Does the United Kingdom's Cyber Security Strategy Represent a Missed Opportunity?

By

Gavin E L Hall

August 2013

Submitted in partial fulfillment of the requirements for the degree of Master of Arts in Terrorism, International Crime & Global Security

Abstract

The United Kingdom Cyber Security Strategy has been criticised as a missed opportunity. This dissertation explores this challenge by analysing the objectives of the Cyber Security Strategy, the core conceptual foundations that underpin the cyberspace environment and criticism that the UK is in a strategic malaise and unable to develop strategy anymore is examined. Whilst there has been success attributed to aspects of the strategy this paper will illustrate that there is scope for improvement for the next instalment in 2015.

A significant problem when discussing the cyberspace environment is the lack of universal terminology which causes a degree of confusion and ambiguity for arguments as there is no common basis of understanding. This paper asserts that developing such a basis is needed to establish a basis for which discussion and analysis can follow. Therefore, consistent terminology is developed by examining the understanding of cyber and cyberspace to enable a clear conception of what constitutes a cyber-crime, cyber-attack and cyber-weapon. This enables the strategy to be examined on a consistent level and conclusions drawn as to whether it is a missed opportunity.

Contents

List of Illustrations

Abbreviations

AV	- Anti-Virus
CCDCOE	- NATO Cooperative Cyber Defence Centre of Excellence
CESG	- Communications Electronics Security Group
CIP	- Critical Infrastructure Protection
CPNI	- Centre for the Protection of National Infrastructure
CSS	- Cyber Security Strategy
DDoS	- Distributed Denial of Service
DOD	- Department of Defence
DOJ	- Department of Justice
ENISA	- European Network and Information Security Agency
EU	- European Union
GAO	- United States Government Accountability Office
GCHQ	- Government Communication Headquarters
ICT	- Information Communication Technology
IMU	- Innovative Marketing Ukraine
MOD	- Ministry of Defence
NATO	- North Atlantic Treaty Organisation
NCA	- National Crime Agency
NCSP	- National Cyber Security Programme
NSC	- National Security Council
NSS	- National Security Strategy
OECD	- Organisation for Economic Co-operation and Development
PLC	- Programmable Logic Controller
POTUS	- President of the United States
SDR	- Strategic Defence Review
SDSR	- Strategic Defence and Security Review
UNDOC	- United Nations Office on Drugs and Crime
ZDE	- Zero Day Exploit

Introduction

This dissertation will analyse the argument whether the UK Cyber Security Strategy (CSS) represents a missed opportunity (McGhie 2012). Jermy posits that there are a number of ways in which a strategy can be challenged (2011). This paper will utilise three of them; the strategic development process, the assumptions used to underpin the strategy and that the strategy derived is in itself weak or ineffectual (Jermy 2011). The analysis will examine the conceptual arguments that underpin the CSS relating to interdependency and the understanding of cyber and cyberspace. Then an overview of the CSS and the process that developed it will be analysed before moving onto to assess the four objectives of the CSS in turn.

Much thought has been given as to how best to assess the CSS. Consideration was given to utilising the ends, ways and means strategic paradigm. However, the disjointed nature of the CSS and general National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) makes this almost impossible to do in individual sections, as the ends, ways and means are entwined within multiple documents without the necessary coherence to enable analysis. Similarly presenting the various different arguments then analysing the UK as a form of case study was discounted as the key points would have been separated between different segments of the paper. Therefore, an appropriate methodology appears to be to study the CSS via the objectives it purses.

The analysis will begin by looking at the conceptual foundations that provide the bedrock of analysis for cyber-security. The chapter starts by outlining whether cyber-security can be enacted on the basis that the world relies on the same level of interdependency, before moving on to analyse the debates surrounding the core conceptions of cyber and cyberspace. These areas enable a clear definition of the core terminology surrounding the debate that is often lacking in the literature.

Chapter 3 introduces the components of the UK CSS and highlights how the strategy was derived. It aims to illustrate the reasoning behind introducing the strategy and to identify the objectives of the strategy and the levels of funding available. The next chapter takes a wider consideration of a strategic malaise within UK strategy making in general into consideration. This will develop a greater understanding of the strategic environment that developed the CSS.

Chapter 5 examines each objective in turn. The guiding principle for each section is to identify the central debates that the individual objective being examined generates. Consequently, this results in Objective #1 and Objective #2 having a larger content due to the areas being analysed. Objective #1 focuses on the elements of the cyber-crime debate and whether this represents a new form of

criminal activity outside existing legislative provisions and who the perpetrators of cyber-crime are. Objective #2 considers that in order to identify with a more resilient UK that the threat has to be identified, and so looks at the threshold for cyber-attack and from this cyber-weaponry. Objective #3 analyses the establishment of international norms for conduct in cyberspace and the debate surrounding an open, vibrant and safe cyberspace. Finally, Objective #4 considers the increase in cyber-security specialists that the CSS calls for.

The arguments raised during this process will be pulled together in the conclusion so that whether the UK CSS represents a missed opportunity can be assessed. A wide range of different sources are used to develop the argument and it should be noted that the CSS has not been the subject of rigorous academic analysis, unlike the NSS and SDSR process. Consequently, some of the main forms of comment on the CSS originate from committee's in both the House of Commons and House of Lords. It should be remembered that it is the role of a committee to critique and scrutinise the government, which results in the potential for a skewered analysis in this direction. Similarly, the cyber-environment is continually evolving with books and journals unable to keep up. Therefore, a number of media sources have been used to ensure that the full scope of the debate is catered for. However, the central arguments of this paper are based on the core academic literature so the effect of reliance on committee reports and the media, for the most recent information, should not lead to impugned conclusions.

A central theme of this paper is the need for precise and defined terminology that can allow a debate and analysis to be generated on the basis of common understanding. Therefore, as well as illustrating the debates regarding what the key conceptions of the cyber-environment entail, consideration was also given as to how to present words with the cyber prefix. For example, cybercrime is also presented in the literature as cyber crime and cyber-crime. Despite, cyberspace appearing to set precedence, the format of cyber-crime will be adopted throughout as it enables clarity and keeps in line with the premise of cyber as a prefix[1].

[1] With the exception of cyberspace as this is already an established term in common usage and direct quotations which remain unaltered.

Conceptual

This conceptual section develops the argument as to whether the CSS represents a missed opportunity on the basis that the assumptions made are considered to be normative, and as a result does not take into account the full scope of the debate regarding the concepts of cyber and cyberspace. Considering Objective #3 of the CSS, which will be analysed in full during chapter 5, relates to establishing acceptable behavioural norms within cyberspace, and the London Conference on Cyberspace it would appear to a cursory glance that the UK is at the forefront of the debate (Hague 2011). However, this section will highlight three key assumptions which impact the discussions throughout this paper, which the CSS demonstrates are able to be challenged, interdependency, cyber and cyberspace. Furthermore, a much clearer understanding of the problems within the cyber environment will be gained thus enabling solutions to a number of the issues that the CSS presently struggles to deal with.

Interdependency

Perhaps the most basic assumption of the Information Age is that global interdependency exists and, furthermore, that it is increasing at an unprecedented rate (Akamai 2012 and Clemente 2013). The CSS concurs by devoting the opening chapter to the assumption where it states that,

> 'the internet is already having a profound impact on the way we live our lives. This social change will only grow and gather pace as the number of users increases. Already it looks like it will be on the scale of the very biggest shifts in human history, such as the coming of the railways, or even learning to smelt metals' (Cabinet Office 2011: 11).

However, this view is contested with arguments that some countries are becoming increasingly hypoconnected as opposed to hyperconnected (Quenqua 2011 and Tofler & Tofler 1993). The origins of the argument are based on the assertion that the developing world is still substantially agricultural in its base economy and lacks lack the necessary economic diversification to require interdependency and connectivity (Tofler 1980 and Tofler & Tofler 1993). The developed Western economies, on the contrary, have already undergone the full process of economic destruction and reconstruction necessary to enter the Third Wave, or the Information Age (Tofler 1980). Essentially, the point made is that the world cannot be viewed as a unified body whilst there is still substantial discrepancy between the Global North and South. This has important implications for the development of a cyber-security strategy, particularly in regard to developing closer ties with allies and international organisations, such as the European Union (EU) or North Atlantic Treaty Organisation (NATO).

Jermy identifies that flawed assumptions are a reason for a strategies failure (2011). In terms of the general cyber debate this is especially true in regards to the 'imprecise terminology [and] a certain reluctance to abandon the notion that cyber conflict is unique and sui generis, rather than being just another new technology applied to warfare' (Lewis 2010: 1). Indeed adopting a universal terminology is central to allowing a debate to be fostered on the basis of common understanding from which analysis can be generated. The issue is confounded by misuse of terminology, which often overlaps and is applied interchangeably, by institutions and authors seeking adaptation to their own agendas and objectives (Yannakogeorgos 2013a). This is confirmed in a report to the Organisation for Economic Cooperation and Development (OECD) which states that 'analysis of cyber security issues has been weakened by the lack of agreement on terminology and the use of exaggerated language' (Sommer and Brown 2011: 6).

The cornerstone of the cyber security debate is the etymological and conceptual understanding of cyber and cyberspace. By examining these two areas it becomes possible to conceive cyber-security issues on a much deeper level.

Cyber

During the formulation of any analysis it is important to develop a base reference point from which analysis can be derived. In terms of the cyber security strategy debate then a logical start is the understanding of the word cyber. This analysis focuses on the etymology of cyber as a prefix that can then be applied to a variety of different terms to denote that specific attention is being drawn to the areas associated with cyberspace.

Cyber is derived from cybernetic, which itself comes from the Greek adjective κυβερνητικός meaning skilled in steering or governing; cybernetics denotes a functional process and the control of speech. This means that the use of cyber as a prefix has a semantic contextual accuracy, as long as it is used to denote control of whatever is represented by the word it precedes (Straubhaar, LaRose & Davenport 2004). Therefore, it follows that cyber-attack is an attack within cyberspace and cyber-crime is a crime within cyberspace.

The example of cyber-terrorism will be used to illustrate the concept of cyber as a prefix. From an etymological standpoint the central word is terror, with a prefix of "cyber" and "ism" as a suffix. As such cyber-terror is a different concept, with a different meaning to cyber-terrorism. Therefore, for an action to be considered cyber-terrorism it must first meet the requirements to be considered an act of terrorism in its own right.

How to define terrorism is a highly contested area. For the purpose of this paper it is noted that terrorism is the use of violence by non-state actors to achieve a political goal (Kydd & Walter 2006). Furthermore, terrorism is also a much more sophisticated rational action that has specific political goals (Drake 1998). Consequently a working definition of terrorism would involve it as a rational action involving the use of violence by non-state actors to achieve a specific political goal. Therefore, for an act to be considered as cyber-terrorism it must be a rational action, use violence, involve non-state actors and be politically motivated. By definition if any of these criteria are not met then it cannot be considered to be act of cyber-terrorism.

Even if a different definition of terrorism is applied then the criteria for the cyber-event would be adjusted on the basis of the changes. However, some authors have tried to rework cyber-terrorism on the basis of actions witnessed in order to try and define them as terrorist acts without any thought to the etymological origins of the word. These attempts devalue the terminology to a point whereby any real meaning is lost. Dorothy Denning proposes such a re-alignment by replacing the violence criteria with any form of cyber-intrusion, even though she specifies that this is 'without engaging in violence' (2009: 7). Furthermore, Denning offers the definition that enables acts to be defined as cyber-terrorism even though they may be removed in both time and space from the actual act of terrorism (2001: 281). Introducing the element of how far removed from the event a precursor action takes place is unhelpful and only seeks to dilute the notion of terrorism (Macdonald 2013 and Macdonald, Jarvis & Chen 2013: 17). This confusion is not just restricted to individuals but also to corporations who are intrinsically involved in the cyber-environment, such as Symantec who argue for different categories of cyber-terrorism by establishing their concept of 'pure cyberterrorism' (Gordon & Ford 2003: 8).

Although this is only a fraction of the debate surrounding cyber-terrorism the importance of having clear understanding of the terminology rooted in the etymology of the core word needs to be appreciated. Attempting to change and adapt the central meaning and conception being analysed only serves to devalue the overall subject being discussed to the point where little true meaning is lost and any common basis for sustained analysis is lost. This remains true for any other term that the cyber prefix is attached to.

Cyberspace

Following on from the analysis of cyber the debate surrounding the nebulous concept of cyberspace can be analysed. The United States takes a different doctrinal position to the UK by considering cyberspace as the 5th domain. The *National Strategy to Secure Cyberspace* (POTUS 2003), the *National Security Strategy* (POTUS 2010), the *International Strategy for Cyberspace* (POTUS 2011),

the *Department of Defense Strategy for Operating in Cyberspace* (DOD 2011), and the review of cyber-strategy by the accountability office all make no attempt to define what cyberspace is (GAO 2013). Only the US Air Force provides a clear definition whereby 'cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers' (USAF 2011: 1). This is the normative view of cyberspace as being a technology which does not consider additional elements of the environment that complete cyberspace (Yannakogeorgos & Mattice 2011).

Despite the different UK doctrinal position, the CSS follows in a similar vein. However, it does contain potential scope for an appreciation for a broader conceptualisation.

> 'Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services. Digital networks already underpin the supply of electricity and water to our homes, help organise the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK. And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances' (Cabinet Office 2011: 11).

Richard Clarke, former White House cyber-tsar, provides a similar line of thought by highlighting that cyberspace is not just the internet and that cyberspace is made up of lots of other networks, which are separate from each other (Clarke & Knake 2010). Similarly, Folsom 'proposes that cyberspace be defined as an embodied switched network for moving information traffic, further characterised by degrees of access, navigation, information-activity, augmentation (and trust)' (2007: 75). Therefore, the premise develops that cyberspace is not just the internet but still a phenomena firmly rooted in the technological sphere.

Analysis of international law does not help to clarify the issue, as there is no universally accepted legal definition for cyberspace or its values (Folsom 2007). The Tallinn Manual has sought to try and address these issues. However, it makes no effort to define cyberspace other than in the glossary which implies that the term is non-contentious. 'Cyberspace: The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks' (Schmitt 2013: 211).

Despite the differences in the strategic perspective of the United States, NATO CCDCOE[2] and the United Kingdom all of these definitions above are focused on the technical aspect, even allowing for the broader concept put forward in the CSS.

Contrary to the debate on cyber there is no etymological basis for analysing cyberspace due to the term having no semantic meaning as the space being controlled is virtual not kinetic. Its origins lie in William Gibson's science fiction novel, Neuromancer (1984). Cyberspace is a metaphor that has been utilised in association with Information Communication Technology (ICT) to such an extent that it is accepted as normative with little question posed to the actual meaning (Betz & Stevens 2011). Indeed the metaphorical concept of machine-mediated communications began over one hundred years ago, with the introduction of the telegraph system (Standage 1999), and it can even be argued that the *Cursus Publicus* from the Roman era and the *agora* of Greek city states fit into the parameters imposed by the restrictive view of this metaphorical concept (Betz & Stevens 2011, Maguire 2013 and Macdonald, Jarvis & Chen 2013: 13). Therefore, the technological focused concepts of cyberspace are only a working concept of cyberspace and a much deep conceptualisation is needed to be able to truly grasp the core issues, as long as computers remain non-sentient then the core threat emanating from cyberspace is people (Betz & Stevens 2011).

'Cyberspace has the sole purpose serving human operators and creating effects in the physical world' (Yannakogeorgos & Mattice 2011: 1). This is a fundamental realisation that cyberspace is not the exclusive domain of the internet but rather that it is focused on a multitude of interconnections between the human and technology (Clark 2010). David Clark in his model of cyberspace highlights four interconnected top-down layers – people, information, logic and physical (2010). It should be instantly apparent that this conceptualisation differs from Richard Clarke's, and a number of other definitions discussed earlier, with the explicit inclusion of people. People are not just passive users within cyberspace but rather how they use and interact within cyberspace helps to define and shape cyberspace, which makes the concept a continually evolving and dynamic idea (Clark 2010). Figure 1 illustrates this conception of cyberspace.

[2] NATO CCDCOE is a private company that is supported by NATO therefore, any publications are not NATO directives but rather the product of a think tank (Atlantic Council 2013).

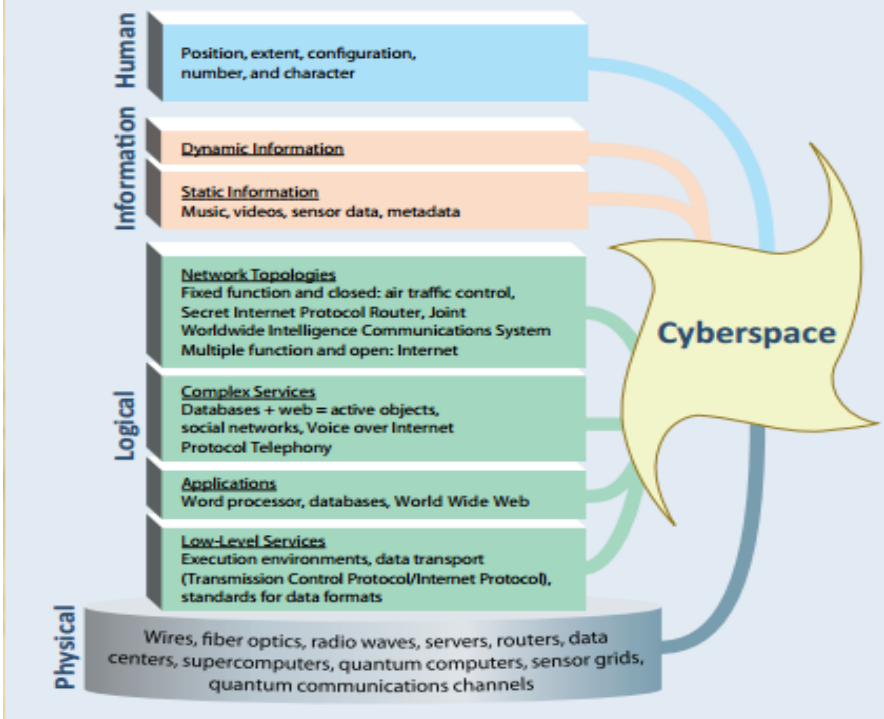


Figure 1. Visualisation of Cyberspace (Yannakogeorgos & Mattice 2011: 2)

Cyberspace can be seen to be the hierarchical nexus ranging from the physical hardware that makes up network systems, to the logic that drives the creation of these systems, to the raw data and information transmitted within and between networks, and concluding with the human interface that provides both instructions to the network and receives data from them (Clark 2010).

The ramifications of this reconceptualization of cyberspace are wide-ranging, as the inclusion of the human, whether a casual user or an information warrior, as a key component of cyberspace means that the basis for cyber-strategy still remains the same as in the Second World War, or the Napoleonic War, or the Hellenic War. Conflict at its core is the reciprocal interaction of human choice and hence 'cyberspace has not had any single, overarching effect on all fields of human activity - cultural, economic and military' (Betz & Stevens 2011: 12). Furthermore, despite the claim that 'cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land and maritime' (USAF 2011: 2), it can be percieved that cyberspace has altered operations in the military sphere far less than it was supposed to, or believed to be (Betz & Stevens 2011).

The United States doctrinal view of the 5th domain, and the establishment of the United States Cyber Command sets cyberspace apart as a separate domain distinct from the kinetic world. It should be rapidly apparent that by utilising the visualisation of cyberspace in Figure 1 that humans provide commands to equipment that retrieves data and information via a physical infrastructure that has

been designed and built by humans. How this paradox will unfold is unclear, although the US Army has made a detailed study that incorporates this broader conceptualisation of cyberspace (Department of the Army 2010: 8). Therefore, questions can be raised as to whether the CSS would have benefitted from giving the conceptual aspects of interdependency, cyber and cyberspace more rigorous thought.

Now that an analysis of some of the core conceptual foundations of cyber-security strategy has taken place this paper can move on and look at the specific detail of the CSS. This will begin with an overview of the strategy itself, before examining the strategic malaise that Britain is said to be in. The four objectives of the CSS can then be analysed as to whether they represent a missed opportunity.

United Kingdom Cyber Security Strategy

The purpose of this chapter is to set out what the UK Cyber Security Strategy entails so that whether it represents a missed opportunity can be analysed in the following sections. Even though a previous attempt at a CSS was made in 2009 the current CSS is still very much seen as part of an inaugural process (Cabinet Office). However, the UK approach to cyber-security strategy is somewhat convoluted and arguably the result of a cost-cutting agenda (Cornish & Dorman 2001 & Fox 2010). There are a number of different organisations that contribute to the provision of cyber-security and there are issues with unity of command that do not help the process (Leonhard 1998 and Farmer 2010). However, this paper is focused on analysing the CSS and limits its terms of reference to the actual document. Therefore, this chapter will outline the core objectives of the CSS so there is no confusion with regards to what is being examined.

In May 2010, shortly after coming to power, the coalition government established the National Security Council (NSC) with the brief to oversee Britain's security and coordinate responses to threats to the UK, military or otherwise (BBC 2010a and MOD 2010). The UK has not had a coordinated body responsible for national security strategy since the Committee for Imperial Defence, which operated from 1904 until 1939 (Johnson 1960 and Lobell 2004). Therefore, this marked a significant change in approach of strategy formulation and the establishment of a National Security Strategy (NSS) represented an opportunity for a fresh examination of threats and capabilities in the modern world (HM Government 2010a). However, Prins posits that a critical difference exists between the NSC and CID, due to the NSC operating by report whereas the CID operated via committee (2011).

This is a significant distinction as it effectively means that the formulation of strategy is constrained to the civil service, which does not necessarily involve the sustained debate and direct outside influence that expert advice brings to a committee (Boys 2012). Furthermore, the NSC is not a statutory institute of the UK Government, rather it is the mechanism that the present coalition have formulated to orchestrate the UK's national security provision (Bangham & Shah 2012). Therefore, it would be perfectly feasible for a new government to remove the NSC. A permanent statutory NSC would not only be a focal point for improving UK strategy but also as a constitutional check on the power of the Prime Minister (Bangham & Shah 2012).

Previously the UK had relied on infrequent Strategic Defence Reviews (SDR) and the occasional update or amendment as situations required. For example, the last SDR was undertaken in 1997 and

focused on traditional military roles (MOD 1998), following 9/11 the New Chapter was added (MOD 2002) and a white paper was presented in 2003 to provide greater focus on terrorism and the proliferation of Weapons of Mass Destruction (MOD). In line with the increasing broadening and deepening of the security debate the most recent review sought to embrace the challenge that defence and security are not necessarily homogeneous by establishing the 2010 Strategic Defence and Security Review (SDSR) (Buzan 1991, Buzan, Waever & de Wilde 1998 and HM Government 2010b). The NSS and the SDSR were published concurrently in October 2010 and, therefore, the overall security of the UK is a product of both documents (HM Government n.d.a).

The substantial changes that have occurred in the global security situation since 1997 provide a clear need for a review of national security priorities. The government has routinely updated its National Risk Assessment (Cabinet Office 2008[3]). Figure 2 shows the diverse range of factors that are considered. For the 2010 NSS the process had become the National Security Risk Assessment (NSRA) and the methodology employed is provided in Annex of the NSS (HM Government 2010a). However, the NSRA is criticised for the methodology employed and that the government appears unwillingly to discuss the issue, citing the need for secrecy (House of Lords and House of Commons 2012). A significant source of tension arises from the following statement in the NSS that the NSRA process,

> 'provides an insight into potential future risks, so as to contribute to decisions on capabilities for the future. It does not directly address immediate security issues. Thus we did not include in the NSRA a risk directly related to a conflict in Afghanistan, since we are already engaged there. But we do include risks of future terrorism and risks of future conflict' (HM Government 2010a: 26).

How this process identifies cyber-events as a Tier 1 threat is confusing as it is considered an immediate threat, which would also mean that it would not come under the purview of the NSRAs brief (House of Lords and House of Commons 2012: 9-10).

[3] Unfortunately the 2010 document, with an update in 2012, has been unavailable for some time while it is checked for a virus <https://www.gov.uk/government/placeholder>

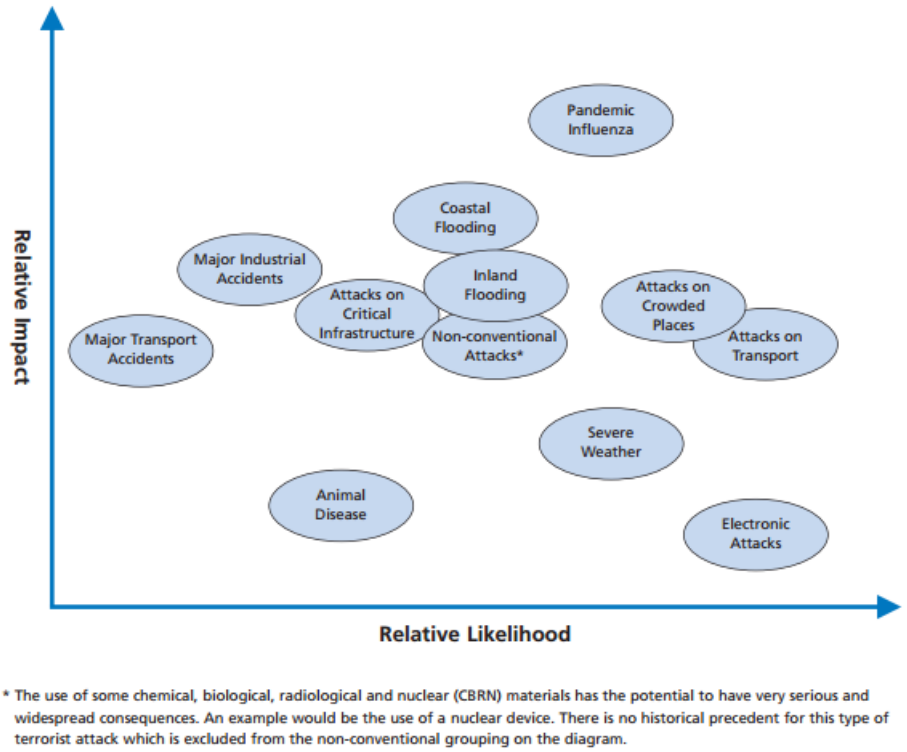


Figure 2. National Risk Assessment (Cabinet Office 2008: 5)

The NSRA enabled the NSS to establish four Tier 1 threats to the UK (HM Government n.d.b), which are international terrorism, international military crises, major accidents or natural hazards and '**cyber attack**, including by other states, and by organised crime and terrorists' (HM Government 2010a: 11). The strategic nexus of ends, ways and means is seperated between the NSS and SDSR. The NSS aims to 'develop a transformative programme for **cyber security**, which addresses threats from states, criminals and terrorists; and seizes the opportunities which cyber space provides for our future prosperity and for advancing our security interests' (HM Government 2010a: 34), whilst the SDSR looks to address how the 'balance between resources and commitments' can be maintained for the next five years (HM Government 2010b: 17).

The Cyber Security Strategy continues with the separation of means from ways and ends. It states the following objective:

> *'Our vision is for the UK in 2015 to 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'* (Cabinet Office 2011: 8).

To achieve this objective the Cyber Security Strategy sets out four objectives, which are illustrated below in Figure 3. It is interesting to note that Objective #4 is set out as the foundation on which the other three objectives are able to be built.

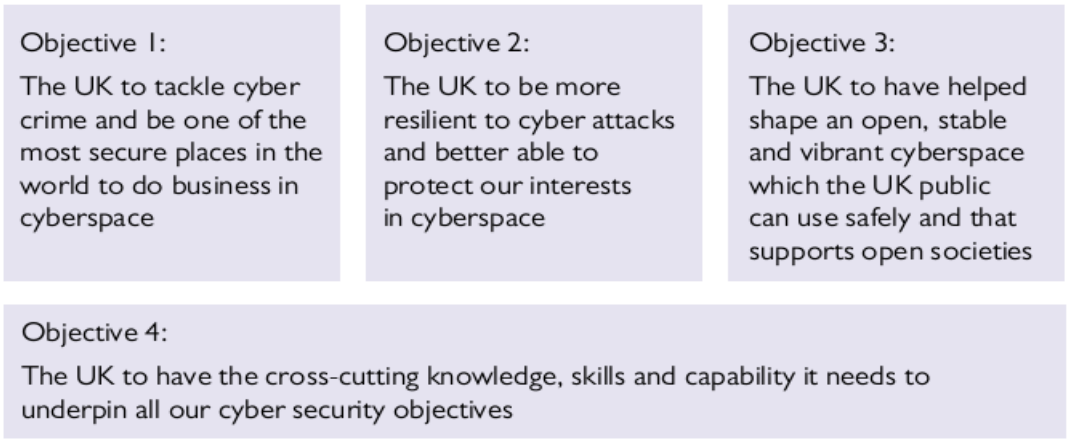


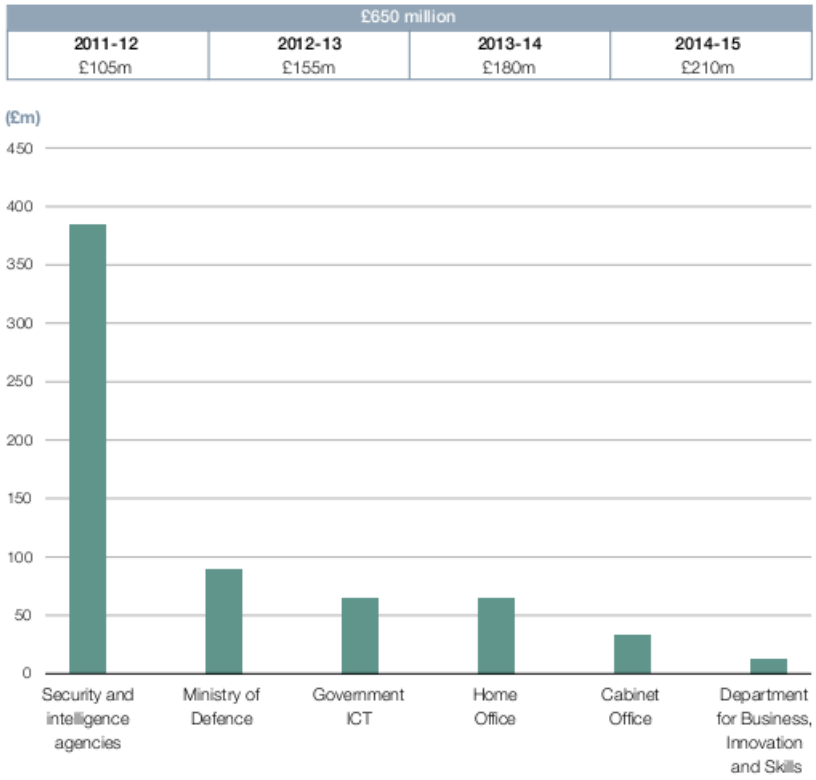
Figure 3. UK Cyber Security Strategy Objectives (Cabinet Office 2011: 21)

Therefore, it would appear that Objective #4 is the most important as it effectively enables the other areas of the strategy. Indeed, when we consider the interdependent relationship between the human and technology it becomes obvious that humans need adequate technology in order to utilise their skills, and that technology needs humans of sufficient calibre in order to gain the maximum benefit from it (Andress & Winterfield 2011).

The means aspect for the provision of cyber security is provided by the National Cyber Security Programme (NCSP), as established in the SDSR, which will be coordinated by the Office of Cyber Security and Information Assurance (OCSIA) (n.d.). The NCSP is supported by £650 million over the period from 2011-2015 (HM Government 2010b: 47). Figure 4 illustrates how the budget is allocated over the four year period and also the different branches of government that the OCSIA coordinates with. The Centre for the Protection of National Infrastructure (CPNI) also falls under the overview of the OCSIA, but is not directly funded by the NCSP.

Breakdown of £650 million funding for the National Cyber Security Programme (2011-12 to 2014-15)

Funding has been allocated to six areas over the four years



	Security and intelligence agencies	Ministry of Defence	Government ICT	Home Office	Cabinet Office	Department for Business, Innovation and Skills
£ million	384	90	65	65	33	13
Percentage	59%	14%	10%	10%	5%	2%

Figure 4. Breakdown of Funding for National Cyber Security Strategy (NAO 2013: 16)

This chapter has provided the contextual origins of the CSS, along with the objectives of the strategy and the resources available to fulfil these objectives. Over the next segment of this paper arguments surrounding the strategic malaise will be analysed

Strategic Malaise

This chapter will analyse whether the CSS represents a missed opportunity as a symptom of a wider British strategy malaise (Baylis 1989, Cohen 2002, Porter 2010). Indeed the Public Administrations Select Committee has argued that the UK has 'lost an institutionalised capacity for, and culture of, strategic thought' and as a result that the 'the term "strategy" has moved out of its narrow military meaning and into general use, it has lost its precision' (House of Commons 2010: 6,7). However, much of the criticism on the present security strategy has focused on critique of the NSS and SDSR and comparatively little comment has focused on the CSS itself. The Public Administrations Select Committee also highlighted the lack of distinction between strategic thought and strategy, and also, between strategy and policy (House of Commons 2010). Therefore, the distinctions will be made in order to assess the strategic malaise argument.

Strategies are developed from strategic theory (Paret 1986), and theories rise to prominence in direct relation to their ability to help decision makers formulate sound strategy (Mahnken 2007). 'Strategic theory opens the mind to all the possibilities and forces at play, prompting us to consider the costs and risks of our decisions and weigh the consequences of those of our adversaries, allies, and others' (Yarger 2006: 2). However, the development of strategic theories is a reflection of the intensely personal relationship between humans and armed conflict. This holds true whether the theory being promulgated stems from an individual or a collective group such as a think tank. Therefore, strategic theories can be tainted by personal bias and individual or collective agendas. This is known as the strategic environment, which is argued to be the crucial

> 'determinant of the information that is available to an actor and the structure within which actors operate. The environment determines what the actors think they know for sure and what they have to infer, if possible, from the behaviour of others' (Harris 2006: 542).

An example of this is provided by the prominent British strategist Basil Liddell-Hart, who was a staunch proponent of professional armies and that the focus of war-fighting should be on manoeuvre and not attrition (1944). The primary reasoning behind this proposition was not that it was the optimal strategy to conduct military operations at that particular time, but rather an attempt to ensure that the total war and mass slaughter that Liddell-Hart had witnessed in the Great War was not repeated (Freedman 1998). Therefore, the strategic environment becomes a key influence in the evolution of strategic theory. This ensures that strategies often fit a given period in history rather than become a grand universal theory that is applicable across the ages.

Strategy and policy are often confused and merged together. Therefore, it is important to clarify what is meant by policy to avoid conflation with strategy. Policy is,

> 'a government's (or organisation's) formed position on an issue, situation or problem, including what political objective the government seeks to achieve, what resources it is prepared to commit to the pursuit of that objective and what course of action it intends to follow' (Jermy 2011: 33).

Strategy is different, for example, Michael Howard states that strategy is the 'use of available resources to gain any objective' (Howard 1983: 86). However, for a strategy to be effective it should address 'what ways should we employ to deliver the ends that our policy seeks within the means that our policy has allocated' (Jermy 2011: 33-34). Therefore, Jermy posits that strategy is primarily focused on the ways component of the strategic trinity (2011).

Hew Strachan develops the distinction between policy and strategy. Whilst assessing the nature of the decline of the use of the word strategy to become synonymous with policy he makes the following statement.

> 'The military historian needs to confront an existential question: why is there strategy on the one hand and naval strategy on other? Why is the use of the adjective 'naval' an indication that those who have written about the conduct of war at sea have not been incorporated into the mainstream histories of war?' (Strachan 2005: 37).

The immediate thought with reference to this study of the CSS is to simply insert cyber instead of naval into the above quotation. Strachan goes onto posit that strategy had lost its true meaning by the end of the Cold-War, and that strategy is concerned the deliverance of military force, or in Clausewitzian terms strategy is defined as 'the use of the engagement for the purpose of the war' (Clausewitz 1984: 177). Strachan essentially argues that we are in a foreign policy malaise, and because that the notion of strategy has been replaced by security and taken to encompass a broad range of policy, even to the extent whereby it could be argued that foreign policy has been militarised (2005). Therefore, the arguments of Porter (2010) and Cohen (2002) that the UK suffers from a strategic malaise would appear to be lacking this extra dimension. With Strachan's approach in mind then the UK would be strategy deficient not because of a malaise but due to the broadening and deepening of security issues (Buzan 1991, Buzan, Waever & de Wilde 1998, Booth 2005 and Booth 2007).

Analysis of the Cyber Security Strategy Objectives

Having identified the objectives of the CSS, in chapter 2, each one will be analysed in turn. The focus will be to analyse the debate bought out by the key terms utilised within each objective. The primary challenges facing each objective are that the ends are too ambitious and not grounded in the reality of what is actually feasible or realistic, that the ways are hindered by being insufficiently honed and are open to interpretation, and that the means are insufficient (McGhie 2012). From the previous section this is arguably due to the CSS being a policy document and not a true strategy.

The overarching end objective of the CSS is clearly established in Francis Maude's introduction.

> 'By 2015, the aspiration is that the measures outlined in this strategy will mean the UK is in a position where: law enforcement is tackling cyber criminals; citizens know what to do to protect themselves; effective cyber security is seen as a positive for UK business; a thriving cyber security sector has been established; public services online are secure and resilient; and the threats to our national infrastructure and national security have been confronted' (Cabinet Office 2011: 5).

Therefore, the CSS is supposed to tackle the challenge of cybercrime, educate the populous in cyber-security and ensure the private sector is able to provide the security required, resilient public services and the removal of threats to critical national infrastructure. Furthermore, this should be achieved within a four year timetable. The level of this challenge seems somewhat akin to King Sisyphus and his attempts to get his boulder to the top of the hill. However, each component will be looked at individually in order to provide an overall picture of whether the CSS is a missed opportunity.

Objective #1: Cyber-Crime

Objective #1 of the CSS is for 'the UK to tackle cyber-crime and be one of the most secure places in the world to do business in cyberspace' (Cabinet Office 2011: 21). However, a recent report by the Home Affairs Select Committee has stated that the UK is failing to meet this objective (BBC 2013f and House of Commons 2013). It can be argued that this is due to the CSS not attempting to make a definition of what cyber-crime is and consequently analysis of how the strategy is performing is impossible as no basis for assessing success exists. However, there have been positive steps taken, such as, the incorporation of the Police Central e-crime Unit (PCeU) and the Serious Organised Crime Agency (SOCA) into a new National Cyber Crime Unit to form part of the National Crime Agency (NCA) (Home Office 2011 and Woolen 2013).

The National Security Strategy sets out a strong economy as being a vital basis for security (HM Government 2010a). The CSS sets out a clear continuation of this position with Objective #1. Therefore, the economic prosperity of Britain is a crucial element of the security agenda, according to the governments aims. This is exemplified by the prevalent focus on cyber-crime which is responsible for an alleged £27 billion annual cost to the UK economy (Detica 2011). Crime has a greater cost to society than just the crime itself as shown in Figure 5. Furthermore, cyber-crime has proliferated throughout the past decade due to the increased availability of botnets, which is further enhanced by toolkits which aid their deployment (Broadhurst et al. 2013).

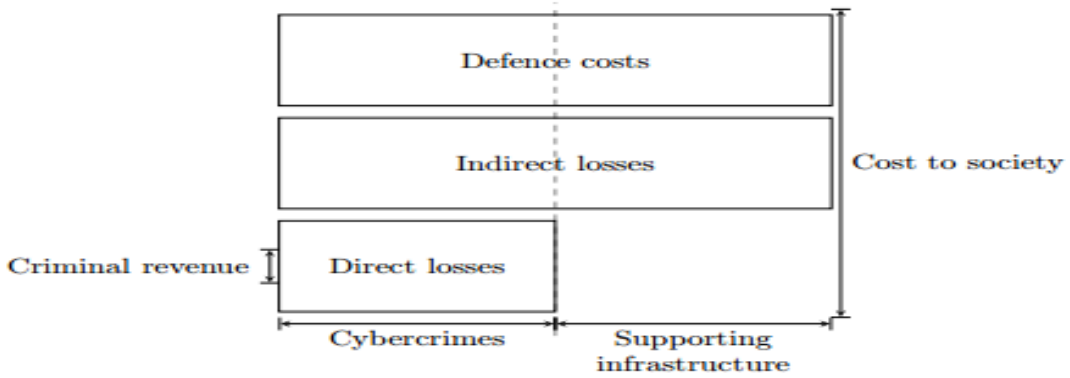


Figure 5. Societal Cost of Crime (Anderson et al. 2013: 4)

Economic security is not solely referent to cybercrime but all crime, therefore, cybercrime initiatives form part of the wider counter-crime strategy. The UK recognises this by establishing the NCA to co-ordinate the various different branches of law enforcement (Home Office 2011). The establishment of the NCA is likely to enhance the integration within the European Union and the members that have ratified the *Convention on Cybercrime* (Council of Europe 2001 and House of Lords 2011).

Therefore, it is important not to assume that every country has the same level of interconnectivity, and thus the same risk profile, which makes a "one-size fits all" strategy harder to deliver.

New Form of Crime?

As a starting point our analysis of whether the CSS represents a missed opportunity will focus on what constitutes a cyber-crime. A Home Affairs Committee report states, 'during our inquiry it became clear that the definitions of what constituted e-crime or cyber crime needed frequent revision if organisations wish to attempt to define the rapidly evolving nature of the e-crime threat' (House of Commons 2013: 6). The RUS 13 case involving British bookmakers provides a good example. In this case the criminals involved extorted British bookmakers by threatening to bring the company's services to a halt via DDoS actions (UNDOC 2012: 111-112). However, it should be pointed out that legislative tools already exist to tackle cases of extortion, and only the means of extortion are new (Paulson & Weber 2006). 'Extortion is extortion and will remain such regardless of the method employed to communicate the threat' (Britz 2009: 5). If the means of coercion were threats of violence or compromising photographs, for example, the offence would still be one of extortion. In this instance it is hard to consider the offence as being a new form of criminal activity that requires specific legislation. Although some articulate that these forms of offence should be considered as cyber extortion (McMullan & Rege 2007).

The case of Full Tilt Poker highlights a slightly different tact. Full Tilt operated as legitimate licensed provider of online poker within the United States, until the introduction of the Unlawful Internet Gambling Enforcement Act (UIGEA) was introduced in 2006. Essentially UIGEA made it a criminal offence for banks, and other financial institutions, to process payments to online gambling operators, who were circumventing US anti-gambling laws in individual states by utilising the global nature of the internet (Rose 2011). However, UIGEA was not universally complied with, mainly due to its terms of reference not being properly defined. In 2010 the US was still the biggest poker market with a turnover of $973.3million representing 25% of the global player base (Fiedler & Wilcke 2011). When the Department of Justice (DOJ) took action, Full Tilt and its company executives who had continued to make its service available to customers within the United States, were charged with offences ranging from bank fraud, money laundering and operating an illegal gambling business (Bowers 2012). They had been able to achieve this by establishing fake companies, most notably in the form of golf club and jewellery sales, to act as payment processors on their behalf (Bowers 2013).

The DOJ seized the domain names and shut down the sites IP addresses in 2011. This led to the discovery that Full Tilt had been operating as a Ponzi scheme, and had not segregated the player

funds accounts from the commercial accounts (Bowers 2012). Some $400million of player funds were used to fund dividend payments to the owners of Full Tilt. The scandal was deeply felt as Full Tilt was the second largest global operator, with a poker market share of 22% in 2010 (Fiedler & Wilcke 2011: 4).

The international nature of the company highlights some of the jurisdictional challenges that arise, within the context of cyber-crime. The company was deemed to be operating illegally in the United States, based off a licence granted by the Alderney Gaming Commission, which utilised servers located in Guernsey, and headquarters in Dublin (Bowers 2013). Furthermore, whilst this is a criminal offence, and the core business operates within cyberspace, and involved customer funds being paid via cyberspace, it can be observed that it is not a cyber-crime, but a traditional form of corporate fraud utilising cyberspace for operational purposes.

An alternative example, although a similar type of offence, involves the case of Innovative Marketing Ukraine (IMU) (Kshetri 2013). The company operated openly out of Kiev and employed around six hundred people around the globe. Its core business was spreading malware which would trigger a bogus anti-virus (AV) fraud and advising the victim to purchase IMU's fake AV product (Broadhurst et al. 2013). If customers had cause for complaint, and around two million did in 2008, they were taken through a series of steps to solve the non-existent problem which left many of them satisfied (Broadhurst et al. 2013). This fraud was proliferated by a network of affiliates who were financially rewarded depending on the number of computers infected with the malware and subsequent AV sales.

In this example we see a company engaged in fraudulent behaviour, like Full Tilt, however, the crucial difference is that although Full Tilt received funds via a medium in cyberspace the criminal offence did not take place there. IMU was totally contained within cyberspace, especially if the broad conceptualisation of cyberspace, highlighted in chapter 2, is applied, then both the human operator and the victim form part of cyberspace. Therefore, for a cybercrime to be considered as such and potentially require new legislative tools, it is important to distinguish between crimes that use the internet from crimes that depend on the internet (Cross 2008). The Home Affairs Committee recognises the importance of this distinction by stating that 'crimes that have been transformed by the internet and those unique to electronic networks should continue to be defined and recorded as e-crime' (House of Commons 2013: 6).

The Involvement of Organised Crime

The next area of analysis of whether the CSS represents a missed opportunity is where the threat originates. The debate largely revolves around whether cyber-criminal enterprises should be considered to be organised crime groups, like *La Cosa Nostra* (Lusthaus 2013). The issue is confused as there is certainly a professional class of cyber-criminal emerging, who have been keen to adopt mafia terminology to describe themselves (Lusthaus 2013). Furthermore, existing organised crime groups do have a presence in cyberspace and commit crime which may be classed as cyber-crime.

For example, in 2008 Gambino crime family capo Nicholas Corozzo was arrested for his role in an illegal online gambling ring (Queens County DA 2008). In this case the criminals essentially provided a technological update for the traditional wire room by utilising web-sites and servers based offshore to collect the funds and proceeds. The involvement of organised crime clouds the identity of who the actual perpetrators of cyber-crime might be. In the Corozzo case it became clear that it involved Gambino family associates, although the main enterprise appeared to be independent of the rest of the Gambino organisation (Queens County DA 2008).

Cyber-crime has evolved from a low volume enterprise, which was the preserve of specialist individuals, to a more common high volume crime which is increasingly organised in its deliverance (Moore, Clayton & Anderson 2009). However, due to the lack of empirical evidence, it cannot be said that cyber-crime is dominated by traditional organised crime groups (Broadhurst et al. 2013 and Lusthaus 2013). Therefore, whilst members of organised crime groups are involved in crime within cyberspace, the evidence is that the structures used to plan and carry out the crime are loose affiliations and networks that only exist for the specific task (Décary-Hétu & Dupont 2012). However, the CSS focuses on 'serious organised crime using the internet to steal personal or financial data to commit fraud, steal intellectual property or launder money' (NAO 2013: 6). This is clearly at odds with the evidence and illustrates a lack of understanding of how the model of criminal groups differs is at variance within cyberspace. This may have a subsequent impact on the ability of law enforcement to be able to deal with the problem.

Due to the global reach of cyberspace the issue of how to tackle the perpetrators of cyber-crime becomes complicated due to the difference in laws from one country to the next. Therefore, the solution to the problem is not the sole preserve of national governments. In this regard the UK needs to ensure that its partners, especially within NATO and the EU, have an acceptable level of cyber-security (House of Lords 2010). Indeed it is in the direct interest of the UK's national security to help EU institutions, and other similar bodies enhance their cyber-security, as 'individual weakness undermines the collective security of the EU' (House of Lords 2011: 47).

There is clear evidence of cyber-crime hubs operating in certain cities, for example Râmnicu Vâlcea in Romania (Bhattacharjee 2011), along with networks in India, Vietnam, Brazil and Nigeria (BBC 2013b). This suggests that a concentrated effort that focuses on eradicating these hubs would lead to a noticeable drop off in cyber-crime. It does appear that the CSS addresses this challenge by stating that the UK has ratified the Budapest Convention 'and will work to persuade other countries to develop compatible laws, so that cyber crimes can be prosecuted across borders and cyber criminals are denied safe havens' (Cabinet Office 2011: 26). Furthermore, the establishment of the NCA will help to co-ordinated the available resources at the national level 'by providing specialist support, intelligence and guidance' (Cabinet Office 2011: 30).

The earlier example of the RUS 13 case involving British bookmakers also resonates with the debate regarding the involvement of organised crime groups in cyber-crime. The case seems to reinforce arguments that a form of protection racket is being run in cyberspace, maybe even to the extent that there is competition to maintain, or seize, control of this market, thereby making it an equivalent to the *pizzo* (Gambetta 1996). The CSS illustrates awareness of the problem by stating that 'serious organised crime has developed an internet-based black market for criminals, which sells stolen identity information and software products to launch cyber attacks as well as technical support for cybercrime' (NAO 2013: 6).

In cyberspace these black markets are basically internet forums that are hidden within the darkweb, or Tor network. These are separate to the normal internet that everyone has access to, and essentially are anonymous which hampers detection (Curtis 2013). For example, Japanese hacker "Demon Killer" has eluded the authorities due to his use of Tor, and as such law enforcement organisations have considered utilising technical process to block the service (BBC 2013c). Similarly, in the UK it is the Tor network that is used by terrorists to disseminate information such as the Al Qaeda magazine *Inspire* (O'Neill 2013).

A closer examination of these forums can identify that they operate purely for business and profit, which differs from the traditional forum model of providing information and discussion (Lusthaus 2013). Furthermore, the forums have a clear and defined hierarchy that becomes accessible based on trust, ability and reputation (Lusthaus 2012). This provides the basis of any criminal organisation, and these forums have been compared to the 'curb exchanges' seen during the prohibition period and provided the foundation for the mafia in the United States (Varese 2011: 114-120). This is because administrators and moderators of these forums provide a form of governance that effectively provides a degree of protection to enable the ability to conduct business between

different aspects associated with cybercrime (Lusthaus 2013). There is even evidence of an escrow service being offered and of a standard 5% or £250 fee being applied to any deals (Davies 2010).

This clearly brings the parallels with the mafia and the *pizzo* into focus, though as Gambetta argues to be considered a mafia then the organisation doesn't just provide protection but seeks to control the supply of protection (1996). The case of the "Iceman" illustrates that this is possible within cyberspace as well (Poulsen 2011: 159-169). The core aspect of this quest for control involved the hacking of rival forums and stealing their membership data and then using the data to undermine confidence in those rival platforms thereby seeking to bring all the criminal market online under a central control (Poulsen 2011: 164).

There are significant definitional issues with regards to organised crime and there is no commonly accepted definition (Abadinsky 2013, Dobovšek 1996, Levi 1998 and Wright 2006). A method of being able to provide assessment without the ability to provide for a definition is presented by Abadinsky's eight characteristics – absence of political goals, hierarchical, limited or exclusive membership, constitutes a unique subculture, perpetuates, willingness to use illegal violence, monopolistic, and is governed by explicit rules and regulations (2013: 3). The internet forums crime model lacks the willingness to use violence, although they can appear to resemble to model of traditional organised crime groups they do not conform to the present understanding of organised crime (Lusthaus 2013). The focus of the CSS on organised crime can, therefore, be called into question.

In terms of the CSS this means that in order for the strategy to have some form of practical utility it needs to either shift its focus away from organised crime or develop a new conception of organised crime. The later process would be extremely complex and would likely lead to even greater disagreement in an already fragile area. This would have a significant impact upon legislative process in the kinetic world. Making a clear distinction between crimes that use the internet from crimes that depend on the internet and, thus a definition of cyber-crime, would enable new legislative tools to be considered (Cross 2008). Therefore, the UK needs to develop a strategy to be able to cope with the individuals and ad hoc organisations that are involved in cyber-crime. This becomes increasingly important when we consider that the CSS seeks to improve reporting standards of offences, which is also reinforced by the United Nations (Cabinet Office 2011 and UNDOC 2013). An adequate definition is clearly needed or it becomes impossible to collect data for analysis as you have to be able to classify what you are collecting (Cross 2008).

In our analysis of Objective #1 questions have been raised as to who the main operators that perpetrate cyber-crime are and whether cyber-crime represents a new form of criminal offence. The significant response of the UK has been identified as the creation of the NCA.

Objective #2: A More Resilient UK

Objective #2 of the CSS is for 'the UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace' (Cabinet Office 2011: 21). The question is raised as to what constitutes a cyber-attack and to what level will the UK be resilient and how this can be measured and the strategy assessed. Furthermore, an additional question arises as to what the threat actual is. However, nowhere within the CSS is any effort made to clearly identify just what the UK considers a cyber-attack. Resilience is similarly open ended as the objective makes no reference to the level of resilience required or illustrates an appreciation that resilience is a product of time and threat vectors (Haimes 2009). Each of these three questions of Objective #2 will be looked at in turn.

Cyber-Attack

The UK appears to adopt a broad conception and does not appear to have given consideration to what the threshold for a cyber-attack should be, which would represent a missed opportunity. Consider the following statement within the CSS, 'attacks on public and private sector websites and online services in the UK orchestrated by **'hacktivists'** are becoming more common, aimed at causing disruption, reputational and financial damage, and gaining publicity' (Cabinet Office 2011: 16). This makes it clear that the UK regards the lowest form of intrusion, cyber-disruption, to be a cyber-attack, and furthermore, as it is incorporated into the CSS that such an intrusion represents a threat to national security. Therefore, in terms of Objective #2 the government has assumed responsibility for protecting the entirety of UK cyberspace from minimal intrusions. This is simple unrealistic and unworkable and even the most extreme examples of this type of activity result in only negligible inconvenience as illustrated by the events in Estonia during April and May 2007.

The cyber-incident in Estonia was highly political in nature and originated from a controversial decision to relocate a statue to remember Soviet soldiers who died during World War II. In response Estonia was subjected to a sustained attack on the availability of information and access, which primarily affected governmental and financial services (Ottis 2008). Estonia made for a vulnerable target for this kind of hactivism as it was one of the most highly ICT dependent countries in the world and has been described as operating a 'paperless government' (BBC 2007). The event has been built up and is commonly portrayed as an act of cyber-terrorism and even suggested that it provides an alternative method for Russian aggression against NATO as it avoids nuclear escalation (Herzog 2011). The conceptual discussion earlier in this paper illustrated that for an act to be consider as cyber-terrorism, it must first meet the criteria for terrorism. The lack of violence, therefore, means that the Estonian example does not go beyond cyber-disruption, which has a lower threshold for violence than cyber-attack (Yannakogeorgos 2013a).

Adequately defining whether or not you are under attack as a nation is a key part of security strategy. It enables a series of legal measures to be enacted and extraordinary measures employed. The legal understanding of a cyber-attack thus provides a country with the legitimisation to invoke either Article 51 of the UN Charter or collective security arrangements, such as the EU Defence Force or NATO. Estonia tried to utilise the collective defence agreements within NATO during the 2007 intrusion into its cyberspace by using provocative language highlighting the "attack". However, NATO decided that the threshold for enacting collective defence had not been breached and thus no action was to be taken by the alliance, although this appears to have been on ad hoc basis not generated by a clear demarcation line. Therefore, the debate will now move forward and examine how to identify the threshold for a cyber-attack amongst the immense range of hostile actions that can be carried out within cyberspace (Waxman 2011).

An attack is an aggressive or violent action against a person or a place defined in the Oxford English Dictionary. Despite such a clear cut definition there is substantial misuse of the terminology across the literature and the starting point for discussion is that the threshold for an attack should be no different in cyberspace than in the kinetic realm (Lewis 2010a). This position is reinforced by the earlier discussion of cyber as a prefix. An example of the misuse of terminology is illustrated by Thomas Rid, in his excellent study on the likelihood of cyber war (2013). He refers to the example of Russia and Georgia in 2008 and the cyber-offense, which he asserts 'may have been the first time an independent cyber-attack has taken place in sync with a conventional military operation' (Rid 2013: 7). The cyber-element of the Russian attack on Georgia does not breach the threshold for violence in its own right, and therefore, cannot be classed as a cyber-attack. Rid goes on to point out the effects of the cyber incident were relatively small and only had the effect of making some Georgian government websites inaccessible for a few hours (2013).

The Tallinn Manual, which aims to provide the industry standard, posits that 'a cyber-attack is a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects' (Schmitt 2013: 106). Considering the previous discussion on the concept of cyberspace and the explicit inclusion of people as part of cyberspace this definition has a logical basis. However, the Tallinn Manual doesn't explicitly include people in its definition of cyberspace, which appears to contradict the cyber-attack definition by not doing so (Schmitt 2013).

Using the example of Georgia and Russia, it would appear that as Rid is highlighting a cyber-attack taking place in alignment with normal military power and that the Tallinn Manual's definition is supporting Rid's use of cyber-attack. However, the cyber-attack that took place in Georgia was a

Distributed Denial of Service (DDoS) (Rid 2013 and Swaine 2008). Cyber-weapons have difficulty in producing casualties, via direct means, and as such the probability of the threshold for cyber-attack being breached is minimal (Lewis 2010b). Consequently, terminology is needed to identify the cyber-events that take place that do not meet the criteria of violence to be classified as an attack. Yannakogeorgos suggests cyber-disruption as an appropriate term and DDoS would be one of the core benchmarks for this category (2013b).

Considering Rid's arguments it is surprising that he does not address the definitional issue, despite extensive arguments on violence and definitions of cyber-war and weapons (2013). 'In an act of cyber-war, the actual use of force is likely to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties' (Rid 2012: 9). Therefore, for Rid, the threshold for an attack is below the standard as set out by the Tallinn Manual reinforced by a more limited conceptual understanding of cyberspace. Indeed it seems that for Rid his definition would follow Waxman's view that cyber-attacks are 'efforts to alter, disrupt, or destroy computer systems or networks or the information of the programs within them' (2011: 422). As such it can be argued that Rid's analysis of cyber-war is based primarily within the technological conceptual constraints and does not fully incorporate the role of the human within cyberspace. What Rid refers to as cyber-attack is in reality a further example of cyber disruption (Yannakogeorgos 2013b).

The closest example of a cyber-attack is Operation Orchard, with arguments that the threshold of violence has been breached (Clarke & Knake 2010 and McGraw 2013). The incident took place on 6th September 2007 when the construction site of a nuclear reactor was bombed at *Dayr ez-Zor* in Eastern Syria. A significant question emerged in the aftermath regarding how it was possible for Syrian air defence systems, which were Russian built and arguably the largest in the world, to be breached without a response (Fulghum, Wall & Butler 2007). Initially suspicions indicated that the radar station at *Tall al-Abuad* had been taken out of commission with a cyber-hack or jamming, which would most likely have been carried out by Unit 8200, part of Israel's special forces (Markoff 2010). However, after the data was analysed, the more prominent theory that a kill switch, embedded in the radar station's software, had been used became the accepted version of events, even if never officially clarified (Adee 2008).

Operation Orchard illustrates an attack that resulted in people dying and a nuclear reactor being destroyed whilst under construction. The attack clearly exceeds the violence threshold as outlined by the Tallinn Manual as being reasonably expected to cause injury or death (Schmitt 2013). However, there is significant debate and argument as to whether or not this incident qualifies as a

cyber-attack due to the cause-effect delay present. The fact that the air defences were disabled by a cyber-event is not disputed. On one hand Rid argues that the time delay is a crucial factor and as a result the consequence of the destruction of *Dayr ez-Zor* was an indirect result of the cyber infiltration of the radar station (2013). Conversely the other side is that the removal of Syrian air defences capability was an enabling act, or pre-cursor, without which the mission would not have been successful (Clarke & Knake 2010, McGraw 2013 and Stone 2013a).

The critical issue here is whether or not there can be a time delay between the action of the cyber-event and the death and destruction that are subsequently caused. The Tallinn Manual is unhelpful as it contradicts itself within the space of a page. Firstly, it identifies that, for the threshold of attack to be met then the cyber-event must be directed against the object of attack, in other words not an indirect effect at a later time (Schmitt 2013: 93). Before going on to say on the next page,

> 'It should be noted that a cyber-operation might not result in the requisite harm to the object of the operation, but cause foreseeable collateral damage at the level set forth in this Rule. Such an operation amounts to an attack to which the relevant law of armed conflict applies' (Schmitt 2013: 94).

To ensure the waters are well and truly muddied the manual goes onto illustrate the following example,

> 'a cyber-operation may be used to disable defences at a target that is subsequently kinetically attacked. In such a case, the cyber operation is one component of an operation that qualifies as an attack, much as laser designation makes possible attacks using laser-guided bombs' (Schmitt 2013: 94).

The debate above highlights exactly why nailing down the terminology and the exact criteria is so important. A country's available response options are dictated by the legal definitions that are put in place. In seeking a clearer understanding perhaps thought should be given to how the UK should consider, for example, someone who dies of radiation poisoning after a nuclear blast, the individual that suffers from drinking bacteria infected water from agents employed upstream, or the family when their building collapses because it is in the house next door to a terrorist inhabited building taken out by a drone. These are parallel examples of a delayed, or indirect, effect of an action to enable harm to be carried out. In this light it is hard to consider Rid's argument that only a direct action qualifies as a cyber-attack (2013).

The Israeli attack on *Dayr ez-Zor* is unquestionable an attack. The arguments about delayed timeframes, and direct or indirect effects, are distracting from the main purpose of identifying the terminology. The specific terminology for debate is cyber-attack. It is the troublesome prefix "cyber"

that creates the real consternation. For an incident to be specifically classified as a cyber-attack then the event must take place within cyberspace, with the violence threshold of damage or death occurring within cyberspace. As the conceptualisation debate of cyberspace identified the inclusion of the human then such a move becomes possible. In this light, therefore, the Israeli action is a military attack that utilised a technology as a force multiplier to enable its success.

The Tallinn Manual's definition should be clarified, and as such view a cyber-attack as a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects, within cyberspace. Furthermore, such a debate within the NSC would not only benefit Objective #2 of the CSS but also Objective #3 by enabling the UK to seize the opportunity of taking an international lead in defining the future conduct of operations within cyberspace.

Resilience

The issue of resilience relates to a two-fold problem. Firstly, by identifying vulnerabilities that exist, where 'vulnerability refers to the inherent states of a given system (e.g., physical, technical, organizational, and cultural) that can be exploited by an adversary to adversely affect (cause harm or damage to) that system' (Haimes, Crowther & Horowitz 2006: 293). Secondly, to develop a resilient system to address the vulnerabilities that can be exploited to generate a threat. Resilience, just as with vulnerability, cannot be quantitatively measured in specific units due to the multi-dimensional combination of outputs, or consequences, in relation to specific inputs, or threats (Haimes 2009). What this means is that the risk associated with an attack on a system is not only dependant on the resilience of the system but also the nature of the cyber-offence it is facing. For any specific threat the system will have a, potentially, different recovery time and cost. Therefore, for any given system different attacks will generate different consequences (Haimes 2009).

Vulnerability and resilience are linked and form a symbiotic relationship. However, the two concepts are distinct so this section will begin by defining what we mean by resilience, so that the distinction between vulnerability is clear. Resilience is not a unique concept for cyberspace, therefore, there is already an established understanding of how the concept operates and fits into an overall risk management strategy. Whilst the term can be applied to a wide range of areas, including naturally occurring events, for example, in terms of the cyber-security debate we are primarily talking about the relevance to Critical Infrasturcture Protection (CIP).

Resilience is similar to the other aspects of the cyber-security debate in that it is often not properly understood. The following basic definition provides a starting point for analysis.

> 'Resilience is commonly defined as the ability of a system to recover from shock, either returning back to its original state or to a new adjusted state. Resilience accepts that disruptions are inevitable and can be considered a "Plan B" in case something goes wrong' (Cavelty 2013: 375).

This definition is unsatisfactory and would be unsuitable for strategic planning purposes, as it does not provide any indication as to how resilience might be measured and the variables of threat. Therefore, if such a definition was applied to gauge the success of the CSS then there would be no basis for assessing how successful, or otherwise, the strategy might be (Haimes 2009). Therefore, it is necessary to think more deeply about our understanding of the concept of resilience. A recent European Network and Information Security Agency (ENISA) report goes into great depth about the nature of resilience and the relationship between different segments that make up cyberspace and illustrates the degree of interconnectivity that may be required to develop pan-European strategies (2011).

There is no doubt about the level of activity that is seen within cyberspace. For example, Sir Michael Rake, Chairman of BT, has stated that during the 2012 Olympics, 112 million malicious attacks were recorded, which peaked at 11,000 per second (*Under Attack: The Threat from Cyberspace - Episode 2: Sabotage and Subversion* 2013). If Cavelty's definition was adhered to, then as long as the system is able to recover at some point then all would be well, notwithstanding that acceptance is required when things go wrong (2013).

Two key areas are missing from Cavelty's definition that would enable the success of a strategy to be more accurately measured. It is crucial to the concept of resilience to understand the importance of the time vector and the acceptable limits. As such resilience is not just about the ability of a system to recover from shock, but also the amount of time that it takes to recover and how much system degradation is acceptable, which is coupled with the capacity that the system is able to return to (Haimes, Crowther & Horowitz 2006 and Hall et al. 2011). In terms of the Olympics, an acceptable level of resilience was seen as a thirty second power outage during the opening ceremony, therefore, the systems in place were resilient to this degree against the perceived threats (Corera 2013). The system may well have been less resilient versus an unperceived threat. Therefore, as Objective #2 does not provide such a quantitative statement of just what level of resilience is acceptable, over what time and against what threats, it can be considered as being open ended and, as such, has little real meaning and minimal practical strategic relevance (McGhie 2012).

Furthermore, if consideration is given to the primary vulnerability associated with resilience, the interconnection of critical infrastructure, it should be immediately clear that some parts of the

infrastructure are more critical than others, as illustrated in Figure 6. Using such a diagram it is possible to analyse potential weak-points, were an incident could affect a much wider area, for example, anything which harms the electricity infrastructure is likely to have a much wider impact. Therefore, electrical systems need to have a much higher resilience threshold in order to provide the same level of security as infrastructure that has less of a knock-effect.

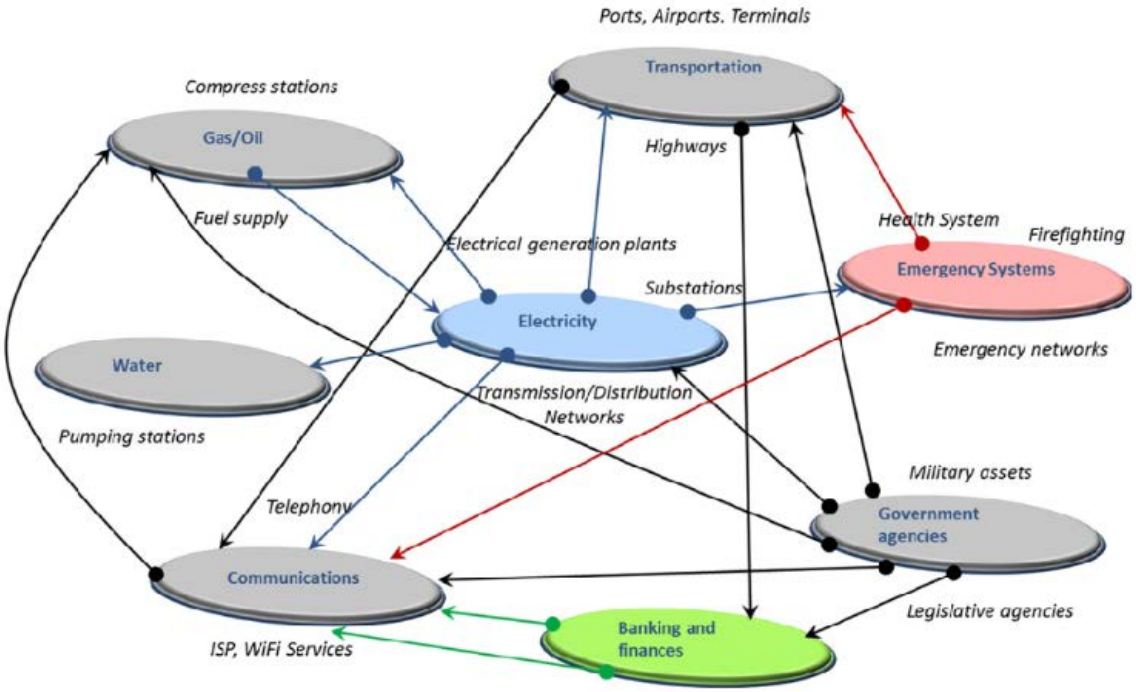


Figure 6. Interconnection of Critical Infrastructure (Yusta, Correa & Lacal-Arántegui 2011: 6101)

The UK does have a structure in place with the CPNI established in 2007 and the establishment of Cyber Incident Response team, as part of the CSS (GCHQ 2013). Therefore, it is apparent that action is taking place towards enhancing the resilience of the UK. However, the lack of clearly defined objective means that the CSS loses some potency and clear standards for success or failure should be adopted. Furthermore, arguably it also hinders the goal of creating a better educated public and business as they left to adhere to a vague over-simplification and as a result either be under, or over, prepared for the reality of the threat. CESGA has produced a document to help the user follow the '10 Steps to Cyber Security' (2012).

So far in this section the debates around what constitutes a cyber-attack and the nature of resilience have been analysed. The final segment of the analysis surrounding whether Objective #2 of the CSS represents a missed opportunity will identify the threat, namely cyber-weapons, and utilise the example of Stuxnet.

The Threat from Cyber-Weapons

The primary threat from cyberspace is considered to be against the integrity of a critical infrastructure system. Such a threat is designed to have an actual effect as opposed to merely acquire information or to stop information being accessed. Therefore, this category represents the most intrusive form of cyber-operations and is focused on cyber-weaponry. It should be noted that the history of weapon development and the implementation of new technology demonstrate that a period of significant consideration occurs during which the old principles are challenged and after a period of reflection the debate settles down, with a reconceptualization to incorporate the new technology into the existing principles and rules that were already prevalent in international law (Dinstein 2002). Indeed as with more traditional weaponry there are moves in place to normalise cyber-weapons via arms control (Andress & Winterfield 2011: 7).

In order to consider what a cyber-weapon is and how such a weapon could be utilised, consideration needs to be given to the understanding of a weapon in more general terms (Rid & McBurney 2012). Weapons provide an extension to the human intent to cause harm. Therefore, the object itself doesn't automatically determine status as a weapon, and weapons are not constrained to warfare, or even violence. For example, a hammer is designed to be used in construction and various other tasks; however, it can also be used to threaten or cause harm, thus the hammer has now become a weapon regardless of its successful use as such (Rid & McBurney 2012). Cyber-weapons have to apply this conception in order to be considered as such, which places the intent for harm as central to any definition.

The fundamental aspect of the debate revolves around whether direct or indirect effects are acceptable. A cyber-specialist from a legal background defines a cyber-weapon as,

> 'A part of equipment, a device or any set of computer instructions used in a conflict among actors, both national and non-national, with the purpose of causing, even indirectly, a physical damage to equipment or people, or rather of sabotaging or damaging in a direct way the information systems of a sensitive target of the attacked subject' (Mele 2013: 10).

By allowing for indirect effects this achieves two primary problems. Firstly, it greatly increases the scope for what can be considered to be a cyber-weapon, as well as enhancing the 'damage' that these weapons can be said to have caused. Secondly, it raises the question of time and how much of it can have elapsed between deployment and affect for it to be attributed to the weapon and how far removed from the process can the original weapon be. Just as in the debate on cyber-attack this would then need further definition, and debate making the issue more complex than it needs to be. Therefore, consistency is needed in both of the definitions of cyber-attack and cyber-weapon.

Rid and McBurney are explicit in stating that any damage has to create direct harm and illustrate a DDoS attack as an example of a non-weapon as any harm created is a secondary effect (2012). Furthermore, they go on to argue that there should be differentiation between low and high end weapons, with the distinction coming from the ability to penetrate a specifically targeted protected system in fulfilment of a specific goal of actual direct physical damage (Rid & McBurney 2012). This is not consistent with Rid's broader conception of cyber-attack (2013). However, it is clear from some of the literature that this area is still one of debate, with arguments presented that developing a weapon is easy and it is only the deployment that is difficult, and that it does not need a complex weapon to destroy physical components or subsystems (Clarke & Knake 2010, McGraw 2013, Peterson 2013 and Stone 2013a). Arguments that highlight the potential ease of a cyber-attack are generally focussed on a myriad of "what if scenarios" and are challenged as being threat inflationary (Brito & Watkins 2011 and Rid 2012).

Stuxnet provides probably the best known example of a cyber-weapon and provides a good illustration of the debates surrounding the threshold for cyber-attack and resilience in critical infrastructure as well. In order to develop Stuxnet the following was required; 4 Zero-Day Exploits (ZDE), 2 stolen digital certificates, 1 Windows rootkit and the first ever Programmable Logic Controller (PLC) rootkit (Rid 2013: 45). It is estimated to have cost at least $3 million and required around thirty programmers working for ten thousand man hours to develop the weapon (Falco 2012). On top of this comes the intelligence and deployment part of the operation. Such an investment in manpower and resources leaves these weapons as the preserve of the cyber-superpowers (Rid 2013). At a stroke this puts fears regarding cyber-terrorism into context and whilst nothing can be ruled out, the risk of a cyber-terrorist attack on the scale of Stuxnet is minimal. An example of the cost of ZDEs is provided in Figure 7.

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Figure 7. Zero Day Exploit Black Market Price List (Greenberg 2012 and Worstall 2013)

The effect of the weapon, which specifically targeted the IR-1 centrifuges at the Fuel Enrichment Plant at Natanz, is highly debated. A report issued in December 2010, about 6 months after the discovery of the weapon, concluded that between 2009 and 2010 Iran had decommissioned or replaced around 1000 IR-1 centrifuges (Albright, Brannan & Walrond 2010). However, just two months later the Director General of the Atomic Energy Agency revised this assessment and stated that there had been no noticeable effect on the Iranian nuclear programme (Amano 2011). There is little dispute today that Iran has fully recovered (Sanger 2012). Furthermore, the weapons deployment is criticised for not being effective, badly timed and potentially of benefit to Iran politically (Barzashka 2013). Iran may well have intentional spread the disinformation regarding the alleged damage to Natanz as disinformation to allow them to continue their development programme (Falco 2012), though Iran has denied that Stuxnet affected its nuclear programme (BBC 2010b).

There is also growing evidence that Stuxnet was just part of a wider US programme known as "Olympic Games" of which the most recent development may well be Flame (Williams 2012 and Finkle 2012). Flame has attracted a lot of recent attention and is reported as being twenty times more complex than Stuxnet (Farwell & Rohozinski 2012). It may very well be a highly sophisticated programme but unlike Stuxnet it is not a weapon. Stuxnet infected around one hundred thousand PCs though it only became active on the PLCs of the centrifuges at Natanz (Rid & McBurney 2012 and Barzashka 2013). However, it has emerged that Flame was a cyber-espionage tool and not weapon (Demidov & Simonenko 2013). Flame was concerned with the gathering of information, including the turning on of microphones and webcams inbuilt into computers and taking screenshots (Farwell & Rohozinski 2012). The recent Home Affairs Select Committee report on e-crime makes a very valid point in this regard.

> 'We also note as a principle, that if personal data is held in any database, no matter how secure, there is a risk of it being accessed inappropriately, either through human error or malice. The only way to ensure data does not leak is not to collect it' (House of Commons 2013: 9).

This section has analysed the various debates the surround Objective #2 of the CSS and has identified the key arguments regarding resilience. If has highlighted the substantive questions regarding how to define a cyber-attack, what threshold for violence should be applied, whether only direct actions should be considered and furthermore, that resilience is not an abstract construct but rather a product of time and threat vectors. Therefore, the recent initiative to share details of cyber-attacks is welcome (Maude 2013).

Objective #3: Open Society and International Norms

Objective #3 of the CSS is for 'the UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies' (Cabinet Office 2011: 21). This is a particularly vague statement that provides little direction as part of a strategy (McGhie 2012). It appears that the Cabinet Office has had similar difficulty in deciding how to translate this objective into action. Its own progress report only identifies six points that have been achieved with regard to this objective, which is the least of the four objectives, and furthermore, only two of these points are actually unique to Objective #3 (Cabinet Office 2012: 4). It also opens up a fundamental question as to how to classify an open, stable and vibrant cyberspace, and whether the open society applies just to the UK or other countries that use cyberspace as well.

To begin with the question of what constitutes an open society will be addressed before moving on to look at the role of the UK in establishing international norms for conduct in cyberspace. In order to start contemplating what an open society would involve consider the address given by former United States President Ronald Reagan to the Guildhall in London, shortly after leaving office in the summer of 1989, where he declared that 'information is the oxygen of the modern age, it seeps through walls topped with barbed wire, it wafts across he electrified, booby-trapped borders' before proceeding to highlight how 'breezes of electronic beams blow through the Iron Curtain as if it was lace' and that 'the Goliath of totalitarianism will be bought down by the David of the microchip' (Rule 1989).

This statement became especially poignant for governments in the light of the Arab Spring (Howard et al. 2011 and Srinivasan 2012). Egypt actually shut down the internet in the wake of the uprising to overthrow Mubarak (Williams 2011), and in a similar vein President Assad of Syria has also denied access to information via the internet (Chulov 2012). There have been examples in the absence of conflict too. China blocks access to a number of sites such as Google (Miller 2012). Consequently, the internet does not provide freedom of access to information but rather the government decides what level of access of information its people should have. Therefore, it would be possible to interpret this objective as stating that the UK will not support governments who do not adhere to the level of freedom of information that the British Government deems acceptable.

The argument deepens when considering what is meant by an open, stable and vibrant cyberspace. The implication is that the UK is against censorship and allows information to pass freely through the internet, with the public deciding what they do or don't want to look at. However, the UK has recently imposed restrictions on access to pornography online (BBC 2013d). The moral argument

behind this is outside the scope of this paper, but the fact remains that pornography is a legal enterprise under UK law yet the Government has decided to restrict access online. The population as a whole probably accepts that laws should be in place to prosecute people who use the internet to download terrorist information, such as Al-Qaeda's online magazine *Inspire* (O'Neill 2013). Interestingly the perpetrators of such an action do not find themselves challenged with some form of cyber-crime but rather under the Terrorism Act 2006, which makes a range of potential charges available, such as the Dissemination of Terrorist Publications (section 2) or the Preparation for a Terrorism Act (section 5) (HM Government 2006).

This is especially interesting as the government has utilised the Terrorism Act against people with no available means for them to carry out an act of terrorism (Macdonald 2013). Consider the case of R v G, where the defendant was convicted of terrorism offences despite being in prison when the offences took place (House of Lords 2009). Somehow the defendant had managed to acquire bomb making literature and, furthermore, was assessed as mentally ill, and substantive questions were raised as to the actual intent of the victim (House of Lords 2009). However, he was convicted and the House of Lords upheld the conviction that he was responsible for his actions, despite accepting that he was suffering from paranoid schizophrenia at the time, utilising case law from 1843 (2009).

The case of Riwzaan Sabir is also relevant, and takes the debate into the cyber realm. He was held for seven days without charge, under the Terrorism Act, for downloading a manual from a US government database, which could have been purchased at a number of high street shops (Townsend 2012). Like the example of R v G, Sabir had in his possession a document which called for answers. At the time Sabir was undertaking research into terrorism as part of a Master's degree at Nottingham University, and the case is further eroded as the Police fabricated the alleged evidence (Townsend 2012). Sabir was released without charge or apology and a paper was published which heavily criticised the role of the university and pressure was exerted to have that paper quashed (Thornton 2011).

The most high-profile question in relation to an open society within cyberspace has recently been exposed by Edward Snowden and the PRISM affair (BBC 2013e, Blake 2013, Gellman & Poitras 2013, Greenwald 2013, Greenwald & MacAskill 2013 and Greenwald, MacAskill & Poitras 2013). The episode challenges us to think about espionage in cyberspace, and how intelligence is gathered. In light of this objective the role of GCHQ, and by extension the UK Government, in carrying out operations spying on its own population, as well as allies and regimes to which it is opposed, questions the commitment to an open, vibrant and secure cyberspace. The full ramifications of the affair is still unfolding and the lack of the UK to properly address the challenges raised by Objective

#3 can be fully analysed once all the facts are known. The situation is evolving even as this paper is being written and the latest development is the arrest of the David Miranda in the UK under the Terrorism Act 2000 (Rucker & Adam 2013). Miranda is the partner of Washington Post journalist Glenn Greenwald who worked with Edward Snowden to expose the US National Security Agency's surveillance programs (Rucker & Adam 2013). A further interesting development, is that security organisations have shun the current technology and reverted back to traditional methods, as within The Kremlin where there is understood to be a reversion to paper and typewriters to provide a more closed and, therefore, a more secure internal communication system (Irvine 2013).

The examples provided illustrate the nature of the debate that can be developed around the issue of open society, cyberspace, and the access to information. Syria, Egypt and China have all demonstrated that it is governments who decide what level of access is available to its people. In this regard the UK is no different, as it too makes determinations about just what should or should not be available to its citizenry. Therefore, in terms of the CSS the inclusion of this objective had the potential to ignite a major debate as to the central role that cyberspace and the freedom of information should have in the day to day lives of the citizens of the UK.

This section will now look at the two unique points that objective #3 has achieved; the organisation of the London Conference on Cyberspace and Get Safe Online Week as part of the global Cyber Security Month (Cabinet Office 2012). It is hard to critically analyse these two initiatives in reference to the overall CSS, whilst they are both commendable in their own right and clearly form part of an agenda to increase educational awareness of cyber-security there is no method of quantifying the success. This is compounded by the general vaguity of the objective which would benefit greatly from having clear signposts as to what it is actually intended to achieve.

The London Conference on Cyberspace involved delegates from sixty countries and covered a broad range of topics (Hague 2011). Considering the conference lasted two days questions are raised regarding how much could actually be achieved in such a short space of time, across a diverse range of topics that involved seven hundred people (Telefonica 2011). Further critique is made in that a lot of talking was done at the conference, however, its real measure of success would be in action (Lazanski 2011). The conference is declared a success by almost every comment that can be found on it, although discovering a real world action that has resulted directly from the conference is significantly harder. Perhaps a narrower focus would have enabled more positive action that could have addressed some of the fundamental conceptual issues to enable explicit strategy formulation.

Get Safe Online week is just as hard to attribute success or failure to. The campaign alleges 56% of the UK populous has been targeted by online criminals and general poor hygiene[4] is used by the majority of the UK (Maude 2012). Apparently the scheme was a great success though no empirical evidence backs this up (Mitchell 2012). Perhaps the continued rise of cyber-crime and the assertions by Verizon that 75% of cyber-intrusion incidents are opportunistic and utilise minimal computing skills suggests otherwise (House of Commons 2013 and Verizon 2013: 6). This is further reinforced by a recent report from the National Audit Office which suggests that '80% of cyber attacks could be prevented through simple computer and network "hygiene"' (2013: 4).

Providing analysis of such a broad and open-ended objective is almost impossible in any great depth, as it arguably develops more questions than it answers. The broad principle appears to indicate a move towards establishing acceptable norms for conduct within cyberspace. However, the opportunity to take the lead in this regard appears to have not been seized. Considering, the conceptual challenges that exist within cyber-security and the lack of any definitive produce from initiatives carried out under this objective it is hard to consider it a success, especially when the Tallinn Manual has proved the first set of international guidelines of acceptable norms within cyberspace (Schmitt 2013).

[4] The specific computer security terminology for best practice

Objective 4: Recruitment and Training of Cyber-Security Specialists

Objective #4 of the CSS is for 'the UK [to] have the cross-cutting knowledge, skills and capability it needs to underpin all our security objectives' (Cabinet Office 2011: 21). Arguably Objective #4 is the most important as the skills base underpins all the other areas of the CSS. However, it also generates the least debate. Positive moves have been made in this regard such as the establishment of the Academic Centre of Excellence in Cyber Security Research award (GCHQ n.d. and Universities News 2012). However, the allocation of the £650 million supplied for the NCSP shows that the Department for Business Innovation and Skills has been allocated only £13 million over four years, the lowest amount of any area, and the Cabinet Office £33 million over four years, the second lowest amount. These are the two government departments specifically charged with delivering Objective #4 (NAO 2013: 14). Furthermore, a report concluded that 'it is not clear what parameters the Government used to arrive at the figure [£650 million] and as such it is difficult to accurately assess whether the investment will prove sufficient' (Lewin 2011: 25).

The UK seeks to generate the necessary expertise required for the provision of cyber security by training reservists (Sengupta 2013) and by relying on a "Dad's Army" cyber defence force of volunteers (Johnson 2012 and Shute 2013). Whilst the increasing reliance on volunteers is in line with other areas of UK security policy it does reinforce the view that the NSS is a method of justifying and enabling cost-cutting measures (Kaldor 2010). Furthermore, a leaked memo has suggested that the targets for the recruitment of reservists are not being met, which will have an effect on the personnel available for cyber security (BBC 2013f). This is compounded by the recent report on e-crime by the Home Affairs Select Committee which states that 'a quarter of the 800 specialist internet crime officers could be axed as a spending cut' (House of Commons 2013: 8).

As a basis for comparison, the US Cyber Command recently announced plans to expand from nine hundred to five thousand employees then serious questions are raised as to whether the measures undertaken by the NCSP are enough (Tilgham 2013). Indeed, some analysts such as Jim Gosler, a former CIA operative, posit that the lack of adequate personnel 'who have the specialised skills to operate effectively in cyberspace' leads to overall weakness in the cyber security of the United States, which 'needs about 20,000 to 30,000 such individuals' (Evans & Reeder 2010: v). Therefore, whether the measures undertaken as part of this objective go far enough to ensure that the UK does have an adequate skills base is open to question.

Conclusion

The CSS has been viewed as a missed opportunity due it being overly ambitious and not having the required means to fulfil these ambitions (McGhie 2012). Throughout the course of this paper the key debates within cyber-security, in relation to each of the four objectives of the CSS have been analysed. Although some positive initiatives have been undertaken their relationship as part of an overall strategy is clouded by the vaguity of the CSS. However, it should be recalled that the CSS is an inaugural strategy due for update in 2015 so there is scope for a much tighter more coherent effort in the near future.

The strategic development process employed by the UK is a convoluted affair. The separation of ends, ways and means into different documents produced by different branches of government ensures that the process lacks coherence and provides an inherent amount of contradiction and conflict between the documents. The NSS and SDSR has attracted the most attention and been criticised as a flawed process, especially given the process was completed within five months. The CSS is a product of the NSS and SDSR process and as such carries on the flaws of those two documents.

It has been argued that the UK suffers from a form of strategic malaise. However, the evidence suggests that a more accurate term would be a militarised foreign policy malaise. Thereby, the symptoms of the decline in UK strategy are a direct result of the loss of core understanding of strategy in its true military sense. Whilst this goes against the current trend towards increased securitisation there is no universal agreement that this approach is beneficial (Booth 2005 and Booth 2007). In this regard a reversion to a more traditional realist approach to security would aid the reinvigoration of strategy as the narrower concept of military power to provide security as was understood until the later part of the Cold War. The debate questions why it is necessary to have the CSS at all, and that the separation of strategy into different aspects, whether naval, cyber or any other of the possibilities, is a further example of the devaluation of strategy as a concept.

The broad terms of reference for the National Risk Assessment have a similar effect of diluting the overall understanding of security and strategy to such a degree that the provision of security ensures that strategy and policy become conflated. The contradiction and confusion created by the non-inclusion of current threats, and the focus on threats within the next five years, with consideration to a broader twenty year period, ensures that cyber-security inhabits a curious place as a Tier 1 threat. If the National Risk Assessment's terms of reference were fully adhered to then cyber-

security would not be a current security threat, so why a separate CSS would be needed is open to question. The alternative interpretation is the National Risk Assessment did not adequately follow its own methodological guidelines. Either way serious questions can be raised as to the validity of the National Risk Assessment in determining the threats to the UK.

The strategic development process raises serious questions about how Britain does strategy. This is not a new challenge. However, it is a challenge that could have been addressed. As such the CSS has not lessened these concerns and can be considered to have missed the opportunity to do so, especially given that the establishment of the NSC and the switch to a NSS approach instead of the traditional SDR appears to have been an ideal time to reinvigorate the core conception of strategy.

The assumptions that underpin the CSS are questionable and considering Objective #3 was designed with putting the UK at the forefront of the cyber-debate it is a failing that the opportunity to do was missed. The fundamental concepts of cyber and cyberspace needed to be developed to ensure that the full breadth of options available within cyber-security can be considered. This enables a clear distinction between different thresholds of violence to establish and clarity provided to what constitutes a cyber-attack. This would allow the government to focus attention on developing a strategy that specifically addresses these threats and is not an all-encompassing attempt to placate the concerns of corporate entities obsessing over the minimal effects of cyber-disruption.

How to deal with the challenges posed to critical national infrastructure continues to provide problems for governments and the commercial enterprises that own the infrastructure. The incorporation of time and threat vectors into contingency planning will enable a better allocation of resources to ensure the most sensitive areas can be best protected. The government is not the best organisation to deal with every form of cyber-intrusion, however, it needs to clearly define what it is and is not taking responsibility for. The deeper understanding of cyberspace and cyber-attack will enable a much clearer picture to be developed and may well be the case that the future role of the government in cyber-security is limited to critical national infrastructure and high-end threats, whereby security against DDoS and other forms of cyber-disruption, which have minimal impact become the preserve of the individual private companies. This is also likely to ensure that the companies are proactive in cyber-security and ensure that all employees adopt good hygiene so that the chances of cyber-disruption affecting the company are minimised.

The London Conference on Cyberspace exemplifies the approach of trying to cover everything and achieving relatively little. The two day conference saw over seven hundred delegates from sixty different countries attend. This undoubtedly created a good showpiece event, however, there is no

evidence of any positive contribution to the conceptual understandings of the key issues, with the numbers involved and the time constraints this is not much of a surprise. A much narrower scope of discussions would have been better and could have enabled a positive outcome for the conference. In other words it missed the opportunity to have an impact right at the centre of the cyber-security debate by not being focussed enough. For example, if the conference had been dedicated to discussion on what constitutes a cyber-attack then the UK could have had the international lead instead of the Tallinn Manual, as well as gaining a coherent understanding for its own strategic benefit.

The incorporation of the vague notion of fostering open society and a vibrant cyberspace is a prime example of the influence of policy over strategy. It has no strategic meaning and only serves to open up a whole host of questions, with regard to what is meant by open society and how to address the criteria for establishing international norms. It highlights the problems associated with a broader and deeper concept of security and provides a distraction, in terms of resources, from the central concern of providing security. However, it was included and with the exception of Get Safe Online week nothing has been achieved. Therefore, this aspect of the CSS has not met its objective and represents a missed opportunity.

The CSS has had some positive outcomes that mean that the strategy is not totally ineffective. Whilst the NCA was not established by the CSS the incorporation of a combined National Cyber Crime Unit into the NCA is a step in the right direction in the fight against cyber-crime, which is currently being lost. Clearly identifying what constitutes a cyber-crime to enable adequate data to be collected and a true means of targeting the criminals identified has to be a priority. The focus of the CSS has been on the role of organised crime despite the lack of empirical evidence to back up this notion. The damage to the economy is growing and the lack of an adequate identification of what constitutes a cyber-crime and identifying the perpetrators of such crimes means that the CSS missed an opportunity to tackle the problem. Furthermore, the importance of working with allies to establish clear jurisdictional guidance and areas of responsibility needs to be enhanced to ensure that cyber-crime safe havens are denied the ability to operate.

Despite the positive moves of establishing academic centres of excellence for cyber-security serious concerns remain as to whether the necessary number of adequately trained cyber-specialists will be available to deal with the variety of tasks that exist. The reliance on volunteers or reservists, whilst cost-effective, may not be enough to fill the gaps, which are expanding and exacerbating the problem. This appears to be a by-product of the £650 million allocated budget for the four-year term of the Tier 1 threat. There appears to be a mismatch between the rhetoric and the resources to

tackle the apparent threat. However, as a strategy is constrained by its means then it is not possible to state that this aspect of the CSS represents a missed opportunity. Although, any future funding increases should consider increasing the allocation of training and recruiting above the current 7% level.

On reflection the CSS does represent a missed opportunity. However, the CSS is an inaugural strategy and there are positive outcomes from the strategy. Whilst a number of possible improvements for the future are suggested it needs to be understood that the basis for developing a strategy needs to be sound. In terms of a cyber-security strategy this is represented by clearly defining, and understanding, the concepts involved so that threats and responses can be developed. This will enable the strategy to be measured for success or failure. Failure should not be viewed as weakness but rather as an opportunity to develop and improve, thereby, ensuring the adequate provision of security. A reversion to a more traditional view of strategy as being a military concern may be benefical.

At the present, it seems impossible for anyone to know just how well or badly the UK is protected in terms of cyber-security. This situation does not befit the status of cyber-incidents as a Tier 1 threat to the National Security of the UK and needs to be rectified to ensure that the chance of future missed opportunities are minimised.

List of References

Abadinsky, H. (2013) *Organized Crime.* 10th edn. Belmont : Wadsworth

Adee, S. (2008) 'The Hunt for the Kill Switch: Are Chip Makers Building Electronic Trapdoors in Key Military Hardware? The Pentagon is Making its Biggest Effort Yet to Find Out'. *IEEE Spectrum* [online] 01 May. available from <http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch> [08 Jul 2013]

Akamai (2012) *The Hyperconnected World: A New Era of Opportunity* [online] available from <http://www.akamai.com/dl/akamai/hyperconnected_world.pdf> [27 Jul 2013]

Albright, D., Brannan, P. and Walrond, C. (2010) 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?'. *ISIS Report* [online] available from <http://www.isisnuclearіran.org/assets/pdf/stuxnet_FEP_22Dec2010.pdf> [29 Jul 2013]

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S. (2012) *Measuring the Cost of Cybercrime* [online] Workshop on the Economics of Information Security. available from <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf> [16 Jul 2013]

Andress, J. and Winterfield, S. (2011) *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham: Syngress

Amano, Y. (2011) 'IAEA's Amano: Iran Still Steadily Producing Uranium'. *The Washington Post* [online] 14 February. available from <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/13/AR2011021302204.html> [28 Jul 2013]

Atlantic Council (2103) *Tallinn Manual Fact Sheet* [online] available from <http://www.acus.org/files/tallinn_fact_sheet_20130322.pdf> [05 Jul 2013]

Bangham, G. and Shah, S. (2012) 'The National Security Council and the Prime Minister'. *The Wilberforce Society* [online] available from <http://thewilberforcesociety.co.uk/wp-content/uploads/2012/04/TWS-National-Security-and-the-Prime-Minister-George-Bangham-Sarang-Shah2.pdf> [12 Jun 2013]

Barzashka, I. (2013) 'Are Cyber Weapons Effective? - Assessing Stuxnet's Impact on the Iranian Enrichment Programme' *RUSI Journal* [online] 158(2), 48-56. available from <http://www.tandfonline.com/doi/full/10.1080/03071847.2013.787735#.UdaeIGLVDNu> [05 Jul 2013]

Baylis, J. (1989) *British Defence Policy: Striking the Right Balance.* London: Palgrave Macmillan

BBC (2007) *The Cyber Raiders Hitting Estonia* [online] 17 May. available from <http://news.bbc.co.uk/1/hi/world/europe/6665195.stm> [04 Aug 2013]

BBC (2010a) *Cameron Chairs First UK Security Council Meeting* [online] 12 May. available from <http://news.bbc.co.uk/1/hi/uk_politics/8679082.stm> [24 Jul 2013]

BBC (2010b) *Iran Denies Stuxnet Disrupted its Nuclear Programmer* [online] 24 November. available from <http://www.bbc.co.uk/news/technology-11821011> [29 Jul 2013]

BBC (2013a) *UK 'Losing Fight' Against Internet Crime, Warn MPs* [online] 30 Juy. available from <http://www.bbc.co.uk/news/uk-politics-23495121> [12 Aug 2013]

BBC (2013b) *Internet's 'Bad Neighbourhoods' Spread Scams and Spam* [online] 15 March. available from <http://www.bbc.co.uk/news/technology-21798829> [16 Jul 2013]

BBC (2013c) *Japanese Police Target Users of Tor Anonymous Network* [online] 22 April. available from <http://www.bbc.co.uk/news/technology-22248692> [16 Jul 2013]

BBC (2013d) *Online Pornography to be Blocked by Default, PM Announces* [online] 22 July. available from <http://www.bbc.co.uk/news/uk-23401076> [19 Aug 2013]

BBC (2013e) *Barack Obama Defends US Surveillance Tactics* [online] 08 June. available from <http://www.bbc.co.uk/news/world-us-canada-22820711> [23 Jul 2013]

BBC (2013f) *Army Cuts: Reservists Slow to Enlist, Leaked Memo Suggests* [online] 11 August. available from <http://www.bbc.co.uk/news/uk-23654334> [12 Aug 2013]

Betz, D. and Stevens, T. (2011) 'Introduction' *Adelphi Series* [online] 51(424), 9-34. available from <http://www.tandfonline.com/doi/pdf/10.1080/19445571.2011.636953> [06 Jul 2013]

Bhattacharjee, Y. (2011) 'How a Remote Town in Romania Has Become Cybercrime Central'. *Wired* [online] 31 January. available from <http://www.wired.com/magazine/2011/01/ff_hackerville_romania/> [16 Jul 2013]

Blake, A. (2013) 'Clapper: Leaks are "Literally Gut-Wrenching, Leaker Being Sought'. *The Washington Post* [online] 09 June. available from <http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/09/clapper-leaks-are-literally-gut-wrenching-leaker-being-sought/> [23 Jul 2013]

Booth, K. (ed.) (2005) *Critical Security Studies and World Politics.* Boulder: Lynne Rienner

Booth, K. (2007) *Theory of World Security.* Cambridge: Cambridge University Press

Bowers, S. (2012) 'Full Tilt Poker Tycoon Arrested by FBI'. *The Guardian* [online] 03 July. available from < http://www.guardian.co.uk/uk/2012/jul/03/full-tilt-poker-bitar-arrested> [17 Jul 2013]

Bowers, S. (2013) 'Ray Bitar, Full Tilt Poker Founder, Strikes Deal with US Prosecutors'. *The Guardian* [online] 09 April. available from < http://www.guardian.co.uk/uk/2013/apr/09/ray-bitar-full-tilt-poker-pleads-guilty> [17 Jul 2013]

Boys, J. (2012) 'Intelligence Design: UK National Security in a Changing World*'. The Bow Group* [online] available from <http://www.kcl.ac.uk/artshums/depts/mems/news/files/Intelligence-Design-Bow-Group-July-2012-(final).pdf> [12 Jun 2013]

Britz, M. (2009) *Computer Forensics and Cyber Crime.* 2nd edn. Upper Saddle River: Pearson

Budiansky, S. (2004) *Air Power: The Men, Machines and Ideas that Revolutionized War, From Kitty Hawk to Gulf War II.* London: Viking

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S. and Da, C. (2013) *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online] available from <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2211842> [15 Jul 2013]

Buzan, B. (1991) *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era.* 2nd edn. London: Harvester Wheatsheaf

Buzan, B., Waever, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis.* Boulder: Lynne Rienner

Cabinet Office (2008) *National Risk Register* [online] London: Stationery Office. available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61934/national_risk_register.pdf> [19 Aug 2013]

Cabinet Office (2009) *Cyber Security of the United Kingdom: Safety, Security and Resilience in Cyber Space* [online] London: Stationery Office, Cm 7642. available from <http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf> [12 Aug 2013]

Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* [online] available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> [12 Jun 2013]

Cabinet Office (2012) *Progress Against the Objectives of the National Cyber Security Strategy – December 2012* [online] available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf> [16 Aug 2013]

Cavelty, M. (2013) 'Cyber-Security'. in *Contemporary Security Studies*. 3rd edn. ed. by Collins, A. Oxford: Oxford University Press, 362-378

CESG (2012) *10 Steps to Cyber Security* [online] available from <http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1121-10-steps-to-cyber-security-advice-sheets> [15 Aug 2013]

Chulov, M. (2012) 'Syria Shuts Off Internet Access Across the Country' *The Guardian* [online] 29 November. available from <http://www.theguardian.com/world/2012/nov/29/syria-blocks-internet> [19 Aug 2013]

Clark, D. (2010) *Characterizing Cyberspace: Past, Present and Future* [online] available from <http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf> [11 Jun 2013]

Clarke, R. and Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to Do About it.* New York: HarperCollins

Clausewitz, C. (1984) *On War*. trans. by Howard, M. and Paret, P. Princeton: Princeton University Press

Clemente, D. (2013) 'Cyber Security and Global Interdependence: What is Critical?' *Chatham House* [online] available from <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf> [11 Jul 2013]

Cohen, E. (2002) *Supreme Command*. New York: Free Press

Corera, G. (2013) 'The "cyber-attack" threat to London's Olympic Ceremony'. *BBC* [online] 08 July. available from <http://www.bbc.co.uk/news/uk-23195283> [22 Jul 2013]

Cornish, P. and Dorman, A. (2011) 'Dr Fox and the Philosopher's Stone: The Alchemy of National Defence in the Age of Austerity' *International Affairs* [online] 87(2), 335-353. available from<http://www.chathamhouse.org/sites/default/files/public/International%20Affairs/2011/87_2cornish_dorman.pdf> [14 Aug 2013]

Council of Europe (2001) *Convention on Cybercrime* [online] available from <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [18 Jul 2013]

Cross, M. (2008) *Scene of the Cybercrime.* 2nd edn. Burlington: Syngress Publishing

Curtis, S. (2013) 'Georgia: Russia "Conducting Cyber War"'. *The Telegraph* [online] 06 August. available from <http://www.telegraph.co.uk/technology/internet-security/10225735/Users-of-darknet-websites-advised-to-dump-Windows.html> [10 Aug 2013]

Davies, C. (2010) 'Welcome to DarkMarket – Global One-Stop Shop for Cybercrime and Banking Fraud'. *The Guardian* [online] 14 February. available from <http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley> [18 Jul 2013]

Décary-Hétu, D. and Dupont, B. (2012) 'The Social Network of Hackers' *Global Crime* [online] 13(3), 160-175. available from <http://www.tandfonline.com/doi/abs/10.1080/17440572.2012.702523#preview> [18 Jul 2013]

Demidov, O. and Simonenko, M. (2013) 'Flame in Cyberspace' *Security Index: A Russian Journal on International Security* [online] 19(1), 69-72. available from <http://www.tandfonline.com/doi/abs/10.1080/19934270.2013.757131?journalCode=rsec20#.UfY42Y3VDNs> [29 Jul 2013]

Denning, D. (2001) 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy'. in *Networks and Netwars: The Future of Terror, Crime and Militancy.* ed. by Arquilla, D. and Ronfeldt, D. [online] Santa Monica: RAND, 239-288. available from <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf> [15 Jul 2013]

Denning, D. (2009) 'Terror's Web: How the Internet is Transforming Terrorism'. in Jewkes, Y. and Yar, M. (eds.) *Handbook on Internet Crime* [online] Cullompton: Willan Publishing, 194-213. available from <http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf> [03 Aug 2013]

Department of the Army (2010) *Cyberspace Operations Concept Capability Plan 2016-2028*. TRADOC Pamphlet 525-7-8 [online] availabe from <http://www.fas.org/irp/doddir/army/pam525-7-8.pdf> [14 Aug 2013]

Detica (2011) *The Cost of Cyber Crime: A Detica Report with the Office of Cyber Security and Information Assurance in the Cabinet Office* [online] available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf> [16 Jul 2013]

Dinstein, Y. (2002) 'Computer Network Attacks and Self-Defence' *International Law Studies* [online] 76, 99-119. available from <http://www.usnwc.edu/getattachment/26796276-0919-4699-b2f0-5f15f46cb894/Computer-Network-Attacks-and-Self-Defense.aspx> [28 Jun 2013]

Dobovšek, B. (1996) 'Organised Crime – Can We Unify the Definition?'. in *Policing in Central and Eastern Europe: Comparing Firsthand Knowledge with Experience from the West.* ed. by Pagon, M. [online] Ljubljana: College of Police and Security Studies. available from <https://www.ncjrs.gov/policing/org323.htm> [19 May 2013]

DOD (2011) *Department of Defense Strategy for Operating in Cyberspace* [online] available form <http://www.defense.gov/news/d20110714cyber.pdf> [10 Jun 2013]

Drake, C. (1998) 'The Role of Ideology in Terrorist Target Selection' *Terrorism and Political Violence* 10(2), 53-85

ENISA (2011) *Inter-X: Resilience of the Internet Interconnection Ecosystem* [online] available from <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report> [21 Jul 2013]

Evans, K. and Reeder, F. (2010) 'A Human Capital Crisis in Cybersecurity' *Center for Strategic & International Studies* [online] available from <http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf> [10 Aug 2013]

Falco, M. (2012) 'Stuxnet Facts Report: A Technical and Strategic Analysis'. *CCDCOE* [online] available from <http://www.ccdcoe.org/205.html> [28 Jul 2013]

Farmer, D. (2010) *Do the Principles of War Apply to Cyber War?* [online] available from <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA522972> [10 Jun 2013]

Farwell, J. and Rohozinski, R. (2012) 'The New Reality of Cyber War' S*urvival: Global Politics and Strategy* [online] 54(4), 107-120. available from <http://www.tandfonline.com/doi/abs/10.1080/00396338.2012.709391#.UfY4N43VDNs> [29 Jul 2013]

Fiedler, I. and Wilcke, A. (2011) *The Market for Online Poker* [online] available from <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1747646> [17 Jul 2013]

Finkle, J. (2012) 'Powerful "Flame" Cyber Weapon Found in Iran'. *Reuters* [online] 28 May. available from <http://www.reuters.com/article/2012/05/28/net-us-cyberwar-flame-idUSBRE84R0E420120528> [29 Jul 2013]

Folsom, T. (2007) 'Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality)' *Tulane Journal of Technology & Intellectual Property* [online] 9, 75-121. available from <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1350999> [06 Jul 2013]

Fox, L. (2010) 'Defence Cuts: Liam Fox's Leaked Letter in Full'. *The Telegraph* [online] 28 September. available from <http://www.telegraph.co.uk/news/uknews/defence/8031385/Defence-cuts-Liam-Foxs-leaked-letter-in-full.html> [14 Aug 2013]

Freedman, L. (1998) 'The Revolution in Strategic Affairs' *Adelphi Paper 318* IISS: Oxford University Press

Fulghum, D., Wall, R. and Butler A. (2007a) 'Israel Shows Electronic Prowess' *Aviation Week & Space Technology* [online] 167(21), 28-31. available from <http://seclists.org/isn/2007/Nov/100> [08 Jul 2013]

Gambetta, D. (1996) *The Sicilian Mafia: The Business of Private Protection*. Cambridge: Harvard University Press

GAO (2013) *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* [online] available from <http://www.gao.gov/assets/660/652170.pdf> [06 Jul 2013]

GCHQ (n.d.) *UK Universities Awarded Academic Centre of Excellence Status in Cyber Security Research* [online] available from <http://www.gchq.gov.uk/press/pages/cyber-security-research-centres-of-excellence.aspx> [12 Aug 2013]

GCHQ (2013) *Cyber Incident Response Scheme Launched – 13 Aug 2013* [online] available from <http://www.gchq.gov.uk/Press/Pages/CIR_Scheme_Launched.aspx> [15 Aug 2013]

Gellman, B. and Poitras, L. (2013) 'U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program'. *The Washington Post* [online] 06 June. available from <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html> [23 Jul 2013]

Gibson, W. (1984) *Neuromancer.* New York: Ace

Gordon, S. and Ford, R. (2003) 'Cyberterrorism?' *Symantec Security Response* [online] available from <http://www.symantec.com/avcenter/reference/cyberterrorism.pdf> [03 Aug 2013]

Greenberg, A. (2012) 'Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits'. *Forbes* [online] 26 March. available from <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/> [29 Jul 2013]

Greenwald, G. (2013) 'NSA Collecting Phone Records of Millions of Verizon Customers Daily'. *The Guardian* [online] 06 June. available from <http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> [23 Jul 2013]

Greenwald, G. and MacAskill, E. (2013) 'Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks'. *The Guardian* [online] 07 June. available from <http://www.guardian.co.uk/world/2013/jun/07/obama-china-targets-cyber-overseas> [23 Jul 2013]

Greenwald, G., MacAskill, E. and Poitras, L. (2013) 'Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations'. *The Guardian* [online] 10 June. available from <http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> [23 Jul 2013]

Hague, W. (2011) *London Conference on Cyberspace: Chair's Statement* [online] available from <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement> [15 Aug 2013]

Haimes, Y. (2009) 'On the Definition of Resilience in Systems' *Risk Analysis* [online] 29(4), 498-501. available from < http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01216.x/abstract> [21 Jul 2013]

Haimes, Y., Crowther, K. and Horowitz, B. (2006) 'Homeland Security Prepardness: Balancing Protection with Resilience in Emergent Systems' *Systems Engineering* [online] 11(4), 287-308. available from <http://onlinelibrary.wiley.com/doi/10.1002/sys.20101/abstract> [22 Jul 2013]

Hall, C., Anderson, R., Clayton, R. Ouzounis, E. and Trimintzios, P. (2011) 'Resilience of the Internet Interconnection Ecosystem' [online] available from <http://weis2011.econinfosec.org/papers/Resilience%20of%20the%20Internet%20Interconnection%20Ecosystem.pdf> [21 Jul 2013]

Harris, L. (2006) 'Introducing the Strategic Approach: An Examination of Loyalist Paramilitaries in Northern Ireland' *British Journal of Politics and International Relations [online]* 8(4), 539-549. available from <http://onlinelibrary.wiley.com/doi/10.1111/j.1467-856X.2006.00237.x/abstract> [03 Aug 2013]

Herzog, S. (2011) 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' *Journal of Strategic Studies* [online] 4(2), 49-60. available from <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss> [04 Aug 2013]

HM Government (n.d.a) *Fact Sheet 1: Our Approach to the National Security Strategy* [online] available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62483/Factsheet1-Our-Approach-National-Security-Strategy.pdf> [13 Aug 2013]

HM Government (n.d.b) *Fact Sheet 2: National Security Risk Assessment* [online] available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62484/Factsheet2-National-Security-Risk-Assessment.pdf> [19 Aug 2013]

HM Government (2006) *Terrorism Act* [online] available from <http://www.legislation.gov.uk/ukpga/2006/11/contents> [19 Aug 2006]

HM Government (2010a) *A Strong Britain in an Age of Uncertainty: The National Security Strategy* [online] London: Stationery Office, Cm 7953. available from <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf> [11 Jun 2013]

HM Government (2010b) *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* [online] London: Stationery Office, Cm 7948. available from <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf> [11 Jun 2013]

Home Office (2011) *The National Crime Agency: A Plan for Creation of a National Crime-Fighting Capability* [online] London: Stationery Office, Cm 8097. available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97826/nca-creation-plan.pdf> [18 Jul 2013]

House of Commons (2010) Great Britain Parliament Select Committee on Public Administration. *Who Does UK National Strategy? 1st Report of the Public Administration Select Committee*. [online] London: Stationery Office (HC paper; 435; Session 2010-11) available from <http://www.publications.parliament.uk/pa/cm201011/cmselect/cmpubadm/435/435.pdf> [14 Aug 2013]

House of Commons (2013) Great Britain Parliament Select Committee on Home Affairs. *E-Crime 5th Report of the Home Affairs Select Committee*. [online] London: Stationery Office (HC paper; 70; Session 2013-14) available from <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf> [15 Aug 2013]

House of Lords (2009) Appellate Committee: *Judgements – R v G (Respondent) (on appeal from the Court of Appeal Criminal Division) R v J (Respondent) (on appeal from the Court of Appeal Criminal Division)* [online] (UKHL; 13; Session 2008-9). available from <http://www.publications.parliament.uk/pa/ld200809/ldjudgmt/jd090304/rgrj.pdf> [19 Aug 2013]

House of Lords (2010) Great Britain Parliament Select Committee on the European Union. *Protecting Europe Against Large-Scale Cyber-Attacks 5th Report of the Select Committee on the European Union*. London: Stationery Office (HL paper; 68; Session 2009-10)

House of Lords (2011) Great Britain Parliament Select Committee on the European Union. *The EU Internal Security Strategy 17th Report of the Select Committee on the European Union*. London: Stationery Office (HL paper; 149; Session 2010-12)

House of Lords and House of Commons (2012) Joint Committee on the National Security Strategy. *First Review of the National Security Strategy 2010 1st Report of the Select Committee on the National Security Strategy*. [online] London: Stationery Office (HL paper; 265; HC paper; 1384; Session 2010-12) available from <http://www.publications.parliament.uk/pa/jt201012/jtselect/jtnatsec/265/265.pdf> [19 Aug 2013]

Howard, M. (1983) *The Causes of War*. London: Counterpoint

Howard, P., Duffy, A., Freelon, D., Hussain, M., Mari, W. and Mazaid, M. (2011) 'Opening Closed Regimes: What was the Role of Social Media During the Arab Spring' *Project on Information Technology & Political Islam* [online] available from <http://pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf> [24 Jul 2013]

Irvine, C. (2013) 'Kremlin Returns to Typewrites to Avoid Computer Leaks'. *The Telegraph* [online] 11 July. available from <http://www.telegraph.co.uk/news/worldnews/europe/russia/10173645/Kremlin-returns-to-typewriters-to-avoid-computer-leaks.html> [23 Jul 2013]

Jermy, S. (2011) *Strategy for Action: Using Force Wisely in the 21st Century*. London: Knightstone

Johnson, F. (1960) *Defence by Committee: The British Committee of Imperial Defence, 1885-1959*. Oxford: Oxford University Press

Johnson, W. (2012) 'Dad's Army of Cyber Security Experts to be Created'. *The Telegraph* [online] 03 December. available from <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9719354/Dads-Army-of-cyber-security-experts-to-be-created.html> [23 Jul 2013]

Kaldor, M. (2010) *Documents at Odds: The UK's National Security Review* [online] available from <http://www.opendemocracy.net/mary-kaldor/documents-at-odds-uk%E2%80%99s-national-security-review> [12 Jun 2013]

Kshetri, N. (2013) *Cybercrime and Cybersecurity in the Global South*. Basingstoke: Palgrave Macmillan

Kydd, A and Walter, B. (2006) 'The Strategies of Terrorism' *International Security* [online] 31(1), 49-80 available from <http://www.mitpressjournals.org/doi/pdf/10.1162/isec.2006.31.1.49> [03 Jan 2013]

Lazanski, D. (2011) *London Cyberspace Conference: It's Good to Talk, but Better to Do* [online] 04 November. available from <http://www.thecommentator.com/article/603/london_cyberspace_conference_it_s_good_to_talk_but_better_to_do> [16 Aug 2013]

Leonhard, R. (1998) *The Principles of War for the Information Age.* Novato: Presidio

Levi, M. (1998) 'Perspectives on "Organised Crime": An Overview' *The Howard Journal* [online] 37(4), 335-345. available from <http://onlinelibrary.wiley.com/doi/10.1111/1468-2311.00104/pdf> [20 May 2013]

Lewin, D. (2011) Keeping Britain Safe: An Assessment of UK Homeland Security Strategy. *Inaugural Report Commissioned by the APPG HS.* [online] available from <http://homeland-security.org.uk/wp-content/uploads/2011/04/APPG-HS-Inaugural-Report.pdf> (Session 2010-11) [12 Aug 2013]

Lewis, J. (2010a) 'Thresholds for Cyber War' *Centre for Strategic and International Studies* [online] 1-9. available from <http://csis.org/files/publication/101001_ieee_insert.pdf> [08 Jul 2013]

Lewis, J. (2010b) 'The Cyber War Has Not Begun' *Centre for Strategic and International Studies* [online] available from <http://dev.csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf> [23 Jul 2013]

Liddell-Hart, B. (1944) *Thoughts on War.* London: Faber and Faber

Lobell, S. (2004) 'Politics and National Security: The Battles of Britain' *Conflict Management and Peace Studies* [online] 21(4), 269-286. available from <http://www.tandfonline.com/doi/abs/10.1080/07388940490882541#.UfZLg43VDNs> [29 Jul 2013]

Lusthaus, J. (2012) 'Trust in the World of Cybercrime' *Global Crime* [online] 13(2), 71-94. available from <http://www.tandfonline.com/doi/abs/10.1080/17440572.2012.674183#.UeQZk43VDNs> [15 Jul 2013]

Lusthaus, J. (2013) 'How Organised is Organised Cybercrime' *Global Crime* [online] 14(1), 52-60. available from <http://www.tandfonline.com/doi/full/10.1080/17440572.2012.759508#.UeQUlI3VDNs> [15 Jul 2013]

Macdonald, S. (2013) *Preventing Acts of Cyberterrorism: The Criminalisation of Preparatory Activities* [lecture] A Multidisciplinary Conference on Cyberterrorism, 11 April. Birmingham: Cyberterrorism Project

Macdonald, S., Jarvis, L. and Chen T. (2013) *Cyberterrorism Project Research Report no. 2*. 'A Multidisciplinary Conference on Cyberterrorism'. held 11-12 April 2013 at Jury's Inn Hotel Birmingham. [online] Swansea: Swansea University. available from <http://www.cyberterrorism-project.org/wp-content/uploads/2013/07/CTP-Conference-Report.pdf> [6 Jul 2013]

Maguire, M. (2013) *Putting the 'Cyber' in Cyberterrorism: Re-reading Technological Risk in a Hyper-Connected World* [lecture] A Multidisciplinary Conference on Cyberterrorism, 11 April. Birmingham: Cyberterrorism Project

Mahnken, T. (2007) 'Strategic Theory'. in *Strategy in the Contemporary World*. 2nd edn. ed. by Baylis, J., Wirtz, J., Gray, C. and Cohen E. Oxford: Oxford University Press, 66-81

Markoff, J. (2010) 'A Silent Attack, but Not a Subtle One'. *The New York Times* [online] 26 September. available from <http://www.nytimes.com/2010/09/27/technology/27virus.html?_r=0> [08 Jul 2013]

Maude, F. (2012) *Get Safe Online Week* [online] 22 October. available from <https://www.gov.uk/government/news/get-safe-online-week> [16 Aug 2013]

Maude, F. (2013) *Government Launches Information Sharing Partnership on Cyber Security* [online] available from <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security> [12 Aug 2013]

McGhie, I. (2012) 'Cyber-Warfare: Vital Ground, 'Emperor's New Clothes' or Strategic Paralysis?' *Royal College of Defence Studies* [online] available from <http://www.da.mod.uk/colleges/rcds/publications/seaford-house-papers/2012-seaford-house-papers/shp-2012-mcghie.pdf> [14 Aug 2013]

McGraw, G. (2013) 'Cyber War is Inevitable (Unless We Build Security In)' *Journal of Strategic Studies* 36(1), 109-119. available from <http://www.tandfonline.com/doi/pdf/10.1080/01402390.2012.742013> [04 Jun 2013]

McMullan, J. & Rege, A. (2007) 'Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges' *Gaming Law Review* [online] 11 (6), 648–665. available from <http://online.liebertpub.com/doi/abs/10.1089/glr.2007.11602> [17 Jul 2013]

Mele, S. (2013) 'Cyber Weapons: Legal and Strategic Aspects - Version 2.0'. *Italian Institute of Strategic Studies* [online] available from <http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf> [07 Aug 2013]

Miller, C. (2012) 'Google is Blocked in China as Party Congress'. *The New York Times* [online] 09 November. available from <http://bits.blogs.nytimes.com/2012/11/09/google-is-blocked-in-china-as-party-congress-begins/?_r=0> [19 Aug 2013]

Mitchell, T. (2012) *Counting the Success of Get Safe Online Week* [online] 31 October. available from <https://www.getsafeonline.org/blog/counting-the-success-of-get-safe-online-week/> [16 Aug 2013]

MOD (1998) *Strategic Defence Review* [online] London: HMSO. available from <http://merln.ndu.edu/whitepapers/UnitedKingdom1998.pdf> [11 Jun 2013]

MOD (2002) *The Strategic Defence Review: A New Chapter* [online] London: HMSO (Cm 5566-I). available from <http://merln.ndu.edu/whitepapers/UK_SDR_2002.pdf> [11 Jun 2013]

MOD (2003) *Delivering Security in a Changing World* [White Paper] London: HMSO (Cm 6041-I). available from <http://merln.ndu.edu/whitepapers/UnitedKingdom-2003.pdf> [11 Jun 2013]

MOD (2010) *New National Security Council Established* [online] available from <https://www.gov.uk/government/news/new-national-security-council-established> [24 Jul 2013]

Moore, T., Clayton, R. and Anderson, R. (2009) 'The Economics of Online Crime' *Journal of Economic Perspectives* [online] 23(3), 3-20. available from <http://www.sfu.ca/iccrc/content/econ.onlinecrime.pdf> [16 Jul 2013]

NAO (2013) *The UK Cyber Security Strategy: Landscape Review* [online] London: Stationery Office, HC 890. available from <http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf> [18 Jul 2013]

O'Neill, S. (2013) 'Downloading al-Qaeda Terror Guide 'Will Lead to Arrest and Prosecution'. *The Times* [online] 07 May. available from <http://www.thetimes.co.uk/tto/news/uk/crime/article3757618.ece> [18 Jul 2013]

OSCIA (n.d.) *Office of Cyber Security and Information Assurance* [online] available from <https://www.gov.uk/government/policy-teams/office-of-cyber-security-and-information-assurance> [13 Aug 2013]

Ottis, R. (2008) 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective' *CCDCOE* [online] available from <http://www.ccdcoe.org/205.html> [04 Aug 2013]

Paret, P. (ed.) (1986) *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*. Oxford: Clarendon Press

Paulson, R. and Weber, J. (2006) 'Cyberextortion: An overview of Distributed Denial of Service Attacks Against Online Gaming Companies' *Issues in Information Systems* [online] 7(2), 52-56. available from <http://iacis.org/iis/2006/Paulson_Weber.pdf> [17 Jul 2013]

Peterson, D. (2013) 'Offensive Cyber Weapons: Construction, Development, and Employment' *Journal of Strategic Studies* [online] 36(1), 120-124. available from <http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.742014#.UfVFhY3VDNs> [28 Jul 2013]

Porter, P. (2010) 'Why Britain doesn't do Grand Strategy' *RUSI Journal* [online] 155(4), 6-12. available from <http://www.tandfonline.com/doi/abs/10.1080/03071847.2010.514098#.Ugtz0pLVDNs> [14 Aug 2013]

POTUS (2003) *National Strategy to Secure Cyberspace* [online] available from <http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberspace_strategy[1].pdf> [06 Jul 2013]

POTUS (2010) *National Security Strategy* [online] available from <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf> [06 Jul 2013]

POTUS (2011) *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* [online] available from <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> [06 Jul 2013]

Poulsen, K. (2011) *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground.* London: Random House

Prins, G. (2011) 'The British Way of Strategy Making: Vital Lessons for Our Time'. *RUSI* [online] available from <http://www.rusi.org/downloads/assets/The_British_Way_of_Strategy_Making.pdf> [12 Jun 2013]

Queens County DA (2008) *Twenty-Six Charged in $10 Million Dollar Gambino Organized Crime Family Gambling, Loan Sharking and Prostitution Operation* [online] available from <http://www.queensda.org/newpressreleases/2008/february/corozzo_02_07_2008_cmp.pdf> [17 Jul 2013]

Quenqua, D. (2011) 'The Hypo-Connected'. *OMMA* [online] 12 September. available from <http://www.mediapost.com/publications/article/157989/#axzz2ZmNRvMmn> [22 Jul 2013]

Rid, T. (2012) 'Cyber War Will Not Take Place' *Journal of Strategic Studies* [online] 35(1), 5-32. available from <http://dx.doi.org/10.1080/01402390.2011.608939> [28 Jun 2013]

Rid, T. (2013) *Cyber War Will Not Take Place.* London: Hurst

Rid, T. and McBurney, P. (2012) 'Cyber Weapons' *RUSI Journal* [online] 157(1), 6-13. available from <http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354> [28 Jul 2013]

Rose, N. (2011) 'Poker's Black Friday' *Gaming Law Review and Economics* [online] 15(6), 327-331. available from <http://online.liebertpub.com/doi/abs/10.1089/glre.2011.15602> [17 Jul 2013]

Rucker, P. and Adam, K. (2013) 'U.S. had Advance Notice of Britain's Plan to Detain Reporter Glenn Grenwald's Partner'. *The Washington Post* [online] 19 August. available from <http://www.washingtonpost.com/world/europe/uk-police-urged-to-explain-detention-of-reporter-glenn-greewalds-partner/2013/08/19/f2a3159c-08d9-11e3-89fe-abb4a5067014_story.html> [19 Aug 2013]

Rule, S. (1989) 'Reagan Gets a Red Carpet from British'. *The New York Times* [online] 14 June. available from <http://www.nytimes.com/1989/06/14/world/reagan-gets-a-red-carpet-from-british.html?pagewanted=2&src=pm> [24 Jul 2013]

Sanger, D. (2012) 'Obama Order Sped Up Wave of Cyberattacks Against Iran'. *The New York Times* [online] 01 June. available from <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0> [29 Jul 2013]

Schmitt, M. (ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare* [online] Cambridge: Cambridge University Press. available from <http://www.ccdcoe.org/249.html> [06 Jul 2013]

Sengupta, K. (2013) 'Army Reserves to Become Cyber Security and Intelligence Specialists – and Receive More Benefits'. *The Independent* [online] 03 July. available from <http://www.independent.co.uk/news/uk/home-news/army-reserves-to-become-cyber-security-and-intelligence-specialists--and-receive-more-benefits-8684012.html> [10 Aug 2013]

Shute, J. (2013) 'It's Cyber War… Send for Dad's Army'. *The Telegraph* [online] 17 January. available from <http://www.telegraph.co.uk/technology/news/9806125/Its-cyber-war...-send-for-Dads-Army.html> [10 Aug 2013]

Sommer, P. and Brown I. (2011) 'Reducing Systemic Cybersecurity Risk' *OECD/IFP Project: Future Global Shocks* [online] available from <http://www.oecd.org/governance/risk/46889922.pdf> [10 Jun 2013]

Srinivasan, R. (2012) 'Taking Power Through Technology in the Arab Spring'. *Aljazeera* [online] 26 October. available from <http://www.aljazeera.com/indepth/opinion/2012/09/201291911534429984 8.html> [24 Jul 2013]

Standage, T. (1999) *The Victorian Internet.* London: Phoenix

Stone, J. (2013a) 'Cyber War Will Take Place' *Journal of Strategic Studies* [online] 36(1), 101-108. available from <http://www.tandfonline.com/doi/pdf/10.1080/01402390.2012.73048> [04 Jun 2013]

Strachan, H. (2005) 'The Lost Meaning of Strategy' *Survival* [online] 47(3), 33-54. available from <http://www.tandfonline.com/doi/abs/10.1080/00396330500248102#.Ugte0pLVDNs> [14 Aug 2013]

Straubhaar, J., LaRose, R. and Davenport, L. (2012) *Media Now: Understanding Media, Culture, and Technology*. 8th edn. Boston: Wadsworth

Swaine, J. (2008) 'Georgia: Russia "Conducting Cyber War"'. *The Telegraph* [online] 11 August. available from <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> [28 Jun 2013]

Telefonica (2011) *Views from the London Conference on CyberSpace* [online] 04 November. available from <http://www.publicpolicy.telefonica.com/blogs/blog/2011/11/04/views-from-the-london-conference-on-cyberspace/> [16 Aug 2013]

Thornton, R. (2011) *Radicalisation at Universities or Radicalisation by Universities?: How a Student's Use of a Library Book Became a "Major Islamist Plot"* [online] available from <http://nottingham.indymedia.org/zines/1762> [19 Aug 2013]

Tilghman, A. (2013) 'U.S. Cyber Command to Hire Thousands of Troops and Civilians'. *Federal Times* [online] 07 February. available from <http://www.federaltimes.com/article/20130207/IT01/302070003/U-S-Cyber-Command-hire-thousands-troops-civiliansl> [10 Aug 2013]

Tofler, A. (1980) *The Third Wave.* New York: Bantam

Tofler, A. and Tofler H. (1993) *War and Anti-War: Making Sense of Today's Global Chaos.* London: Warner Books

Townsend, M. (2012) 'Police "Made Up" Evidence Against Muslim Student'. *The Guardian* [online] 14 July. available from <http://www.theguardian.com/uk/2012/jul/14/police-evidence-muslim-student-rizwaan-sabir> [19 Aug 2013]

Under Attack: The Threat from Cyberspace - Episode 2: Sabotage and Subversion (2013) Radio 4 [8 July 2013, 20:00]

UNDOC (2012) *Digest of Organized Crime Cases: A Compilation of Cases with Commentaries and Lessons Learned* [online] available from <https://www.unodc.org/documents/organized-crime/EnglishDigest_Final301012_30102012.pdf> [16 Jul 2013]

UNDOC (2013) *Comprehensive Study on Cybercrime* [online] available from <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> [18 Jul 2013]

Universities News (2012) *UK Intelligence awards 8 Varsities for Cyber Security* [online] 06 April. available from <http://www.universitiesnews.com.previewdns.com/2012/04/06/uk-intelligence-awards-8-varsities-for-cyber-security/> [16 Aug 2013]

USAF (2011) *Cyberspace Operations: Air Force Doctrine Document 3-12* [online] available from <http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf> [06 Jul 2013]

Varese, F. (2011) *Mafias on the Move: How Organized Crime Conquers New Territories.* Princeton: Princeton University Press

Verizon (2013) *Data Breach Investigations Report* [online] available from <http://www.verizonenterprise.com/DBIR/2013/> [16 Aug 2013]

Waxman, M. (2011) 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' *The Yale Journal of International Law* [online] 36(2), 421-459. available from <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf> [28 Jun 2013]

Williams, C. (2011) 'How Egypt Shut Down the Internet' *The Telegraph* [online] 28 January. available from <http://www.telegraph.co.uk/technology/news/9305704/Barack-Obama-ordered-Stuxnet-cyber-attack-on-Iran.html> [29 Jul 2013]

Williams, C. (2012) 'Barack Obama "Ordered Stuxnet Cyber Attack on Iran"'. *The Telegraph* [online] 01 June. available from <http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html> [29 Jul 2013]

Woolen, J. (2013) 'Launch of National Cybercrime Unit a Significant Moment'. *The Guardian* [online] 26 March. available from <http://www.theguardian.com/media-network/media-network-blog/2013/mar/26/cybercrime-unit-security-threats> [15 Aug 2013]

Wright, A. (2006) *Organised Crime.* Cullompton: Willan Publishing

Xin, Zhang and Lan, T. (2010) 'Can Cyber Deterrence Work?'. in *Global Cyber Deterrence: Views from China, the U.S., Russia, India and Norway*. ed. by Nagorski, A. [online] New York: EastWest Institute, 1-3. available from <http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf> [29 Jul 2013]

Yannakogeorgos, P. (2013a) *Keep Cyberwar Narrow* [online] available from <http://nationalinterest.org/commentary/keep-cyberwar-narrow-8459> [11 Jun 2013]

Yannakogeorgos, P. (2013b) *On the Terrorist Misuse of the Internet* [lecture] A Multidisciplinary Conference on Cyberterrorism, 11 April. Birmingham: Cyberterrorism Project

Yannakogeorgos, P. and Mattice, L. (2011) 'Essential Questions for Cyber Policy: Strategically Using Global Norms to Resolve the Cyber Attribution Challenge' *Air Force Research Institute* [online] Maxwell AFB: Air University Press available from <http://afri.au.af.mil/cyber/Docs/Questions.pdf> [06 Jul 2013]

Yarger, H. (2006) *Strategic Theory of for the 21st Century: The Little Book on Big Strategy.* [online] Carlisle: Strategic Studies Institute. available from <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub641.pdf> [03 Aug 2013]

Yusta, J., Correa, G. and Lacal-Arántegui, R. (2011) 'Methodologies and Applications for Critical Infrastructure Protection: State of the Art' *Energy Policy* [online] 39(10), 6100-6119. available from <http://dx.doi.org/10.1016/j.enpol.2011.07.010> [22 Jul 2013]

Low Risk Research Ethics Approval

Where NO human participants are involved and/or when using secondary data - Undergraduate or Postgraduate or Member of staff evaluating service level quality

Project Title

Why has the United Kingdom focused on resilience building as a key component of its National Cyber Security Strategy?

Principal Investigator Certification

I believe that this project **does not require research ethics approval**.	X
I confirm that I have answered all relevant questions in the checklist honestly.	X
I confirm that I will carry out the project in the ways described in the checklist. I will immediately suspend research and request a new ethical approval if the project subsequently changes the information I have given in the checklist.	X

Principal Investigator

Name: Gavin Hall .....

Date: 18/03/2013.....

Student's Supervisor (if applicable)

I have read the checklist and confirm that it covers all the ethical issues raised by this project fully and frankly. I confirm that I have discussed this project with the student and agree that it does not require research ethics approval. I will continue to review ethical issues in the course of supervision.

Name: Simon Massey .....

Date: 22/07/2013.....

Low Risk Research Ethics Approval Checklist

Applicant Details

Project Ref:	P12202
Full name:	Gavin Hall
Faculty:	[BES] Business, Environment and Society
Department:	[IS] International Studies and Social Science
Module Code:	M20ISS
Supervisor:	Simon Massey
Project title:	Why has the United Kingdom focused on resilience building as a key component of its National Cyber Security Strategy?
Date(s):	18/03/2013
Created:	18/03/2013 14:50

Project Details

To account for the challenges posed to the United Kingdom's National Cyber Security Strategy and how well they are being met.

Participants in your research

Questions	Yes	No
1. Will the project involve human participants?		X

Risk to Participants

Questions	Yes	No
2. Will the project involve human patients/clients, health professionals, and/or patient (client) data and/or health professional data?		X
3. Will any invasive physical procedure, including collecting tissue or other samples, be used in the research?		X
4. Is there a risk of physical discomfort to those taking part?		X
5. Is there a risk of psychological or emotional distress to those taking part?		X
6. Is there a risk of challenging the deeply held beliefs of those taking part?		X
7. Is there a risk that previous, current or proposed criminal or illegal acts will be revealed by those taking part?		X
8. Will the project involve giving any form of professional, medical or legal advice, either directly or indirectly to those taking part?		X

Risk to Researcher

Questions	Yes	No
9. Will this project put you or others at risk of physical harm, injury or death?		X
10. Will project put you or others at risk of abduction, physical, mental or sexual abuse?		X
11. Will this project involve participating in acts that may cause psychological or emotional distress to you or to others?		X
12. Will this project involve observing acts which may cause psychological or emotional distress to you or to others?		X
13. Will this project involve reading about, listening to or viewing materials that may cause psychological or emotional distress to you or to others?		X
14. Will this project involve you disclosing personal data to the participants other than your name and the University as your contact and e-mail address?		X
15. Will this project involve you in unsupervised private discussion with people who are not already known to you?		X
16. Will this project potentially place you in the situation where you may receive unwelcome media attention?		X
17. Could the topic or results of this project be seen as illegal or attract the attention of the security services or other agencies?		X
18. Could the topic or results of this project be viewed as controversial by anyone?		X

Informed Consent of the Participant

Questions	Yes	No
19. Are any of the participants under the age of 18?		X
20. Are any of the participants unable mentally or physically to give consent?		X
21. Do you intend to observe the activities of individuals or groups without their knowledge and/or informed consent from each participant (or from his or her parent or guardian)?		X

Participant Confidentiality and Data Protection

Questions	Yes	No
22. Will the project involve collecting data and information from human participants who will be identifiable in the final report?		X
23. Will information not already in the public domain about specific individuals or institutions be identifiable through data published or otherwise made available?		X
24. Do you intend to record, photograph or film individuals or groups without their knowledge or informed consent?		X
25. Do you intend to use the confidential information, knowledge or trade secrets gathered for any purpose other than this research project?		X

Gatekeeper Risk

Questions	Yes	No
26. Will this project involve collecting data outside University buildings?		X
27. Do you intend to collect data in shopping centres or other public places?		X
28. Do you intend to gather data within nurseries, schools or colleges?		X
29. Do you intend to gather data within National Health Service premises?		X

Other Ethical Issues

Questions	Yes	No
30. Is there any other risk or issue not covered above that may pose a risk to you or any of the participants?		X
31. Will any activity associated with this project put you or the participants at an ethical, moral or legal risk?		X

Other Documents submitted
