
John Iles

Technical Report
RHUL–MA–2014– 5
01 September 2014

www.ma.rhul.ac.uk/tech

Supervisor: John Austen

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date:
Table of Contents

Table of Contents ................................................................. 2
List of figures & tables ........................................................... 3
List of abbreviations & acronyms ............................................. 4
Authors Notes and definition of ‘Cyber’ and ‘Cyber Security’ ........ 6
Executive Summary ................................................................... 7

Chapter 1 - The National Cyber Security Threat .......................... 8
Section 1.1 - Cyber Security: Threat, Source & Impact ............... 8
1.1.1 Cyber Security Threat Model ........................................ 8
1.1.2 Threat Sources ............................................................ 9
1.1.3 Impact of Cyber-Attack ............................................... 9
1.1.4 Cyber Threat Areas and UK Law .................................. 10
1.1.5 Cyber Crime ............................................................... 10
1.1.6 Cyber Warfare, Espionage & Terrorism ........................ 11
Section 1.2 - ‘Cyber Crime’ ..................................................... 12
1.2.1 Setting the scene ....................................................... 12
1.2.2 Traditional Crime vs. Cyber Crime ............................... 12
1.2.3 Cyber Crime Terminology .......................................... 13
1.2.4 Fundamentals of cyber crime ...................................... 14
Section 1.3 - Cyber Warfare, Espionage and Terrorism ............. 15
1.3.1 Setting the Scene and Terminology ............................... 15
1.3.2 Cyber Warfare ........................................................... 18
1.3.3 Cyber Espionage ........................................................ 23
1.3.4 Cyber Terrorism ........................................................ 28
1.3.5 Concluding Remarks ................................................ 29

Chapter 2 - The Government Response ..................................... 30
Section 2.1 - UK Government Cyber Security Strategy ............. 30
2.1.1 Background and Strategic Objectives ............................ 30
2.1.2 Content of the National Cyber Security Strategy .......... 30
2.1.3 The National Security Strategy 2010 (NSS 2010) ........... 31
2.1.4 The Strategic Defence and Security Review 2010 (SDSR 2010) 32
2.1.5 The 2009 National Cyber Security Strategy ................. 33
2.1.6 Cyber Crime Strategy 2010 ......................................... 33
2.1.7 Historic Documents .................................................. 34
Section 2.2 - Discussion and Analysis .................................... 34
2.2.1 Overview ................................................................. 34
2.2.2 Initial 2011 comments .............................................. 35
2.2.4 Prior Government Strategy ......................................... 37
2.2.8 Summary ................................................................. 41

Chapter 3 - The Challenges ..................................................... 44
Section 3.1 - The Cyber Crime Challenge ............................... 44
3.1.1 UK Law Enforcement Overview .................................. 44
3.1.2 Law Enforcement Cyber Crime Structure ..................... 45
List of figures & tables

Figure 1 - The Dimensions of Cyber Security (modified from Cavelty & Suter, 2012)

Table 1 – NSCP (SDSR 2010) actions mapped to Cyber Security Strategy objectives

Table 2 - Outline of NSCP spending (Cabinet Office, 2011, p.25)

Table 3 – NSCP sub objectives to lead Govt. department. (Cabinet Office, 2011, p.36-42)
List of abbreviations & acronyms

ACPO - Association of Chief Police Officers

BotNet - A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.

Chatham House - Home of the Royal Institute of International Affairs. A world-leading institute for debate and analysis of international issues

CPNI – Centre for the Protection of the National Infrastructure

CSS – Cyber Security Strategy

DCOG – Defence Cyber Operations Group

DDoS - Distributed Denial of Services attack – A coordinated and concerted attack whereby an organisation is deliberately prevented from providing or receiving a particular service via the Internet or networked computers.

E-Crime - The use of networked computers or Internet technology to commit or facilitate the commission of crime

Hacktivist – a person who gains unauthorised access to computer files or networks in order to further social or political ends.

IDS – Intrusion Detection System

ISO - International Organisation for Standardisation

MI5 – The Security Service, formally military intelligence 5

MoD – Ministry of Defence

NCA – National Crime Agency

NCS – National Crime Squad (merged into SOCA)

NCSP – National Cyber Security Programme

NFA – National Fraud Authority

NHTCU - National Hi-Tech Crime Unit

NISCC – National Infrastructure Security Coordinating Centre

NPIA - National Police Improvement Agency

NSS – National Security Strategy

PCeU - Police Central e-Crime Unit
Phishing - A type of fraud where victims are deceived into responding to an apparently legitimate e-mail from a reputable organisation, allowing the fraudster to gather sensitive information such as user names and passwords.

SDSR – Strategic Defence & Security Review

SOCA – Serious Organised Crime Agency (reformed into the NCA)

Spam - speculative e-mail sent in high volume (junk mail)

SPF – Security Policy Framework
While researching this project it became very clear from an early stage that the term ‘cyber security’ and the prefix ‘cyber’ can be fairly vague. In this work there are mentions of ‘cyber’, ‘cyber space’, ‘cyber security’, ‘cyber warfare’, ‘cyber-attack’ and ‘cyber-crime’. In the author’s opinion these ‘words’ have often been used as a ‘political sound bites’ with little substance. The connection of cyber to security could be considered due to the word ‘cyber’ being evocative of the modern digital ‘cyber age’. The term ‘cyberspace’ was coined by science fiction writer William Gibson and used by him in a short story published in 1982. Since then ‘cyberspace’ has been increasingly used to describe the internet, it is the author’s opinion that this is due to ‘cyber’ showing the human and social element of the internet.

There is still widespread confusion with regard to the meaning of words; the Oxford Dictionary defines ‘cyber security’ as “the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this” while the International Standards Organisation addresses ‘cyber security’ or in the ISO/IEC 27032 standard. In this standard cyber security is defined as the “preservation of confidentiality, integrity and availability of information in the Cyberspace”. In turn ‘cyberspace’ is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”. It is notable that there are terms already in existence such as computer, network, communications and web/internet security that provide security from the internet. In a lot of models the former are considered to be sub-domains of information security. Interestingly ISO define information security as the “preservation of confidentiality, integrity and availability of information” so the difference of ISO cyber/information security is the addition of cyber space.

The ISO view is perhaps trying to apply a technical view to an abstract concept, the authors view is that cyber security is a concept and takes on board the political and social dimensions while disciplines like computer and information security are technical and procedural in nature. Therefore in the authors opinion encompasses a number of security related technical, legal, political and social issues arising from globalisation and the evolution of cyberspace.
Executive Summary
This report is focused at the strategic cyber threat to the UK and the Governments response to this threat. Chapter 1 provides context and analysis of the cyber threat where it is broken down into cyber warfare, terrorism, crime and espionage. It concludes that the major threat to the UK is from cyber espionage and fraud based cyber-crime but the UK needs to invest in cyber warfare capabilities to be future proof. Chapter 2 describes the UK Government’s historic and current documented response to this threat and pulls out the pertinent points which are an additional £650 million of cyber security funding and a set of four wide ranging strategic objectives led by various government departments. However this funding is predominantly channelled to classified government programmes that are likely geared towards cyber attack capabilities and the strategic objectives have little substance in the form of actions behind them. When comparing the Chapter 1 threats of espionage and cyber-crime the governments response is seemingly weak on the controlling measures of good information security and law enforcement including crime prevention activities. Chapter 3 is based on the major challenges around cyber-crime and the challenges facing the government in preventing a joined up response to cyber espionage. So chapters 1, 2 and 3 are about; the risks, the countermeasures the government is putting in place and the gap in coverage of threats in comparison to the conclusion at the end of Chapter 1.

In conclusion the government response has seemingly adequately set the foundations for its own cyber warfare capability but has shown no real progress in tackling the difficult cyber-crime aspect and in improving its resilience to cyber espionage which is predominantly an information security issue in ensuring the computer systems are sufficiently difficult to hack. To tackle cyber-crime the government must invest in law enforcement focused on cyber fraud, invest in awareness and lead industry in anti fraud technology. To tackle espionage the government needs to simplify responsibilities of the large number of agencies involved, enforce standards through legislation and audit to ensure it follows its own advice that the vast majority of cyber-attacks can be stopped by good information security.
Chapter 1 - The National Cyber Security Threat
This chapter is intended to provide an overview of the threats against which effective cyber security will provide protection from. It will model, define and provide detail to threats with a UK context where possible. It is broken down into the following sections.

- Section 1.1 – Cyber Security: Threat, Source & Impact
- Section 1.2 – Cyber-Crime
- Section 1.3 – Cyber Warfare, Espionage and Terrorism

Section 1.1 is an overview of concepts, while the following sections provide more detail and analysis on these themes.

Section 1.1 – Cyber Security: Threat, Source & Impact

1.1.1 Cyber Security Threat Model
The whole concept of security is to provide ‘security’ against a threat. For cyber security the threat is fairly complex and this section is about modelling the cyber security threat at a high level to provide context, categorisation structure and consistency to further arguments within this project.

Figure 1 – The Dimensions of Cyber Security (modified from Cavelty & Suter, 2012)
Figure 1 breaks down ‘cyber’ threat areas (crime, warfare, espionage & terrorism) on the lines of their main impact (economic or national security) and the threat actor source (state or non-state). The following subsections provide a high level description of each element appearing in Fig.1.

1.1.2 Threat Sources
Any threat has a source, a human element at a personal or group level. In this model threat sources are broken down into state and non-state actors. The term ‘state actors’ refer to sovereign states agencies such as intelligence services or military units acting at the behest of the state. The range of the threat is from espionage to outright warfare. Non State Actors refer to individuals or groups who are acting for their personal or group’s aims. These aims can be criminal, ideological or political in nature and range from criminal acts such as fraud to acts of terrorism. It has to be noted that that there is some overlap between state and non-state, for example a political group (non-state actor) could be encouraged by a state; a terrorist group could be trained by a state and an ideological group could ‘act’ on behalf of a state, even if a state potentially did not want that outcome. In the former states may want to distance themselves from direct linkable action for damage limitation purposes if they are caught. Hence it is in the state’s interest to blur the lines.

1.1.3 Impact of Cyber-Attack
The impact of cyber-attack is broken down into three terms; economic, mixed and national security impacts. Economic impact as the term implies is the economic impact upon a private or public organisation. This can be a direct financial loss (theft), damage to reputation (affecting share price) or simply the cost of putting things right. Impacts to national security are those that can or will affect national security. National security is a loose term and can be interpreted in many ways, there is no legal definition of UK National Security but the UK Security Service (2013) define the term national as referring to “the security and well-being of the United Kingdom as a whole”. A mixed Impact is simply coverage of the ‘grey area’ between outright economic or national security harm. This area covers social/political impacts that fall short of
national security but are clearly not purely an economic impact. Protestor activity such as ‘hacktivists’ are a good example as IT security breaches have an economic impact but the political and social issues can make these events headline news and discussed in parliament. In this event they affect the whole of the UK but not necessarily the security of the UK in general.

1.1.4 Cyber Threat Areas and UK Law
Before discussing these areas it is worth noting that in legal terms ‘cyber espionage, crime, terrorism’ and to a certain extent ‘cyber warfare’ will be considered unlawful acts under UK criminal law. Therefore all the following ‘areas’ could be considered ‘cyber-crime’; in this case however, these areas are based more on sociological/criminology dimensions for the categorisation of ‘acts’ into threat sources and actors. For example hacking into a computer is an offence under UK law in the Computer Misuse Act 1990, if a foreign government intelligence service agent hacked into government systems with the intent of stealing government secrets and was caught by the police, he/she could potentially be charged under UK law. If an individual hacked into a bank with intent to steal money (transfer money into different account) he/she could be charged under UK law. The former ‘act’ would be considered ‘Cyber Espionage’ by a state actor with a national security impact while the latter would be ‘Cyber Crime’ by a non-state actor with an economic impact (personal gain). War and terrorism both have an impact of damage and loss of life but differ with regard to people working for a state’s objectives (war) or for a non-states political or ideological objectives.

1.1.5 Cyber Crime
Cyber Crime in the main is concerned around cyber acts for criminal gain such as theft, fraud, blackmail which is conducted by non-state actors such as organised crime and individual criminals. The impact is mainly economic on the financial institutes, business and private individuals. This area also covers aspects which impact society, such as content crime (illegal images) and ‘cyber protest’ such as ‘hacktivism’ and pure computer crime such as hacking. This element is elaborated in section 1.2.
1.1.6 Cyber Warfare, Espionage & Terrorism
Espionage as defined by the Oxford Dictionary is "the practice of spying or of using spies, typically by governments to obtain political and military information". This is a fairly simple definition and captures the traditional ‘human’ spying quite well but cyber espionage has additional complications on the technical side in that there are two distinct methodologies. Firstly there is the option to intercept communications and secondly there is the option to attack computer systems themselves. Espionage is not always conducted by states, industrial espionage conducted by organised crime and large corporations often look to illegally obtain information or intellectual property for mainly economic advantage. In the main industrial espionage is an aspect of cyber-crime as it is a criminal act involving breach of copyright, theft, interception of communications or computer misuse (involving hacking). However there are grey areas where no criminal law has been broken. Cyber espionage is considered to lean towards an economic or social/political impact but there are national security implications with the crossover of espionage on government and linked private sector information systems. This can be another grey area as generally most defence sector development is undertaken by private companies and cyber espionage on a defence firm could be a competitor trying to copy a tank design or a foreign state looking to understand the technology (thickness of armour etc) for defence intelligence purposes. It has to be noted though that a lot of state espionage is often for political and economic advantage, not just for warfare.

Cyber warfare covers sovereign states conducting cyber-attacks against another sovereign state; it has been further broken down to into ‘cyber-attack’ and ‘cyber war’ on the basis of damage. Cyber war is also a more of a futuristic scenario and acts as another domain of warfare alongside air, sea, land and space domains. Cyber-attack is intended to cover actions short of outright war such as sustained low level attacks such as distributed denial of service (DDoS) attacks and hacking critical computer systems from one state to another that collectively affect national security. Terrorism is similar to cyber warfare with the main difference that it is not conducted by legitimate states, though it has to be accepted that some terrorism is state supported or
sponsored. For domestic terrorism it differs to cyber-crime in that the impact is strongly biased towards impacting state security through mass fatalities, fear or other large impact to the state as a whole. There is some crossover with cyber-crime such as the blurred point between terrorism and political extremism. This element is elaborated in section 1.3

Section 1.2 – ‘Cyber Crime’

1.2.1 Setting the scene
In the last 20 years information communications technology; computers, telecommunications and networking has experienced enormous advances in capability. This has led to extensive usage and a high degree of dependency in the Western world and information technology is now vital in business, public services, defence and in running a country’s infrastructure. Crime has long been linked with technology and the opportunity of cyber-crime has been followed with relish (Wall, 2007, p.70) with Interpol in 2008 considering cyber-crime to be the fastest growing criminal act. (Interpol). The fact is that cyber-crime can be committed anywhere in the world against a victim in any part of the world. In 2005 a YouGov poll indicated that one in twenty had lost money to some sort of online scam. (Wall, 2007, p.70). Norton estimated that more than 12.5 million people in the UK had fallen victim to cyber-crime within the past twelve months. (Home Affairs, 2013, p.16). In 2010 the UK cost of cyber-crime in security breaches to UK business was estimated at several billion pounds per year. (PWC, 2010). In 2008 internet based card fraud is believed to cost business £181.7 million while online bank fraud cost £52.5 million. (APACS, 2009). In 2013 the Department for Business, Innovation and Skills (BIS) information security breaches report stated that 93% of large organisations had suffered a breach with the average of 113 breaches per year (BIS, p.2).

1.2.2 Traditional Crime vs. Cyber Crime
Cyber-crime is also different in many ways to more traditional crimes. For example a bank robbery will leave an investigatory audit trail of money, CCTV footage, eye witness’s accounts and forensic evidence. This contrasts with an online bank ‘robbery’ which could leave a computer evidence trail over several countries. It is obvious which crime will be easier to investigate and which
offender it will be easier to catch. Some consider that current law enforcement is unsuccessful at combating cyber-crime. In 2008 a report found that “cross law enforcement at every level remains ad hoc and ill-equipped to cope”, that “border law enforcement remains a long-standing hurdle to fighting cyber-crime” and that “cyber-crime isn’t yet enough of a priority for governments around the world”. (McAfee).

1.2.3 Cyber Crime Terminology
Cyber-crime is a modern term used to denote crimes committed on the internet and using computer technology. In theory this sounds simple but defining cyber-crime is not. There are a large number of definitions and terms used and ‘cyber crimes’ generally fit into traditional crime categories such as fraud. This can be both in legal terms as well as descriptive terms. For example in the UK a cyber-crime such as a ‘phishing’ email would not be a crime. Though using the information obtained to extract money from the bank would be a fraud by deception. Phishing would be described and accepted by many as a cyber-crime but not a legal crime until the ‘phished’ information is acted upon. Another example is hacking into a bank account remotely would be an offence of ‘unauthorised access’ under the Computer Misuse Act 1990, a cyber-crime. A subsequent electronic transfer of money could be described as a virtual bank robbery or cyber-crime but overall it would likely be considered a theft offence, especially when the money taken is turned into some physical thing. In simple terms the overall result is that money has been unlawfully taken from a bank and a cyber-crime but in legal terms a little more complex and open to interpretation.

The current UK law enforcement definition for cyber-crime is ‘e-crime’. E-crime is defined as “the use of networked computers or internet technology to commit or facilitate the commission of crime”. (ACPO, 2009, p.2). This has differed from the previous term used of ‘high tech crime’. High tech crime was defined as “any criminal activity that uses electronic devices to assist plan, or execute a crime”. (NSLEC, 2005). These high tech crimes were grouped into old and new; the old were traditional crimes committed in new ways with a computer or through the internet while new crimes were those committed

\[1\] Cash or a new car
completely through a computer, such as hacking. The fact that the example above with the bank hack and the ‘phishing’ email are both ‘new’ computer crimes but the final act is an ‘old’ crime probably explains the current ACPO definition. It also shows how cyber-crime has evolved and that it can be a hybrid of old and new ways. Some cyber-crimes are considered to “fall out of legal and criminal jurisdictions” (Wall, 2007, p.48) and in the UK identity theft is not a crime, it is not until the data is used for a fraudulent use that the crime is committed but this could be in another legal jurisdiction. Another example is a virtual vandalism of a website, there is no physical damage, nothing has been taken, has someone had unauthorised access to a computer or is the website in the public domain and therefore open to change? A further example is in 2004 where a teenager bombarded his former employer with approximately 5 million emails. He was convicted under the Computer Misuse Act 1990 in 2006. (Turner, 2010). This case is interesting as in an original trial in 2005 the judge dismissed the case on the grounds that as an email server is set up with the express purpose of receiving emails and sending it emails, albeit millions of them, could not be considered “unauthorised modification”. The case was appealed and in 2006 the Computer Misuse Act was amended by other legislation for clarification purposes. (Met Police, 2007, p.2). The main point of this section is that a general view of cyber-crime is not legally correct as a criminal statutory offence and that there are numerous grey areas.

1.2.4 Fundamentals of cyber crime
Wall (2007, p.36) describes the focus of cyber-crime as “to acquire information in order to extract its value”, this in my opinion captures the fundamental principle of cyber-crime. Computer systems and the internet essentially provide, store, collect and transport information which has value and extracting it for criminal purposes is the essence of cyber-crime. Wall also describes the development of cyber-crime in three generations. The first generation is considered to be “crimes using computers to assist traditional offending”. (2007, p.44). The second generation consisted of “opportunities for crimes across a global span of networks”. (2007, p.45). The third and last generation are “true cyber crimes”, which are “wholly mediated by

---

2 Wikipedia is an example of a community website that is open to change
technology". (2007, p.47). The first and second generation are based on traditional or old crimes and essentially differ from being both local and global. The third generation is where the entire crime happens over a computer system; an example being a ‘botnet’ and a distributed denial of service attack (DDoS). The European Union in their communication ‘Towards a general policy on the fight against cyber-crime’ split cyber-crime into three areas. These are ‘traditional crime on electronic networks’, ‘illegal content’ and ‘crimes unique to electronic networks’. (2007, p.2). Wall also categorises cyber-crime into three main areas. These are; computer integrity crime, computer assisted crime and computer content crime. (2007, p.49-50). Integrity crimes are attacks on computer systems such as DDoS, computer assisted are the hybrid crimes where traditional crimes such as fraud have modernised and computer content crimes can be child pornography on the internet. The ACPO term e-crime is perhaps a better definition as it is more cyber in nature with the adding of internet and networked computers; however it is open for some situations. For example paedophilic images on a standalone PC would not be an e-crime but downloading or sharing them from the internet would be. This e-crime definition is consistent with UK legislation in that there are few ‘cyber crimes’, just new ways (e-crime) of committing ‘old’ crime such as theft and fraud. These previous examples and definitions show the subtle difference in definitions, they show the evolving nature of cyber-crime and how cyber-crime gets classified into pre-existing legislation for legal and prosecution purposes. It also shows the difficulty of classifying cyber-crime.

Section 1.3 – Cyber Warfare, Espionage and Terrorism

1.3.1 Setting the Scene and Terminology
This section will explain and clarify the terminology around the three distinct threat areas before each are individually explored.

1.3.1.1 Differences and Jurisdiction
The difference between cyber-crime and cyber war, espionage and terrorism is that crime is essentially a law enforcement problem while the latter are collectively a problem for law enforcement, the military, politicians and security agencies. For example unauthorised access or hacking of a sensitive
defence computer is both a crime and an act of espionage or security issue. Terrorism is both a criminal act which falls under the criminal justice system and a threat to national security. For jurisdiction and ownership this creates an interesting mix of government agencies (police, MI5, GCHQ, SOCA, Armed Forces) at the operating level and differing departments at the government level (Home Office, MoD, FCO and the Cabinet Office). For government this mix is quite new as historically the intelligence services only dealt with military intelligence and state espionage and only operations against the IRA and the end of the cold war has seen them increase activity against terrorism. In these matters government strategy, policy and historical factors\(^3\) decide which agency or group of agencies has the primary responsibility. The other consideration is whether the incident is ‘dealt with quietly’, pursued through the criminal courts or by military action, this is usually decided by the investigating agency. Military action is quite a new development with the US government State Department Legal Adviser on September 18, 2012 essentially stating that certain cyber-attack is a ‘use of force’ and direct attack is an option for the US should they come under cyber-attack (Schmitt, 2012 p14-15).

1.3.1.2 Cyber Attack as a Press and Political term
Cyber-attack is a good descriptive term for espionage, terrorism and warfare as essentially all three are a form of attack by different actors and to varying degrees of severity. It is also used interchangeably in the media and by government as a generic threat and even covers cyber-crime. The rationale for a generic term such as cyber-attack is that ‘cyber-attack’ is easy to quantify but harder to classify. This is due to that IT security systems will pick up the electronic/digital signs of intrusion or attack but they will not be able to identify the human intent behind the attack, was the attack a potential act of war, terrorism, espionage or a criminal act? This factor makes it difficult to ‘classify’ or ‘categorise’ a cyber-attack. Chatham House commented with regard to cyber space that “differentiating between actors with ‘warlike’ intentions and those who are merely malicious or criminal and whose actions fall short of ‘acts of war’ is therefore problematic”. (Cornish et al, 2010, p.5).

\(^3\) Precedent is a big decider
Therefore cyber-attack is a very easy term to describe but doesn’t have a consistent meaning.

1.3.1.3 Cyber Attack and Espionage
Historically a lot of espionage activities have been based on visual surveillance (satellite & human), human intelligence (bribery, blackmail, extortion) and signals intelligence (interception of communications or bugging) and security services agents. With the advent of computers this has changed matters considerably as the vast majority of counter espionage was based on physical and personnel security controls to ensure only vetted staff had access to physically vulnerable areas. Computer technology and inter-networks has enabled espionage to be carried out in a new format and it is now very difficult to differentiate intent between espionage to low level acts of cyber warfare or cyber-attack. This is very difficult at the political level in that espionage itself has massively changed from the cold war era and the advent of cyberspace has meant that perhaps ‘rules’ are not understood by all parties. In 2012 Major General Shaw (Hopkins) stated that hackers have managed to breach some of the top secret systems within the Ministry of Defence. It was said that the “number of successful attacks was hard to quantify” and the number of serious incidents were quite small. It was also noted that these are the attacks the MoD knows about and acknowledged that the “likelihood is there are problems in there we don’t know about.” What this means is that the MoD knows they were attacked but can’t always tell what the objective was and that the MoD have the fear or uncertainty around their network defence. This has meant that politicians have more and more used the term cyber-attack, Chatham House have commented on this and stated:
“It becomes politically attractive simply to conflate cyber espionage with cyber war, a step which, by definition, would plunge most countries into an immediate state of conflict (although, because of attribution difficulties, they might not know who their adversaries are or indeed whether and when they have been attacked)”. (Cornish et al, 2010, p.18). This is due to the fear and uncertainty that the new methods of espionage have created in comparison to the traditional spy or ‘bug’.
1.3.1.4 Clarification on terminology
In simple terms cyber-attack can be broken down into crime, espionage, terrorism and warfare as the intent is understood. To reiterate and add some structure to this work I have defined cyber-attack as a sub division of cyber warfare, essentially breaking down warfare on the basis of severity. I will carry on with the rest of the section on warfare, espionage and terrorism with ‘attack’ being referred to as the lower end of warfare and as a collective loosely descriptive term for any attack from cyberspace.

1.3.2 Cyber Warfare
“Cyber warfare is arguably at the most serious end of the spectrum of security challenges posed by – and within – cyberspace”. (Cornish et al, 2010, p.vii). Historically military action has been concerned with land and sea domains. In the last century air and space were added and now the virtual environment is being added as a tactical domain on which war can be fought and superiority gained. Cyber warfare is not totally new, there are existing terms such as electronic and information warfare which share similarities and which help make clarification of cyber war difficult. Chatham House commented that the cyber warfare ‘problem’ “is not only urgent and complex but also, to a surprising extent, still very under-developed” with an “absence of consensus regarding the principal terms of reference”. In relation to terms they comment “‘Cyber war’, although preferred by some commentators, seems to exaggerate the problem, although not ridiculously so. Yet the more cautious ‘state-sponsored cyberattacks’ is too narrow”. (Cornish et al, 2010, p.2)
Therefore the term cyber warfare was used instead of war as warfare is far more flexible a term and is defined as “engagement in or the activities involved in war or conflict” while war “is a state of armed conflict between different countries or different groups within a country” according to the Oxford Dictionary.

1.3.2.1 Impact of Cyber Warfare
True cyber warfare has a wider impact than just damage to computer systems; it can cause national psychological and economic impacts. The psychological element to cyber-attacks stems from the infiltration of what are assumed to be secure systems and critical infrastructure highlights national vulnerabilities and weaknesses. This can provoke feelings of insecurity and
Chatham House point out that “engendering this sense of insecurity could indeed be the attacker’s goal, in the same way that the fear of terrorism and its potential harm can have a detrimental and disabling effect almost as great as the terrorist act itself”. (Cornish et al, 2010, p.10). This leads to great future possibilities with the dependence of nations on IT systems, an attacker could potentially force a state to surrender due to being psychologically weakened. Economic impacts will also have a psychological element but also have a reputational impact, for example international banking systems use electronic transfer systems, bringing these systems down and both damage a country economically but affect its reputation as a trusted secure partner.

1.3.2.2 Political and Legal Issues of Cyber Warfare

Cyber warfare has thrown up debate over political and legal issues due to lack of clarity over terms such as cyber-attack and global state legal jurisdictions. Terminology and legal frameworks are mutually supportive and in acknowledging this Chatham House state that “it is difficult to see, for instance, how a coherent legal framework could result from the current proliferation of cyber terms”. (Cornish et al, 2010, p.21). Due to this it is currently unclear with regard to domestic and international law when a sustained cyber-attack will cross over into an act of war in the political and legal spectrums of most states, it is also unclear whether states would support the actions of a state that has declared war on a perceived cyber adversary due to a lack of harmonisation of international law, accepted behaviours and procedures and a lack of consistency of terminology. Schmitt (2012, p.37) has observed that the US and NATO have made “initial forays into the demanding process of exploring how the extant norms of international law will apply in cyberspace” through the previously mentioned Koh speech and the NATO Tallinn Manual and that the journey for consensus on international law has begun.

Although this journey has begun it could be a bumpy ride, globalisation and the internet has challenged the control of sovereign states on this medium with Chatham House providing an excellent summary:

“Several national governments are strengthening their cyber security organizations to conduct defensive and offensive operations, and virtual drawbridges are being raised. The internet is often described as an inherently dangerous place, which is a perspective difficult to dislodge when these
warnings emerge into the public domain from a vault of secret knowledge. Traditional notions of warfare, based on attack and defence, are being challenged by the complexity of cyberspace, and the pace of change in the medium threatens to overwhelm all but the most technologically competent. These challenges are like the waves of a storm crashing higher and higher against the walls of the modern state, undermining traditional notions of power and discomfiting those within” (Cornish et al, 2010, p.18).

This is a good description of the current political position which has the internet as a dangerous place where cyber-attack and security is one vector. Other elements that will trouble politicians are criminal enterprise and conspiracy, information on the internet, for example wiki leaks and overall the lack of state control. This is the crux of the statement from Chatham House, the modern state is overwhelmed and uncomfortable with the change brought about by globalisation and its major enabler; cyberspace. Therefore there will undoubtedly be a lot of difficulty in global agreement as states will want to ‘own’ and control there part of the internet.

Another difficulty is that even allies sometimes struggle to agree and work well together, for example the UK is a member of NATO and the EU, the former is a military alliance while the EU is a political and economic group but both have similar groups of states. In October 2008 NATO set up the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn (Estonia) to support its 2008 cyber defence policy which essentially was an agreement of mutual aid from NATO Member States. (House of Lords, p.25, 2010). The EU however had formed the European Network and Information Security Agency (ENISA) in 2004 and published a Cyber Security Strategy in 2013. Like the Tallinn centre ENISA was designed to be a centre of excellence for exchanging information, best practice, brokerage, cooperation and exchange of views (House of Lords, p.30, 2010). The House of Lords review noted that “there is considerable overlap between the roles of the EU and NATO in relation to cyberattacks, and cooperation between them should be put on a more formal basis. (p.26, 2010). Both the CCD DOE and ENISA are roughly the same size with ENISA currently has a staff of around 65 and is located in Crete. (House of Lords, p.31, 2010).
The last political issue is one of the factors that disrupts international cooperation is political one-upmanship. During the Cold War the US pursued a policy of nuclear deterrence\(^4\) where the US stated that if they were physically attacked to any degree they may or may not use nuclear retaliation which created doubt, they also stated that they would know if anyone attacked them through their surveillance capabilities which were vast and secretive. The US Cyber Security policy is very similar in that they say that they can attribute attacks (pointed towards China) and that they may use direct kinetic force in response to cyber-attack. The difficulty though is that cyber-attacks are very hard to attribute and constant low level attacks make it hard for the US to proof that they can always accurately attribute cyber-attack.

1.3.2.3 Critical National Infrastructure
During the Cold War sabotage of the UK’s Critical National Infrastructure (CNI) was considered a major risk and plans were drawn up to protect electricity generation and supply, water, oil and gas supply, communications and transportation from physical sabotage. At the time the vast majority were government owned; now the risk has been expanded to include cyber-attack on a CNI which has transferred from state to private ownership. In 1999 the risk of cyber or electronic attack (as it was called then) on the CNI was identified and acted upon in when National Infrastructure Security Coordinating Centre (NISCC) was formed. This organisation was set up for the sole purpose of to minimise the risk to the CNI from electronic attack. (Morgan, 2005). In a modern cyber war or attack it is quite obvious that the CNI would be the likeliest attack vector as a state without functioning power or water supplies could lose a war without the military ever firing a shot.

1.3.2.4 Cyber Warfare Case Studies
The following section highlights cyber warfare examples covering support to political aggression, support to conventional warfare and pure cyber warfare. In 2007 a three week wave of cyber-attacks hit Estonia after a Soviet war memorial was moved to a less prominent location which caused unrest amongst Estonia’s ethnic Russians. This led to complaints from Russia and a wave of unrest followed the movement of the war memorial which led to a

\(^4\) As did the UK
series of DDoS attacks which caused parliamentary email being out of order for 4 days, ATM’s out of action and government communications reduced to radio. The attacks were described as being fairly modest but had a large impact due to Estonia’s dependence on the internet (House of Lords, 2010, p.10). It was alleged that Russia was behind the DDoS attack to support political aggression. Similar to Estonia in 2008 Georgia invaded South Ossetia and its relationship with Russia worsened as the dispute developed into military action. Georgia was subsequently hit with large scale DDoS attacks that were bigger in scope than those in Estonia a year before. Attributing these attacks to the Russian state is hard and Nazario (2009) states that “we appear to see attackers using DDoS attacks to express support of an official government position, either against external or internal foes”. Using DDoS to support political aggression is an interesting development in cyber as it is hard to categorise, Chatham House say that the Estonia and Georgia incidents are “not espionage, but nor was it traditional warfare in which the ultimate objective would surely be the surrender of sovereignty to an adversary” (Cornish et al, 2010, p.19).

Supporting the more traditional attack in 2007 the Israeli Air Force carried out an air strike on a suspected nuclear reactor in the early stages of construction. It was considered (Borger, 2007) that “such a reactor could take from three to six years to build and would produce enough weapons grade plutonium to make a bomb in about a year of operation”. Gasparre (2008) adds detail to the air strike in that the Israeli Air Force disabled the Syrian air defence system by exploiting the Syrian IT system. It was believed that the Israeli Air Force used a system called SUTER that works by “beaming electronic pulses into the antennas that effectively corrupt, if not hijack, the processing systems that present the enemy operators with their physical picture of the battlefield”. This was different to classic radar jamming attacks that flood enemy electronics with excess ‘noise’ or power, but instead insert customised signals, including specialised algorithms and malware, into the vulnerable processing nodes. According to one intelligence source, Israel also used network attack techniques to perform “higher-level, non-tactical penetrations, either directly or as diversions and spoofs, of the wider Syrian command-and-control capability”. Whether Israel conducted these penetrations using SUTER or other military
means, clandestine operations, or even 'geek-style' hacking is unknown but nonetheless Syria's ADS network is centralised, dependant on mainstream IT and used dedicated radio frequencies all of which make the system more 'modern' and susceptible to attack.

At the lower of cyber warfare or cyber-attack is malware such as Stuxnet which are pure cyber warfare tools. Stuxnet was used to attack an Iranian Nuclear Research site and interfered with Industrial Control Systems (ICS), which were configured by Programmable Logic Controllers (PLC), and more specifically Windows systems using Siemens Step-7 software. After infecting such systems, Stuxnet would reprogram the PLC to make centrifuges operate at speeds outside acceptable limits, causing their malfunction and eventual destruction. It was believed that Stuxnet travelled via infected removable drives and was deliberately developed to only attack machines which met its requirements. Stuxnet in its earliest identified form dates from June 2009 (Virvilis, Gritzalis, p.2) and was identified to an anti-virus security company in 2010 when the attacks were discovered. The general expert opinion of the malware is that it required significant effort for development as well as “insider knowledge and support from a large team of experts” (Virvilis, Gritzalis, p.1). Stuxnet was also designed for pin-point accuracy as its impact across the world was minimal. Stuxnet however may not be the first malware attack in 2004, Thomas C. Reed, an Air Force secretary in the Reagan administration, wrote that the United States had successfully inserted a software Trojan horse into computing equipment that the Soviet Union had bought from Canadian suppliers. This was allegedly (by Reed) used to control a Trans-Siberian gas pipeline, the doctored software failed, leading to a spectacular explosion in 1982. What is clear though is more systems and functions are becoming vulnerable to cyber-attack due to the dependence on IT and techniques are becoming more widely known.

1.3.3 Cyber Espionage
As discussed earlier the advent of cyberspace has brought far more opportunity to espionage in new avenues such as internet connections, global email and removable media to infiltrate systems and on using internet connected computers to extract information. This is a major global problem
with the US Defence Science Board releasing a report last year where the classified version was reputed to state that major US defence projects had been infiltrated, this included current missile defence system and several of the latest aircraft designs (Eddy, 2013). The Washington Post that had obtained a copy of the classified report stated that ‘senior military officials’ with knowledge of the breaches said that the vast majority had come from China (Eddy, 2013). Either way there has been no denial from the US government that these breaches have taken place\(^5\) but also there has been little detail.

For the UK the Intelligence and Security Committee in its Annual Report 2010–11 considered espionage in cyberspace. They observed that “Cyber space means that countries no longer have to invest in global networks and pursue complex operations with high-level agents when it comes to espionage: they can access much of the same information using relatively inexpensive cyber attacks.” (Defence Select Committee, 2012, p.13). Further to this the Director General of the Security Service told the Defence Select Committee in 2011 that “the barriers to entry to cyber espionage are quite low. We have found a number of countries taking an interest in this”. In summary espionage is not new in principle, cyber espionage is just a new methodology and similar to cyber-crime; old crime new ways concept cyber espionage has massively expanded the existing espionage threat.

**1.3.3.1 Cyber Espionage (Hardware)**
An increasing avenue of attack for espionage and mistrust between states is the increasing proportion of electronic equipment (hardware) made in foreign states. In 2009 it was reported (Markoff) that for the US now securely manufactures only about 2 percent of the more than $3.5 billion of integrated circuits bought annually for use in military equipment. The concern from the military is that this electronic circuitry could contain Trojan style vulnerabilities built in through unscrupulous manufacture. Due to how complex modern electronics are detection of problems is nigh on impossible.

The UK MoD has similar concerns in the Defence Committees recent report on Cyber Security in the MoD the issue came up. The MoD was seen to be

\(^5\)There is tacit acknowledgement of the breach from officials but little detail, just lots of speculation.
quite open and frank of the work required “on securing its supply chain and industrial base”. The Defence Committee took the view that “It is imperative that we see evidence of more urgent and concrete action by suppliers to address this serious vulnerability, and of energy and determination on the part of the MoD to enforce this action” (p.3). For the MoD the issue had come about in addition to manufacturing capability on the change from using its own proprietary electronics and IT systems to commercial off the shelf (COTS) products which were using IP technology. Using COTS over propriety systems often weakens security in that propriety is not widely understood while COTS uses standard technologies and the product itself is often easily obtained. However there is a reverse logic in that propriety systems can be poorly engineered and tested while COTS are open and often widely tested and attacked.

For the UK the potential problems surrounding foreign equipment is personified by Huawei. Most of the concerns surrounding Huawei relate to its “perceived links to the Chinese State” and that “China is suspected of being one of the main perpetrators of State-sponsored attacks, which are focused on espionage and the acquisition of information” (ISC, p.5, 2013). In 2005 Huawei successfully bid for BT infrastructure with the equipment going online in 2007 (ISC, p.4, 2013). At the time BT referred the issue to the government for approval and although there appeared to be some opposition to the deal government officials felt that the potential trade, financial and diplomatic consequences of blocking the deal would be significant. (ISC, p.8, 2013). In 2011 the situation was different when Huawei offered to donate £50m of equipment to seal a deal to provide mobile phone coverage in the London Underground prior to the Olympics. The deal was officially turned down due to high project costs according to BBC News (2011) but other sources (Verkaik) cite concerns over spying. Either way there is a shortage of reputable articles on why the deal failed but as the deal reached ministerial approval it would be unlikely that the involved corporations would pull the financial plug.
1.3.3.2 Cyber Espionage (Software)
Another example of the difficulties of categorising cyber-attack is malware. Recently there have been four quite [in]famous malware espionage attacks that have been identified and exposed in the public domain. These are named as; Duqu, Flame, Red October and Net Traveller\(^6\).

Duqu is considered to have significant similarities with Stuxnet by a number of researchers which has created comment that both items of malware were produced by the same team (Virvilis, Gritzalis, p.3). Either way the major difference was the objective of the malware, like Stuxnet, Duqu was a clearly targeted malware and according to estimations infected no more than 50 targets worldwide, it included a key logging component which was used to collect sensitive information, such as passwords. (Virvilis, Gritzalis, p.3). After initial infection, Duqu remained active for 30 days before self-destructing, although attackers could command it to persist for as long as needed, presumably once password information was obtained the malware was a liability as it may be detected. Flame was first detected in May 2012 but there is speculation that it had been active for 5-8 years before industry detection. It is alleged to have infected thousands of Windows systems, mainly in Middle East. It had a key logging module similar to Duqu, took screenshots, intercepted email messages and used the internal microphone of the computer to record conversations. Similar to Stuxnet it made use of two zero-day vulnerabilities (Print Spooler MS10-061 & Windows Shell MS10-046). The most advanced feature of the malware was an impersonation of a Windows Update Server (WSUS). This had to use a cryptographic attack against Microsoft software to 'fool' the Windows operating systems as it checked digital signatures of updates. Essentially the malware spoofed valid digital signatures and was a very significant endeavour. It is suggested that an advanced cryptanalytic attack required a team of skilled cryptographers costing an estimated 200K to 2M USD to develop. (Virvilis, Gritzalis, p.3)

On the less sophisticated side are Red October and Net Traveller. Red October was discovered in October 2012 and was believed to have been active since May 2007, targeting diplomatic, governmental and scientific

\(^6\) There are a lot of technical differences of opinion on malware and this section's intent is to highlight the threat and not discuss in detail these examples of malware.
institutions. Red October sent targeted emails containing malicious Word and Excel documents, which exploited known vulnerabilities. It was said to have a minimalistic architecture, having a basic component responsible for downloading encrypted modules and executing them in memory. This allowed it to remain undetected without having to perform additional evasion techniques. (Virvilis, Gritzalis, p.4). Net Traveller victims get infected in the same manner as Red October through spear-phishing attacks using Office documents which exploit two publicly known vulnerabilities - CVE-2012-0158 and CVE-2010-3333. Although these vulnerabilities have been patched by Microsoft, they remain effective as not all organisations are effective in patching their computer systems and due to this Kapersky Labs say they are among the most exploited in targeted attacks. (2013, p.4). The Kapersky Labs (2013, p.3) report on Net Traveller say that they have identified 350 high profile victims in 40 countries, targets include Tibetan/Uyghur activists, oil industry companies, scientific research centres and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors.

In summary the first two examples are specifically targeted and controlled using new attack vectors which are very difficult to mitigate, the latter examples are almost a simple fire and forget weapon, an email containing an attack against a known vulnerability praying on systems that have not been updated with uneducated users being unaware of the risk. All these examples of malware have been detected by commercial providers of anti-virus products and there is often a view that these malware examples have been around some time before detection. All have commonality in that they are designed to avoid anti-virus software and are often only detected when specialists are called in to look at a problem computer system or ‘dodgy’ email.

Knowledge of espionage malware has only been from the commercial anti-virus companies presumably due to their commercial interest to ‘hype’ the problem and ‘sell’ their skills. As the very intent of espionage (like crime) is to act undetected and governments are reluctant to publish details of malware there is very likely to be a lot more undetected or unknown complex malware designed for espionage.
1.3.4 Cyber Terrorism

Terrorism is a constantly changing environment and in 1989 was legally defined as “the use of violence for political ends, and includes any use of violence for the purpose of putting the public or any section of the public in fear (Lord Carlile, p.3). This was due to the use of violence by bombs, shootings and mortar attacks by the IRA. By 2000 in the UK the scope had widened with the Terrorism Act adding damage to property and “is designed seriously to interfere with or seriously to disrupt an electronic system” to influence the government; intimidate the public for the purpose “of advancing a political, religious or ideological cause”. (Lord Carlile, p.5). So for the UK in 2000 cyber terrorism was legally born but there is still not a definition for terrorism that commands full international approval. (Lord Carlile, p.47). As yet cyber terrorism has not become a reality though the National Security Strategy (2010, p.30) acknowledges that “Terrorists use cyberspace to organise, communicate and influence those vulnerable to radicalisation” so a national security goal would be to restrict or monitor the use of terrorists within cyberspace but this isn’t a major threat compared to a full on attack causing a direct loss of life. In a speech in 2012 Jonathon Evans the head of the UK Security Service (MI5) stated “So far, established terrorist groups have not posed a significant threat in this medium, but they are aware of the potential to use cyber vulnerabilities to attack critical infrastructure and I would expect them to gain more capability to do so in future”.

There is however a blur between state actor attacks and terrorist groups taking responsibility for the actions of the state for their own benefit. The Shamoon virus in 2012 affected as many as 30,000 PC’s across the Saudi Arabian Oil Company who are the world’s biggest supplier of oil. The purpose of the virus was indiscriminate deletion of data on the computer (Bronk, Tikk-Ringas, 2013, p.3). The confusion around the cyber terrorism issue comes from a group calling themselves ‘The Cutting Sword of Justice’ claiming that they were the perpetrator, however there is speculation that Iran was behind the attack, although Iran have denied this. (Bronk, Tikk-Ringas, 2013, p.22).
1.3.5 Concluding Remarks

“Astonishing – with industrial-scale processes involving many thousands of people lying behind both State sponsored cyber espionage and organised cyber crime”. Jonathon Evans – MI5 Director General (2012)

The author concurs with Jonathon Evans in that the highest risk areas of cyber security are the above as the UK is clearly under sustained attack according to the evidence that government and industry are pushing out. Therefore on this basis the author’s simplistic strategic cyber security response would be focused on organised cyber-criminal and cyber espionage and would consider the upcoming threats of cyber terrorism and warfare. In the latter case the UK’s ability to conduct its own offensive warfare operations would be assessed as a new form of warfare enabling the UK to remain current in military technology and capabilities. To achieve the above the assumed measures would be; improved law enforcement and crime prevention including technical security and awareness for organised crime and enhanced information security across the CNI and vulnerable industry to ensure that communications are secured against interception and computer networks are sufficiently hardened to prevent them being successfully attacked. Indeed the governments published advice is that “80% of known attacks would be defeated by embedding basic information security practices” within the organisation. (CESG, 2012, p.1).

This chapter’s intent was to inform the reader of the threats so that he next chapter which explores the governments documented response to cyber security can be put into context. Chapter 2 will also come back to the above simplistic cyber security response as a point of comparison.
Chapter 2 – The Government Response
This chapter will summarise the UK Government’s Cyber Security Strategy as the government’s response to the threat. It will discuss the historical context, supporting strategy documentation and provide a high level analysis of the response. It is broken down into the following sections:

- Section 2.1 – UK Government Cyber Security Strategy
- Section 2.2 – Analysis of the Cyber Security Strategy 2011

Section 2.1 is predominantly a document review of the published strategic HMG documentation and section 2.2 is a critical analysis of the 2011 Cyber Security Strategy.

Section 2.1 - UK Government Cyber Security Strategy

2.1.1 Background and Strategic Objectives
In 2011 the Cabinet Office announced the Cyber Security Strategy as a follow up to the 2009 Cyber Security Strategy and in response to the 2010 National Security Strategy and the Strategic Defence & Security Review. The strategy (p.21) sets out four objectives in which to achieve a vision that by 2015 the UK “derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society”.

2.1.2 Content of the National Cyber Security Strategy
The document is made up of four chapters; chapter 1 describes cyber space and the UK’s growing dependence on it, chapter 2 describes the changing threats of cyber space, chapter 3 carries the vision for 2015, principles and roles and responsibilities. Chapter 4 details the actions the government will take. The vision is essentially a paraphrase of the four objectives in that by 2015 objective 1 will be met by the vision of strengthening law enforcement and tackling cyber-crime; objective 2 is met by building “capacity to detect and defeat high-end threats” and reducing vulnerabilities in government systems and in the critical national infrastructure. Objective 3 is met by the UK helping “shape an international consensus on ‘norms of behaviour’ in cyberspace”. Objective 4 is met by growing “the cadre of cyber security professionals, improved prevention and public awareness, raised business awareness and
working with industry and academia to boost our share of the cyber security market and cemented the UK’s status as a safe place to do business online” (p.23). The action of chapter 4 carries the detail of a National Cyber Security Programme (NCSP) of £650 million over 4 years. The chapter covers 8 pages of actions but one action and short paragraph accounts for around half of the NCSP funding. This will go to GCHQ for “enhancing the UK’s core capability to detect and counter cyber attacks”. The specific detail of this work is classified and therefore cannot be quantified (p.27). The actions linked to their respective objectives are contained in annex at the end of the document.

Essentially the strategy takes the NSCP goals and adds background context in the first two chapters, a 2015 vision linked to the end of the NSCP, four objectives and a set of actions linked to the objectives.

2.1.3 The National Security Strategy 2010 (NSS 2010)
This strategy sets the scene for the risks the UK faces from conventional warfare, terrorism and issues such as energy security. It grades risks into three tiers with “hostile attacks upon UK cyberspace by other states and large-scale cyber crime” as one of four Tier One risks, explaining that “Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals and that unless the government takes action this threat could become worse”. (p.29). After discussing the threats the document covers the HMG response which is split across two complementary strategic objectives [paraphrase]:

- ensuring a secure and resilient UK – protecting our people, economy, infrastructure, territory and way of life from all major risks that can affect us directly – requiring both direct protection against real and present threats such as terrorism and cyber attack and resilience in the face of crime.

- shaping a stable world – acting to reduce the likelihood of risks affecting the UK or our interests overseas. (p.22)

The key points are direct protection from cyber attack and resilience to crime which is taken to mean quick adaption to criminal trends.
2.1.4 The Strategic Defence and Security Review 2010 (SDSR 2010)

This document provides the detail and response to the NSS 2010. In the main it discusses changes to the armed forces to meet the UK’s strategic direction but part 4 details the wider security issues such as terrorism, civil emergencies, energy security, organised crime, border security and cyber security (p.41). The key part of part 4 for cyber security was the government’s intention to produce the NSCP to meet the risk gap identified in the NSS 2010 (p.47). The document lists (p.47-p.49) the stated aims of the NSCP which are paraphrased in the below alongside the four Cyber Security Strategy objectives.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Crime - Tackling cyber crime by; providing a single point of contact where the public and business can report cyber crime, introducing a programme of skills development for those involved in combating cyber crime and for the Home Office to publish a Cyber Crime Strategy</td>
<td>Objective 1: The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace</td>
</tr>
<tr>
<td>Cyber Attack &amp; Defence - Improving the UK’s ability to detect and defend against cyber attack by enhancing investment in national intelligence capabilities, by creating a Defence Cyber Operations Group within the MoD, by ensuring a trusted industrial base in the CNI and the creation of a Cyber Infrastructure Team within the Department for Business, Innovation and Skills (BIS).</td>
<td>Objective 2: The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace</td>
</tr>
<tr>
<td>Cyber Relationships - Build cyber security relationships. This includes improving good relationships (UK-US) by signing Memorandum of Understanding for cyber operations and creating new relationships.</td>
<td>Objective 3: The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies</td>
</tr>
<tr>
<td>Cyber Knowledge - Sponsor long term cyber research and introduce a programme of cyber security education</td>
<td>Objective 4: The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives</td>
</tr>
</tbody>
</table>

Table 1 – NSCP (SDSR 2010) actions mapped to Cyber Security Strategy objectives
2.1.5 The 2009 National Cyber Security Strategy

The 2009 Strategy was the UK Government's first attempt at a cyber security strategy and its aim was to "to secure the UK's advantage in cyber space by the following strategic objectives of reducing risk and exploiting opportunities by improving knowledge, capabilities and decision-making" (p.4). To achieve this aim the Government’s intention was to establish an 'Office of Cyber Security' and a 'Cyber Security Operations Centre'. The former was to provide strategic leadership within the Cabinet Office while the latter was to co-ordinate incident response through CESG/GCHQ (p.20). It also intended to establish a cross-governmental programme to address priority areas and to work closely with the wider public sector, industry, the public and with international partners (p.5).

Creation of the Office of Cyber Security did leave the Cabinet Office with two organisations with similar aims; the Central Sponsor for Information Assurance (CSIA) and the Office of Cyber Security (OCS) and it was noted that parts of the cross governmental plan had already been started under the auspices of the Information Assurance strategy led by the CSIA (p.11). One interesting point of the 2009 strategy in relation to cyber warfare is that "the defence and exploitation of information systems are increasingly important issues for national security" (p.14) which shows that offensive capabilities were increasingly being thought about. OCS and CSIA did merge shortly afterwards and formed the Office of Cyber Security & Information Assurance (OCSIA).

2.1.6 Cyber Crime Strategy 2010

The Home Office linked their document to the ACPO E-Crime Strategy and Cyber Security Strategy. Its intent was to make "the internet a hostile environment for financial and child sexual predators" (p.17), creating a classification scheme for recording cyber-crime (p.21), launching Action Fraud (p.22) and by forming the Police Central e-crime unit (PCeU) "to lead the police response within the UK" though the ACPO e-crime strategy, published in 2009 set out the work of the PCeU in delivering an operational response to
the most serious of e-crime incidents. (p.23). To improve international working
the Home Office proposed to support the specialist police units develop their
own international relationships, especially SOCA who would lead

2.1.7 Historic Documents
The Cyber Security Strategy 2009 has its roots in documents dating back to
2003 when the Cabinet Office published their first Information Assurance
strategy with the aim to harmonise and improve security in government IT. In
2004 the Cabinet Office CSIA produced ‘Protecting our Information Systems’,
which supported the 2003 strategy by setting the “Government’s approach to
dealing with the various risks and threats facing information systems across
the UK” and expanding its reach to cover public and private IT. The document
covered five ‘key’ areas that Government were addressing, these were
combating hi-tech crime; promoting education and awareness; increasing
protection; addressing training and skills for professionals and international
coopération (p.10). It is very notable that these work areas are very similar to
the objectives in the 2011 strategy.

By 2007 a revised National IA Strategy was developed which broadened the
2003 approach to cover the whole of the UK (p.1). This strategy proposed a
2011 vision that ensured “A UK environment where citizens, businesses and
government use and enjoy the full benefits of information systems with
confidence”. It was widened due to the Government intent “to bring wider
benefits to industry and the general public” (p.2) due to “significant increase in
the threat to information and information systems, particularly that associated
with the rise of the internet and the ability to attack and disrupt at a distance”
(p.5). These historic documents highlight that the government cyber security
response began 10 years ago and the vision for 2011 is very similar to the
2015 vision.

Section 2.2 – Discussion and Analysis

2.2.1 Overview
The Cyber Security Strategy in the author’s opinion is a hybrid document;
firstly it provides further detail on the NSCP and secondly it is a historic
continuation of previous Cabinet Office documents as noted in the previous sub-section. It also takes input from Home Office strategic documents on organised crime, e-crime, fraud and various reports to further detail the threat. It is worth noting that the authors of the document the OSICA are also responsible for publication of the Government Security Policy Framework (SPF) which is not mentioned in the strategy even though it is the cornerstone of government security. One reason for this is gleaned from the introduction by Francis Maude MP which states that the strategy sets out the actions taken to reduce risk for businesses and individuals (p.5) and presumably not to the government. This sets out the hybrid nature of the document, the comment from Francis Maude and the lack of linkage to government security machinery makes the strategy detached but the NSCP funding to reduce the T1 threat is clearly linked to the broader national picture. The main point is whether this document is a serious piece of work that will shape the government response to cyber security or a piece of waffle attached with detailed information of the unclassified half of the NSCP?

2.2.2 Initial 2011 comments
Following publication of the NCSS there were a number of industry comments; a commentator from Information Security magazine was quite dismissive of the strategy describing it has having “little meat on the bone” and that its help for the information security community was to "support GetSafeOnline.org to become the single authoritative point of advice on responding to cyber threats." (Barwise, 2011). As it transpired Get Safe Online received £395,000, 0.06% of the total budget. (Home Affairs, 2013, p.35). John Colley, Managing Director of (ISC)2 in 2012 commented that an annual law enforcement spend of approximately £16 million was woefully inadequate and websites such ‘Get Safe Online’ do not provide basic advice geared towards the home user and not the professional community. Colley also mentioned the lack of consultation with the information security profession during the development of this strategy (Colley, 2012). Anderson (2012) has his own view and that was less spending on technical countermeasures at GCHQ and more on law enforcement, backed up with stronger consumer protection.
2.2.3 NSS, SDSR & NSCP 2010

The NSS 2010 approach was quite simple, it used a risk based methodology based on likelihood over impact, with high impact and high likelihood risks being T1, in this manner state cyber-attack and large scale criminal cyber-attack came as a T1 threat. To address this risk funding was allocated in the form of the NSCP detailed in the SDSR 2010, the NSCP was very true to the NSS 2010 risk with the vast focus of effort being on national cyber defence, for instance a very limited set of capabilities were promised to combat cyber-crime. This makes sense that the T1 NSS risk for cyber-crime was for large scale only and it had made a significant increase in organised crime a T2 risk. As the majority of cyber-crime is low level fraud carried out in the main by organised crime it would appear that for the NSS 2010 that most cyber-crime was ‘business as usual’ for organised crime and that the NSCP was targeting large scale crime that would make the national news, hence the resilience to crime objective in the NSS 2010. On this basis a minimal law enforcement response was required from a small specialised unit to deal the high end cyber-attack threat and offer some resilience.

In the NSCP section of the SDSR there was a section to address shortcomings of the CNI, this included ensuring that online public services are secure and support is given to the private companies running the majority of the CNI. The support, “strategic leadership” and “regulatory oversight” would be provided by a new Cyber Infrastructure Team (p.47/48). In the 2011 strategy the Cyber Infrastructure Team had disappeared and its NSCP funding breakdown allocated 10% of the NCSP to improving online public services. This was detailed as providing towards the ‘Digital by Default Agenda’ and ensuring that these services are “safe and resilient against fraud and cyber attack” (Cabinet Office, 2011, p.28), later on in the strategy under action 5 objective 2 (p.39) additional emphasis was placed on the building and maintenance of secure government networks. In their report after one year the Cabinet Office stated that they had made improvements to the Public Services Network (PSN) which included “Single Sign-on, security monitoring, more effective policing of compliance and greater network resilience”. In the Cabinet Office forward plan (2012a, p.5) that the “next phase of projects
delivered to ensure the security of information across public services”. This in
the author’s opinion is quite a significant change; instead of investing in the
security of the wider CNI the Cabinet Office has focused funds on the
upcoming PSN a project that one commentator expressed surprise that
“surely their plans already incorporate secure building of these services”
(Colley, 2012). Essentially this means that rather than fund new work the
NSCP funds are being used to support existing programmes that potentially
have gone over budget as surely the PSN programme wasn’t started without
enough funding? The PSN is a public-private partnership where private
companies build the government’s framework network to ensure that
government departments can securely communicate with each other, it
replaces the Government Secure Intranet (GSi).

2.2.4 Prior Government Strategy
One of the author’s views from reading all of the Cabinet Office strategy
documents over the last decade is that there is a lot of ‘fluff’. There are a lot of
vision statements and ‘we want’ comments. For example in the 2011 strategy
it purports to “apply a risk based approach to prioritising its response” but
unlike the NSS 2010 does not give any methodology or reference the NSS
2010. (Cabinet Office, 2011, p.22). The 2009 strategy vision is now clearly
abandoned along with the others and there is no apparent review of previous
strategies. Repeating of actions is a key point and the 2011 strategy simply
repeats a number of actions from the Home Office Cyber Crime strategy as
noted in Annex 1. Other actions are just abandoned such as in the Home
Office objective to “develop a classification scheme for recording cyber crime”
by 2010 (p.20). The lack of a clear way to record cyber-crime as made difficult
to calculate its impact and allowed hype and confusion. A despondent view is
that a lot of strategies are never implemented or followed to any sort of
conclusion, they just get replaced and recycled.

One improvement from the previous strategies released by the Cabinet Office
is that the NSCP funding ironically fix one of the major criticisms of the 2009
strategy which was to do with funding, or the lack of funding. In 2009 Dame
Pauline Neville-Jones said the 2009 strategy was a “missed opportunity” and
that “It is impossible to know how significant these announcements are
because we do not know what funding will be made available to enhance our ability to tackle cyber threats. It is also not clear how these new cyber security structures fit into the existing national security machinery." (BBC News, 2009).

Clearly both aspects funding and linkage to National Security machinery have been fixed but perhaps not how Dame Neville-Jones intended, especially the linkage to the NSS 2010 but not the SPF. Another generally good point is on the historical side the Cyber Security Strategy has followed the precedent of previous documentation aims and objectives but the negative side a lot of these documents have generally failed to deliver and the 2011 strategy could join them.

2.2.5 Statistics and Hype

Statistics for the document are another element of contention. OSICA commissioned Detica to provide a report on the cost of cyber of which choice statistics were published. On the flip side and supporting the earlier ‘fluff’ remark these statistics were widely criticised. ZDNet (Espiner) questioned the £27bn annual cybercrime cost figure by quoting a number of experts summarizing the overall opinion that (the figure) "is little more than a sales exercise for Detica, the company that researched the report". Professor Peter Sommer of the London School of Economics (LSE) called the report an "unfortunate item of British Aerospace puffery" that OSICA have put their ‘name’ to. Comment from spectators is not unusual but the Chief Scientist at the MoD due to the Detica report requested a Cambridge University team to query the figures. The team were asked to set out "what are known, what can reasonably be estimated and what can only be guessed". (Anderson et al, 2012, p.2). The subsequent report shied away from providing a annual figure due to the amount of estimates, but cast significant doubt on the accuracy of the Detica figures. This advice was followed by Price Waterhouse Coper (PWC) in the Information Security breaches report for BIS. The PWC survey based there results on 104 responses which indicated that the worst breach cost between £450,000 to £850,000 for a large organisation and £27,000 to £55,000 for a small organisation (BIS, p.18). However the Home Office and other government departments have been using the Detica figures probably for their impact value. This debate then led to Home Affairs Select Committee
in 2013 recommending that the Government “publicly distances itself from the £27bn estimate of the annual cost of e-crime to the UK economy”. (p.14)

2.2.6 Cyber Attack or Defence?
At the national security level there is a blurred line between offence and defence, quite simply defending the nation can mean that our armed forces attack first. The same works for the Intelligence Services who at times will carry out aggressive espionage for the benefit of the state. To put this into context within the NSS 2010 investment in cyber security capability is fairly complicit that it could be for offence, defence or deterrence in the same way as a nuclear missile or fighter aircraft. This is slightly outside ‘normal’ computer security in that this level of cyber security is usually based on computer system security, for example a UK business will protect themselves from cyber-attack by utilising IDS, anti-virus and other technical and procedural controls. Back to the 2011 strategy the terminology of objective 2 is based on ‘resilience to attack’ and ‘protecting our interests in cyberspace’ which will mean different things to an information security professional, a politician and the military. This issue has caused comment on the “offensive character” and hearsay MI6 Officers saying that "We can achieve a tremendous amount these days through remote exploitation rather than face to face meetings with agents". Another comment is "GCHQ's offensive capability gives the UK an edge" and John Bassett, now at RUSI and formerly GCHQ's Senior UK Liaison Officer in Washington states “that much of the new government funding has gone on, existing programmes... designed to get a really strong grip on global situational awareness" (Urban, 2013). My translation of global situational awareness is espionage. For the MoD and their element of funding it is implied that their Joint Cyber Unit impetus “came from Nato's bombing campaign in Libya” (Urban, 2013).
2.2.7 The NCSP – One year on

The following table summarises the figures from the NSCP:

<table>
<thead>
<tr>
<th>NSCP Stream</th>
<th>Percentage</th>
<th>Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Intelligence Account – building cross cutting capabilities, including information assurance</td>
<td>59%</td>
<td>£383.5m</td>
</tr>
<tr>
<td>MoD – mainstreaming cyber in defence</td>
<td>14%</td>
<td>£91m</td>
</tr>
<tr>
<td>Home Office – Tackling Cyber Crime</td>
<td>10%</td>
<td>£65m</td>
</tr>
<tr>
<td>Government ICT – Building secure online services</td>
<td>10%</td>
<td>£65m</td>
</tr>
<tr>
<td>Cabinet Office – Co-ordinating and maintaining a view of operational threat</td>
<td>5%</td>
<td>£32.5m</td>
</tr>
<tr>
<td>BIS – Working with private sector and improving resilience</td>
<td>2%</td>
<td>£13m</td>
</tr>
<tr>
<td>Total NSCP</td>
<td>100%</td>
<td>£650 million</td>
</tr>
</tbody>
</table>

Table 2 – Outline of NSCP spending (Cabinet Office, 2011, p.25)

In December 2012 the Cabinet Office produced an update of the NSCP after one year, they announced that they had spent a total of £260 million and provided a summary of the actions taken so far. The main aspects against NSCP objectives were:

- Objective 1 - £28 million to the Home Office with the main achievement of trebling the PCeU in size.
- Objective 2 - £157m on GCHQ capability, £31m on the MoD creating a joint service unit at GCHQ and £12m on improving the resilience of the Public Sector Network
- Objective 3 - International engagement and capacity building (FCO, £2m)
- Objective 4 - engagement with the private sector by BIS totalling £17m and £13m to the Cabinet Office for programme coordination, trend analysis and education, skills and awareness

Some casual analysis shows that the 13 million allocated to the BIS in table 1 has been spent and the Cabinet Office has spent half their allocation for coordination as did GCHQ spend half there allocated funding. There was some comment (Urban 2013) that an “investment averaging £162.5m per year
over four years could only have a limited effect on such a huge problem” but it is clear at the present spending rate the money will not last the 4/5 years and it is debatable whether the £650 million was anyway near enough. This was echoed by the Defence Committee who held the view that the NSCP “represents only the tip of the iceberg of the necessary cyber-security activity across government”. (2012, p.6).

The following table sets out the objectives and the government departments with the lead responsibility to take the objective forwards. Each objective has a number of actions assigned to it.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Govt. Lead</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a - Tackling cyber crime</td>
<td>Home Office</td>
</tr>
<tr>
<td>1b - Making it safer to do business in Cyberspace</td>
<td>BIS</td>
</tr>
<tr>
<td>2a - Defending our national infrastructure from attack</td>
<td>Cabinet Office</td>
</tr>
<tr>
<td>2b - Ensuring that the UK has the capability to protect our interests in cyberspace</td>
<td>MoD</td>
</tr>
<tr>
<td>3a – Helping to shape the development of cyberspace</td>
<td>DCMS</td>
</tr>
<tr>
<td>3b – Protecting our way of life</td>
<td>FCO</td>
</tr>
<tr>
<td>4a – Extending knowledge</td>
<td>BIS</td>
</tr>
<tr>
<td>4b – Enhancing skills</td>
<td>BIS</td>
</tr>
<tr>
<td>4c – Expanding Capability</td>
<td>Cabinet Office</td>
</tr>
</tbody>
</table>

Table 3 – NSCP sub objectives to lead Govt. department. (Cabinet Office, 2011, p.36-42)

Objective 2 has 83% of the NSCP funding allocated to it but it is surprising that the Cabinet Office have the lead for the actions, and that there is no action listed for the GCHQ funding element (p.39). This is again the disconnect between the NSCP funding and the additional actions of the document; objective 2 has the most funding but the actions listed in Annex A of the strategy have the Cabinet Office as lead for a minimalistic set of actions for defending the national infrastructure from attack.

2.2.8 Summary

The NSS 2010 recognised cyber-attack as a Tier 1 threat and provided funding through the SDSR 2010 for program of work to mitigate the risks (NSCP). The subsequent 2011 strategy added context, further detail, changes to the NCSP and broke down the NSCP funding. It also added a government vision, objectives and actions assigned to various government departments which were over and above the original NSCP. On analysis of the various documents the following issues became apparent:
1 Funding – Although the NSCP provides funding 83% of it is for resilience to cyber-attack and protecting cyberspace interests. At its current rate the NSCP is unlikely to last the full five years raising concern that the funding was inadequate.

2 Attack or Defence? – There is a lack of clarity caused by elements being classified of whether this is an UK cyber-attack or defence initiative. Of the funding 10% is clearly marked for securing government networks, albeit a new government network while the rest is for GCHQ and the MoD.

3 Law Enforcement – Home Office NSCP funding has gone towards trebling the PcEU in size. Clearly a benefit but potentially not enough, however consistent with the NSS but not the 2011 strategy which intends to tackle cyber crime.

4 Government or industry? – Investment has been in government infrastructure while industry is left with advice and partnership initiatives. With the majority of the CNI in private hands this may cause a security imbalance.

5 Economic of National Security impact? – The NSCP is focused on national security impacts and the strategy has mirrored this even though it purports to help business and the individual. This is due to the lack of funding for non NSS risks and the weak additional actions within the strategy.

6 Classified – The government has classified much of the work leaving a small number of specific and measurable minor actions.

7 ‘Business as usual’ – The ongoing commitment of securing government IT systems and the work of the police has been both neglected and mixed up in the actions of the strategy. The strategy fails to make the distinction between the current cyber security position (baseline) and what actions it is going to take to raise that baseline.

Going back to the first chapters concluding remarks a case was made for organised crime, espionage and cyber warfare capabilities as the priorities from the identified threats. On the face of it these issues concur with the 2011
strategy in its broad objectives but this is as far as it goes, on analysis the earlier response to organised crime is seemingly deficient; espionage is unclear due to the lack of detail while warfare capabilities appear to have been taken forward with some vigour and funding. There is clearly a reason why this has happened and the complexities of managing cyber security risk have not been examined in previous chapters where general threat and strategic response were looked at. Therefore the next chapter considers the challenges that the government faces in meeting the organised crime threat from cyber-crime and the challenges surrounding resilience to cyber-attack and protecting the UK’s interests.
Chapter 3 – The Challenges
This section is based on the major challenges in meeting the government’s response to cyber security:

- Section 3.1 – The Cyber Crime Challenge
- Section 3.2 – The National Security and Wider Challenges

Section 3.1 is focused on cyber crime as this aspect was identified as a major threat but little has been done while section 3.2 is a wider review of complex issues facing the government in its response to cyber security.

Section 3.1 – The Cyber Crime Challenge

3.1.1 UK Law Enforcement Overview
The enforcement of UK criminal law is mainly down to the police with 43 separate police forces in England and Wales. These are local territorial police forces which have the responsibility for crime in their area. They vary in size and capability from forces like the Metropolitan Police with approximately 30,000 officers to small forces of around 800 officers. The police use a system called the national intelligence model for the classification of crime and intelligence. In brief there are three levels; with level 1 being minor, local volume crime, affecting local police divisions, level 2 being cross border and slightly more serious crime and level 3 being serious crime and can be international. (Centrex, 2005, p.12). In the main police forces are predominantly focused on level 1 crime with a small, mainly reactionary specialist resource pool for dealing with serious level 3 crimes, such as murders. Larger forces have more specialist recourses but numbers can often still be small in comparison to the overall size of the force. Cyber-crime by way of its nature is in the main not serious, cross border and thereby a level 2 crime. Unfortunately for the victims of cyber-crime the police service is considered to be weak, or provides a gap in service for level 2 crime. Contrastingly the level 1 service is considered to be good. (HMIC, 2005, p.17). A reason for this is that police forces work within tightly controlled budgets and ‘cannot cope’ with demand. (Wall, 2007, p.210). In addition to local forces specialist units for level 3 crimes there are a number of national specialist police units that deal with issues such as terrorism, serious fraud, child exploitation and organised crime.
3.1.2 Law Enforcement Cyber Crime Structure

The initial level 2 cyber-crime response for the UK police service was in 2001 when the National High Tech Crime Unit (NHTCU) was formed. This unit was part of the National Crime Squad (NCS) and had a UK wide remit for cyber-crime. In 2006 the unit had a strength of 55 directly attached officers and 62 officers serving in local police forces. (Hynds, 2006). In 2006 the NCS and through it the NHTCU were joined with other law enforcement agencies to form the Serious Organised Crime Agency (SOCA) as part of law enforcement modernisation. At the same time there were planned mergers of the local police forces but this failed to materialise due to financial difficulties. (Tendler & Webster, 2006). SOCA has a serious crime or level 3 only remit and the level 2 gap was going to be plugged by regional police forces who would be better at dealing with level 2 crime. Due to regional forces not being formed the level 2 gap reappeared. Due to this in 2008 the Police Central e-Crime Unit (PCeU) was formed. (ACPO, 2009, p.1). The PCeU however had been formed on a much smaller scale and budget than the NHTCU. In 2011 Halliday\(^\text{7}\) reported that the unit had quadrupled in size to 85 officers to combat threats from ‘Hactivist’ groups such as Anonymous. Comparison of the NHTCU and the PCeU is difficult as there is now a plethora of policing units covering the responsibilities of the NHTCU. These units are; the SOCA E-crime unit for serious e-crime, the Child Exploitation and Online Protection Centre (CEOP) for child harm and the City of London police for national fraud. In the latter case the City of London police maintain the National Fraud Intelligence Bureau (NFIB) and in conjunction with the National Fraud Authority (NFA) run a reporting website called ‘Action Fraud’. It has to be noted though that the City of London police’s national services are separately funded from its core services which are delivered to the City of London. Funding for the NFIB comes from the Home Office NFA.

In 2010 Paul Stephenson an ex Commissioner of the Metropolitan Police stated that there were “385 police officers in England and Wales dedicated to online work of all kinds, around 85% are tackling child exploitation and the internet trade in child abuse images”. This figure is likely to be broken up into

\(^{7}\) This was undoubtedly funded from the NSCP, before publication of the 2011 strategy
several hundred in the various county forces making up their forensic investigation units, approximately a hundred officers in CEOP and the rest from PCeU and SOCA. However a year late this figure would have increased by around 60 as the PCeU expanded. In June 2011 the Home Office announced its detailed intention to form the National Crime Agency (NCA); this agency would absorb SOCA, CEOP and the PCeU and would have a level 2/3 remit. The level 2/3 remit was to address criticism of SOCA in its ability to “tackle organised crime at all levels”. Lord Blair another ex Commissioner of the Metropolitan Police stated “The problem is that you have three things that those agencies are supposed to do, regional, national and international, and each one has only done one or one and a half of those.” The other criticism of SOCA was that it did not succeed in building relationships with other law enforcement bodies as well as it should have. (Home Affairs, 2011, p.33). The NCA will comprise of four commands divided into border policing, economic crime, organised crime and child exploitation (CEOP). At its centre would be the National Cyber Crime Unit (NCCU). However the City of London police fraud section would remain independent and remain as the lead for internet based fraud. (Home Affairs, 2013, p.20). Another element considered to be part of the NCA was Counter-Terrorism but this was dismissed in due to the threat from terrorism would outweigh serious organised crime and the remit of the NCA would swing towards terrorism and organised crime would not get its full intention (Home Affairs, 2011, p.42).

3.1.3 The global law enforcement problem
Cyber-crime is still a global problem and the ‘local’ police are never going to completely succeed without international cooperation from other law enforcement agencies. Law enforcement also needs to cooperate at the local and national level. It needs to have the ability to liaise with business and the providers of internet services and telecommunications. Law enforcement needs the ability to progress investigations in other jurisdictions and be able to successfully extradite criminals. If another jurisdictions courts do not recognise the crime then extradition will never work. International cooperation has been described to be at two levels; procedural and organisational. The procedural level is the use of ‘soft law’ such as treaties designed to harmonise efforts. At the organisational level are organisations that can broker services
and information between law enforcement agencies and facilitate cooperation. (Wall, 2007, p.161). For the UK at the organisational level are the law enforcement bodies Interpol and Europol. At the procedural level the UK is a member of the European Union, NATO and the Council of Europe. There has been a great deal of international ‘procedural’ meetings regarding cyber-crime over the last 30 years. (Schjolberg, 2008).

In 2001 the Council of Europe (COE), a body attempting to harmonise internal and external European relations created the COE Convention on Cybercrime. The COE is different to the European Union as it has no power to legislate into domestic UK law and the Convention was voluntary. The Convention was open to international signatories and one of the leading champions was the United States. The Convention sought to improve international cooperation by; defining criminal offences and sanctions under domestic laws for four categories of computer-related crimes, establishing domestic procedures for detecting, investigating, and prosecuting computer crimes, and collecting electronic evidence of any criminal offence and lastly to establish a rapid and effective system for international cooperation. (Archick, 2006, p.2). The four categories of crime were categorised as fraud, child pornography, copyright infringements and security breaches such as hacking. (Archick, 2006, p.2). With regard to the ‘effective’ international cooperation this was to be a 24/7 scheme of law enforcement contacts. This was based on a G8 system established in 1997. (COE, 2010a). In 2009 the Federal Bureau of Investigation reported that there were 55 members of this scheme. (FBI, 2009). However since the Convention the EU have noticed that cyber-crime is rising and “the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase”. (2007, p.3). Take up has been slow and by 2013 40 (29 in 2010) countries have ratified, or put in place the convention while 51 have signed it (COE, 2013). The UK ratified it in 2011 after signing it in 2001. It is notable however that China and Russia have not signed the convention. This is the biggest problem for international cooperation, not everyone will agree to harmonise law and even when they do other law such as human rights will mean that offenders cannot always be sent to another country in case their human rights are infringed. Also even
when procedures are in place on the evidential and investigation side there is a perceived or real difficulty in the speed in which requests are processed through other law enforcement bodies. In 2013 it was said to the Home Affairs committee that law enforcement officers “often experienced difficulty in retrieving data (evidence) from sites based abroad” (p.23).

This is the crux of the matter for an e-crime in the UK originating from a third party state there is a significant bureaucratic overhead even from cooperating countries and no cooperation from many. This means that many police forces will write off e-crime as not worth the time or resource due to the difficulties involved. If law enforcement investigate and find that the originating country will not cooperate it is a waste of time and effort, if they investigate and the country will cooperate then it will likely become a long and drawn out process and the police effort will then become an issue of time and cost over reward. This means that only the most significant of e-crime will be investigated.

3.1.4 Fiscal vs. Dangerous Crime
Cyber-crime is roughly broken down into fiscal and dangerous crime. On the fiscal side cyber-crime in is just one of many areas affected by fraud. For example the British Retail Consortium’s (BRC’s) stated that retail crime of all types cost UK shops £1.1 billion in 2008/09. (British Retail Consortium, 2010). Of this figure in 2011-12 the total cost of e-crime to the retail sector was £205.4 million (Home Affairs, 2013, p.15) Around £1.1 billion of over payments were estimated to be due to fraud according to the Department of Work and Pensions and the best part of 2 billion were believed to be ‘overspent’ due to errors. (Irvine, 2010). All in all the National Fraud Authority estimated that the total cost of fraud in 2009 was £30 billion with 15.2 billion of this alone in tax evasion! (Cole, 2010). By 2013 the NFA reckoned the annual cost of fraud was £52 billion (NFA, 2013, p.2). With this kind of monetary loss the current estimated cost of cyber-crime just blends in amongst this distressing collection of figures. The dangerous side, linked to child abduction and government security could be argued is correctly the current policing priority.
3.1.5 Hyping the police response
One of the headline figures for the PCeU is the amount of ‘savings’ the unit has generated. In 2011 the Metropolitan Police published a news article stating that the unit has saved the UK economy more than £140 million in the last six months and is well on course to exceed its four-year harm reduction target. Operational activity targeting online criminals has seen the unit deliver nearly 30% of its £504 million harm reduction target in this initial period alone. The article noted that the PceU was formed based on a business case which evidenced that for every £1 invested, the PCeU would deliver £21 of harm prevention. In this case it was noted that the PceU has delivered a £1:35 harm reduction ratio. This appears to have mainly come from ‘Operation Pagode’ which resulted in ‘£84 million worth of harm’ saved and five defendants being jailed for a total of 15.5 years. The crux of the Operation Pagode case was an online forum which traded unlawfully obtained details (personal information, credit card details), BotNet details and tools and advice to commit computer offences. Evidence was obtained during 11 months surveillance that the forum was used by approximately 8000 members. Another major operation was ‘Dynamaphone’ which resulted in £5.5 million worth of harm saved and three men being jailed for 13.5 years. This was for an organised internet phishing attack on the UK and international banking system. Evidence indicated that over 900 bank accounts and 10,000 credit card details were compromised.

These ‘harm reduction’ figures have to be compared with the Dedicated Cheque and Plastic Crime Unit (DCPCU). This unit is a small unit of the Metropolitan Police which is entirely funded by the UK banking/payments sector. In 2011 (Wilson) the DCPCU contacted UK Payments, the bank-backed body representing the UK payments system, with a view to asking for more money to increase the size of its currently 25-strong operation. It was stated then that the DCPCU has an annual budget of £5m and that since being set up in 2002, the unit has prevented £370m in fraud losses, according to UK Payments. It is interesting to note that both the DCPCU and PCeU at the time had a similar number of staff and a business case based on ‘harm reduction’ in order to show ‘value for money’. However the DCPCU in 9/10 years has prevented £370m in fraud losses according to UK industry, while in 6 months the PCeU has prevented £140m in losses. This could be conceived
to be a deliberate action by the PCeU to keep police number crunchers at bay. Policing over the last decade has become more business focussed on statistics and policing units need to ensure a good return on investment in detections (crimes solved) and their seriousness. In the latter case this means that a volume crime unit (level 1 crime) will arrest and submit cases in large numbers and a major crime unit will submit sporadic murder and serious drug trafficking cases. Because of this the PCeU will be constantly measured for value and its funding subject to government grants while the DCPU is fully funded by industry and fairly secure as it provides a niche capability. The PCeU could go the same way as the NHTCU when it joined SOCA with the advent of the NCA.

3.1.6 Police capability in tackling Cyber Crime

Academically there are some concerns over the capability of the police in combating cyber-crime. Wall stated that “operationally and organisationally” the police are local “whereas cyber-crime is globalised”. (2007, p.160). Cyber-crime as stated earlier is a cross border or globalised problem and the internet has contributed to the acceleration of globalisation by its effect in “collapsing traditional geographies of distance”. (Wall, 2007, p.32). For an email, distance is the same regardless! Technology and globalisation have helped give rise to cyber-crime. Wall (2007, p.38) stated that cyber-crime “is built on ideas that transcend cultural and geographic boundaries”. He further stated that from the law enforcement point of view that globalisation “changes the relationship between the global and the local”. (2007, p.38). A common academic view is that the police were formed in the 1800’s to deal with public order and dangerous members of society and were organised at the local level. Brenner stated that the police’s sole task is to “maintain order and react to crimes and apprehend the perpetrators” (Brenner, 2007, p.13). Brenner also considered that the current policing model “is not effective against cyber crime”. (Brenner, 2007, p.13). Wall felt that the police focus on cyber-crime is based on their culture, history and tradition to deal with offenders who are ‘dangerous’, such as paedophiles and the most notorious hackers. (2007, p.166). This apparently has not changed and it will probably come as no surprise that Deputy Assistant Commissioner Leppard of City of London
Police told the Home Affairs Committee that the police are not winning the war on e-crime. (2013, p.8)

### 3.1.7 Technology change and criminality trends

Crime trends have always been changing; the author can remember joy riding in the eighties, higher burglary rates and phone fraud with the 1st generation mobile phones. All of these though have gone down due to technology; car immobilisers have stopped joy riders hotwiring cars, uPVC doors and windows with enhanced locks have reduced burglary and mobile phone GSM sim card authentication has reduced counterfeit phones. Other trends such as email account hijacking are going down as technology improves, for example the number of Google accounts hijacked had decreased by 99.7% since Google improved their security (Home Affairs, 2013, p.29). As stated in section 1.2.1 fraud figures in 2009 for electronic commerce were high but by 2011 they appear to be going down with the most notable being high street card fraud dropping by 80% since peaking at £218m in 2004. This decrease is due to the success of chip and pin and in 2011 the figure was £43.2 million. Banks now use fraud detection software to monitor and spot suspected fraudulent transactions as well as providing customers with improved software to log on which has caused a cost decrease of 24% (Financial Fraud Action UK, 2012). It is notable that the banks invest more in technology than they do in law enforcement such as the DCPU. The latter is used mainly for the most audacious of organised crime and for intelligence.

The above trends have been easy to detect and analyse as industry track the financial impact of crime while the police record reported crime. The difficulty for cyber-crime is that for recording purposes currently only violations of the Computer Misuse Act 1990 are recorded as electronic crimes. (Home Affairs, 2013, p.24). This means that other crimes are recorded as frauds, theft, content crimes and the matter is not helped by the Computer Misuse Act often been used when other traditional offences don’t fit and cannot be used. Without the quantity of e-crime or cyber-crime being understood, multiple policing units with varied responsibilities, legal carrying on with the old crime, new methods methodology and different strategic responses response cyber-crime will always be a tricky criminological discipline. With regard to the
strategic responses cyber-crime fits in the Home Office fraud strategy, the organised crime strategy and the cyber-crime strategy, as well as the Cabinet Office strategy.

### 3.1.8 Cyber-Crime Challenges Summary

So in summary:

- There is a police wide gap in cross border Level 2 crime of which cyber-crime fits
- There is no accurate picture on reported/recorded cyber-crime due to crime being recorded on traditional offences which doesn’t matter whether it is a cyber-crime or not
- There is no focused government direction to industry on improving security through technology
- There are issues with out of state law enforcement
- Cyber-crime is one of many fraud problems facing the UK and dangerous cyber-crime is the policing priority
- Police face massive demands on budgets and time meaning they go for the ‘danger’ crimes more than the fiscal, especially those with low monetary value

This led to the Home Affairs Committee stating that there “appears to be a ‘black hole’ where low-level e-crime is committed with impunity. Criminals who defraud victims of a small amount of money are often not reported to or investigated by law enforcement and banks simply reimburse victims”. (2013, p.26). The author completely agrees with the remark.

### Section 3.2 – The National Security & Wider Challenges

#### 3.2.1 GCHQ and signals intelligence

The Tier 1 Cyber Security Threat to the UK was for large scale cyber-attack and the requirement was for the UK to detect and defend against cyber-attack and to protect our interests. This resulted in the lion’s share of the NSCP funding going towards mitigating this risk and improving the capabilities of GCHQ of which details were classified. However details of GCHQ’s recent activities have been leaked by an NSA contractor Edward Snowdon. The
question that has to be asked is whether the NSCP funding has been used for defence or protecting our interests?

GCHQ is currently the largest of the UK’s intelligence agencies and takes the lion’s share of the £1.9bn budget for the intelligence services, and has a staff that is more than twice the size of the combined workforces of MI5 and MI6 (Hopkins, 2013). In 2010, it suffered what it called a £60m "super cut" in funding as part of the coalition government's efforts to bring down Whitehall spending (Hopkins, 2013). GCHQ has a long history of intelligence sharing with the United States since shortly after the second world war, when the US, UK, Canada, Australia and New Zealand signed a secret agreement on signals intelligence. The US equivalent of GCHQ, the NSA even has an intelligence site at RAF Menwith Hill in North Yorkshire. In the modern age the use of signals intelligence has broadened to law enforcement who previously only had a need to ‘bug’ telephone lines, now as a central part of organised crime strategy investment in communications interception capability will “strengthen the response as criminals move to email and other forms of internet communication”. (Home Office, 2011, p.36).

3.2.2 GCHQ and the UK-US Special Relationship
The NSA is alleged to have paid GCHQ roughly £100m since 2009 and also funds half the cost of one of the UK’s main eavesdropping capabilities in Cyprus. In return it is again alleged that GCHQ has to “have the American view in mind when prioritising work”. (Whitehead, 2013). This work it is again alleged is to intercept communications from trans-Atlantic telecommunications cables due to US law being too restrictive and the UK having a lighter legal regime and accountancy (MacAskill et al). To aide this the TEMPORA programme has meant that BT, Vodafone Cable, and the American firm Verizon Business with four other smaller providers have given unlimited access to their cables and internet traffic (Ball, 2013). For TEMPORA GCHQ is alleged to have “placed more than 200 probes on transatlantic cables and is processing 600m "telephone events" a day as well as up to 39m gigabytes of internet traffic". (Davis 2013). In June 2013 it was alleged that TEMPORA had started in January 2012 and the UK claims it has access to more internet data than the US. (MacAskill et al, 2013).
It is quite apparent that the UK puts its special relationship with the US above its relationship with the EU. In 2011 the EU produced a report about ECHELON a signals intelligence system ran predominantly by the UK and US which raised concerns over possible breaches of EU law and human rights infringements. (European Parliament, p.133-134). In 2013 the same issues have resurfaced with a US NSA programme called PRISM. PRISM is a system allowing the NSA easy access to the personal information from the databases of technology companies such as Apple, Google, Microsoft and Yahoo. The EU was alarmed by PRISM as its member states were targeted by the surveillance, in short the populace had accounts with these companies, email for instance. The EU at the time the allegations broke were in trade talks with the US and wished to bring up the PRISM issue, however Traynor (2013) stated that “Britain has blocked the first crucial talks on intelligence and espionage”. The UK, with Sweden vetoed the content of talks on PRISM to only data privacy with intelligence matters now off limits following the use of the UK veto. This effectively brings the talks to a close on jurisdiction as privacy laws in Germany for example don’t have to be followed by a US technology company whose European office is in Ireland.

Some consider that GCHQ fears disappointing the NSA and the government fear a weakening of the UK-US special relationship such as in 1973 when the US president ordered the end to intelligence sharing with the UK due to the UK’s improving relationship with Europe. (Hopkins, 2013). Overall the UK-US relationship is thought to give significant advantage to the UK and the US Congressional Research Service believe that as a close ally of the US has “often served to enhance its global influence”. (Nix, 2013, p.7). The report further states that the main areas of cooperation are on defence, intelligence sharing and economic relations, the latter bringing in substantial funds to UK business. Either way TEMPORA would have required substantial investment and there is a strong possibility that the funds came out the NSCP, especially with the dates.
3.2.3 Shaping the Cyber Space

The US has increasingly been involved in a diplomatic argument with the Chinese government. It is again alleged that Chinese hackers stole information from over two dozen weapons programs, including the Patriot missile system and the F-35 joint strike fighter. Yet neither airing grievances nor naming culprits have seemed to bother China. Chinese officials argue that China is under cyber-attack from the US (Segal, 2013). The crux of the issue appears to be that the US, unlike China, distinguishes between attacks on private industry and political and military espionage. The US is said to want to limit Chinese theft of intellectual property from US companies, but wants to ensure that US intelligence gathering is not similarly constrained. This is a fairly difficult subject and Michael Hayden, former director of the CIA and NSA said that is a hard conversation as essentially the argument is "you spy, we spy, but you just steal the wrong stuff". (Segal, 2013). The UK unsurprisingly takes a similar view to the US and Minister Lord West has stated “the UK has the ability to launch cyber attacks but does not use it for industrial espionage like some other countries”. (BBC News, 2009). In 2013 the NAO analysed the Cyber Security Strategies of 9 other countries and only the USA shared “the UK’s objective of helping to shape an open vibrant cyberspace to support open societies” (p.23). It is likely that the latter UK/US mutual goal is to gain agreement on the rules of the road for cyber espionage and stop the hacking of systems for espionage. This however will never succeed when it is for political advantage and due to this it is unlikely that cyberspace will ever be shaped to everyone’s liking.

3.2.4 Government agility and change

In 2007 DEMOS argued for a national security strategy due to government departments creating their own ad-hoc and conflicting strategies involving security. They said that government departments often claim to have a comprehensive mission and their “policies and missions are pursued by departments that are in conflict with each other, resulting in poor coordination, failure to meet policy goals and objectives, and a sense of confusion in government”. (Edwards, 2007, p.13). This reasoning has been echoed by the former head of GCHQ and CESG head Nick Hopkinson, who said that “the UK was lagging behind in our ability to respond to cyber-attacks because of a
"lack of cohesion" across agencies. This was particularly so for commercial
cyber-attack (Onwurah, 2013). For DEMOS three years later the government
followed their advice and created a strategy but some things take much
longer, in 2007 the House of Lords recommended a national cybercrime and
fraud online reporting centre should be established and that the Council of
Europe cybercrime treaty be ratified by the UK. (p.78-79). The latter was
taken care of 4 years later and cyber-crime reporting has still not happened.

Another problem is that Government departments and agencies with
responsibilities for cyber security have been in a constant state of flux. At the
steering level the Cabinet Office CSIA formed in 2001 and in 2009 it changed
into the Information Security and Assurance (IS&A) team as part of the Office
of Government CIO. It then was merged with the OCS to form OSICA. On the
law enforcement side the NHTCU merged into SOCA, remit changed and
PceU appeared. Both are now being merged to become part of the NCA.
NISCC under the Home Office became part of the FCO under MI5 and called
CPNI. Only the Security Services that have remained fairly constant but their
responsibilities are changing with more and more overlap with law
enforcement. Some new structures are also confused form the start as with
the NCA the government were unsure whether to focus the NCA on organised
crime and have a second body for economic crime (SDSR, 2010, p.52). In the
end the NCA were to have an economic unit but would not lead for fraud.

3.2.5 Government Agility for Security
The 2011 strategy talks about managing risk and for government ICT systems
the approach is fairly mature at least in structure. For government security the
SPF includes Information Assurance requirements that government
departments must follow. This policy framework mandates specified security
roles and responsibilities, high level policy documents and technical standards
to be followed. Technical standards are supplied by CESG (GCHQ Business
Unit) and are based on a series that started in approximately 2001. What this
means is that government departments are mandated to follow set standards
which if followed correctly will appropriately manage their information risk and
will provide cyber security. However pan government standards such as the
SPF are quite new, in 2010 Paul Shanes an accreditation officer for the MoD
stated that prior to the introduction of the SPF in 2008 its predecessor the Manual of Protective Security was “complex and burdensome” and that “the document was originally designed for the Cold War era, was last updated in 1994 and its content relates primarily to the threats of its time, focusing upon physical and procedural security” (p.36). The point here is even though in 2008 the government published the SPF it took them a good 10 years to reach that position and it could be argued that the impetus for the SPF was due to several serious government data losses. It is also worth noting that the author is aware of a few small government quangos where they are still getting to grips with following the SPF. The US do things slightly different with security in government departments by enacting legislation\(^8\), enforcing standards which are subject to an independent audit regime, where results are published annually. This helps focus government and public attention on departments with poor security. For the UK scrutiny of Government departments is through an annual pro-forma Security Risk Management Overview (SRMO) return to the Cabinet Office which is mainly concerned at the policy level.

The MoD is a good example of the speed in which large government department’s manoeuvre. The House of Commons Defence Committee carried out a review of cyber security within the MoD and noted the best internal structure thought process was still developing, that the role of the Defence Cyber Operations Group (DCOG) was more illusory than real and roles and responsibilities were unclear. For example the security of MoD IT systems sit under the Chief Information Officer, DCOG sits under the Joint Forces Commander, both are separate ‘business units’ within the MoD (p.4). Just like the wider government the internal parts of the MoD battle over responsibilities and structure. Why is this important, the Defence Committee made the observation that the cyber threat “has the capacity to evolve with almost unimaginable speed and with serious consequences for the nation’s security”, they pointed out the inadequacies of the government’s position and said it is time “the Government approached this subject with vigour”. (2012, p.6). The question the author has to raise is that with the many overlapping

\(^8\) Federal Information Security Management Act 2002
responsibilities across department and agencies, the government’s slow speed and other priorities such as terrorism and austerity can cyber security be properly addressed?

3.2.6 The Critical National Infrastructure

The vast majority of the CNI is run by private companies and electronic attack was seriously in the later 1990s with the introduction of NISCC. At the same time the US started a Critical Infrastructure Programme after they considered a ‘cyber Pearl Harbour’ to the nation’s infrastructure. This direction changed slightly when NISCC changed to CPNI where its remit became wider focussing in this order on physical, personnel security and then cyber security, this was due to the likelihood of a terrorist attack either physically attacking an installation or getting an insider agent into the CNI facility. CPNI are often co-located with The National Counter Terrorism Security Office (NaCTSO) who are a policing unit specializing in physical security, explosives and chemical weapons. Subsequently terrorism is the main driver for security in the CNI with security regulation and legislation⁹ being set for counter terrorism, examples in the CNI being airports and nuclear. Predominantly these regulations are in the main geared towards physical security but for the nuclear industry there is a legal definition called Sensitive Nuclear Information (SNI), protection of SNI involves the nuclear industry following a modified version of the governments SPF and associated technical IT security standards in a similar way to a government contractor which provides some defence against cyber-attack.

In the main though most of the CNI are free to act as any other UK business and maintain security as they see fit in which the core motivation was seen as “short-term self-interest” (Cornish et al, 2011, p.27). This is not surprising at the UK government would see a failure of a power station as a risk to the community or nation as people and industry go without power, perhaps leading to loss of life. For a power company the risk would be; a loss of income, potential regulatory sanction and a likely fall in share price. In short for a power company a cyber-attack leading to the lights going out in the UK is

not a risk they consider, it is a government risk. A private company only looks at the business risk which is linked to profit, or the lack of it. For companies acting outside of legislation there is no incentive to carry out security above the business risk profile. Obviously some industries in the CNI such as banking have substantial reason to follow good security practice but overall Chatham House felt that “the quality and effectiveness of cyber security management vary dramatically between and within CNI sectors”. (Cornish et al, 2011, p.27).

A view presented by private-sector participants to Chatham House is that the “government’s cyber security organization is fragmented and does not show an identifiable lead” and that data sent to the government goes into a black hole where little is received back (p.29). This is understandable as for CNI sectors are the CPNI for advice, DECC for energy security, the Dept. for Transport (Transec) for transport, the Home Office for terrorism, OSICA for co-ordination, BIS for working with business and improving skills. The latter department was also earmarked for establishing a Cyber Infrastructure Team to help regulate the CNI. This is the fundamental question does the CNI need advice or regulation, I argue that the majority of cyber risks could be mitigated by getting the basics right as per the government advice and legislation enforcing the basics will greatly improve cyber security in the CNI. To do this effectively will mean the government departments working with industry and providing a capability to audit and approve security standards without all the cost falling on the already heavily regulated industry.

3.2.7 National Security and Wider Challenges Summary
So in summary:

- TEMPORA was possibly funded by NSCP for signals intelligence to benefit the UK-US relationship.
- Political arguing and manoeuvring will limit attempts to shape cyberspace for rules on cyber-attack or crime.
- Government agility, change in responsibilities, overlapping remits at all levels will stifle the speed and quality of response.
- Legislation should be considered to ensure that both the CNI and government place more effort into cyber security.
Conclusion
Firstly the cyber threat was looked at and concluded that the main risk to the UK came from espionage and fraud based cyber-crime. Next the government response was examined which showed that cyber-attack was a high priority, that significant funding and a strategy with broad objectives were put in place to meet the cyber threat. Despite the ambiguity on what cyber-attack referred to; espionage or warfare the government response demonstrated that they took the threat seriously and that they were taking action to address the risks. On subsequent analysis it became clear that through the 2011 strategy the actions would not overly impact cyber-crime and there was doubt about whether the UK would be better able to defend itself against cyber-attack. The latter was due to the lack of clarity in improving IT security across industry and government and what GCHQ were spending their substantial funding on. The ambiguity was due to secrecy and terms such as protecting our interests in cyber space and recent leaks hinting that GCHQ has invested heavily in its core role; signals intelligence. In general the 2011 strategy provided limited actions, except those with allocated funding. This means that the strategy is unlikely to fully achieve the spirit of its objectives. I would argue that the funding has not been wasted, and will benefit the country especially in investment in cyber warfare capabilities, law enforcement and signals intelligence.

So what does this mean; cyber-crime is predominantly a fraud issue which to be tackled effectively will need substantial resource and overall is very challenging due to its international aspect and constant change. Fraud generally is a low policing priority and this is understandable due to the nature of other crimes. While regrettable that more is not being done there is progress and the issue is very visible. For cyber espionage and low level cyber warfare (cyber-attack) the strategy is seriously deficient, firstly we have no transparent idea of where the UK collectively is with regard to security, secondly there is no mechanism to track progress or co-ordinate. Government action so far has been to provide security standards, advice to industry and to publish a large number of strategies and policies. Coordination from government is the biggest problem with multiple government departments and
agencies involved all coming from different angles. So in similarity with cyber-criminal which has no accurate statistics the government has no idea how resilient its IT security posture is.

From this I think the term cyber security has caused confusion as it is essentially an umbrella term for things that were already happening. Government and industry have been securing their IT systems since the 1990’s but the major change is the level of reliance, at the same time existing crime, espionage and warfare disciplines evolved in line with IT. These existing disciplines are now causing confusion as they are still ongoing, hence for cyber-criminal an e-criminal strategy, a fraud strategy and an organised crime strategy. So in recommendation I consider that it is probably best to split cyber security into three threads; cyber-criminal as a fraud and e-criminal problem, the threat of cyber espionage and cyber-attack as an information assurance problem and cyber warfare as a domain for the MoD. To tackle cyber-criminal the government must invest in fraud capability, specialist police e-criminal units and lead industry in awareness and technology based prevention. To tackle espionage the government needs to improve information assurance by simplifying responsibilities of the large number of agencies involved and enforce standards through new legislation and audit in a similar way to the US. This will ensure it follows its own advice that the vast majority of cyber-attacks can be stopped by good information security. The three threads can be linked together to form a cyber strategy statement for overall visibility.

This work has described cyber security in the UK, described the threat and the government response personified in the 2011 strategy. It has met the objectives that were set in the PDF and I believe contributes new insights into the government’s strategic documents and brings together a number of ideas into a broad document. Most other research tends to focus on a single aspect of cyber security and this it is believed provides a broad overview of the current picture. I have enjoyed the research and overall feel the government response to cyber security an interesting mixed bag of good and bad.
Bibliography


Annex 1 – Comparison - Home Office / Cyber Security Actions

Home Office Actions
We will review the current legislation with the aim of future-proofing it and ensuring the continued relevance of it to the fast-moving world of the internet particularly with regard to the ability to commit crimes on an industrial scale. We will ensure that legislation across relevant departments considers the impact of cyber crime.
As part of the work led by the Ministerial group to consider whether the existing legislation is adequate for tackling cyber crime, we will also consider whether the sentences for crimes committed on the internet fully reflect the seriousness of the crime, and the scale on which they are attempted or perpetrated.
The Government will continue to support these specialist units, and will work with the ACPO e-crime Committee to ensure that there is a police and law enforcement agency response to financial crime.

We will learn from the experience of developing Action Fraud (the National Fraud Reporting Centre (NFRC)) and the Consumer Direct online reporting facility, as well as that of CEOP, and consider how best to receive and record reports of crime and attempted crime not only of fraud on the internet, but also for other internet crimes where there is no existing reporting centre.

We will work with Get Safe Online and business to raise awareness of the issues, and will consider how best to publicise the safety message through that website.

We will encourage Get Safe Online to link with Consumer Direct and Direct.gov to ensure that this is available to the public.
We will work with industry to ensure that GSO contains clear guidance on where to go to get further information on specific topics, and where to get practical solutions, such as antivirus software and updates for existing software.
We will work to make sure that Government webpages contain a link to Get Safe Online, and that GSO also shows links to other Government activity, such as CEOP, to protect children. We will identify how the GSO message can be communicated effectively.
We will consider, with international partners, whether the existing arrangements for securing data for use as evidence is quick enough.
Through international negotiation we will seek to further changes to ensure that unacceptable, damaging and harmful conduct against computers and committed through computers investigatory powers are effective to assist in investigating computer crimes.
We will seek to improve the standards of international legislation pertaining to e-crimes, international cooperation and associated investigatory powers through the UK’s participation in international fora, and overseas influence and assistance.

Cyber Security Strategy 2011 Actions

Review existing legislation, for example the Computer Misuse Act 1990, to ensure that it remains relevant and effective.

Encourage the courts in the UK to use existing powers to impose appropriate sentences for crimes committed on the internet.
Create a new national cyber crime capability as part of the new National Crime Agency by 2013.

By the end of 2011, build a single reporting system for citizens and small businesses to report cyber crime so that action can be taken and law enforcement agencies can establish the extent of cyber crime (including how it affects individuals and the economy).
Support GetSafeOnline.org to become the single authoritative point of advice on responding to cyber threats (for example, the recent publication of an internet safety guide).

Promote greater levels of international cooperation and shared understanding.