between 2009 and 2013. This part of your request is unclear as you do not state which police database this refers to. Please could you specify the name of the police database.

I confirm that information about the numbers of cyber-attacks made against the MOD between 2009 and 2015 and how many were successful is held. All of this information has been withheld under the exemptions: Section 24(1) (National Security); Section 26(1)(a) and (b) (Defence) and Section 31(1)(a) (Law Enforcement) of the Freedom of Information Act

The information that you have requested is exempt under section 24(1) of the Freedom of Information Act, which exempts information from disclosure if its exemption is required for the purpose of safeguarding national security. By virtue of section 17(4) we are not obliged to give any explanation of why this exemption applies because to do so would involve the disclosure of information which would itself be exempt. Section 24 is a qualified exemption and I have considered whether the balance of the public interest favours releasing or withholding this information. The Cabinet Office recognises there is a general public interest in openness in public affairs in order to ensure that the public are able to scrutinise the manner in which public

authorities reach important decisions. This makes for greater accountability, increases public confidence in government decision-making and helps to encourage greater public engagement with political life. There is also a public interest in disclosure of information relating to cyber-attacks. I have weighed these public interests against a very strong public interest in safeguarding national security. I believe it would not be in the interest of the UK's national security for the Cabinet Office to provide this information. Taking into account all the circumstances of this case, I have determined that the balance of the public interest favours withholding this information.

Sections 26(1)(a) and (b) have been applied because knowledge of the number of cyber-attacks against MOD's IT systems being detected, their success and the nature of any information stolen could reveal to an adversary the cyber defence capabilities employed by the MOD. Release of such information could enable adversaries to deduce how to circumvent our cyber defence capabilities. Their ability to conduct damage assessments on any attacks they might have conducted would be enhanced, as would evaluation of the effectiveness of UK defences, or components of those defences, against cyber threats. Release of such material could thus increase the risk of a successful attack on MOD computers, with the risk of further information being consequently released which could further compromise the defence of the UK. For these reasons I have set the level of prejudice against release of the exempted information at the higher level of "would" rather than "would be likely to". Section 26 is a qualified exemption and I have considered whether the balance of the public interest favours releasing or withholding this information. There is a general public interest in disclosure of information and I recognise that openness in government may increase public trust in and engagement with the government. There is a definite public interest in members of the public being able to understand the defence of the country. I have weighed these public interests against a strong public interest in the government maintaining a robust national defence capability and in not disclosing information that would prejudice this capability. Taking into account all the circumstances of this case, I have determined that the balance of the public interest favours withholding this information.

Additionally, the Information you have requested is exempt under section 31(1)(a) of the Freedom of Information Act. This exemption protects information if its disclosure under this Act would, or would be likely to prejudice the prevention or detection of crime. By virtue of section 17(4) we are not obliged to give any explanation of why this exemption applies because to do so would involve the disclosure of information which would itself be exempt. Section 31 is a qualified exemption and I have considered whether the balance of the public interest favours disclosing or withholding this information. There is a general public interest in

openness. I also recognise that there is a public interest in understanding the number of cyber-attacks on public departments. These public interests have to be weighed against a stronger public interest in the effectiveness of law enforcement. The Cabinet Office takes the view that disclosure of this information would prejudice the effectiveness of the enforcement of the law. It would not be in the interest of the UK's national security for departments to provide information about the number of attacks against their IT systems as this would enable individuals to deduce how successful the UK is in detecting these attacks. Confirming exactly what information is held could assist someone in determining the effectiveness of the UK in detecting such attacks. Taking into account all the circumstances of this case, I have concluded that the balance of the public interest favours withholding this information. You requested information about the role of the MOD under the Cyber Security
Strategy. This information is already available in the public domain and is available at: www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-3years-on. Of particular interest to you will be "The UK Cyber Security Strategy – Report on Progress and Forward Plans" document: www.gov.uk/government/publications/national-cyber-security-strategy-2014-progressand-forward-plans.

I was unclear what information you are requesting when you state "(Capacity development) of cyber report of the MOD from 2010 – 2015". This information might be held by the Ministry of Defence, so you may wish to submit a more fully explained request to the Ministry of Defence.

Lastly, you requested an electronic copy of the National Cyber Incident Management
Plan (NCIMP). The Cabinet Office intends to publish the NCIMP later in the year. The Information you have requested is being withheld as it is exempt under section 22(1) of the Freedom of Information Act. Section 22(1) protects information intended for future publication.

Section 22 is a qualified exemption and I have considered whether the balance of the public interest favours maintaining the exemption in section 22(1) or disclosing the information. The Cabinet Office recognises there is a general public interest in disclosure and the fact that openness in government may increase public trust in and engagement with the government. I also recognise there is a public interest in evaluating the NCIMP. On the other hand, disclosure of the information requested now would delay the publication of the NCIMP and there is a stronger public interest in the timely publication of the NCIMP. Taking into account all the circumstances of the case, I have determined that the balance of the public interest favours withholding this information.

If you have any queries about this letter, please contact the FOI team. Please remember to quote the reference number above in any future communications.

If you are unhappy with the service you have received in relation to your request or wish to request an internal review, you should write to:

Roger Smethurst
Head of Knowledge and Information Management
Cabinet Office
1 Horse Guards Road
London
SW1A 2HQ

email: foi-team@cabinetoffice.gov.uk

You should note that the Cabinet Office will not normally accept an application for internal review if it is received more than two months after the date that the reply was issued.

If you are not content with the outcome of your internal review, you may apply directly to the Information Commissioner for a decision. Generally, the Commissioner cannot make a decision unless you have exhausted the complaints procedure provided by Cabinet Office. The Information Commissioner can be contacted at:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely

FOI Team
Cabinet Office

Re: Prof Doc: Research Ethics

KF

Klaus Fischer <k.fischer@londonmet.ac.uk>

Ethics Approval Email

Reply

Wed 05/03/2014, 09:03

You;

Tara Young (T.Young@londonmet.ac.uk);

Nicholas Ridley (n.ridley@londonmet.ac.uk);

+1 more

PHD

Dear Chikaodi,

Thank you for submitting your revised research ethics application via your supervisor. I am pleased to tell you that we are satisfied with your adjustments and research ethics approval is hereby given.

Godd luck with your research which looks important.

Best wishes,

Klaus

Appendix 2 - PC 2

No	QUESTIONS	RESPONSE	REMARK
1	Looking at the effects of the pluralisation of policing, what is the role of the police with regards to the national security strategy especially cyber? How does it work. What areas have the police collaborated with other policing agencies and partner agencies like the banks and ISPs; MOD?	The police as well as their primary role are one of the key stakeholders in the NCSS. The role of investigating cybercrime with partner agencies and safe guarding the police computer system is our main remit. The police force has a labyrinth of partners of which the MOD is one.	
2	What frame work is employed for categorizing cyber incidents? Is the framework uniform across policing agencies and widely available to officers?	This is still ongoing as the scope of crime survey data is expanding to include cybercrimes. Currently in place is a tiered system starting with the local, national and international levels. There are also specialist units that work across these tiers. As a developing area of study, uniformity is hard to define due to the autonomy of each force but the framework exists. How it is adhered to is up to respective forces and the nature of the crime. Overlaps will always exist	.
3	What are the rules for escalation of cyber incidents and is the MOD involved, also what other agencies are involved?	.fighting and policing cybercrime is a joint role involving other agencies. Global and national incidents are dealt by GCHQ, NCA and MOD	
4	What is the nature of Police military relationship in cyber strategy (if any)?	There is no strict or restricted role for both forces however military police partnership exists in many operations such as peace keeping and when and if a need to work together in cyber related incident, both	

		forces are by law expected to collaborate. Areas like infrastructure and equipment sharing.	
5	What percentage of your workforce received or attended cyber security courses in the past six months? How many are qualified cyber forensic. Is cyber a mandatory course or restricted to certain department. Ask of manpower, recruiting etc?	Currently the figures are not consolidated but it depends on what aspect of cyber security. Cyber security is now a mandatory course for new intakes. As we speak, courses are running across the country.	
6	Does cyber-attacks reports, threat and vulnerability information released to the public and partner agencies reflect reality. To what extent is this information tactically restricted bearing in mind the cross government collaboration scheme and EU policies?	National security dictates that certain data are withheld. So the extent of information released is security dependant. Also certain Acts restrict public availability of certain data. No comment.	
7	Is the relationship between the police and partner agencies reflected in the policing Cyber Strategy?	As always each police force have local and national agencies they work with. Yes. Such relationships I expect are mutually understood amongst partners.	
8	What areas or points in policing do you think that a future Cyber strategy should focus on? On the other hand are there areas that were ignored in the CSS.	More funding, issues of human rights, etc. Existing barriers to collaboration… Time and tier pose a few barriers.	

Appendix 3

Table Of Codes

PC 1	PC 2	PC 3	AF 1	AF 2	AF 3	AF 4	AF 5
Cyber reports	**Role/responsibility).**	Plural partners	Role	Public partnership	Role	Role	NSS
Guidelines	**Role/ other responsibility).**	Difference in roles	Public partnership	Role	Guideline	Guideline	Restricted guideline
Plural partners	Partnership	Restricted framework	Willingness to work	Vital role	Restricted guideline	Restricted guideline	Reluctance to comment
No strict framework	Cybercrime category	Levels of crime referral	Recognised partner	Wide scope	Complexity of cyber	Reluctance to comment	Other guideline
Levels of responsibility	Absence of uniformity	Plural policing/partnership	Plural partners	Guideline	Mandatory knowledge	Plural agencies	Vague response
Partnership/agencies	Framework	Overlap of responsibility	Complex	Restricted guideline	Negative past influence	Defence policy	Future research
Lead organisation	Autonomy of forces	Level of crime referral	Plural partners	Single reference?	Criticism of current strategy	Future research	Deficiencies of current strategy
Areas of training	**Role/responsibility).**	Difference in roles	Guideline	Reluctance to comment	Guideline	Role	
Partnership Reluctance to comment	**Role/ other responsibility).**	Areas of collaboration	Restricted guideline	Plural partners	Criticism of current strategy	Guideline	
Partnership	Partnership	Partnership	Reluctance to comment further	NCIMP the only guideline or strategy		Restricted guideline	
Collaboration n	Cybercrime category	Ongoing specialist training	Plural partners	Area lacking awareness	Future research	Reluctance to comment	
Future research	Absence of uniformity	Funding limiting	Uncomprehensive		Military	Plural agencie	

		training	strategy		doctrine	s	
	Framework	Restricted information	Future research areas	Future research area		Defence policy	
	Autonomy of forces	Cyber rime assessment still novel		Challenges to organisations		Future research	
	Overlap of responsibilities	Collaboration is statutory					
	Partner agencies	Plural partnership mandatory					
	Levels of responsibility	Barriers to collaboration exists					
	Existing partnership	Barriers to collaboration					
	Cyber security training	NSS should be all inclusive					
	Restricted information	Future research					
	Reluctance to comment	Cyber security approach is capitalist					
	Plural partners						
	Future research						

Appendix 4

Phrase frequency

Some top phrases containing 8 words (without punctuation marks)	**Occurrences**
The ncimp is available on a need to	5
Is available on a need to know basis	5
Ncimp is available on a need to know	5
The UK in the event of any threat	4
The mod has the task of defending the	4
Mod has the task of defending the UK	4
Has the task of defending the UK in	4
The task of defending the UK in the	4
Task of defending the UK in the event	4
Defending the UK in the event of any	4
Of defending the UK in the event of	4
The police in the event of a cyber	2
Ncimp is the umbrella that connects all relevant	2
Police and the ncimp is the umbrella that	2
The police and the ncimp is the umbrella	2
And the ncimp is the umbrella that connects	2
The ncimp is the umbrella that connects all	2
Police in the event of a cyber attack	2
Some top phrases containing 7 words (without punctuation marks)	**Occurrences**
Available on a need to know basis	5
Is available on a need to know	5
Ncimp is available on a need to	5
The national cyber incident management plan ncimp	5
The ncimp is available on a need	5
Has the task of defending the UK	4
Up in the event of any threat	4
Mod has the task of defending the	4
The mod has the task of defending	4
The UK in the event of any	4
Task of defending the UK in the	4
Defending the UK in the event of	4
The task of defending the UK in	4
Of defending the UK in the event	4
Police and the ncimp is the umbrella	2
The police and the ncimp is the	2

Appendix 5

Absence of uniformity

Area lacking awareness

Areas of collaboration

Areas of training

Autonomy of forces

Barriers to collaboration

Challenges to organisations

Voluntary Collaboration

Statutory Collaboration is

Complexity of cyber

Criticism of current strategy

Cyber reports

Cyber crime assessment still novel

Cyber security approach is capitalist

Cyber security training

Cybercrime category

Defence policy

Deficiencies of current strategy

Difference in roles

Existing partnership

Framework

Funding limiting training

Future research area

Future stability

Grey areas

Guidelines

Is NCIMP the only guideline or strategy?

Lead organisation

Level of crime referral

Levels of responsibility

List role

Mandatory knowledge

Military doctrine

Negative past influence

No strict framework

NSS should be all inclusive

Ongoing specialist training

Other guidelines

Overlap of responsibility

Partner agencies

Partnership

Partnership/agencies

Plural agencies

Plural partners

Plural partnership mandatory

Plural policing/partnership

Public partnership

Recognised partner

Reluctance to comment

Restricted framework

Restricted guideline

Restricted information

Role

Role/ other responsibility

Single reference

Uncomprehensive strategy

Vague response

Vital role

Wide scope

Willingness to work

Appendix 6

Code	Source	Source Material:
collective responsibility	AF1-CODED.docx	However, I would argue that the military, police, government companies and individuals all have a role to play
plural partners	AF1-CODED.docx	Source Material:
		I would argue that the military, police, government companies and individuals all have a role to play. Cyberspace doesn't have physical boundaries so you can't defend it in a traditional military matter. All have a responsibility to defend cyberspace where they interact and use it.
NICMP	AF1-CODED.docx	Source Material:
		The National Cyber Incident Management Plan (NCIMP).The NCIMP is available on a need to know basis.
Guideline but cannot elaborate	AF1-CODED.docx	Source Material:
		The NCIMP contains guideline on this
Areas not clearly dealt with in the strategy	AF1-CODED.docx	Source Material:
		Areas like the defence of CNI (SCADA, Banking etc), corporation/info sharing with PAGs and multi-national agencies, what limits sovereignty places on DCO-RA when CNE/A originates overseas.
Role	AF 3 -coded.docx	Source Material:
		The MOD has the task of defending the UK in the event of any threat.
NICMP	AF 3 -coded.docx	Source Material:

		The National Cyber Incident Management Plan (NCIMP).The NCIMP is available on a need to know basis.
Mixed feelings about cybersecurity	AF 3 -coded.docx	Source Material:
		Cyber means all things to all men. There is much hype, some of which is justified, some of it not. However in the Information Age, having a competence in Cyber warfare is a must for all commanders. Unfortunately I sense Industrial Age warfare still dominates much of the military's doctrinal thinking.
Deficiencies in the strategy	AF 3 -coded.docx	Source Material:
		Any strategy needs to have a clear, deliverable 'end-state', with balanced 'ways' and 'means' to achieve. Sadly most strategies are high on ambition, and delusional on 'ways' and 'means'. So my focus would be on achieving something that is actually deliverable and not just a pipe-dream
criticism of cyber strategy	AF 3 -coded.docx	Source Material:
		The strategy must highlight who is responsible for what – too many 2* think they own the issue which is creating friction and empire building. The need for better doctrine – the JDP isn't well written
Role	AF 4-CODED.docx	Source Material:
		The MOD has the task of defending the UK in the event of any threat.
NICMP	AF 4-CODED.docx	Source Material:
		The National Cyber Incident Management Plan (NCIMP).The NCIMP is available on a need to know basis.
reluctant to elaborate	AF 4-CODED.docx	Source Material:

		It depends on what type of incident recorded. Cannot comment.
Deficiencies in the strategy	AF 4-CODED.docx	Source Material:
		National vulnerability impact assessment to assure appropriate proportional effort is expended on defence (thus denying adversaries easy access through national weak points, regardless of ownership)
Role	AF 2- coded.docx	Source Material:
		The MOD has the task of defending the UK in the event of any threat with other government bodies like industry partners the police in the event of a cyber-attack. It's wider than MOD, who have a vital part to play, but are not lead Dept.
plural partners	AF 2- coded.docx	Source Material:
		The MOD has the task of defending the UK in the event of any threat with other government bodies like industry partners the police in the event of a cyber-attack. It's wider than MOD, who have a vital part to play, but are not lead Dept.
Public partnership	AF 2- coded.docx	Source Material:
		The MOD has the task of defending the UK in the event of any threat with other government bodies like industry partners the police in the event of a cyber-attack. It's wider than MOD, who have a vital part to play, but are not lead Dept.
NICMP	AF 2- coded.docx	Source Material:
		The National Cyber Incident Management Plan (NCIMP).The NCIMP is available on a need to know basis.
reluctant to elaborate	AF 2- coded.docx	Source Material:

		The NCIMP contains guideline on this. No comments.
plural partners	AF 2- coded.docx	Source Material:
		There is a relationship that exists among agencies not only the police and the NCIMP is the umbrella that connects all relevant partners.
Relationship with agencies contained in NCIMP	AF 2- coded.docx	Source Material:
		There is a relationship that exists among agencies not only the police and the NCIMP is the umbrella that connects all relevant partners.
Deficiencies in the strategy	AF 2- coded.docx	Source Material:
		There is still more to come. Cyber is a new challenge for many organisations and the MOD is not exempt.
complexity of cyberspace	AF 2- coded.docx	Source Material:
		There is still more to come. Cyber is a new challenge for many organisations and the MOD is not exempt.
Deficiencies in the strategy	AF 2- coded.docx	Source Material:
		The relationship between military mission critical assets and the network. The value of information within the MOD. The value and subsequent criticality of applications and networked enabled platforms.
NICMP	AF 5-CODED.docx	Source Material:
		The National Cyber Incident Management Plan (NCIMP).The NCIMP is available on a need to know basis.
NICMP	AF 5-CODED.docx	Source Material:
		As laid down in the NCIMP and any Defence policy release for such purpose.

Deficiencies in the strategy	AF 5-CODED.docx	Source Material:
		Provision of an integrated National Capability. CONOPs for delivery of tactical cyber effects in a Joint Operational Area (JOA). Authorities to execute cyber missions at the tactical level. The industrial base needed to provide the enduring national and tactical capabilities. A concept of operations (CONOPs) outlines the Commanders intent regarding an operation.
plural partners	PC 1-CODE.docx	Source Material:
		Currently there is no specialist department in this force. Cybercrime is referred to CERT UK or resolved through the ACTPOOL.The force has collaborated with MOD, as well as other organisations on issues of personal protection, infrastructure protection, and public crime.
Levels of Responsibility	PC 1-CODE.docx	Source Material:
		The force works with NCA and MI5. Officers will link up with regional cyber unit and partners with full collaboration on both side. When participation is required.
plural partners	PC 1-CODE.docx	Source Material:
		There is no framework that we strictly adhere to. Local cybercrime are dealt with locally while crimes that have a national scope are delegated to a higher authority. Yes
local and national levels of crime reporting	PC 1-CODE.docx	Source Material:
		There is no framework that we strictly adhere to. Local cybercrime are dealt with locally while crimes that have a national scope are delegated to a higher authority. Yes

Levels of Responsibility	PC 1-CODE.docx	Source Material:
		MI5 provides liaisons in areas of collaboration, infrastructure and equipment sharing
plural partners	PC 1-CODE.docx	Source Material:
		Current policy and training has been given on personal protection. There is no priority for a specialist course as the need is met through partner agencies.
Public partnership	PC 1-CODE.docx	Source Material:
		Current policy and training has been given on personal protection. There is no priority for a specialist course as the need is met through partner agencies.
Cyber Crime records and reports	PC 1-CODE.docx	Source Material:
		There is significant caution on the reported figures. The media paints disproportionate information. Accurate figures are still being collated. Can't comment on that due to security implications.
reluctant to elaborate	PC 1-CODE.docx	Source Material:
		There is significant caution on the reported figures. The media paints disproportionate information. Accurate figures are still being collated. Can't comment on that due to security implications.
Deficiencies in the strategy	PC 1-CODE.docx	Source Material:
		Media collaboration, victim support group. Legislation on cyber forensics such as removal of malicious data online.
plural partners	PC 2-CODE.docx	Source Material:

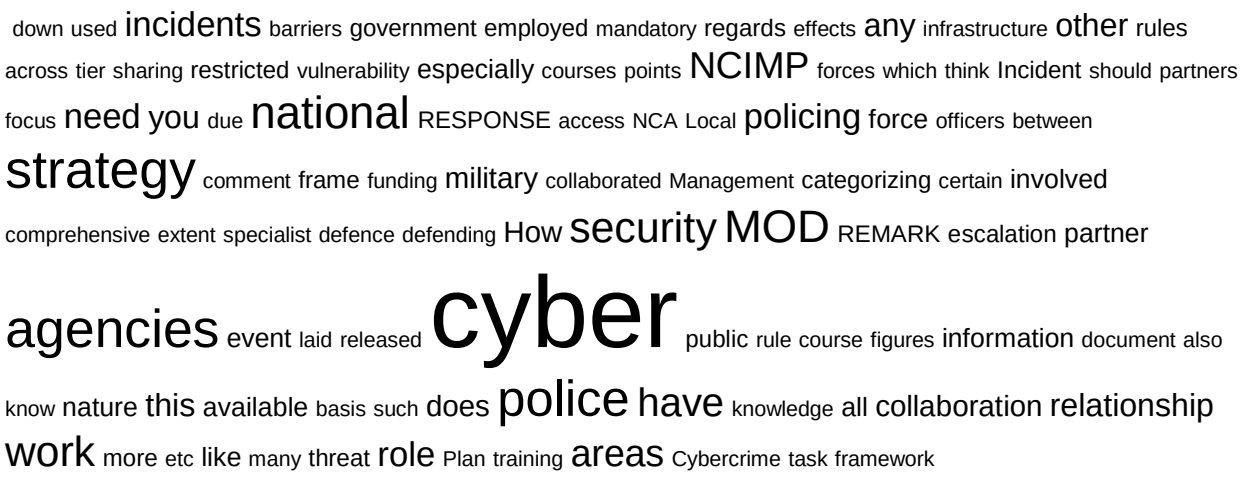
		The police as well as their primary role are one of the key stakeholders in the NCSS. The role of investigating cybercrime with partner agencies and safe guarding the police computer system is our main remit. The police force has a labyrinth of partners of which the MOD is one.
Levels of Responsibility	PC 2-CODE.docx	Source Material:
		This is still ongoing as the scope of crime survey data is expanding to include cybercrimes. Currently in place is a tiered system starting with the local, national and international levels. There are also specialist units that work across these tiers. As a developing area of study, uniformity is hard to define due to the autonomy of each force but the framework exists. How it is adhered to is up to respective forces and the nature of the crime. Overlaps will always exist
local and national levels of crime reporting	PC 2-CODE.docx	Source Material:
		fighting and policing cybercrime is a joint role involving other agencies. Global and national incidents are dealt by GCHQ, NCA and MOD
Role	PC 2-CODE.docx	Source Material:
		There is no strict or restricted role for both forces however military police partnership exists in many operations such as peace keeping and when and if a need to work together in cyber related incident, both forces are by law expected to collaborate. Areas like infrastructure and equipment sharing.
reluctant to elaborate	PC 2-CODE.docx	Source Material:

		National security dictates that certain data are withheld. So the extent of information released is security dependant. Also certain Acts restrict public availability of certain data. No comment.
plural partners	PC 2-CODE.docx	Source Material:
		As always each police force have local and national agencies they work with. Yes. Such relationships I expect are mutually understood amongst partners.
Deficiencies in the strategy	PC 2-CODE.docx	Source Material:
		More funding, issues of human rights, etc. Existing barriers to collaboration… Time and tier pose a few barriers.
Role	PC 3-CODED.docx	Source Material:
		The force has little to do with MOD due to the difference in role however there is a good relationship with other agencies depending on the level of the offence and in view of the police role as an instrument of the state. .
local and national levels of crime reporting	PC 3-CODED.docx	Source Material:
		There is a consistent framework in use which is restricted. The breakdown is a 3321 tier. Tier 1. Highest, global and National Cyber Security. Tier 2 Dealt with by NCA and Tier 3 is the remit of Local police forces. There is a grey area of overlap but progress is being made to fine tune this.
local and national levels of crime reporting	PC 3-CODED.docx	Source Material:
		Like the previous question; depending on the scale. GCHQ, NCA and MOD deal with Tier 1.
Role	PC 3-CODED.docx	Source Material:

		Very limited due to difference in roles. Areas of collaboration include infrastructure and equipment sharing. Note that the MOD does not have operational independence. Collaboration is possible were the need arises.
Relationship with agencies contained in NCIMP	PC 3-CODED.docx	Source Material:
		Yes. The Cyber Strategy is National and like mentioned, collaboration is a statutory duty. But there are known barriers to collaboration which we have touched on already.
Deficiencies in the strategy	PC 3-CODED.docx	Source Material:
		Key thing here is that the strategy should be all inclusive down to the citizens on the street. Priority should be reassessed. Funding made available. Other issues are the commercial interest and capitalist base in the cyber industry should be addressed. There are disparate areas that make up cyber security strategy in need of harmonisation.

Appendix 7a

Word Cloud



Appendix 7b

WORD FREQUENCY

WORDS	OCCURRENCES	FREQUENCY	
CYBER	25	1.66	
NCIMP	18	1.19	
NATIONAL	17	1.13	
POLICE	13	0.86	
MOD	13	0.86	
NEED	11	0.73	
AGENCIES	11	0.73	
COLLABORATION	9	0.6	
SECURITY	8	0.53	
ROLE	8	0.53	
FORCE	8	0.53	
INCIDENT	8	0.53	
MILITARY	6	0.4	
AREAS	6	0.4	
TIER	6	0.4	
AVAILABLE	6	0.4	
EVENT	6	0.4	
STRATEGY	6	0.4	
INFORMATION	6	0.4	
UK	5	0.33	
FUNDING	5	0.33	
TRAINING	5	0.33	
KNOW	5	0.33	
PLAN	5	0.33	
BASIS	5	0.33	
PARTNERS	5	0.33	
MEANS	5	0.33	
SPECIALIST	5	0.33	
DEFENCE	5	0.33	
MANAGEMENT	5	0.33	
WE	4	0.27	
TASK	4	0.27	
GOVERNMENT	4	0.27	
BARRIERS	4	0.27	
FORCES	4	0.27	
PUBLIC	4	0.27	
CRIME	4	0.27	
SHARING	4	0.27	
THREAT	4	0.27	
DATA	4	0.27	
INFRASTRUCTURE	4	0.27	
FIGURES	4	0.27	
CYBERCRIME	4	0.27	
NCA	4	0.27	
WORK	4	0.27	
COMMENT	4	0.27	

Appendix 8 – Thematic Table

Main Theme and Subthemes	Extract and location
The Role in NSS • Collaborative Governance • Partnership	• The MOD has the task of defending the UK in the event of any threat with other government bodies like industry partners the police in the event of a cyber-attack. It's wider than MOD, who have a vital part to play, but are not lead Dept.(AFI 2 Q1) • The police as well as their primary role are one of the key stakeholders in the NCSS. The role of investigating cybercrime with partner agencies and safe guarding the police computer system is our main remit. The police force has a labyrinth of partners of which the MOD is one.(PFI 2 Q1)
Levels or Responsibility • Definite Areas • Official Secret Act • Blurring of Boundaries	• Currently in place is a tiered system starting with the local, national and international levels (PFI 2 Q2) • The National Cyber Incident Management Plan (NCIMP).The NCIMP is available on a need to know basis. (AFI 1,2,3,45 Q2) • As a developing area of study, uniformity is hard to define due to the autonomy of each force but the framework exists. How it is adhered to is up to respective forces and the nature of the crime. Overlaps will always exist (PI2 Q2)
Pluralization of policing • Diverse policing?	All references above