Adrian Venables, B.Sc. (Hons), M.Sc., M.A.

The changing character of power projection and maritime security in a digital age

Thesis submitted for the degree of Ph.D. International Relations

August 2017

Adrian Venables, B.Sc. (Hons), M.Sc., M.A

The changing character of power projection and maritime security in a digital age

Thesis submitted for the degree of Ph.D. International Relations

August 2017

Abstract

The ability to fully understand the composition and properties of cyberspace and successfully exploit its potential is now regarded as being an essential component in the economic success and prestige of modern networked societies. This dependence has resulted in cyberspace being utilised to project national power and influence and is a key component in the establishment and maintenance of international relationships, trade, and security. Although providing both opportunities and threats in terms of a nation's foreign policy and more broadly in the defence of a nation's critical national infrastructure, the relationship between the maritime and cyber environments is one that is neither well researched or understood, but is becoming increasingly important. This thesis examines how the properties of these two environments can be harnessed to project power and influence over a target audience through three research objectives. The first is to introduce a novel three-dimensional model of cyberspace optimised to better understand how its properties and attributes can be measured in terms of power projection and to demonstrate that the environment does not exhibit universal characteristics but that its structure and use may differ at the source and destination of a cyberpower campaign. The second is to investigate the close relationship and interdependence between the maritime and cyber environments within the context of power and security leading to the new concept of maritime cyberspace. Finally, by classifying cyberattacks as acts of intelligence gathering, sabotage, or subversion, the third objective develops a more nuanced and complex appreciation of how power can be projected in maritime cyberspace to reach a target audience. The thesis concludes by reflecting on the usefulness and applicability of these three objectives and how they go beyond current thinking to enable the UK's defence cyber doctrine to be re-examined and expanded to incorporate these new ideas.

Declaration

I certify that this thesis is my own work and has not been submitted in substantially the same form for the award of a higher degree elsewhere.

Word count: 79950

Table of Contents

List of Figures

List of Tables

Acronyms

ACD	Active Cyber Defence
ACINT	Acoustic Intelligence
AIS	Automatic Identification System
AJP	Allied Joint Doctrine Publication
APT	Advanced Persistent Threat
BIMCO	Baltic and International Maritime Council
Blog	Web Log
C2W	Command and Control Warfare
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEMA	Cyber and Electromagnetic Environment
CLIA	Cruise Line International Association
CMS	Content Management System
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CNI	Critical National Infrastructure
COTS	Commercial Off The Shelf
COMINT	Communications Intelligence
DCDC	Development, Concepts and Doctrine Centre
DCO	Defensive Cyber Operations
DDoS	Distributed Denial of Service
DoS	Denial of Service
EEZ	Exclusive Economic Zone
ELINT	Electronic Intelligence
EMS	Electromagnetic Spectrum
FBI	Federal Bureau of Investigation
GBPS	Gigabit per second
GCHQ	Government Communications Headquarters
GDP	Gross Domestic Product
GEOINT	Geospatial Intelligence
GMDSS	Global Maritime Distress and Safety System
GPO	General Post Office
GPS	Global Positioning System
HF	High Frequency
HINTELL	Deductions drawn from hints and opinion
HUMINT	Human Intelligence
ICS	Industrial Control Systems
ICT	Information Communication Technology
IDS	Intrusion Detection System
InfoOps	Information Operations
INMARSAT	International Maritime Satellite
IMINT	Imagery Intelligence
IMSN	International Mobile Subscriber Number
IMO	International Maritime Organisation
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6

IPMS	Integrated Platform Management System
IPS	Intrusion Prevention System
ISIL	Islamic State in Iraq and the Levant
ISP	Internet Service Provider
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JTRIG	Joint Threat Research Intelligence Group
MASINT	Measurement and Signature Intelligence
MBPS	Megabits per second
MISO	Military Information Support Operations
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organisation
NCSC	National Cyber Security Centre
NSRA	National Security Risk Assessment
OCO	Offensive Cyber Operations
OSINT	Open Source Intelligence
PC	Personal Computer
PIME	Political, Information, Military, Economic
PNT	Position, Navigation, and Timing
PSYOPS	Psychological Operations
QR	Quick Response
RF	Radio Frequency
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SIGINT	Signals Intelligence
SOE	Special Operations Executive
SHF	Super High Frequency
SSL	Secure Socket Layer
TAA	Target Audience Analysis
TECHINT	Technical Intelligence
TCP/IP	Transmission Control Protocol / Internet Protocol
UNCLOS	United Nations Convention on the Law of the Sea
UN GGE	United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
URINT	A ‘feeling in the water’
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

Acknowledgements

My greatest debt is owed to my supervisors Mark Lacy and Daniel Prince for accepting me onto this programme of study and for their assistance in defining my research objectives and aims. Mark has always been available for guiding me through my arguments and for his suggestions as to the direction of my study I am eternally grateful.

Lancaster's Department of Politics, Philosophy and Religion has been very supportive throughout the process and I am especially grateful for Clare Coxhill and Sheila Constantine for their help in administrative matters, particularly as I have conducted much of my study away from the University. Funding for conferences has also been provided both by the Department and the Faculty of Arts and Social Sciences, which gave me a valuable opportunity to discuss my work with other maritime professionals.

Finally, this thesis is dedicated to my wife Steph and son Jakob for their patience during the long periods that I have been in my study and to Eddy and Pearl who spent this time lying at my feet waiting for their next walk.

Chapter 1: Introduction

Control of the sea by maritime commerce and naval supremacy means predominant influence in the world … [and] is the chief among the merely material elements in the power and prosperity of nations.

Mahan, 1890[1]

As an innovation in warfare, we anticipate that cyberwar may be to the 21st century what *blitzkrieg* was to the 20th century.

Arquilla and Ronfeldt, 1993[2]

…cyberwar has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future.

Rid, 2013[3]

Background

This thesis examines for the first time how the properties of the maritime and cyber environments can be combined and exploited to project power and influence over a target audience. Power in this context is defined as the ability to affect the behaviour of *people* such that A can be regarded as having power over B to the extent that they can get B to do something that they would not otherwise do.[4] This can be achieved either through coercion by threats or intimidation or willingly by emphasising the positive attributes of behavioural change and is realised in cyberspace by targeting people directly or by altering the environment in which they operate.

The maritime environment is at the heart of global trade and security. Covering 72% of the earth's surface and with 80% of the world's population living within 100 miles of the coast, it is a fundamental factor in the lives of many people whose society depends upon freedom of access for trade, food, and its natural resources. With rising populations increasing the demands placed upon the seas and coastal regions, the security of the maritime environment is vital to a

country's national interest to protect and maintain access to its territorial waters and exclusive economic zones.

Allied to maintaining access to the physical maritime environment is an understanding of the virtual one of cyberspace, with the two increasingly becoming interdependent for operations across the spectrum of peace, through times of tension and limited conflict to high intensity warfare. This has now been recognised with cyber threats and vulnerabilities acknowledged as gaining in importance, particularly in what has often been referred to as *ambiguous war* or the *grey zone* in which nations vie for superiority without recourse to overt military action. Recent events have shown that cyberspace has become a key battleground for the conduct of this hybrid form of warfare and there is a debate as to how competition for superiority in this environment changes the character of war. Despite the increasing threat of conflict in cyberspace, it is clear that these concerns have yet to receive the level of attention needed to explore how it affects maritime operations and what types of cyber strategies need to be developed to ensure that freedom of access to the oceans can be maintained.

The ability for coastal nations to be able to effectively use the maritime environment has long been recognised as being vital for their national interest and increasingly cyberspace is now also regarded as a critical element in the functioning of a modern society. This thesis seeks to address the gap in the literature by exploring how power and influence can be projected through cyber means in the maritime environment through the prism of the debate surrounding cybersecurity and cyberwar. It argues that while the debates that have taken place so far can provide a useful framework for providing a greater understanding of the maritime security issues, it can be increasingly valuable to explore cyberspace in a more specific context such as in relation to the terrain in which its infrastructure and users are located.

By proposing that the cyber environment is increasingly central to the maritime and that the two are mutually dependent, this thesis addresses an area of research that has not been fully explored by linking these two elements that

previously only have been regarded in isolation. It achieves this by setting out to provide a means to understand the technical, strategic, and political challenges and opportunities of cyberpower projection in the maritime environment. This is critical to national interests and highlights the need to consider the geographical environment and its effect on the regional properties of cyberspace and not to assume that its characteristics remain universally constant.

The maritime environment

The maritime operating environment is one of five recognised within the Defence Doctrine of the United Kingdom; the others being Land, Air, Space, and Cyberspace.[5] Covering nearly three quarters of the earth's surface, it is of critical importance to global trade, communication, security and as a source of food and fuel.[6] With the increasing globalisation of the world's economy reliant upon international trade and the movement of energy supplies, raw materials and finished goods, freedom of access to the seas will continue to be fundamental to today's society for the foreseeable future.

With 80% of the world's population living within 100 miles of the coast, the maritime environment is a significant source of influence and has the potential to directly affect the way of life of billions of people.[7] As climate change and population growth have the potential to increasingly affect coastal regions, the role played by the seas in these areas is predicted to increasingly become the catalyst for conflict between nations and a cause of internal tension. This immediate region formed between the sea and the adjacent land, termed *the littoral*, is also becoming increasingly important as the focus of national interest as it can be used to exert influence as part of a campaign of power projection targeted at local populations.

Although it may not be immediately apparent, the familiar land environment is similar in many ways to the more remote maritime in that they are both comprised of several distinct political and geographic zones, with the former

closely related to the latter. These may be important for ethnic or historical reasons, but also may contain natural resources that could provide significant national wealth. Although some of these regions are universally accepted as being associated with a single country, there are many areas where territorial ownership is contested and with national pride and economic advantage at stake, some of them have the potential to provide flashpoints for conflict. With over three quarters of the member states of the United Nations having a coastline linking them directly to the seas, international treaties strictly limit the extent that can be claimed as part of nation's territory to 12 miles from the coast.[8] The rest are mostly ungoverned as part of the *Global Commons*, which are defined as the areas that lie outside of the political reach of any one nation state and are open to all vessels, both mercantile and military. With this area open to all, it presents an opportunity for seafaring nations to operate and survey for resources close to the coast of less advanced nations, potentially increasing tensions between them. This also presents an area where non-state actors and criminals may operate outside the jurisdiction of national laws.

Due to the intense interest that nations have in their coastal regions if they are reliant on them for trade, security, and natural resources, they have become a centre for political and military activity. Despite well-established agreements being in place for the use of the seas in both territorial and international waters, some regions have become heavily militarised. States with maritime assets or trade routes to defend operate naval forces tasked with roles ranging from the protection of local interests to global power protection. However, as the size of the oceans prevents any one nation from controlling its entirety all of the time, navies concentrate on maintaining local control for only the period necessary to achieve a particular task. This can lead to a very dynamic situation in which countries may vie for superiority in areas of mutual interest either to demonstrate capability or to deter others from seeking influence in the same waters.

The ability of shipping to manoeuvre to and within an area where they can potentially influence the behaviour of an adversary's population highlights the

role of maritime power in being able to change the course of global events. In addition to being able to access countries that be may geographically distant to a belligerent, maritime power exercised through military vessels is mobile, can carry large numbers of troops, and remain on station for extended periods to provide a threatening presence over a large area. This can achieve a range of political and military objectives including deterrence, coercion and demonstrating to a local population the intent to act if required.[9]

The cyber environment

The importance and maturity of the globally interconnected networks and devices collectively known as *cyberspace* has been acknowledged in that it is now regarded as an equal to the other naturally occurring operating environments of Land, Maritime, Air, and Space. This is despite it being essentially artificial and reliant upon humans for its creation, development, maintenance, and ultimate destruction. As a concept, it has developed from being solely a way for geographically distant computers to exchange data to become, like the maritime environment, a critical element for the functioning of modern society.

Although the relationship between the maritime and the other natural environments have been well explored as demonstrated through maritime airpower, amphibious warfare, and satellite communications systems, the connection with cyberspace has not. Indeed, it has often been regarded as an ethereal environment somehow detached from the others and with its properties independent of them. This thesis seeks to counter this view and address this research gap by examining the relationship between the cyber and maritime environments to demonstrate that the properties of the former are very much dependent on the latter, particularly within the context of power projection.

A key element in the projection of maritime power is for vessels at sea to be able to communicate and exchange a variety of information types including

voice, video, data, and *metadata*, which can be described as data about data. This is required in order to be able to coordinate their tasking with other ships at sea and their controlling authority ashore as well as enable their crews to remain connected to social media and other forms of communications, which is now regarded as an essential component of 21st century life. In addition, when engaged as a means to project power to influence the actions of those living and working in the coastal regions of a target country there is also a need to be able to communicate using compatible technologies and in a language that will enable them to both receive and understand the message. With the increasing use of the Internet and the World Wide Web for one to one and one to many information exchange, entertainment, and commerce, cyberspace is becoming the main communication medium of the age and this link between the virtual cyber and the physical environments where populations reside is now being brought into sharp focus.

Although demonstrating physical differences, the cyber and maritime environments do exhibit significant similarities. This is despite the natural maritime environment being well understood, visible and largely unchanging with the artificial construct of cyberspace invisible and continually evolving and adapting to accommodate new requirements and technological advancements. Both however are similar in that they are so large that they cannot be controlled by a single entity. There are also other parallels between the two environments. Both are used for trade, communication, recreation and to influence the behaviour of others. This means that as for the seas, cyberspace can be used for the creation of wealth and power projection, and is therefore an important national asset to be protected and controlled. Understanding how the properties of the maritime contributes to the cyber environment enables its strengths to be optimised, whilst mitigating its weaknesses to achieve a condition of competitive advantage known as *information superiority*. [10]

Defining the nature of cyberspace is difficult for several reasons. Firstly, as a primarily technical medium, it is an artificial operating environment existing as a virtual entity but dependent upon its physical components. Although

manufactured resources are needed to operate fully in the maritime, air and space environments, the entirety of cyberspace is a human creation and as such it relies on technology for its existence and requires the use of dedicated systems, which themselves need a degree of competence to be able to operate. Also, as cyberspace continues to grow and evolve, new uses are found for the networks and infrastructure that extend beyond that originally conceived. These contain not just the data storage devices and the communication networks connecting them, but now include the management of industrial control systems and domestic devices. With users engaging with cyberspace for an increasingly wide range of purposes, this requires a continual re-evaluation of how the environment is defined and used. More recently these include commerce, recreation, social networking, education and influencing others by persuasion through advertising to coercion through criminal means. Although cyberspace is a virtual medium, its relationship with the geographic location of its infrastructure and physical configuration also contributes to its definition as does an understanding of the computer protocols and electromagnetic properties to appreciate how information is passed from source to destination. Finally, the role of the human component needs to be considered to be aware of how information is presented, assimilated, and understood by the users to achieve the desired purpose. This wide range of uses means that attempting to develop an all-encompassing definition is a challenging proposition. The complexity of trying to understand all aspects of cyberspace has led to several descriptions being developed, such as comprising of a physical layer that can be seen, a virtual layer that enables it to be used as intended and a cognitive layer to interpret the information that it contains.[11]

As for the maritime environment, security in cyberspace is an important aspect in its operation and use. However, whereas at sea, security is considered in terms of the free passage of ships, in the virtual environment it can be regarded as the ability for information to pass from source to its intended destination without delay or interference. As security in cyberspace can be compromised at any of one of more of its constituent components, ensuring that information within it is confidential, retains its integrity and is readily available to authorised

users on demand is a significant challenge. However, not all users of cyberspace are human operators and increasingly the environment is used to transfer data between industrial components that may then be subject to further processing or provide an input to another system before its final output is of use to a human. This may present additional security challenges as a system compromise or manipulation of data may not be immediately apparent and may lead to erroneous information being fed into control systems affecting physical components.

Although the use of a communications medium to project power is not a new concept as evidenced by the role of printed media, radio and latterly television, the range of information, quantity, and speed by which it can now be disseminated through cyberspace presents new challenges and opportunities. The increasing use of mobile devices has led to an environment in which some societies are permanently connected and are fed with information from a variety of sources, some reliable and some less so. For those generating the message and depending upon the circumstances, the options can range from a coercive hard power content to a soft power campaign of attraction and imitation, with smart power combining and coordinating both.

Research objectives of this thesis

Investigating the projection of cyberpower in the maritime environment requires the consideration of a range of factors related to the nature of cyberspace and how they relate to operating from the sea, many of which have yet to be fully understood. To enable this relationship to be better explored, a novel three-dimensional model of cyberspace is introduced to understand how its properties and attributes can be measured in terms of power projection. This also demonstrates that the environment does not exhibit universal characteristics but that its structure and use may differ at the source and destination of a cyberpower campaign. This model has been optimised to explore the complexity of power projection in cyberspace and that its deployment and focus is dependent upon the characteristics of the chosen target. Containing eight

layers, the model provides a comprehensive view of cyberspace ranging from the geographic area in which its infrastructure is located to the human user and their purpose for engaging with the medium. These layers provide an understanding of how users interpret the content of cyberspace, how data is exchanged, its electromagnetic properties, physical infrastructure and supporting services. Unique amongst other representations of cyberspace, this model also explains the environment in terms of three dimensions by including a representation of distance between the source and destination of an information flow and distinguishes between different types of power projection.

Having established a baseline by which the properties of cyberspace can be described, the second research objective is to investigate the close relationship and interdependence between the maritime and cyber environments within the context of power projection and security. This relationship is becoming increasingly important as mariners, both civilian and military, are now becoming reliant upon it for the safe and effective use of the seas. In addition to the common requirements of navigation and engineering functions, the merchant marine now also relies on the automation of cargo handling systems afloat and port installations ashore for their vessels to function as designed with the military dependent upon computer systems for the operation of their weapons systems. In addition to the attributes of cyberspace supporting the maritime environment, the oceans are also fundamental to facilitating global communications by hosting a network of undersea fibre optic cables that enable transcontinental data exchange and provide reliable and economical global communication.

By investigating the mutual dependencies that support the use of the maritime and cyber environments, this thesis introduces the new concept of *maritime cyberspace* to enable this relationship to be better understood. Maritime cyberspace incorporates those aspects of cyberspace that are essential for shipping to operate effectively and safely and highlights those aspects of the maritime environment that enable cyberspace to function in the manner that is expected in the 21st century. In terms of power projection in maritime

cyberspace, two new concepts are developed; *maritime cyberpower* and *cyber seapower*. These extend the methods by which power at sea is exerted in the physical environment and proposes how the properties of cyberspace can be utilised to achieve a similar effect.

Finally, by classifying cyberattacks as acts of intelligence operations, sabotage, or subversion, the third objective develops a more nuanced and complex appreciation of how power can be projected in maritime cyberspace to reach a target audience. As nations seek to exert influence through their navies and in cyberspace, the opportunity exists to combine the properties of both to enable the cyber environment to be used to project power in and from the maritime environment, thereby demonstrating the importance of geography in determining the regional properties of cyberspace. In addressing the previously unaddressed aspect of how the attributes of the sea and cyberspace can be used to project and counter power, the work of two significant scholars are developed and applied. In the discussion of the nature of power, both in the physical and cyber environments, the work of the American political scientist Joseph S Nye Jr is used as the starting point for this research. His analysis of the attributes of hard, soft, and smart power enables the capabilities of the two environments to be placed in context. [12] Nye's spectrum of power projection is considered with that of Thomas Rid, formally of King's College, London, who reassessed the concept of cyberwar and hostile acts in cyberspace and concluded in a 2013 publication that *Cyberwar will not take place*, and that it will always fall short of the accepted definition of warfare. [13] At the time of publishing, his assessment of the viability of conflict in cyberspace contravened with that of the prevailing literature and in particular that of John Arquilla and David Ronfeldt who predicted a future that has not as yet materialised in which cyberweapons would be regarded as having a similar effect to that of their conventional kinetic equivalents.[14]

In providing a more nuanced and pragmatic assessment of the potential for conflict in cyberspace and how behaviours may be changed through coercion or persuasion, Rid proposes that offensive acts in cyberspace will always fall

into one of three categories; espionage, sabotage, and subversion. In expanding espionage to incorporate all aspects of intelligence collection activities and subversion to include psychological operations, this research extends each of these three activities and explains their role within the context of maritime cyberspace. This reveals the complexity of how power projection can be facilitated or prevented through effective security measures within the maritime and cyber environments. This demonstrates that the characteristics, structure and use of cyberspace may be different at the source and destination of a cyberpower campaign and must be considered separately to ensure that what may be transmitted by the originator can still be received and understood at the destination.

Thesis content

This thesis comprises nine chapters that together address the three objectives of this research. The initial objective introduces the novel three-dimensional model of cyberspace optimised to better understand how its properties and attributes can be measured in terms of power projection and to demonstrate that the environment does not exhibit universal characteristics but that its structure and use may differ at the source and destination of a cyberpower campaign. The second demonstrates the link between the maritime and cyber environments within the context of power projection by using the new model of cyberspace to highlight how the virtual and physical environments are related. Finally, by classifying cyberattacks as acts of intelligence gathering, sabotage, or subversion, this third objective develops a more nuanced and complex appreciation of how power can be projected in maritime cyberspace to reach a target audience. By demonstrating the link between the cyber and the maritime environment, this shows that cyberspace is not independent of the other environments but that its properties are dependent upon the physical environment in which its users reside and where its infrastructure is located. The choice of infrastructure type, each of which have different propagation properties. is also a decision that may be based on the geographic environment

and further highlights the role of the physical in determining the properties of the virtual.

Following this introduction, chapter 2 provides a critical review of the significant publications concerning the nature of power, cyberspace, cyberpower. The nature of power itself is a contested issue that is difficult to define and measure and this chapter explains how the most significant literature on the subject addresses the issue and the circumstances for the use of hard, soft, and smart power. In modern conflict, these different types of power are combined and coordinated within the concept of hybrid warfare that can limit offensive action to that just below the threshold of what may be regarded as war like actions, but still achieve strategic effects. As for power, achieving consensus on what constitutes cyberspace is equally challenging and this chapter describes the evolution of the term as cyberspace itself has developed with advancing technology finding new uses for the medium. Introducing the notion of cyberpower, the chapter traces its development from being initially regarded with suspicion to becoming an integral component of strategic planning and how its dependency upon the information environment has led to the need to achieve the competitive advantage of what is known as information superiority. This leads to a description of the militarisation of cyberspace and the spectrum of thought ranging from cyberwar being a decisive factor in a future conflict to being a superficial component that can only ever achieve limited effect.

Chapter 3 builds on the review of the significant literature regarding power and its relationship with cyberspace to examine in detail the issues of power and security in maritime environment. Initially highlighting the issues of protecting the physical environment and the risks to national security that the maritime environment presents, it introduces a cyber component to the challenges of operating at sea and how maritime cyber security has now been recognised as a threat actively being researched and mitigated by industry and academia. This leads to the new issue of how cyberpower at sea may be defined and its contribution to the traditional role and components of seapower.

Chapter 4 addresses the initial research objective by introducing a new eight-layer, three-dimensional model of cyberspace optimised for power projection. Beginning with a review of how cyberspace has evolved and been described from its earliest conception in terms of layers, four new layers incorporating Mission, Human, Services and Geographic considerations are added to previous descriptions of the environment. Second and third dimensions of cyberspace are then added, introducing the notion of distance and that potential variance in the characteristics of the medium in different areas can determine whether hard, soft, or smart types of power projection provide the optimum means to harness the properties of cyberspace.

The maritime environment is at the core of this research and chapter 5 examines its nature and composition. A key argument of this research is that the maritime and cyber environments exhibit many of the same features, which are determined to a large extent by the physical attributes of the oceans, seabed, and littoral regions. With power comes security and the importance of maritime security is emphasised with the risks and threats that countries face in securing their borders, trade routes and associated infrastructure. By considering the mutual dependencies of the maritime and cyber environments the new concept of *maritime cyberspace* is introduced, which illustrates the mutual dependence that each have on each other. By linking power at sea with control of the information environment to achieve information superiority, the two distinct concepts of *maritime cyberpower* and *cyber seapower* are introduced and developed, with the latter comprising of *cyber sea control* and *cyber sea denial*.

With the previous chapters providing the background to the research by explaining the maritime and cyber environments and developing the model, the subsequent three chapters seek to address to the lack of previous research into the relationship between them. Using the concept of maritime cyberspace and the new model of the environment as its basis with the main tenet of Rid's argument that offensive actions in cyberspace comprise just three activities; intelligence gathering, sabotage, and subversion, each are examined in detail

using new case studies to provide additional complexity and understanding. These provide the foundation for understanding how these three methods can be applied to maritime cyberspace to achieve dominance over an adversary at sea or ashore.

Chapter 6 begins this study by considering the full spectrum of intelligence gathering activities that can be employed in support of power projection. At its most straightforward this includes deriving useful information from material that is freely available without the need to take specific action to penetrate systems as well as that which has been released unintentionally by their owners. To acquire information that is restricted or sensitive and not intended to be publicly accessed, techniques associated with espionage may be used. This implies a degree of covertness and subterfuge to gather material such that its owner may be unaware that it has been retrieved with the more advanced techniques usually associated with the role of state agencies. Finally, the importance of metadata is discussed, which is embedded information containing the properties of the data itself. Together, these four types of intelligence sources can provide a comprehensive understanding of an adversary to enable an assessment to be made as to what types of power projection may be most appropriate to achieve the desired end state. Combined with an understanding of maritime cyberspace, this information can be used to plan a cyberpower campaign that has the best chance of altering attitudes and behaviour.

Although an important feature in an overall cyberpower campaign, intelligence operations alone cannot alter behaviour. This is investigated in chapter 7, which in addressing sabotage, is the first of two that focusses on the actual delivery of maritime cyberpower in terms of chapter 4's model of cyberspace. Sabotage in terms of the delivery of power is related to targeting systems with the intention of adversely affecting their performance. Depending upon what effect is possible with the time, resources, and level of access available, this may involve efforts to physically destroy the target, achieve a temporary denial or degradation of its performance or an intermittent disruption of its capability.

The final type of activity that can achieve an effect in maritime cyberspace is detailed in chapter 8, which discusses subversion. This effect differs from the sabotage operations described in the preceding chapter that are designed to affect systems as subversion directly targets people. The objective of subversion is to undermine the authority of an existing order, which may involve changing the behaviour of a single leader or encouraging sufficient numbers to act, causing a popular uprising. In this regard, it is the purest form of cyberpower, but also in some respects the most challenging as it requires an intimate knowledge of the target and their psychological weaknesses. This highlights the importance of intelligence gathering as underpinning all cyberpower projection activities to ensure that the correct target is selected with the right effect at a time in which it will be most effective.

Chapter 9 concludes this thesis by drawing together the themes of the earlier chapters and demonstrating how they have combined to meet the aims of this research. The first was to develop a new three-dimensional model of cyberspace designed to better understand how the properties and attributes of the environment can be assessed and to demonstrate that it does not exhibit universal characteristics but that its characteristics may differ at the source and destination of a cyberpower campaign. Using the model, it was possible to determine that the properties of cyberspace are not universal or unique across the whole environment and may exhibit stark differences depending upon the terrain or geographic location. The second objective was to illustrate how the cyber and maritime environments are connected and this was achieved by introducing the new concept of maritime cyberspace and its use for power projection. Finally, the work of Thomas Rid was used as the basis to provide a more nuanced understanding of cyber amidst some of the more dramatic positions on the use of cyber effects highlighting in the chapter 2. The use of the model in conjunction with the three activities of intelligence gathering, sabotage, and subversion provided evidence of the connection between the maritime and cyber environments and their use for power projection.

Chapter 1 Endnotes

[1] Livezey, W. E., 1985 *Mahan on Sea Power*. 1st ed. Oklahoma: University of Oklahoma Press. Pp281-282.
[2] Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is coming. *Comparative Strategy,* 12(2), pp. 141-165.
[3] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst.
[4] Dahl, R., 1957. The concept of power. *Behavioral Science,* 2(3), pp. 201-215.
[5] Development, Concepts and Doctrine Centre, 2014. *Joint Doctrine Publication 0-01 UK Defence Doctrine.* 5th ed. London: Ministry of Defence.p3
[6] Ibid. p.1-6
[7] Ibid. p.1-6
[8] United Nations, 1982. *TERRITORIAL SEA AND CONTIGUOUS ZONE.* [Online] Available at: http://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm. [Accessed 12 Apr 2016].
[9] Global Firepower, 2015. *Oil Consumption data.* [Online] Available at: http://www.globalfirepower.com/oil-consumption-by-country.asp. [Accessed 11 Apr 2016].
[10] Development, Concepts and Doctrine Centre, 2010. *Future Character of Conflict,* London: Ministry of Defence.
[11] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence.p.1.26
[12] Nye, J. S., 1990. *Bound To Lead: The Changing Nature Of American Power.* 1st ed. New York, NY: Basic Books.p16.
[13] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst.
[14] Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is coming. *Comparative Strategy,* 12(2), pp. 141-165.

Chapter 2: Power, cyberspace and cyberpower

Introduction

This chapter identifies the key authors and the literature that have influenced and shaped the academic discourse regarding the nature of power and how it can be exercised in cyberspace. Commencing with a summary of the nature of power and how the use of different types has evolved and are being applied in the 21st century, the notion of cyberspace is introduced and how cyberpower can be characterised and used to influence a target population through what has become known as the *information environment*. By investigating the concept of power and the means by which it can be targeted in a range of ways to achieve behavioural change, it highlights how it has historically been explained within the context of cyberspace and details the more recent developments noted by contemporary commentators. In reviewing the military use of cyberspace and how it can complement traditional warfighting disciplines, this analysis provides the foundation for the subsequent chapters that investigate the relationship that cyberpower has with the maritime environment and the role of security in limiting or preventing interference in the operation of seaborne activities. Together these fulfil the overall research objectives by better appreciating the unique attributes of the cyberspace and its relationship with the maritime environment in projecting power at and from the sea.

Understanding power and influence

Being able to appreciate how one person, group or country can exert their will over another has been a continual preoccupation of society. This has resulted in the evolution of a variety of power projection methods ranging from the peacetime activities of diplomacy and persuasion through to coercion and low-level conflict, leading ultimately to high intensity warfare. This final threat of being able to exercise power by resorting to violence and destruction to achieve what has not been possible through other more benign means has been

frequently demonstrated by the numerous conflicts seen in the land, sea and air environments and has now extended to space with the development of anti-satellite weapons.[1] However, within the fifth operating environment of cyberspace this has proved to be problematic as seen in the academic discussion regarding the nature of warfare. This is due to the assertion that although code within a computer's memory has been used to affect the operation of industrial systems such that it causes physical damage, it has yet to be seen to directly cause death or injury to persons in the same way as a conventional weapon and without this threat its ability to coerce others through what has traditionally been regarded as warfare is limited.

The aim of a campaign to project power and influence was defined in 1957 by Robert Dahl as the intent to affect the behaviour of *people* such that A can be regarded as having power over B to the extent that they can get B to do something that they would not otherwise do.[2] This definition is expanded on by Joseph Nye, who in describing the nature of power, concluded that not only is it a contested concept, but it remains an elusive one to define and measure. He describes the *three faces of power* used in modern social science definitions, with the first being to get others to do what they would not normally do. The second element is agenda setting and framing issues such that coercion is not required and the final form is to exercise power by determining others' wants.[3] Nye describes national power as being derived from three distinct strategies; hard, soft, and smart. Hard power is regarded as the traditional means of influencing others at the state level and uses coercion or payment to change behaviour to get desired outcomes against an initial preference or strategy.[4] Hard power is not subtle and the coerced party is both aware that it is taking place and from whom. It may also take several forms, the most extreme of which is military action but can also include diplomatic or economic pressures.

The concept of soft power was introduced by Nye in 1990 in his book *Bound to Lead*, with its definition being *to get others to want the outcomes that you want through the power of attraction* and includes non-material means such as the promotion of the positive aspects of a nation's culture, political values and

foreign policies.[5] After over a decade of US led military operations in the Middle East from 2001 - 2014, during which it may be argued produced unclear long term outcomes, the benefits of soft power using a policy of attraction over coercion have been widely seen as offering an alternative means to achieve national objectives when deployed as part of a regional strategy. Depending on how it is defined, hard power can also include not only the use of military power, but draws on the potential economic strength that a large population can realise as part of diplomatic and political engagement. As these can also typically be regarded as tools of soft power, it has been noted that at times the distinction between these two types of power can to some extent become blurred and can depend on how it is perceived by those affected by it.[6] Soft power may also be regarded by some as subordinate to the effects that can be achieved from its hard counterpart in terms of achieving tangible, measurable results. However, it is nevertheless often the preferred initial method used by states that favour persuasion over compulsion and offers an alternative, attractive, and possibly more economical means to achieve strategic objectives.[7]

Nye proposes that the countries that are most likely to gain soft power should display three attributes to optimise their attraction on the global stage.[8] The first of these is that their dominant culture and ideas should align to the prevailing global norms, which include liberalism, pluralism, and autonomy. This sets the standard to which other countries might seek to attain, including a structure that encourages free debate and an active engagement across a range of diverse topics with individuals able to make informed, un-coerced decisions. However, these can be viewed as being very much western ideals and it can be argued that to gain soft power in countries without these traditions or ambitions it is necessary instead to meet local norms that the target population is familiar with and aspires to. Second, to be able to effectively disseminate the desired message it is necessary to have access to multiple channels of communication to enable influence to be exerted over a wide range of formats. To provide a coherent message, this must be available through the entire range of media types that the target has access to. This credibility as an information source is an attribute that can only be achieved over a long period to establish a strong

reputation as being reliable and truthful to both domestic and international audiences. Finally, for a country to gain soft power, it must be seen to be dependable in terms of its domestic and international performance in order for it to be attractive to the target it wishes to effect. This requires the influencing country to be highly regarded, trustworthy and be seen to have a good reputation on the world stage in terms of its national values and behaviour.

With the publication of *Soft Power* in 2004, Nye documented an alternative vision of how nation states traditionally exercise power.[9] Peacetime politics utilise soft power by drawing on the cultural and diplomatic strengths of nations to influence others, but should that fail they could call on the more traditional tried and tested means of using military might and economic pressures to alter behaviours. However, international politics in the 21st century is more complex than during the Cold War in which adversaries were regarded as being either in a state of peace or war and a spectrum exists within these the two extremes in which tension and limited conflict may occur. This is now being recognised by nations that are seeking to achieve more than can be gained from soft power alone but without crossing the threshold of what may be regarded as the warlike behaviour of hard power projection. These tactics themselves are nothing new, but what is novel is that there now appears to be a formal appreciation of how nations can use a range of methods to achieve their strategic aims without being accused of overtly aggressive behaviour.[10] This leads to a confused situation in which countries are not in a state of outright war, but are manoeuvring to gain strategic advantage using a wide range of approaches optimised for an individual region or adversary and for which there is no single means to counter them. States employing these tactics typically may have expansionist policies or traditionally regard themselves as world powers and wish to maintain global influence. As these acts are conducted within an interconnected global economy where the uncertainty and instability caused by overt conflict will have significant consequences for the aggressor as well as their opponent, there is also a natural reluctance to escalate retaliatory actions by resorting to hard power measures. Furthermore, this approach of combining the strengths of a range of political strategies has the advantage that by

understanding the detail of United Nations resolutions and international law, actions may be taken that fall within a grey area of legal precedence and by exploiting doubts as to whether they are overtly hostile international censure can be avoided.

Hybrid Warfare

This strategy of indirect hostility that deliberately combines a range of hard and soft methods deployed in novel ways to achieve a desired end state has been termed *hybrid warfare* and is becoming regarded as the way nations conduct themselves in the 21st century.[11] These activities take place in what has been termed a *grey zone* or *ambiguous war* and sits between the traditional conceptions of war and peace, which is becoming increasingly contested with different countries vying for control in contested areas. It is also an area of interest to scholars of international relations as they do not fit into the classic interpretations of what constitutes the routine peacetime interactions of nation states or how conflict is conducted between them when diplomacy fails.[12]

Although presented by some commentators as a new concept, hybrid warfare combines the traditional methods of conventional warfare employed by a nation's armed forces with irregular warfare using guerrilla or unorthodox tactics against military and civilian targets, in what has also been termed *compound warfare*.[13] According to Frank Hoffman, one of the primary advocates of the concept, hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including discriminate violence and coercion, and criminal disorder. Hybrid wars, he believes, can be conducted by both state and non-state actors, with or without state sponsorship. These multi-modal activities can be conducted either by separate organisations or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict.[14] For groups that do not have the resources or capability to engage in conventional warfare and would be militarily inferior in conflict,

hybrid warfare thus presents an opportunity to combine unconventional tactics with agility to gain a political advantage over an otherwise superior adversary.

Highlighting its use by irregular forces that are equipped and sponsored by nation states, the UK MoD noted in a 2007 publication that *hybrid warfare is conducted by irregular forces that have access to the more sophisticated weapons and systems normally fielded by regular forces*.[15] The UK Government's 2015 Defence Review recognised the threat of hybrid warfare with the promise of an extra £12 billion to strengthen Britain's defences. Accepting that whereas in the previous review in 2010 it was believed that the UK faced no existential threats, it acknowledged that the global situation had since changed.[16] Russia and China have been identified as strong proponents of hybrid warfare and have seen some startling success in achieving their foreign policy objectives through their use. Although not recognised as a nation state, *Daesh* has also been acknowledged as widely employing a range of soft and hard power methods that are designed to both intimidate its opponents and attract supporters across the world. Between them they use a mixture of deception, coercion, corruption, subversion, ideology, and third-party provocation to weaken the resolve of their adversaries.[17]

Russian strategists have written extensively on the subject of hybrid warfare, often termed the *Gerasimov doctrine* after the Russian General who advanced the concept, with a practical application demonstrated in the use of the so called *Little Green Men* who made an appearance in the Russian annexation of Crimea.[18] Preceded by a cyber-attack that blocked websites and telecommunication systems, personnel with military appearance appeared on the streets.[19] Wearing Russian style uniforms without any distinguishing insignia, armed with Russian weapons, speaking Russian, and using vehicles with Russian number plates, they were, according to Russian President Vladimir Putin, in fact, local 'self-defence groups who had bought their equipment at local shops'.[20] At the same time as they appeared local Russian based media projected the image of 'polite men' who were there to ensure stability.[21] Although their presence fooled few, their image and lack of formal

identification as Russian troops presented the NATO and Western nations with a challenging task to develop a response.

As if encouraged by the success of their hybrid strategy in Crimea in March 2014, Russia continued its incursions in Ukraine in June of the same year using similar tactics. However, whereas their activity in the predominantly ethnic Russian Crimea was relatively peaceful, their involvement in east Ukraine was less benign and employed the full spectrum of hybrid operations including subversion, cyber-attacks, proxies, military operations disguised as 'exercises' and conventional military interventions to deter and subdue the population.[22] This operation demonstrated Russia's mastery of being able to coordinate all levers of hybrid warfare by commencing with a soft power strategy and then transitioning to its harder form when it was no longer seen to be effective and continuing these activities until all its military and political objectives were achieved. This highlighted that the key aspect of successfully employing hybrid warfare is the ability to appreciate when soft power is no longer achieving an effect and then being able to migrate seamlessly into a new phase of the campaign utilising conventional forces to maintain operational tempo and pressure on the target.

However, despite the success of Russia's campaign, Samuel Charap, writing for the International Institute for Strategic Studies, proposes that NATO and the West have overstated the prominence of hybrid warfare in Russia's military thinking.[23] Whilst admitting that military strategists in Moscow have written extensively on the subject, he argues that should non-conventional tactics not achieve their aim, hybrid warfare has failed. However, this does not consider that a campaign involving hybrid warfare includes from the start an assessment of all elements of power projection and how they may be employed to best effect and in what order. Thus, a campaign that begins using soft measures and only turns conventional later might still have had some success in its early phases by reducing the morale and motivation of the enemy forces, resulting in the final military phase being less destructive and shorter than if it had not been utilised at all.[24]

Interestingly, although western commentators have regarded Russian hybrid tactics with mistrust, similar policies employed by the US have unsurprisingly been regarded with suspicion by the Russians. Moscow views America's use of hybrid war as the employment of both non-kinetic and kinetic means to replace unfriendly regimes with ones that are more amenable to the western model of government and believes that Russia itself may already be targeted in this way.[25] However, whereas Russia's use of hybrid war may be regarded in the west as being slightly sinister, with its aim being to destabilise nations, NATO's term of a *comprehensive approach* is promoted as using the same methods to stabilise them; as reinforced in a speech made in 2015 by the NATO Secretary-General Jens Stoltenberg in which he said:

> Hybrid is a dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use them to destabilize them… So NATO must be ready to deal with this new reality from wherever it comes. And that means we must look closely at how we prepare for; deter; and if necessary defend against hybrid warfare.[26]

From the Chinese perspective, Michael Raska argues that information operations have been at the heart of Chinese statecraft and military power and that they have been used to direct influence in areas of strategic competition.[27] Noting that China's foreign policy has previously relied on soft power to achieve power projection, their hybrid warfare strategy now incorporates three mutually reinforcing strands of strategic psychological operations, overt and covert media operations and what is termed *legal warfare* or *lawfare*, which is intended to exploit international agreements to alter the policies and perceptions of target audiences abroad. An example of this final tactic is China's policy in the disputed waters of the South China Sea in pursuance of its territorial claims. Whereas Russia used *Little Green Men* in the takeover of Crimea, China has employed what have been termed *Little Blue Men* in the form of irregular maritime forces. These are suspected government forces posing as fishermen

that operate within contested areas and harass other nations' seafarers in the same region. Whereas a similar action conducted by identifiable military forces would be regarded as hostile and escalatory in an area that is already tense, these 'fishermen' can operate with impunity and at times contravene international law. It has been reported that whereas the 'official' Chinese Navy behave professionally in the presence of foreign, and especially foreign military, shipping, other vessels suspected of being manned by a maritime militia posing as civilians are more aggressive.[28] This confuses the Rules of Engagement processes that are usually written to counter what are clearly military units operating under the international law of armed conflict. The presence of a confusing mixture of shipping operating under the Chinese flag in disputed waters complicates the activities of other nations and gives the initiative to the Chinese.

Smart Power

The use of hybrid warfare has been seen to coordinate a range of differing tactics and techniques to achieve a desired end state. At either end of the spectrum these may be analogous to soft and hard power, with the former being associated with the behavioural analysis of an opponent leading to a tailored information campaign and media operations policy and the latter based on conventional destructive warfare. However, altering the behaviour of an adversary is more complex than purely being attractive or threatening; an issue recognised by hybrid warfare doctrine and by Nye in his proposal of the concept of smart power. This third form of power combines hard power coercion and economic sanctions with the soft power attributes of persuasion and attraction into a single coordinated strategy.[29]

Ernest Wilson looked beyond the original definitions of hard and soft power to the concept of smart power, which he defines as the combination of both elements such that they are mutually reinforcing.[30] He views the imperative for smart power as being the move of the G8 nations to post-industrial economies with power resting on a nation's ability to create and manipulate knowledge and

information. This, he believes, can be more powerful than pure military capability, but can be enhanced by high technology, and especially digital networked and flexible assets, when combined with other non-military capabilities such as the communications infrastructure. The need to consider smart power strategies is also enhanced by their target populations becoming better informed with an increased access to higher education and a range of media outlets. In reviewing the different types of power, Gregory Treverton and Seth Jones also concluded that the distinction between the criteria may become blurred as some soft power techniques may be perceived as hard under some circumstances.[31] Thus, careful use of a combination of techniques within a smart power campaign is attractive and as Wilson highlighted, there is a growing interest in its utilisation, with a contributory factor being the perceived failure of recent US foreign policy, which have previously concentrated on the deployment of hard power tactics and disregarded the importance of an effective soft power campaign.[32] He further argues that the effective deployment of smart power is underpinned by a thorough understanding of the strengths and limitations of each instrument and the recognition of which combinations to deploy in each circumstance, which is ultimately dependent upon the political will of the countries involved.

In deploying power, Nye cautions that in its purest form it is neither good nor bad and that too much can be as damaging as too little and that what is significant is finding ways to combine resources into successful strategies to obtain preferred outcomes.[33] As a strategy relates means to ends, it is important to have clarity about what is hoped to be achieved with the assets that are available, which includes the time allocated for the operation. To achieve this Nye proposes five questions that will be answered by a smart power strategy:[34]

- Identify what are the preferred goals or outcomes, which will involve prioritising and seeking trade-offs to optimise the use of limited resources.

- Knowing what resources are available and under which circumstances they can be used as not all assets may be available at all time.

- Consider the positions and preferences of the targets of influence, which will involve an appreciation of their capability, intents, and strategies, with an assessment of how likely they are to change their course of action after the start of a campaign against them.

- Identify which forms of power are most likely to succeed against a target as there is little point investing in a predominantly soft power campaign, if the target is only likely to be influenced by coercive force.

- Be realistic at estimating the probability of success as there is little benefit in investing time and resources in a campaign that will probably fail.

Commenting on the imbalance favouring hard as opposed to soft power application in countries such as the US, Nye also acknowledges the advantages of smart power and the tempering of hard weaponry with the power of persuasion and cultural attraction using the quote of *leading through the power of example instead of the example of power*.[35]

Nye's consideration of the three types of power and in particular of soft power and the softer elements of smart power, which utilise non-violent methods, is particularly significant for the information based cyber environment that can simultaneously target large numbers of an Internet or mobile telephone connected population. This can be seen in how some smaller, less powerful countries have leveraged smart power to exert influence among their neighbours. This is highlighted by Alan Chong who provides as examples Singapore, which combines relatively high levels of defence spending with diplomatic leadership, Switzerland, which has both compulsory military service and an advantageous banking regime, Qatar, which hosts both US forces and Al Jazeera – a media channel critical of US military activity and finally Norway,

which is a prominent member of NATO and also a leading proponent of promoting overseas development.[36]

In today's interconnected society, many nations that seek to exert power over others are also more dependent upon a stable world order as disruption of any sort that impact financial markets could have a greater economic and political impact on the perpetrator than the target. For this reason, hybrid warfare and smart power present a philosophy in which nations can by default seek to achieve their aims through a broad spectrum of effects. For states that understand the potential benefits of utilising cyberspace, it can be an ideal medium for power projection and for targeting key influencers. However, the territory in which the target resides must clearly have a suitable infrastructure to exploit and this can be a double-edged sword as it can also be used as a means for their adversaries to retaliate with their own information campaign. Therefore, to fully appreciate the potential benefits and threats of cyberspace it is important to understand the medium, its strengths and weaknesses.

Although much of the historical discussion on the concept of power has concentrated on the role of the state, increasingly the influence of non-state actors has become a recurrent theme. In any analysis of global power there can be competition between governments and independent groups both within and outside their borders in the level of impact that each can wield on their populations and beyond. Nye notes that assisted by the spread of communication technologies, there has been a diffusion of power away from states and their institutions to smaller groups and individuals. These range from the economic power exercised by large, well established legitimate corporations with a global presence such as the technology companies Microsoft, Apple and Samsung and the Russian energy provider Gazprom to the cultural influence of non-governmental bodies such as the BBC or film industries. In addition, international terrorist organisations such as *Daesh*, criminal gangs and loose collectives such as the hacking group *Anonymous* have also gained influence.[37] Furthermore as the Eric Schmidt, the Executive Chairman of Google's parent company Alphabet notes, modern

communications methods enable the duplication, storage, and distribution of information to be achieved at low cost and potentially are able to reach large audiences using the plethora of readily available tools and technologies. Governments have thus lost control of the type and quantity of information within their jurisdictions enabling non-state actors to become a significant factor in any assessment of power. Their impact in some areas has risen to such a degree that the methods by which they exert influence have become a framework within which states must also seek to exercise power to mitigate their threat or to counter their activities.[38]

Defining Cyberspace

As with understanding the concept of power, achieving consensus on a definitive description of what constitutes cyberspace is a notoriously difficult task with Franklin D Kramer identifying 28 different definitions of the term as far back as 2009.[39] The provenance of the word is not helpful either in that it was first used to describe a *consensual hallucination* in William Gibson's 1994 science fiction novel *Neuromancer*.[40] This lack of a formal accepted definition does, however provide the flexibility for it to be described in terms to suit a user's particular purpose and to evolve as technology and requirements develop.

Daniel Kuehl, also writing in 2009, initially discusses cyberspace within the context of the previously understood environments of the land, sea and air noting that although the land environment is fully accessible without the need for additional assistance, to fully exploit access to the sea and air requires man-made technology.[41] David Betz and Tim Stevens later highlighted the debate surrounding the classification of cyberspace and that many countries have developed a bespoke definition of the term to suit their own purpose with little consensus between them.[42] However, some common themes have occurred such as those highlighted by John Sheldon that cyberspace is inherently artificial and for it to exist relies on both the electromagnetic spectrum and manufactured objects. Another key attribute that makes it unique is that it can

be constantly replicated and exist in many forms.[43] Variations on what elements are included or excluded in the definition can also have significant implications in the projection of power through the medium and the effects that are hoped to be achieved. This is particularly so when the remit of what constitutes cyberspace moves beyond just the network to include the data being stored, processed, and transported across it. More recently, the addition of peripheral devices that monitor and automate industrial control systems and domestic devices have continued to expand what might be regarded as elements of cyberspace.[44]

In examining the evolution of the definition for cyberspace, particularly when considered from a military perspective, Kuehl noted that some descriptions include the phrase *until further notice* acknowledging that its meaning evolves with technology and the development of methods to exploit it. Referring to it as a domain – contrary to current UK and US doctrine, which uses the term *environment* - he offers his own definition, which both builds on previous versions and includes his own elements such as incorporating global connectivity, informational content, and human cognition. His all-encompassing definition describes cyberspace as:

> ...an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information communication technology based systems and their associated infrastructures.[45]

The unique attribute of the medium as being man-made is regularly commented on with reference made to its malleability and the ease by which non-state actors and small states can play a significant role, due to the low cost and ease of entry. Gregory Rattray refers to the artificial nature of the environment and that hardware and software govern its interactions. This means that what he refers to as the geography of cyberspace is much more mutable than other environments. He provides as an example that whereas mountains and oceans

are permanent features, elements of cyberspace can be turned on or off, created or moved. However, he does caution that cyberspace is not infinitely adaptable and is limited in what can be achieved by the laws of physics, logical properties of code and the capacities of organisations and people.[46]

At this point, it should also be highlighted that although cyberspace is variously referred to as both a domain and as an environment with the two terms seemingly used as synonyms, differences in meaning do however exist between countries. These are generally based on variations in definitions used by their military forces that have sought to incorporate cyberspace into existing doctrinal policy. The US for example has four domains; air, land, maritime and space within which there are three operational environments; physical, cognitive, and informational within which cyberspace resides.[47] NATO, which does not engage in activities in space, has four operational domains; land, sea, air, and cyberspace.[48] The UK however, has five operational environments of air, land, maritime, space and cyberspace with three domains; cognitive, virtual, and physical. In this respect, cognitive refers to information that connects people to cyberspace, the virtual domain as the software and applications that connect the network nodes and the physical being the network components and associated geography. Hence, both describe cyberspace as an environment, but within different contexts.[49] Many other nations also use their own definitions with Finland, which is also a member of NATO; an organisation that is becoming increasingly aware of the importance of the military use of cyberspace, regarding it as a domain, as does Saudi Arabia.[50] In order to present cyberspace as being an equal to the other physical areas of operations, the UK classification of cyberspace as an environment will be used with the domains redefined and expanded in chapter 4 in terms of layers.

Within the UK Defence context, its Development, Concepts, and Doctrine Centre (DCDC), in acknowledging the lack of a formal definitive definition, draws on the Concise Oxford English Dictionary's definition of cyberspace as relating to *Information Technology, the Internet and virtual reality*. Their *Joint Doctrine Note 3/13* provides a formal description of cyberspace in Defence as:

> ... the interdependent network of information technology infrastructures, (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein within the information environment.[51]

In trying to describe cyberspace, it has also been referred as a global fluid implying that it is in a state of constant flux that cannot simply be dismantled and that the relationship between the multitude of actors that contribute to it means that it will never be stabilised.[52] The ubiquitous nature of the cyber environment in being able to affect all the other environments of sea, land, air and space simultaneously makes it unique when considered in terms of power projection.[53] Part of its distinctiveness is that as well as nation states, it has a wide range of stakeholders each with varying degrees of potential impact including individual users, commercial enterprises, Intelligence agencies, criminals with a range of motivations, the media and multinational corporations. Each of these entities can exercise power in one form or another and the speed of electronic communication gives them worldwide influence, even if transient. However, the range and number of these actors and the dynamic nature of the medium makes the precise effects of power in cyberspace difficult to predict and may result in unexpected and unintended consequences that may have an effect in the physical world.[54]

Characterising Cyberpower

Although technology has been largely understood to be a constitutive and material element of state power, the concept of cyberpower was initially met with suspicion.[55] Professor Colin Gray, an advisor on policy and maritime strategy to the US and British Governments, noted its novelty and increasing profile, but also expressed doubts as to its utility and effectiveness.[56] Google's Eric Schmidt and Jared Cohen, who was previously a member of the US State Department's Policy Planning Staff, also expressed reservations when they described the Internet as one of the few things that humans have built that they

do not truly understand and as the world's largest ungoverned space.[57] Their view of cyberspace was as the realisation of an environment in which there is no universally accepted leader or single superior coercive power in control of its development, use or in a position to resolve disputes in what could be regarded as an anarchic, chaotic system.[58] This compares to the other four physical environments in which there are United Nations Charters, Conventions or Agreements regulating their use with agreed procedures to resolve issues where disagreements arise.

Since Gray's comments in 1995 that cyberpower had not attracted serious thought and that technology was in advance of a policy and strategy there has been considerable academic effort in defining and refining the concept.[59] In translating the nature of national power into cyberspace, four forms of cyberpower were identified by David Betz and Tim Stephens.[60] The first echoes Robert Dahl's definition in its use of direct coercion by one actor to modify the behaviour and the conditions of existence of another with the second being from the neoliberal institutionalist perspective of an indirect control of one actor by another through the mediation of formal and informal institutions. Structural cyberpower is regarded as Betz and Stephen's third form, which aligns to hegemonic power by seeking to either maintain or disrupt the status quo by dominating or influencing the environment in which the actors operate. This can involve facilitating or constraining the connectivity of networks that determines how cyberspace can be influenced and is coherent with the view of the environment as being the linking of inter-connected information communication technology based systems. Productive cyberpower is suggested as representing the final example and as with soft power relates to how attitudes and opinions can be formed and shaped by reinforcing established beliefs or creating new ones.[61]

In attempting to define the strategic purpose of cyberpower John Sheldon described it as:

> …the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment.[62]

In this respect, he approaches cyberpower as a means to contribute to the policy objectives of a nation and defines it as the sum of strategic effects generated by cyber operations. Although regarding it as distinct from other instruments of (primarily military) power he identifies it as still requiring a strategy and that it is not a means to an end, but seeks to serve the purpose of a wider policy. It is an important point that cyberpower does not exist in isolation but is intimately connected to the physical world. For nation states, this represents a link with that of national power however it is defined and signifies it as an extension of the aims of national policy, but in cyberspace.[63]

With smart power increasing in prominence as potentially the most effective means to achieve a desired end state and cyberspace becoming a potent means to reach an audience, the opportunities to combine the two in a coordinated strategy are now a prime area for future research. The challenge though is that cyberspace is an information based medium better suited to the cultural and persuasive aspects of power than as a means of executing the harder elements of the smart power spectrum. The ability for a wide range of users including government, multinational industries, non-state actors, and individuals to be able to employ cyberspace as a medium for the delivery of the softer aspects of full spectrum power projection operations is important as accessibility is one of the environment's key attributes.

Nye refers to this dissipation of power from governments as *power diffusion* and emphasises its significance as it has the potential to mark the decline of the dominance of the sovereign state as being central to people's lives.[64] This he deduces has been possible because the information revolution has resulted in technology becoming both more advanced and cheaper with the ability to store, process and transmit large amounts of data no longer being prohibitively expensive or requiring specialist facilities. This has enabled information to be

decentralised and no longer in control of governments. Individuals and organisations, including terrorist groups, can create, control, and disseminate their own message online through a range of media such as e-mail, websites, social media, web logs (blogs) or wikis, which are web based resources developed collaboratively by a community of users. Combined, these can reach and potentially influence a wide audience through a range of technologies such as personal computers, laptops, tablets, mobile phones, and more recently wearable devices. Once the initial investment is made in the computing and networking components required to enter the cyber environment, the key that determines power is the quality, credibility, and impact of the information, which unlike physical media, can be produced once and consumed many times. Nye also notes that the ability for smaller states and organisations to contribute without the inertia and bureaucracy associated with larger countries can result in more agile and flexible ways of working. Developed countries with large, fixed networks can also be more vulnerable and attractive targets for attack than smaller groups with a more widely distributed, smaller physical infrastructure.[65]

In reviewing the use of information resources as the basis of power, Nye notes that although it is not a new concept, cyberspace has the advantage of being developed as an environment created with the sole purpose of exploiting information. He defines cyberpower in terms of *resources that relate to the creation, control, and communication of electronic and computer-based information - infrastructure, networks, software [and] human skills*, emphasising that this includes not just the Internet, but internal intranets, mobile telephony, and space based communications.

Looking further at how it can be described behaviourally, Nye described cyberpower as *the ability to obtain preferred outcomes through the use of the electromagnetically information resources of the cyber domain.* Importantly, in defining cyberpower Nye notes that it can be used both to produce desired outcomes within cyberspace or can be used as an instrument to produce preferred outcomes in other environments outside cyberspace.[66] To explain this Nye distinguishes *intra cyberspace power* and *extra cyberspace power*, in

which the effects are felt either within or outside the cyber environment, a key element of which is the inclusion of the infrastructure in any definition as its role is fundamental to everything that occurs beyond the user interface.[67] The intra cyberspace model also considers the technology involved including the physical networks, software and protocols. As a man-made environment, entry requires the use of electronic technologies to harness and exploit the energies and properties of the naturally occurring features of the electromagnetic spectrum.[68] This is analogous to the use of ships using the attributes of steel and fuel to exploit the naturally occurring oceans. It is also widely commented on that the cost of entry into cyberspace is cheap and the barriers so low that generating a strategic effect does not require a budget of billions with many cyber weapons now commoditised.[69]

Table 1 replicates Nye's demonstration of intra and extra cyberspace and how they can be used to target cyberpower. He further defines *Information instruments*, which relate to the network characteristics and the physical components that are defined by economic and political realities. In his examples, Nye is clear that cyberpower can be used to generate both hard and soft effects, with the former illustrating the coercive effects that were experienced by the Denial of Service (DoS) attacks experienced by Estonia in 2007 and the 2010 STUXNET attack on the Supervisory Control and Data Acquisition (SCADA) systems in the Iranian Nuclear enrichment facilities at Nantanz. Soft power is illustrated in terms of its focus on the psychological and behavioural nature of the target and using cyber information to create power by attracting citizens in another country.[70]

Targets of cyberpower		
	Intra-cyberspace	Extra-cyberspace
Information Instrument	Hard: Denial of Service attack Soft: Setting of norms and standards	Hard: Attack on SCADA systems Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: Government control of companies Soft: Software to help human rights activists	Hard: Bomb routers or cutting of cables Soft: Protests to name and shame cyber providers

Table 1: Physical and Virtual Dimensions of Cyberpower

Nye also relates his *three faces of relational power* to cyberspace where he provides evidence of hard and soft power as shown in table 2 below, demonstrating again that it can be argued that there are both hard and soft techniques for each aspect of power projection. His comprehensive assessment of the different types of power and how they can be utilised to different effect provide evidence that there is not a 'one size fits all' approach to achieving the desired behavioural change on a target. By detailing how soft and hard power are positioned at each end of the spectrum, the essential role of utilising smart power to draw on whatever component is assessed to be best to influence the target can be seen. As yet, a process to examine how smart power can be fully optimised for cyberspace has still to be developed, with the literature tending to regard them as unrelated components. However, should such a methodology be developed to formalise the link between cyberpower and smart power and the techniques that could be most effectively used in any particular scenario, a key element would be the requirement for a comprehensive understanding of the target. This would demonstrate the intimate dependency between power projection and intelligence collection or as it is known in its covert form, espionage. This has become a prominent feature particularly in offensive cyber operations with numerous examples of how it has been employed by nation states as part of a wider strategic campaign. This is examined in the next section that explores the military use of cyberspace and the debate that surrounds it.

Aspect of Power	Hard Power	Soft Power
A inducing B to do what B would not initially otherwise do	Denial of Service attack Inserting of malware SCADA disruption Arrest of bloggers	Information campaign targeting hackers to change their behaviours Campaign to counter recruitment of terrorists
A precluding B's choice by excluding B's strategies	Firewalls and filters Pressure on companies to exclude material	Encourage self-monitoring of ISPs Rules on permitted domain names Promoting software standards
A shaping B's preferences so that some strategies are never considered	Threats to punish bloggers who publish censored material	Information to create preferences such as encouraging 'patriotic hackers' Development of norms of revulsion online

Table 2: Nye's three faces of power in the cyber domain

In response to the use of cyberspace to project power, the role of cyber security can be seen to be a counter power strategy with former US President Barak Obama describing cyber security as *one of the most serious economic and national security challenges we face*.[71] This can be seen in Lene Hanson's application of securitization theory in which she defines security as *the ability of a society to persist in its essential character under changing conditions and possible or actual threats.*[72] Within the context of cyberpower, this involves the use of methods to prevent access by others to their networks with the aim of influencing people either by communicating with them directly or indirectly by affecting the systems that they use. The role of cyber security at a national level can range from censoring and filtering information from both domestic and external, that is foreign, sources that are regarded as objectionable as well as preventing systems being accessed for the purposes of sabotage or extracting information.[73]

The subject of Internet censorship restricting this flow of information was researched from 2004-2014 by the *OpenNet Initiative* (ONI), a collaborative partnership of three US and Canadian Institutions.[74] Their aim was to investigate, expose and analyse what they believed to be the increasing

amount of filtering and censorship of Internet content in a credible and non-partisan fashion. The ONI concluded that over three dozen states, clustered mainly in East Asia, the Middle East, North Africa, and central Asia were actively filtering Internet traffic, with China having the most extensive filtering regime in the world. It was noted though that content was also blocked within the US and Europe with restricted subjects including material related to extreme pornography or imagery related to Nazism or holocaust denial. The ONI claimed that control of the Internet was becoming increasingly important to countries seeking to curb dissent and that the main topics filtered were in relation to political, social and security issues. Interestingly, they also identified a fourth theme, that of the use of Internet tools, which included networking applications designed to allow the sharing of information, translation of websites, anonymisers, blogging or Voice over Internet Protocol (VoIP) services.[75] Social media, which is one of the key methods of spreading a soft power message at a peer to peer level was recognised by the ONI as a particularly popular subject for censorship with varying methods of Internet control employed to limit or deny its use.

The information environment and cyberpower

In assessing what he refers to as the *information revolution*, Nye discusses cyberpower in terms of the *third industrial revolution* after the first, which was the mechanisation of previously hand-crafted goods and the second of the introduction of mass production. He asserts that as knowledge is the main lever of power in cyberspace, as for other technologies, its proliferation is beyond the control of nation states.[76] This he suggests is due to the significant reduction in the cost of exchanging information to almost an almost negligible figure, whilst also increasing the speed at which it can be transmitted. This has led to speculation that the role of the state itself will diminish as cross border networked communities, multinational institutions and non-profit making organisations play a larger role in people's lives. Although this is perhaps an extreme view, he notes that states will be less able to control the flow of information and therefore influence within their boundaries.

The P/DIME (Political/Diplomatic, Informational, Military, Economic) model is one of several approaches to describing the elements of national power and British Defence Doctrine states that Information underpins the other three instruments of power. [77] However, although it states that information is not doctrinally regarded as a discrete instrument of power, it is considered as a critical resource and as such can be expected to be contested in time of conflict. [78] This means that the preservation of information flows should be carefully maintained as it facilitates understanding and decision-making within the wider battlespace and the advantage that can be achieved by managing, in relative terms, the information flow better than your opponent is known as *Information Superiority*. Despite the use of the phrase and its acknowledged importance there was prior to 2013 no consensus across UK defence as to what Information superiority was or how it could be formally described. However, when published in 2013 the UK Ministry of Defence Joint Doctrine Note 3/13 on the subject proposed the following definition:

> *The competitive advantage gained through continuous, directed and adaptive employment of relevant information principles, capabilities, and behaviours.* [79]

Within a NATO environment, the UK alternatively describes information superiority as *possessing a greater degree of information about the battlespace and being able to exploit that information more rapidly than an adversary in order to prevent them from obtaining or exploiting information which would give combat advantage*.[80] This ability to collect, exploit and act on information faster than an opponent is critical in the information environment and requires a combination of people, processes, equipment and infrastructure, both internal and external. As suggested in the UK Ministry of Defence's Development, Concepts, and Doctrine Centre (DCDC) in their Future Character of Conflict paper, it can be expected that adversaries will attack physical and electronic lines of communication that there will also be a battle for information superiority, which necessitates the requirement for sophisticated and resilient

communications.[81] The availability and affordability of modern communication technology will also enable a range of non-state actors to deploy their own information campaign targeting the same groups as state organisations further emphasising the importance of the battle for information superiority. The vulnerability of cyberspace to attack is however highlighted emphasising that a successful compromise could result in a slowing of the command process leading to incorrect decisions being made.[82]

Nye regards cyberpower as the ability to use cyberspace to create advantages and influence events in all operational environments and across the instruments of power. This acknowledges that although it compares capability between powers, it should be regarded in context of the other attributes of national power and how they relate to many different actors. Fundamental to this is the role of the technology required to be able to enter cyberspace and that it is constantly evolving. The adoption of new technologies may give one actor an advantage over another, which requires an organisational effort to introduce, emphasising the impact of the human perspective and attitude in their wishing to engage fully with the domain. [83]

Kuehl also highlights how the increasing ability to generate, disseminate and possibly control information emphasises its importance as the Informational instrument of power. Noting that cyberspace and cyberpower are now clearly dimensions of the Informational instrument of power he also describes it as playing an increasingly vital role in contributing to the economic strength of a nation and therefore an important component to be considered in developing national policy. This means that it now affects how governments connect with their citizens in all levels of society and links people and organisations in new ways and across national borders. Whereas in the past governments spoke to governments, they can now communicate at all levels from national to regional and even to individuals and that it is transforming how we create data itself, which can be described as the raw material that fuels modern society. This has resulted in a nation's cyberpower being defined as having three dimensions; coordination of operational and policy aspects across government, coherency

of policy through international alliances and legal frameworks and achieving the cooperation of non-state actors. This further emphasises the importance of assimilating the non-state sector as a significant factor in the development of an integrated national cyber capability.[84]

The military use of cyberspace

Much has been written regarding the military use of cyberspace to project power and the tactics and techniques that may be employed in any future conflict, but all in anticipation of how they may be used in the future. Opinion is divided as to whether a full cyberwar has yet to occur or indeed may not happen at all, particularly as noted by Madeline Carr that under international law what constitutes a use of force or an armed attack in cyberspace remains unclear.[85]

This uncertainty as to the legality of the military use of cyberspace and indeed cyberwar in general has been the subject of some academic legal debate, but has been hindered by the clandestine nature of cyber operations and the limited number of incidents that have been made public. This lack of interest in regulating cyberwarfare may be due to the proponents of the activity being reluctant to agree to the regulation of their activities and so lose any strategic military advantage. There has however been some work in this area and although not legally binding, the United Nations Mandated Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has been credited with introducing the principle that international law applies to the digital space.[86]

NATO has also been active in attempting to interpret existing international law within the context of cyber operations with the publication of two volumes of the *Tallinn Manual*.[87] Initially the product of a three-year project, the first volume, which was published in 2013 identified ninety-five specific rules that could be applied to a cyber conflict and considered issues such as sovereignty, State responsibility, the concept of just war, humanitarian law, and the law of

neutrality. A significant conclusion of the authors of the manual included the statement in Rule 66 that cyber espionage or other forms of information gathering during an armed conflict do not violate the law of armed conflict. This aligns with the grey area of state sponsored espionage in peacetime, which is governed by each nation's own domestic law and not international law. Cyber-attacks are covered in Rule 30 and defined as operations that can reasonably be expected to cause injury or death to persons or damage or destruction to objects. Although subversion is not specifically mentioned, psychological operations are covered in Rule 61, which permits cyber operations that qualify as ruses of war. Following the publication of the first volume of the Manual, in 2017 NATO published a second volume, which extended the range of legal scenarios addressed to include cyber operations in the maritime environment in Rules 45-54, peacetime cyber espionage in Rule 32 and the actions of non-state actors that are not regulated by international law in Rule 33.[88]

In considering the use of offensive action in cyberspace, John Sheldon concluded that due to the open nature of protocols, the number of ways in which attacks can be deployed, the worldwide reach of assailants, and the difficulties of attribution that it is offensive actions rather than defensive that will always have the advantage and will be the dominant factor in any cyber conflict. This is because defensive measures will always be reactive in having to mitigate for new forms of attack as they are encountered and can only be developed after they have taken place.[89] He also suggests that in any future conflict cyberpower will not be used as an independent coercive instrument, but will be a complementary capability to other activities in the physical world. Thus, it will be regarded as a resource that will be used in support of other operations and that its role will be to complicate an adversary's decision-making process by disrupting, degrading, or denying their communication channels. This could also be supplemented by subverting, exfiltrating or destroying information or infrastructure as part of a wider intelligence led politico-military strategy.[90]

The concept of cyberwar first came to prominence in a 1993 paper by John Arquilla and David Ronfeldt dramatically entitled *Cyberwar is coming!* [91] In

acknowledging the information revolution and its ability to disrupt established hierarchies, the authors anticipated a transformation in the nature of warfare such that it was the combatant with the best method of being able to turn information into actionable knowledge that had the advantage. This is because data on its own has very limited value – it is the interpretation of information such that it becomes usable intelligence that is valuable. They predicted that the battlefield of the future would be shaped by a decentralised, less hierarchical command structure, and that there would be a reassessment of how conflict and strategic interaction occurs based on innovation and technological advances. These wars will centre on knowledge and be fought at two levels: a societal conflict waged through communications media spanning political, economic, and social issues and a cyberwar at the military level targeting an enemy's command and control infrastructure. Highlighting the inherently non-violent nature of code based conflict, reference was made to parallels with other conventional military techniques utilising the electromagnetic spectrum such as jamming, disrupting, and overloading information channels to achieve the desired effect.

This view was further expanded on by James Adams in 2001 who predicted that that *the information age is revolutionizing warfare for the twenty-first [century]*.[92] In providing examples of website defacement and information theft, he was also one of the first to suggest the asymmetrical nature of conflict in cyberspace which favours non-state actors and smaller states. Although inferior in terms of conventional military forces to the major world powers, they do not have the same reliance on technology and are thus less vulnerable to network based attacks that target private as well as government systems. This is one of the themes explored by Madeline Carr in 2016, when in quoting Barak Obama she referred to *the great irony of the information age* that *those states which have most successfully adopted and exploited the opportunities afforded by the Internet are also the most vulnerable*.[93] Noting that no previous technology has been regarded concurrently as a source of power and vulnerability in quite the way that the Internet is she highlights that the proliferation of non-state actors have impacted on state power by eroding the institution of sovereignty.

Although not referring specifically to the wider concept of cyberpower, she asserts that the Internet can both enhance and undermine state power, not least in part because of decisions by politicians.[94]

Writing in 2005, Colin Gray also predicted the militarisation of cyberspace, but less as a technological based exercise and more a personal one as each belligerent's cyber champions engage in a geographically dislocated gladiatorial combat. He makes the important point that cyberwar will not be fought in isolation or change the nature of war, but will be integrated with the other environments of land, sea, air, and space.[95] He also predicted that although it had an important role as a force enabler, it will not replace the nature of warfare or by itself deliver defeat or victory. Subsequent commentators however have differed in their examination of the military use of cyberspace. Two significant publications are Richard Clarke & Robert Knake's 2010 book *Cyberwar* and Rid's 2012 publication *Cyberwar will not take place* that drew on similar information but came to very different conclusions with the former presenting a considerably more alarmist and pessimistic view of conflict in cyberspace than the latter.[96] [97] Clarke & Knake proposed a scenario in which the western nations' networked society is extremely vulnerable to attack and that software may already have been inserted into a nation's critical national infrastructure by hostile intelligence services. This would remain dormant until a time of conflict or tension when it would be activated to disable a networked infrastructure and delete data, resulting in explosions at oil refineries, the release of gases from chemical plants, interference with air traffic control and the shutdown of the power grid.[98]

In support of the view that the militarisation of cyberspace has or will take place, it should be noted that several countries have already stated publicly that they are active in this area and are preparing to engage in offensive cyber operations, which may also act as a credible deterrent to future attacks. The UK's Ministry of Defence, for example stated in 2013 that it has established a specialist military cyber capability and had developed a doctrine for its use.[99] The then Defence Secretary Phillip Hammond later announced at that year's

Conservative Party Conference that the UK would develop a dedicated counter attack and strike capability in cyberspace.[100] Although this was the first formal declaration of a nation's intent to develop offensive military cyber capabilities, China has also reportedly had cyber warfare units since 2003 with the US Cyber Command achieving an initial operating capability in 2013.[101]

This view of cyberspace as being the environment for a future conflict is countered by Rid who believes that what he defines as cyber war *has never happened in the past, it does not occur in the present and it is unlikely that it will disturb our future.* The main tenet of his argument being that all offensive activities in cyberspace instead fall into one of three categories; espionage, sabotage and subversion.[102] Rid even goes as far as to believe that cyber-attacks will *help to diminish rather than accentuate political violence*.[103] This is due to his belief that *computer code can only directly affect computer-controlled machines, not humans.*[104] However this is only a valid argument if the intention is to reduce violence and not, as pointed out by Justine Chauvin, that the aim of groups such as terrorists are to cause as much damage as and when they can.[105]

The timing and content of Rid's book was opportune as it was published at a time when there was a general consensus that cyberwar was going to be an aspect of any future conflict. It was even suggested that to be a significant component it did not even require both belligerents to have comparable infrastructures as it could be argued that the greater a state is networked and reliant on cyberspace, the greater its vulnerability to a lesser foe. This was seen in the highly significant Sony network compromise in which the company suffered a serious security breach with the release of confidential e-mails and commercial data. In its subsequent investigation, the Federal Bureau of Investigation (FBI) publicly accused the government of North Korea, one of the least connected countries in the world, as being responsible.[106]

In common with other commentators on cyberwarfare in quoting the 19th century Prussian military theorist General Carl von Clausewitz, Rid bases his

argument that for offensive action to be described as an act of war it must be political in motivation, instrumental in character and lethal in potential. Agreeing with Gray, he describes war's political nature as requiring eventual attribution for one side's will to dominate over another. For an act in cyberspace to achieve this it would be a very complex evolution and in referring to several case studies referencing publicly known offensive cyber events, he argues that they do not themselves exhibit these characteristics, only the consequences.[107] In expanding his theory, Rid uses a comprehensive range of examples to argue that an act of sabotage may not in itself be an act of war but as by definition it targets infrastructure not people, it may be an ideal target for cyber weapons. Espionage is also described as not being an act of war and it may not even be regarded as a crime for a state to attempt to access and exfiltrate another's sensitive information and that this is believed to be the most widespread use of state-sponsored cyber capabilities. Finally, in defining subversion, he notes that it targets minds and not machines in seeking to erode social bonds, beliefs, and trusts to undermine the authority, integrity, and constitution of the target. In achieving its aims, subversion differs from insurgency in that it targets people in non-violent manner and this, combined with the difficulties of attribution and the range of connected media that can be targeted, also makes it an ideal cyber weapon.[108] Throughout his thesis on cyberwar, Rid also emphasises the role of the human factor and that sabotage, espionage and subversion may all be dependent upon the critical knowledge of someone 'on the inside' for it to be successful, emphasising the continuing role of traditional human intelligence.

Although acknowledging its significant contribution in countering the prevailing consensus that cyberwar is inevitable, criticism of Rid's work has centred on an academic discussion of what defines war. John Stone, a colleague of Rid at King's College, London, countered that the *efforts to determine whether cyber-attacks should be considered acts of war…..are hampered by our loose understanding of what war itself amounts to.*[109] Specifically he highlights the under explored and unspecified relationship between violence and lethality in the context of war and that this issue has been brought into sharp focus by the new and unconventional realm of cyber warfare. Although Stone has no issue

with Rid's requirement for war to be political and instrumental, he focuses on the requirement for lethality and quotes the following, which also has implications when considering the concept of power:

> 'War is an act of force to compel our enemy to do our will', wrote Carl von Clausewitz on the first page of *On War*. All war, pretty simply, is violent. If an act is not potentially violent, it is not an act of war…. A real act of war is always potentially or actually lethal, at least for some participants on at least one side.[110]

Although Rid merges force, violence and lethality, Stone argues that war demands no causal connection and regards them as three separate issues and although war requires force, it does not imply violence or lethality. Separating force from having to involve injury to human bodies, he quotes the Oxford English Dictionary to include damage to objects as well as people to the definition and that violence and lethality are not inexorably linked. This is important as modern warfare, particularly when committed by western democracies, seeks to deliberately reduce casualties to a minimum – the use of (expensive) precision smart weapons as opposed to (cheap) carpet bombing for example. Rid prefers to use the term *sabotage* when the intention is to damage a target, but Stone suggests that this does not prevent it from being warlike and to do so would require re-describing the whole liberal way of war.[111] Stone also investigates the relationship between force and violence and that violence may arise from a cyberattack, but would it be the result of an act of force? He answers his own question by concluding that technology enables a small amount of force in the form of a few key strokes that could translate into potentially a large amount of violence. He concludes that contrary to Rid's assertion, events in cyberspace *could* constitute acts of war as they may involve the application of force in order to produce violent, but not necessarily lethal, effects and that cyber-attacks represent a particularly efficient means of doing so.[112] However, these semantic definitions of what constitutes warfare are regarded as inconsequential by Gray who also quotes Clausewitz in arguing that although *war is an act of force to compel our enemy to do our will*, it can

utilise several instruments, including cyber activities, to achieve this in contributing to the coercion of an opponent. Ultimately, Gray's response to cyberwar not being itself violent is 'so what' and that it is still warfare, particularly if regarded as such by the victim.[113] There is though some common ground with Rid, particularly in that cyberwar is just the latest development in conflict and will not fundamentally change its nature or compensate for failings elsewhere.

Rid's assertion that conflict in cyberspace cannot be regarded as cyberwar *because it fails to conform to conventional definitions of conflict* is also criticised by Erik Gartzke who suggests that the argument may become a *purely academic exercise*.[114] The concept of what exactly cyberwar may comprise of is also raised by Julia Muravska, who senses confusion as to what Rid is actually attacking and that he fails to set out what such a war may look like and why the concept needs debunking. She also questions Rid's link between violence and war noting the increasing development and use of non-lethal weapons and efforts to reduce collateral damage in conflict.[115]

Valeriano and Maness offer a significant contribution to the cyberwar debate by emphasising that cyberspace and the activities that occur within it are intimately connected to wider international relationships. They argue that the consequences of an all-out cyberwar are such that there is restraint in the level of conflict that occurs in cyberspace and that interactions are mainly regional and at the international, not tactical, level.[116] This can be seen in that despite the concepts of power, cyberspace and cyberpower having attracted considerable research effort, its application within the context of the other environments has not. Accepting that cyberspace is a unique environment alongside land, air, sea, and space, these do not exist in isolation, yet although the dependencies between these physical elements is recognised, each one's unique link to cyberspace is not.

The role of attribution in cyberwar and indeed all forms of power projection is a significant one and was also discussed at length by Rid who noted that *military history knows no major battle where the enemies did not reveal themselves.*[117]

According to David Clarke and Susan Landau, attribution can be described as *the ability to identify the agent responsible for an action*.[118] The ability to accurately trace the true originator of an information campaign or cyber-attack is becoming an important element in the analysis of cyberpower projection, particularly when several countries are involved in a complex political scenario in which multiple messages are being promulgated. Clarke and Landau describe the elements of attribution as being in the form of who owns the machine from which an activity took place, the location from which it took place and who was responsible for the action.[119] Earlier commentators such as James Adams make the link between being able to identify an attacker and their allegiance with deterrence. In stating that *effective defence means deterring attacks before they occur [and] the threat of retaliation is a good preventative strategy;* he acknowledges that identifying attackers is difficult as are the legal and moral questions regarding retaliation. By drawing parallels with the positive effects of inter-agency and international governmental collaboration against terrorism, he predicts that the same level of cooperation will be required to defeat cyber-attackers.[120] The importance of attribution and deterrence has also been highlighted by Leon Panetta, former Director of the Central Intelligence Agency, and Secretary of Defence in 2012 who said [that] *In addition to defending the department's networks, we also help deter attacks. Our cyber adversaries will be far less likely to hit us if they know that we will be able to link to the attack or that their effort will fail against our strong defenses.*[121] This emphasises that the anonymity of cyberspace, so valued by its users, it regarded as something to be defeated by the Intelligence Agencies.

Within the context of coercive hard power, being able to accurately attribute cyber-attacks to the originating agent is important for two main purposes, that of deterrence and retaliation to counter their activity.[122] If an attacker cannot hide behind a cloak of anonymity and is aware that their identity will be quickly determined, they may be dissuaded from committing the act. Similarly, it is equally important that when offensive action is taken against an adversary that the true originator can be identified by the victim in order that retaliation can be considered. It is a core tenant of conflict in any environment that for military

force to be effectively deterred or to be able to defend against aggression, a nation must be able to reliably respond to attacks as they occur. Accurate attribution is also a vital legal, tactical, and technical requirement as without it, retaliation cannot be justified due to the threat of collateral damage. However, there may also be times in which an attacker may want or need their cyber-attack to be correctly attributed. This may be in order to clearly demonstrate capability as a means of hard power projection or to deter other attacks against them in the future. It is important that to prevent collateral damage a victim correctly traces the source of an attack to prevent them retaliating against the wrong target and so expand the conflict beyond its original borders.

Accurate attribution is also important as a tool of soft power. The ease by which information can be made readily available in cyberspace has resulted in a range of organisations providing sometimes conflicting reporting and a variety of commentators vying for audiences for their opinions. This may result in consumers of information choosing to seek out certain sources for their reputation of being known as being credible or for their political viewpoint. This may make the information providers targets for attack themselves and lead to the creation of imitation sites seeking to deceive their audience. This emphasises the importance that both information producers and receivers must be certain that their message is correctly attributed, particularly if it may affect peoples' actions or opinions.

The US Department of Defence strategy for operating in cyberspace has at its central focus *deterrence by denial* with the development of attribution technologies considered key if the country is to successfully deter and respond to attacks.[123] Their active defence strategy comprises three distinct stages termed *intrusion detection, traceback* and *counterstrike*.[124] Traceback comprises a range of forensic and technical methods to track the source of an attack with a counterstrike to disrupt or disable an attacker by sending countermeasures to its location. Once the origin has been identified, attribution could then be used as a legal tool to facilitate a successful prosecution. Counterstrike highlights contentious role of what is known as *Active Cyber*

Defence (ACD). Described by NATO as *A proactive measure for detecting or obtaining information as to a cyber intrusion, cyber-attack, or impending cyber operation or for determining the origin of an operation that involves launching a pre-emptive, preventive, or cyber counter-operation against the source*, it combines proactive real-time detection with aggressive countermeasures outside the victim network.[125] The UK Ministry of Defence has a slightly different definition as *Activities that target hostile offensive cyber operations in order to preserve our freedom of manoeuvre within cyberspace.*[126] This does not imply the need to operate within an aggressor's network to conduct active defence, but does indicate that it is requires proactive measures to counter an attacker to maintain control of systems and networks.

The issue of the legality of operating within the networks of others to undertake active defence measures has been highlighted by Robert Dewar as if conducted by state actors against a target in another country they could be construed as a hostile act.[127] As well as the legitimacy of a so called *hack back*, Dewar also notes that this also emphasises the increased importance of accurate attribution in identifying an intruder and that this capability could be abused by extending it to the originators of content that is banned or deemed politically sensitive. As an alternative to these active defence measures, he suggests that non-aggressive passive measures could be enhanced to include what he terms *Fortified Cyber Defensive* activities comprising firewalls and filters designed to prevent a system breach and *Resilient* defence consisting of measures to enable a system to withstand a compromise and remain functioning.[128]

More recently, the UK has also adopted a more proactive stance to countering cyber threats. Following his announcement when Defence Secretary of the UK's development of a dedicated counter attack and strike capability in cyberspace, Philip Hammond, in his later role of Chancellor of the Exchequer launched the 2016 National Cyber Security Strategy by stating that the Government would take a more active cyber defence approach.[129] This would support the use of automated defence techniques to block, disrupt and

neutralise malicious activity before it reached the user and strengthen law enforcement capabilities to identify, track, apprehend and prosecute cyber criminals. He also highlighted the UK's investment in offensive cyber capabilities as the *ability to detect, trace and retaliate in kind is likely to be the best deterrent* and that the UK needed to develop a *fully functioning and operational cyber counter-attack capability*.[130] This would enable the UK not only to defend itself in cyberspace, but strike back in kind when attacked. A year later in a speech at the Cyber 2017 Chatham House Conference, the UK Defence Secretary Sir Michael Fallon highlighted the role of the country's new National Cyber Security Centre (NCSC) in understanding, containing, and mitigating cyber threats. As well as the ability to detect and attribute attacks he emphasised that retaliation is an important aspect of a credible deterrence strategy and significantly this may not be restricted to the cyber environment. As well as announcing that offensive cyber was now an integral aspect of the UK's arsenal he stated that the price of an online attack could invite a response from land, sea, or air as well as cyberspace.[131] To emphasise this point he confirmed that as well as the use of conventional munitions, the UK were routinely using offensive cyber in the war against Daesh, which was beginning to have a major effect on degrading their capabilities.

Although Rid emphasised the importance of being able to attribute an attack as an essential component of conducting warfare and noted the difficulty of using cyber means to trace a cyber-attack, the need to identify the source of an attack by means through which it was made is questioned by Julia Muravska. Stating that *just because some attacks cannot be unequivocally attributed….does not mean that these states were not in fact behind them*, a point is also raised by Brandon Valeriano and Ryan Maness who argue that cyber conflict does not take place in isolation, but within the wider backdrop of international politics.[132] They suggest that successful attribution can be made in terms of global relations and does not require a cyber attribution to a cyber-attack.[133] However although they correctly state that while cyberspace is a separate environment, it is not unconnected from the normal political domain and the challenges of tracing an attack can be exploited. This could be in the form of a deception plan,

so called *false flagging*, by one nation to goad others into conflict during periods of tension by conducting unattributed attacks, a point highlighted by Carr in that the difficulties in attributing an attack could be used to entrap others into conflict.[134]

Cyber attribution is also an issue raised in a short paper published by John Arquilla in 2012, partly in response to Rid's rejection of the notion of the concept of cyberwar. Here he argues that in the two decades since his original paper, many of his predictions had become a reality and that although many of the examples of cyber conflict that had come to public attention were low level attacks, they had potential to be scaled up. Although on their own he suggests that cyber-attacks may not achieve a strategic effect, they may contribute to the degradation of an opponent's overall military capability. This in turn could tip the balance in determining the chance of a campaign in the physical environment being successful and increase the possibility for offensive action in cyberspace leading to conflict.[135]

Having dismissed the concept of cyberwar, in a further paper Rid discusses the role and effectiveness of cyber weapons, which he defines as *instruments designed to cause physical, functional, or mental harm to structures, systems or living beings*.[136] He concludes that they span a wide spectrum of effects ranging from the generic, but low-potential tools to the specific, but high probability of achieving a significant impact. The former typically comprises malware, which is cheap to develop and may affect a wide range of systems from the outside but is incapable of penetrating and causing direct harm. Examples of this type of activity include Distributed Denial of Service (DDoS) attacks and malware that generate botnets or are designed to spread rapidly across systems. In discussing cyber weapons at the high end of the spectrum several distinctive attributes are identified. These include combining the ability to penetrate a specifically identified system, which is likely to be protected and the capacity to achieve physical harm to the target in a subtle manner so as not to be immediately detected. Although these high yield weapons will have more destructive potential they come at a cost in terms of the resources, intelligence

and time required to develop and deploy, which may put them out of reach of non-state actors and individuals. They will also be more specific in terms of the targets that they can be used against, which reduce the risk of collateral damage, but will also limit their wider use. Typical targets of this highly specialised type of weapon are Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems, which typically run on legacy versions of the Microsoft Windows platform, which were notoriously porous and easily penetrated.[137]

Although the use of a cyber weapon to achieve a physical effect may be the goal of the cyber warriors of the future, what should be considered is under what circumstances they can deliver an effect that cannot be achieved from a conventional munition. *Smart* weapons targeted by satellite based Global Positioning System (GPS) or by lasers are already in service and achieve high levels of accuracy and although not as cheap as unguided munitions can be used against a range of targets at very short notice. The investment required to achieve a similar effect through cyber channels may not be comparable in terms of time or cost to delivery and this should be considered as part of any investment appraisal into cyber weapon development.[138] Rid also makes the important point that code designed for espionage alone cannot be regarded as weapons as *the law of conflict does not see espionage an armed attack.*[139]

The increasing reliance on the cyber environment for information exchange has also been raised as a potential vulnerability for those nations that have made major investments in extensive command and control networks. There are significant advantages to being a networked military force with access to high speed communications in terms of the ability to draw on large amounts of data to enable decisions to be made based on accurate and up to date information; what is termed the *freedom to manoeuvre* in cyberspace. However, to be effective this must also involve guaranteeing the confidentiality, integrity, and availability of information by protecting the networks from attack. In recognising this issue, John Sheldon wisely counsels that the overuse use of cyberspace for the projection of power in both war and peace across all domains can be

disadvantageous.[140] An over reliance on communications and information can stifle initiative and adaptability as junior officers become less used and practiced in determining the best course of action themselves without recourse to senior leadership for advice or guidance. This in turn may distract commanders into becoming too focused on the battle at the lowest echelons and less involved with taking the initiative and focussing on the strategic aims of a campaign. The degradation, denial and deception of these systems will then become the prime target for an adversary and ensuring the resilience of the network becomes the strategic imperative for the defender.

The great strength of a successful military force is that which encourages the concept of *Mission Command*, in which commanders in the field are tasked with the *what* and not the *how*, but this is in danger of being undermined by an over reliance on readily available communications with higher authority. Worse still is the prospect of politicians, armed with the same tactical picture as their military officers, proffering advice based on short term political objectives rather than long term military ones. It must be remembered that the UK's greatest naval victory at the Battle of Trafalgar in 1805 was achieved by Nelson communicating only six messages to his Fleet of 27 ships commencing with the famous *England expects* flag hoist and ending with *Anchor on completion*.[141] Converted into binary format, these messages would comprise 1856 bits of information, which were transmitted over the course of the four hour battle.[142] This compares to the bandwidth requirements of a typical Joint Force Headquarters detailed in the UK's Joint Doctrine Publication 6-00 from 2008 which specifies a minimum requirement for 6400 bits per second and which no doubt has risen with advances in technology and in particular with the increased use of drones able to transmit real time high definition video feeds of a target.[143]

Conclusion to chapter 2

This chapter has introduced the core components of this thesis and the evolution of their relationship to achieve power and influence over a target audience. Although power itself can be simply defined as resulting in

behavioural change to the advantage of another, there are several ways in which this can be achieved with some more subtle than others. Indeed, it may even be that the victim does not know that they are being affected by the deliberate actions of an external influence if they are amenable to the change. Warfare is the ultimate form of power projection and that too may now be conducted in such a way that it does not cross the threshold of what may be regarded as hostile action by a nation state if conducted by proxy forces under a hybrid strategy combining a range of unconventional strategies to achieve the desired end state.

As for power, cyberspace can also be envisaged in a range of different ways particularly as it is a continually evolving environment with no universally accepted definition as to its composition and use. Combining the attributes of both power and cyberspace this provides a powerful means to access and influence an individual or group and cyberpower is now recognised as an important element as part of an overall campaign plan. However, despite the enthusiasm to exploit cyberpower to achieve strategic objectives, it must be understood that cyberspace is essentially an information based medium and has limitations on what can be achieved, particularly when comparing cyberpower to the effects of conventional military power and kinetic munitions.

Notwithstanding the legal debate of the status of cyberweapons, there is still disagreement over what the militarisation of cyberspace can hope to achieve with a spectrum of views ranging from near parity to conventional weapons to only very limited and specific effects being achievable. Indeed, there is still debate as to whether conflict in cyberspace can actually be described as warfare at all. Despite these doubts, some nations are keen to announce that they are developing or have developed cyber weapons and have units trained and prepared for their use. In addition to complexities of developing the weapons themselves cyberwar presents additional challenges in deterring potential adversaries, attributing attacks when they do occur and then being able to successfully respond in kind. This has led to a key decision being made by some countries in declaring that cyberattacks may be met by retaliation from

any environment. This is nothing new in that a maritime attack may result in airpower being used against the aggressor, but it is an important milestone in the acknowledgement that cyberspace is not unique and is now regarded as an operational environment equal in status to that of the land, maritime, air and space.

The use of cyberspace for power projection, which is regarded as an offensive activity, has demonstrated that the existing literature provides a valuable resource from which to investigate the changing character of power projection and maritime security in a digital age. Exploring cyberspace and its relationship with the concepts of power and influence is a complex and multifaceted exercise involving an appreciation of how the existing, but differing definitions of what constitutes power can be integrated into an ever changing and evolving cyber environment. Understanding both these aspects in isolation are challenging undertakings and combining them even more so. It is however attracting considerable research as the potential to alter the behaviour of a target audience at distance without resorting to conventional military means is an attractive one. As a response, nations have realised that in order to counter the efforts of others robust security measures are required to limit their access and ability to spread their message unhindered.

The issue of how to conduct warfare in cyberspace has been the subject of considerable research and discussion and has been debated in sufficient detail to appreciate both the nuances of what constitutes conflict in the cyber environment and the effects that can potentially be delivered. Nye's comprehensive development of the concept of power and the nature of its hard, soft, and smart forms can be applied to Rid's analysis of cyberwar and how cyberspace is used as part of a strategy of power projection. When combined with the broader findings of this chapter it provides a perspective of how cyberpower can be derived using a range of techniques and mechanisms. Importantly it should be considered that as cyber defence and security is a reactive discipline that responds when system vulnerabilities, both known and unknown, are exploited by attackers. This makes cyberspace a potentially a

fruitful medium through which influence can be exerted if a threat vector can be identified and exploited to the advantage of an attacker. The interconnectedness of information and power also enables cyberspace to be used to achieve an effect in the other physical environments to attain a positive regional outcome.

Drawing on Rid's assertion that activities in cyberspace fall short of the conventional definition of war, his categories of espionage, expanded to include all intelligence gathering activities, subversion and sabotage can be neatly assigned to the notion of hybrid warfare in which states are engaged in a grey area between peace and war. Viewing hybrid warfare within the spectrum of the path from peacetime activities to high intensity conflict and combining these with Nye's categories of power, they can be brought together as shown in table 3 showing its the central role and link to smart power in the cyber operating environment. This shows that Rid's triptych of cyber effects span the spectrum of Nye's power categories and that to be effective all aspects should be considered as part of an operation to determine the one that will achieve the optimum result. However, within any campaign of cyberpower, the issue of attribution is an important once to accurately identify the source, whether it be declared, falsely presented, or intended to be anonymous. How attribution is perceived will have a significant impact in determining what type of response it may elicit.

Political state	**Power projection**	**Cyber operation**
Peacetime Diplomacy	Soft	Intelligence gathering / Subversion
Tension / Hybrid war	Smart	Intelligence gathering / Subversion / Sabotage
High Intensity Warfare	Hard	Intelligence gathering / Sabotage

Table 3: The relationship between political state, power projection and cyber operations

The relationship between a range of political states and their associated types of power projection and the method of cyber operation that can most effectively achieve the desired behavioural change provides the foundation upon which this thesis is based. The next chapter investigates how the unique characteristics of the maritime environment can present a range of opportunities and constraints when combining its attributes with that of cyberspace to achieve power and security.

Chapter 2 Endnotes

[1] Billings, L., 2015. *War in Space May Be Closer Than Ever.* [Online]
Available at: http://www.scientificamerican.com/article/war-in-space-may-be-closer-than-ever/ [Accessed 15 May 2016].
[2] Dahl, R., 1957. The concept of power. *Behavioral Science,* 2(3), pp. 201-215.
[3] Nye, J. S., 2010. Cyberpower. p.2 [Online]
Available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf [Accessed 19 10 2015].
[4] Nye, J. S., 1990. *Bound To Lead: The Changing Nature Of American Power.* 1st ed. New York, NY: Basic Books.p16.
[5] Ibid.
[6] Treverton, G. F. & Jones, S. G., 2005. *Measuring National Power.* P.12. [Online]
Available at: http://www.rand.org/pubs/conf_proceedings/CF215.html#download [Accessed 19 10 2015].
[7] Ibid.
[8] Nye, J. S., 2004. *Power in the Global Information Age.* 1st ed. New York, NY: Routledge.
[9] Nye, J.S., 2004 *Soft* Power. 1st ed. New York, NY: Public Affairs.
[10] Gray, C. S., 2005. *Another Bloody Century.* 1st ed. London: Orion. p.319.
[11] Bond, M. S., 2007. *Hybrid War: A new paradigm for stability operations in failing states.* US Army War College, Pennsylvania.
[12] US Army War College. 2016. Outplayed: Regaining Strategic Initiative in the Gray Zone. Carlisle barracks, PA. p.21.
[13] Wilkie, R., 2009. Hybrid Warfare. *Air and Space Power Journal*, Winter, pp. 13-17.
[14] Hoffman, F. G., 2007. *Conflict in the 21st Century: The Rise in Hybrid Wars,* Arlington, VA: Potomac Institute for Policy Studies.
[15] Defence Concepts and Doctrine Centre, 2007. *Joint Doctrine Note 2/07 "Countering Irregular Activity within a Comprehensive Approach".* 1st ed. London: Ministry of Defence.
[16] HM Government, 2015. National Security Strategy and Strategic Defence and Security Review, London: Her Majesty's Stationery Office.
[17] Shaw, J., 2015. Defence Review: The rules of conflict have changed. *The Financial Times*, 24 November. Online.
[18] Monagham, A., 2016. *The 'War' in Russia's 'Hybrid warfare'.* [Online] Available at: http://www.strategicstudiesinstitute.army.mil/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf [Accessed 13 Jan 17].
[19] Talbot, D., 2014. *Watching for a Crimean Cyberwar Crisis.* [Online]
Available at: https://www.technologyreview.com/s/525336/watching-for-a-crimean-cyberwar-crisis/ [Accessed 3 May 2016].
[20] Ibid.
[21] Shevchenko, V., 2014. *"Little green men" or "Russian invaders"?.* [Online]
Available at: "Little green men" or "Russian invaders"? [Accessed 3 May 2016].
[22] Charap, S., 2015. The Ghost of Hybrid War. *Survival - Global Politics and Strategy*, 23 Nov, pp. 51-58.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] NATO, 2015. *Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar.* [Online] Available at:
http://www.nato.int/cps/en/natohq/opinions_118435.htm [Accessed 3 May 2016].
[27] Raska, M., 2015. *Hybrid Warfare with Chinese Chacteristics,* Singapore: S. Rajaratnam Schol of International Studies.
[28] Gady, F.-S., 2015. *'Little Blue Men:' Doing China's Dirty Work in the South China Sea.* [Online] Available at: www.thediplomat.com [Accessed 2 May 2016].
[29] Nye, J. S., 2011. *The Future of Power.* 1st ed. New York: Public Affairs.p.19.
[30] Wilson, E. J., 2008. Hard Power, Soft Power, Smart Power. *The ANNALS of the American Academy of Political and Social Science,* 616(110), pp. 110-123.
[31] Treverton, G. F. & Jones, S. G., 2005. *Measuring National Power.* [Online]
Available at: http://www.rand.org/pubs/conf_proceedings/CF215.html#download [Accessed 19 10 2015]. p.ix.

[32] Wilson, E. J., 2008. Hard Power, Soft Power, Smart Power. *The ANNALS of the American Academy of Political and Social Science,* 616(110), pp. 110-123.
[33] Nye, J. S., 2011. *The Future of Power.* 1st ed. New York: Public Affairs.p. 207.
[34] Ibid. pp.208-9.
[35] Nye, J. S., 2009. Obama's Smart Power. *Non-profit quarterly,* Volume Spring, pp. 7-9.
[36] Chong, A., 2010. Small state soft power strategies: virtual enlargement in the cases of the Vatican City State and Singapore. Cambridge Review of International Affairs, 23(3), pp. 282-405.
[37] Nye, J. S., 2011. *The Future of Power.* 1st ed. New York: Public Affairs.p.118.
[38] Schmidt, E. & Cohen, J., 2013. *The New Digital Age.* 1st ed. London: John Murray. P6.
[39] Kramer, F. D., 2009. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In: F. D. Kramer, S. H. Starr & L. K. Wentz, eds. *Cyberpower and National Security.* Dulles, Washington: Potomac, p. 4.
[40] Gibson, W., 1994. *Neuromancer.* 1st ed. London: Harper Collins.
[41] Kuehl, D., 2009. Cyberspace to Cyberpower: Defining the Problem. In: F. D. Kramer, S. H. Starr & L. p.2
[42] Betz, J. D. & Stevens, T., 2011. Power and cyberspace. In: D. J. Betz & T. Stevens, eds. *Cyberspace and the state.* London: Routledge, p. 36.
[43] Sheldon, J. B., 2011. Deciphering Cyberpower. *Strategic Studies Quarterly,* Issue Summer, p. 96.
[44] Ghernaouti, S., 2013. *Cyberpower.* 1st ed. Lausanne: CRC Press. p.143.
[45] Kuehl, D., 2009. Cyberspace to Cyberpower: Defining the Problem. In: F. D. Kramer, S. H. Starr & L. K. Wentz, eds. *Cyberpower and National Security.* 1st ed. Dulles(Virginia): Potomac, pp. 24-42.
[46] Rattray, G. J., 2009. An Environmental Approach to Understanding Cyberpower. In: F. D. Kramer, S. H. Starr & L. K. Wenz, eds. *Cyberpower and National Security.* Dulles, Virginia: Potomac, pp. 253-274.
[47] Department of Defense, Joint Chiefs of Staff, 2014. *Joint Publication 3-13 - Information Operations,* Washington, DC: Department of Defense. p.x.
[48] Lin, H., 2016. *NATO's Designation of Cyber as an Operational Domain of Conflict.* [Online] Available at: https://www.lawfareblog.com/natos-designation-cyber-operational-domain-conflict [Accessed 19 June 2017].
[49] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence.p.1.26
[50] NATO Cooperative Cyber Defence Centre of Excellence, 2015. *Cyber Definitions.* [Online] Available at: https://ccdcoe.org/cyber-definitions.html [Accessed 22 October 2015].
[51] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence.p.1-1.
[52] Betz, J. D. & Stevens, T., 2011. Power and cyberspace. In: D. J. Betz & T. Stevens, eds. *Cyberspace and the state.* London: Routledge, p. 38.
[53] Sheldon, J. B., 2011. Deciphering Cyberpower. *Strategic Studies Quarterly,* Issue Summer, p. 99.
[54] Betz, J. D. & Stevens, T., 2011. Power and cyberspace. In: D. J. Betz & T. Stevens, eds. *Cyberspace and the state.* London: Routledge, p. 38.
[55] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.
[56] Gray, C. S., 2005. *Another Bloody Century.* 1st ed. London: Orion. p.319.
[57] Schmidt, E. & Cohen, J., 2013. *The New Digital Age.* 1st ed. London: John Murray. p3
[58] Ibid. p.83
[59] Gray, C. S., 2005. *Another Bloody Century.* 1st ed. London: Orion. p.320.
[60] Betz, J. D. & Stevens, T., 2011. Power and cyberspace. In: D. J. Betz & T. Stevens, eds. *Cyberspace and the state.* London: Routledge, p. 42.
[61] Kuehl, D., 2009. Cyberspace to Cyberpower: Defining the Problem. In: F. D. Kramer, S. H. Starr & L. K. Wentz, eds. *Cyberpower and National Security.* 1st ed. Dulles(Virginia): Potomac, p. 8.
[62] Sheldon, J. B., 2011. Deciphering Cyberpower. *Strategic Studies Quarterly,* Issue Summer, p. 95.
[63] Ibid. p.95.
[64] Nye, J. S., 2011. *The Future of Power.* 1st ed. New York: Public Affairs.p.113.

[65] Ibid. p.118.
[66] Ibid. p.123.
[67] Nye, J. S., 2010. Cyberpower p.2 [Online]
Available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf [Accessed 19 10 2015].
[68] Kuehl, D., 2009. Cyberspace to Cyberpower: Defining the Problem. In: F. D. Kramer, S. H. Starr & L. K. Wentz, eds. *Cyberpower and National Security.* 1st ed. Dulles(Virginia): Potomac, pp. 28.
[69] Sheldon, J. B., 2011. Deciphering Cyberpower. *Strategic Studies Quarterly,* Issue Summer, p. 96.
[70] Nye, J. S., 2011. *The Future of Power.* 1st ed. New York: Public Affairs.p.127.
[71] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.p.77
[72] Hansen, L., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, Volume 53, p. 1159.
[73] Ibid. p.1157
[74] OpenNet Initiative, 2014. Home. [Online] Available at: https://opennet.net/ [Accessed 27 May 2016].
[75] Deibert, R., Palfrey, J., Rohozinski, R. & Zittrain, J., 2008. *Access Denied - The Practice and Policy of Global Internet Filtering.* 1st ed. Cambridge, Massachusetts: MIT Press.p.12
[76] Nye, J. S., 2014. The Information Revolution and Power. *Current History,* 113(759), pp. 19-22.
[77] Kuehl, D., 2009. Cyberspace to Cyberpower: Defining the Problem. In: F. D. Kramer, S. H. Starr & L. K. Wentz, eds. *Cyberpower and National Security.* 1st ed. Dulles(Virginia): Potomac, p. 39.
[78] Development, Concepts and Doctrine Centre, 2014. Joint Doctrine Publication 0-01 UK Defence Doctrine. 5th ed. London: Ministry of Defence.
[79] Ministry of Defence, 2013. *Joint Doctrine Note 2/13 Information Superiority.* [Online]
Available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/239342/20130813_JDN_2_13_Info_Super.pdf. p 1-1 [Accessed 12 Apr 2016].
[80] Development, Concepts and Doctrine Centre, 2011. *United Kingdom Supplement to the NATO Terminology Database.* 8th ed. London: Ministry of Defence.
[81] Development, Concepts and Doctrine Centre, 2010. *Future Character of Conflict,* London: Ministry of Defence.
[82] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.3-22
[83] Nye, J. S., 2010. Cyberpower. p.2 [Online]
Available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf [Accessed 19 10 2015].
[84] Klimburg, A., 2011. Mobilising Cyber Power. *Survival: Global Politics and Strategy,* 53(1), p. 43.
[85] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.p.41
[86] DigitalWatch Observatory, 2017. UN GGE [Online] Available at: https://dig.watch/processes/ungge [Accessed 20 June 2017].
[87] Schmitt. M. N., 2013. Tallinn Manual On The International Law Applicable to Cyber Warfare. 1st ed. Cambridge: Cambridge University Press.
[88] Schmitt. M. N., 2017. Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations. 1st ed. Cambridge: Cambridge University Press.
[89] Sheldon, J. B., 2011. Deciphering Cyberpower. *Strategic Studies Quarterly,* Issue Summer, p. 98.
[90] Ibid. p. 98.
[91] Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is coming. *Comparative Strategy,* 12(2), pp. 141-165.
[92] Adams, J., 2001. Virtual Defence. *Foreign Affairs,* 80(3), pp. 98-112.
[93] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.
[94] Ibid. p.31
[95] Gray, C. S., 2005. *Another Bloody Century.* 1st ed. London: Orion.
[96] Clarke, R. A. & Knake, R. K., 2010. *Cyber War.* 1st ed. New York, NY: Harper Collins.

[97] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst.
[98] Clarke, R. A. & Knake, R. K., 2010. *Cyber War.* 1st ed. New York, NY: Harper Collins.p.65.
[99] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence.p.1.26
[100] UK Government, 2013. *New cyber reserve unit created.* [Online]
Available at: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit [Accessed 5 Nov 2015].
[101] NATO Parliamentary Assembly, 2009. *173 DSCFC 09 E bis - NATO and Cyber Defence.* [Online]
Available at: http://www.nato-pa.int/default.asp?SHORTCUT=1782 [Accessed 5 Nov 2015].
[102] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst.p.xvi
[103] Ibid. p.xvi
[104] Ibid. p.13
[105] Chauvin, J., 2013. *[Review Essay] Rid, Thomas. Cyber War Will Not Take Place. London: Hurst & Company, 2013..* [Online] Available at: https://www.academia.edu/7493468/_Review_Essay_Rid_Thomas._Cyber_War_Will_Not_Take_Place._London_Hurst_and_Company_2013 [Accessed 7 May 2016].
[106] Federal Bureau of Investigation, 2015. *Update on Sony Investigation.* [Online]
Available at: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation [Accessed 8 May 2016].
[107] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst.p.3
[108] Ibid.p.10
[109] Stone, J., 2013. Cyber War Will Take Place!. *Journal of Strategic Studies,* 36(1), p.101.
[110] Rid, T., 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35(1), pp. 5-
[111] Stone, J., 2013. Cyber War Will Take Place!. *Journal of Strategic Studies,* 36(1), p.106.
[112] Ibid. p.107.
[113] Gray, C. S., 2005. *Another Bloody Century.* 1st ed. London: Orion. p.294.
[114] Gartzke, E., 2013. The Myth of Cyberwar. *International Security,* 38(2), p. 49.
[115] Muravska, J., 2013. *Book Review: Cyber War Will Not Take Place.* [Online]
Available at: http://blogs.lse.ac.uk/politicsandpolicy/book-review-cyber-war-will-not-take-place/ [Accessed 07 May 2016].
[116] Valeriano, B. & Maness, R., 2015. *Cyber War versus Cyber Realities.* 1st ed. Oxford: Oxford University Press. p.xi
[117] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst. P.141
[118] Clark, D. D. & Landau, S., 2010. Untangling Attribution. In: *Proceedings of a Workshop on deterring cyberattacks.* Washington, DC: The National Academies Press, pp. 25-41.
[119] Ibid. pp. 25-41.
[120] Adams, J., 2001. Virtual Defence. *Foreign Affairs,* 80(3), p.109.
[121] Panetta, L., 2012. *US Department of Defense.* [Online]
Available at: http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136 [Accessed 9 May 2016].
[122] Clark, D. D. & Landau, S., 2010. Untangling Attribution. In: *Proceedings of a Workshop on deterring cyberattacks.* Washington, DC: The National Academies Press, pp. 25-41.
[123] Mudrinich, E. M., 2012. Cyber 3.0: The Department of Defense Stratrgy for Operating in Cyberspace and the Attribution Problem. *Air Force Law Review,* Volume 68, pp. 167-206.
[124] Ibid. p. 182.
[125] CCDCOE, 2013 *Cyber Definitions.* [Online] Available at: https://ccdcoe.org/cyber-definitions.html. [Accessed 20 June 2017].
[126] Ministry of Defence, 2016. *Cyber Primer.* 2nd Ed. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf. [Accessed 20 June 2017]. P.52.
[127] Dewar, R. S., 2014. The "Triptych of Cyber Security": A Classification of Active Cyber Defence. Tallinn, NATO CCD COE.
[128] Ibid.
[129] Hammond, P., 2016 *Chancellor Speech: Launching the National Cyber Security Strategy*. [Online] Available at: https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-securitystrategy. [Accessed 7 June 2017].
[130] Ibid.

[131] Fallon, M., 2017. *Defence Secretary's speech at Cyber 2017 Chatham House Conference* [Online] Available at: https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference. [Accessed 12 July 2017].
[132] Muravska, J., 2013. *Book Review: Cyber War Will Not Take Place.* [Online] Available at: http://blogs.lse.ac.uk/politicsandpolicy/book-review-cyber-war-will-not-take-place/ [Accessed 07 May 2016].
[133] Valeriano, B. & Maness, R., 2015. *Cyber War versus Cyber Realities.* 1st ed. Oxford: Oxford University Press. p.15
[134] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.p.95.
[135] Arquilla, J., 2012.*Cyberwar Is Already Upon US.* [Online] Available at: http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ [Accessed 07 Dec 2016].
[136] Rid, T. & McBurney, P., 2012. Cyber-Weapons. *The RUSI Journal,* 157(1), pp. 6-13.
[137] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.p.61.
[138] Rid, T. & McBurney, P., 2012. Cyber-Weapons. *The RUSI Journal,* 157(1), pp. 6-13.
[139] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst.p.46-47.
[140] Sheldon, J. B., 2011. Deciphering Cyberpower. *Strategic Studies Quarterly,* Issue Summer, p. 106
[141] Broadside, 2012. *www.nelsonsnavy.co.uk.* [Online]
Available at: http://www.nelsonsnavy.co.uk/traf-signals.html [Accessed 26 October 2015].
[142] Roubaix Interactive, 2011. *Binary to Text (ASCII) Conversion.* [Online] Available at: http://www.roubaixinteractive.com/PlayGround/Binary_Conversion/Binary_To_Text.asp [Accessed 26 October 2015].
[143] Ministry of Defence, 2008. *JDP 6-00 3rd Edition: Communications and Information Systems Support to Joint Operations.* [Online]
Available at: https://www.gov.uk/government/publications/jdp-6-00-3rd-edition-communications-and-information-systems-support-to-joint-operations [Accessed 26 10 2015].

Chapter 3: Maritime cyberpower and security

In order to fully address the second objective of this thesis, which is to investigate the close relationship and interdependence between the maritime and cyber environments within the context of power and security, it is necessary to understand how a nation views the role of maritime security and how it contributes to the wider issues of protecting individuals and the state from external threats. This chapter discusses the existing literature and national doctrine that describes these concepts in the maritime and information environments, highlighting the conditions required for cyberpower both at and from the sea to be achieved and exercised. This emphasises that although the unique attributes of the maritime environment can also be levered for cyberpower projection, to be effective they must circumvent or overcome the range of security measures that are designed to protect shipboard systems, their infrastructure ashore and their operators from the interference of others.

Power and security in the maritime environment

There is a direct correlation between power and security, which is applicable in all environments including maritime and cyberspace. As power seeks to influence the behaviour of people or the course of events, this may be perceived as a threat, particularly if they are detrimental to their government or society's policy, social norms, or strategic ambitions. Among multiple definitions of *security,* the Oxford English Dictionary includes *Freedom from threat or danger*, and *safeguarding the interests of a state*.[1] Effective security can thus be used to counter the effects of a campaign of power projection or influence – it is a counter power strategy. However, as noted by Carr, security and power are not the same thing highlighting the argument that states seek power because it is the most reliable way to ensure survival. Power can also be regarded as a means to an end and is useful for ensuring security.[2] At sea, maritime security can be utilised to counter some of the measures used to exert control over people or systems by a threat actor, be they a state sponsored or a non-state sponsored group seeking either ideological change or criminally motivated for

financial gain. These methods may range from efforts to exercise power through sea control of an area for their own use or denial of its use by others such as to protecting fisheries or maintaining the operation of offshore oil platforms from the adverse influence of others, the importance of which are highlighted in a range of UK doctrinal publications.

The UK's National Security Strategy published in 2010 describes the country's national interests as security, prosperity, and freedom and as core objectives, the protection of people, economy, infrastructure, territory, and way of life from all major risks that can directly affect the country.[3] Within the maritime environment, this is enhanced by the UK National Strategy for Maritime Security, which defines *maritime security* as:

> *…the advancement and protection of the UK's national interests, at home and abroad, through the active management of risks and opportunities in and from the maritime domain, in order to strengthen and extend the UK's prosperity, security and resilience and to help shape a stable world.*[4]

Today's increasingly interconnected society is highlighted in the strategy through trade, emerging markets, common interests, technology, and cyberspace. This trend towards globalisation through technology and trade has resulted in an interdependency of nations such that events anywhere in the world has the potential to have an effect on domestic markets. Maritime forces with their global reach can contribute to maintaining stability in many ways by exploiting the full spectrum of their capabilities to counter threats that originate from international waters as well as sovereign territory. This role is highlighted in the National Strategy for Maritime Security, which emphasises the link between maintaining stability and its crucial role in providing resilience to the national economy.[5] The National Security Strategy also makes specific reference to the risks of operating in cyberspace by listing them alongside terrorism, conventional military conflict, and natural disasters as the greatest threat to the stability of the country. In particular, the threat of cyber espionage

and the disruption of critical services are highlighted with the additional threat of criminality being included in the Strategy for Maritime Security, which also includes law enforcement as a lever of international cooperation.[6] In addition, UK Maritime Doctrine emphasises the versatility and mobility of seaborne assets as a tool of political and diplomatic leverage in international relations and that they can be regarded as a key tenet of a country's security strategy. This role in conflict prevention requires long term engagement and establishing trust to encourage the development of cooperation and conciliation in international affairs. Noting that this takes time, effort and persistence with relationships having to be nurtured through regular dialogue, this echoes the essential elements of soft power reinforcing the international capabilities of maritime forces in the delivery of the diplomatic, cultural, military, and economic elements of smart power.[7]

Although prominent in their discussions of power and conflict in cyberspace, neither Joseph Nye nor Thomas Rid acknowledge that the unique properties of each physical environment may affect the attributes of cyberspace within the context of either defensive or offensive activities. Indeed, the concept of cyberpower in the maritime environment or an assessment of how cyberwarfare could be conducted at or from the sea has not attracted much, if any, discussion. This may be due to a lack of understanding of the unique conditions of the coastal and oceanic regions or that they are not considered suitably different from the other environments to warrant investigation. The case studies used by Rid for example in arguing that cyberwar did not meet the criteria for true warfare did not speculate as to what its consequences might be to Nye's description of power projection if either the target was a ship or that an effect was being delivered from the sea and their consequential impacts in a regional conflict.

Within the military context, British Defence Doctrine notes that the role of national security encompasses the safety of the state and its protection from both external and internal threats, but is also integrated within, and dependent upon, the security of neighbouring states and partners.[8] The former of these

may lead to invasion, attack or blockade and the latter includes the dangers from terrorism, subversion, civil disorder, criminality, insurgency, sabotage, and espionage. The role of cyberspace is referred to within the context of an attack on the country's critical national infrastructure. The doctrine also obliquely refers to the maritime component by highlighting that the government's primary duty is to maintain the freedom and integrity of the UK and that its stability, prosperity, and well-being depend on international trade and investment. This it notes requires raw materials being imported and goods exported by sea and are facilitated through access to global information flows. In highlighting the threat posed to the UK by criminals operating in the maritime environment, terrorism, disruption to trade or the freedom of navigation, maritime attack against the national infrastructure, arms proliferation, drugs and people smuggling are all listed in the National Strategy for Maritime Security.[9] In stating methods to counter them, the strategy includes international collaboration and governance, protecting UK citizens, infrastructure and shipping, securing trade routes and finally protecting against serious organised crime and terrorism. To achieve this, it identifies five core Maritime Security Tasks and five Maritime Security Objectives, which are described below:

Maritime Security Tasks

Understand: This involves gathering and analysing data and intelligence, building partnerships, and sharing information with allies when concerns are identified.

Influence: This draws on a range of methods ranging from diplomacy, law enforcement, and economic measures to military engagement with the aim of changing behaviour thereby linking this activity to the concept and methods of smart power.

Prevent: Should influence methods fail these are activities to prevent potential issues from developing or escalating. This may take the form of building security capacity in areas of instability, but can also include responsive actions.

Protect: If a valid threat does emerge, measures can be taken to reduce the vulnerability of the maritime or shipping infrastructure or increasing the resilience to an attack.

Respond: Throughout the above tasks, the UK will continue to consider a range of responses varying from law enforcement action or interdiction to in extreme cases, military action.

Maritime Security Objectives

To achieve the above five core security tasks, the UK has identified five maritime security objectives as detailed below:

Promote and uphold the norms of a secure international maritime domain: This is achieved through an active and activist foreign policy with the aim being to strengthen the international system based on compliance with the United Nations Convention on the Law of the Sea (UNCLOS).

To develop the maritime governance capacity and capabilities of strategically important states: Acknowledging that Maritime Security is an international responsibility, some states are more able to meet their obligations than others and this objective seeks to build intelligence, law enforcement, coastguard, and the military capabilities of weaker states.

To support the safety and security of ports, offshore installations, and UK registered shipping: Using intelligence led security advice and compliance monitoring activities, government agencies will ensure the protection from terrorism of entitled personnel, ships, oil rigs and wind farms.

To assure the security of trade and energy transportation routes: As global economies depend on international trade and energy, naval forces will be used

in collaboration with global partners to build understanding, deter threats and protect shipping, using force if necessary.

To protect the resources and population of the UK from illegal and dangerous activity: Highlighting the threat from organised crime, terrorism, illegal immigration and unlawful exploration of natural resources, law enforcement agencies will carry our surveillance to deter these activities, interdicting suspect vessels where necessary.

To fulfil the Maritime Security Tasks and Objectives, forces can be deployed to meet the requirements of a specialist intelligence collection, surveillance, and reconnaissance (ISR) role. The worldwide presence of maritime forces, their organic sensors and ability to position just outside territorial waters or out of sight over the visible horizon has been long recognised as key attributes for information gathering tasks and is conducted both in peace and at times of tension and conflict. The aim of ISR is to achieve as comprehensive a situational awareness as possible, which is defined as the perception of the area of interest, problem or situation bounded by time and space in the context of the commander's mission or task.[10] In a maritime context it is used to describe the aspiration of warships to be able to determine the identity of other sub surface, surface and air contacts of interest and be able to track them. In times of war, this information can be fed to weapons systems to provide a firing solution, but in peacetime it adds to a better understanding of what routine activity looks like in an area and to provide the ability to classify contacts based on previous known behaviour. Although British Maritime Doctrine recognises the role of information superiority, situation awareness and ISR, the role of cyber is not explained in detail other than to state that its scope is beyond that of just information systems and extends into command, control, intelligence, and surveillance. This is despite the information environment being crucial for both the management of ship systems and navigational safety. This can be seen from the reliance upon data from satellite navigation systems, terrestrial navigation beacons or transmissions from other ships relating to their position and activities as well as non-data transmissions such as the use of radar.

Maritime Security Risks

As part of the UK's maritime security strategy, a specific Maritime Risk Assessment was conducted in 2013 as part of the biennial National Security Risk Assessment (NSRA) process, which was used to prioritise all major areas considered a risk to national security. This assessment concluded that the following issues were the highest priority based on both likelihood and impact:[11]

- Terrorism affecting the UK and its maritime interests, including attacks against cargo or passenger ships.

- Disruption to vital maritime trade routes because of war, criminality, piracy, or changes in international norms.

- Attack on UK maritime infrastructure or shipping, including cyber-attack.

- The transportation of illegal items by sea, including weapons of mass destruction, controlled drugs, and arms.

- People smuggling and human trafficking.

Although the risk of cyber-attack is specifically mentioned, the use of cyber facilitated crime can be a contributory factor in many of the other high priority risks. In particular, terrorism can be inspired and planned through cyberspace, trade routes can be analysed through online ship tracking applications and the transportation of illegal items and human trafficking can be coordinated through the communications medium of cyberspace. The assessment and mitigation of maritime risk is therefore inextricably linked to the cyber environment.

In his book, *Tubes*, author Andrew Blum investigates a risk to cyberspace that few consider; the physical infrastructure that forms the global network.[12] Inspired by curiosity of where the cable from his home router ultimately led, Blum traces the wired connections and associated technology that comprise

the Internet and houses the data that users access when downloading material from the World Wide Web. A key finding from his book is that whereas the routing equipment is often housed in anonymous, but secure buildings and the data centres owned by *Google* and *Facebook* are the most protected aspects of cyberspace, the transoceanic cables that circumnavigate the world are not. Laid in shallow waters approaching the coast and making landfall in well documented locations, these cables carry virtually all international Internet traffic and yet despite being a fundamental component are a largely unpublicised aspect of cyberspace. Although Blum alluded to the potential vulnerabilities of the cables, he does so from the perspective of accidental damage from ship's anchors or earthquakes, not from a deliberate attempt to limit a country's cyberpower by cutting its international connections.[13] The subject of undersea cables is also examined by Nicole Starosielski, but mostly from their impact on the natural ecology of their environment and the political impact of their presence. Historical examples of disconnection and probably false accusations of cold war adversaries engaged in deliberate interference are addressed, but not from a perspective of how that will affect a nation's cyberpower.[14] The issue of protecting these cables from accidental or deliberate damage is an important one that has until now been disregarded by many commenters and is a subject explored more thoroughly in the later chapters of this thesis.

Maritime cyber security

To date, the focus on the issues regarding the role of cyber power at sea has been primarily concentrated on the defensive aspects and how to secure shipping from cyber-attack, which in 2017 is now gaining increased interest from academia and the mercantile industry. For example, Plymouth University in the South West of the UK has a dedicated Marine Institute, which includes a specialist Maritime Cyber Threats Research Group. This department has been active in investigating merchant ship cybersecurity and specialises in multidisciplinary research and has access to marine simulation environments to investigate threats at all levels from the theoretical to practical applications.[15]

This includes the presentation of a specialist MA in Applied Strategy in Maritime Security that includes an optional module dedicated to Security Threats in Cyberspace.[16]

Lancaster University's Security Lancaster group has also been active in researching the relationship between the maritime and cyber environments in terms of security and in 2015 held a workshop in collaboration with the Royal Navy. This resulted in the publication of *The future of maritime cyber security*, which was one of the first attempts to address the unique issues of securing ships from cyber-attack.[17] Lancaster University is one of thirteen universities recognised by the UK Government as excelling in cyber security research. These institutions have been acknowledged as being able to assist the public sector and business in gaining a deeper understanding of the work being undertaken that could be harnessed to protect the UK from cyber-attack.[18] The key conclusion of their report was that the maritime cyber environment comprises three elements; Information, Technology, and People and as such is an integral element of the modern interconnected global network, which the report acknowledged presented challenges. This reinforces the acceptance that the maritime community afloat can no longer be regarded as platform centric and detached from cyberspace, but is part of it if connected via satellite, mobile telephony, or by radio transmission of digitised navigation or other maritime related information.

Lancaster's report identifies the information component as relating to the data that sustains maritime operations and technology as encompassing computer systems including the hardware and software in ships and port facilities. The people aspect also forms an integral part of the maritime environment due to the interactions between individuals and the electronic systems that they rely on to operate at sea. Although this brings advantages, it also exposes the maritime industry to the same threats and vulnerabilities as their land based contemporaries. In considering the security of the information component, the report acknowledges that the maritime community is now part of a wider information environment as recognised by the increasing quantity of data

transmitted to and from platforms afloat and the need to ensure its confidentiality, integrity, and availability, particularly when used by mission critical systems. The increasing quantity of information being processed also requires a means to prioritise traffic to ensure that effective decision making can take place without commanders suffering from information overload. This can only be achieved through the training of personnel to recognise the symptoms and be able to operate whilst under cyber-attack while taking measures to regain control of systems.

In assessing risks to the technology component, Security Lancaster concluded that contrary to the prevailing trend to increase automation, consideration should be given to only procuring essential capabilities for use in ships to reduce the overhead of maintaining superficial systems and that there should be a comprehensive systems knowledge of their interconnections. This further emphasises the integrated nature of cyberspace and that cyberattacks at sea must not be investigated in isolation, but that evidence, precedence and developments in other environments should be considered as part of a holistic approach in assessing the threat.[19] This also highlights the increasing importance of the littoral in terms of its role in supporting, facilitating and supplying maritime operations and that this land component should be regarded as part of the maritime environment when considering the technology component of maritime cyber security.

The role of system resilience is recognised in that the level of required should be understood in terms of the refresh cycle of replacing or upgrading technology being faster than that of other ships' systems, which would require a longer-term review of the investment model of how vessels are maintained. In particular, this emphasises the issue of software aging in which a ship's lifespan will exceed that of the software that is required to operate it. This will require regular, but potentially expensive and time consuming *software refits* to mitigate for their vulnerabilities that might necessitate the vessel being taken out of service for a period alongside for the update at considerable cost, but which may in reality offer no additional functionality and may even reduce

performance if the hardware upon which it is running is not upgraded at the same time.[20] This process of updating systems may well also be combined with the increased automation and the integration of different functions into a single system to reduce the manpower required onboard ships, which further limits the ability to operate without the aid of the computer systems. In their assessment of the information and technical components of the maritime environment, the report also included the vulnerability of the supply chain. Ocean going vessels are reliant upon a robust logistics organisation to provide global support – a system that is now totally dependent upon Internet based communications. Disruption of such networks may well have a significant effect on the seaworthiness or ability of a ship to embark on a voyage beyond coastal waters.

Finally, in reviewing the people component, Lancaster concluded that education was considered a fundamental component of effective overall cyber security to mitigate human induced compromise and that this should be combined with clear procedures that are understood by all. Despite this, it must be assumed that at some point an attack on a system will be successful and to mitigate for this the report encourages system resilience using practised back-up procedures and operators only having access to those elements of a system that are essential for their role onboard. In this respect, the people component of maritime cyber security presents the same issues as any connected enterprise, but with the additional challenges of perhaps a lack of expertise onboard to prepare for, identify, contain, resolve, recover, and learn from cyber security incidents when they inevitably occur.[21]

Industry's attempt to address the unique issues of cybersecurity at sea has been seen through an initiative of a consortium of shipping industry groups including the Baltic and International Maritime Council (BIMCO), Cruise Line International Association (CLIA) and International Chamber of Shipping. Their guidelines on cybersecurity onboard ships provide a risk-based approach to identifying and responding to cyber threats.[22] Acknowledging existing practice and the types of common attack affecting all computer users, they highlight the

specific cyber security issues facing the shipping industry. These include targeting the logistics support, cargo and crew management, navigation displays or machinery management systems. It also highlighted that the interface between ships systems and shore infrastructure connected to the Internet or when third party technicians are onboard present particular threats. The guidelines offer advice on assessing and reducing the overall risk as well as developing contingency plans to respond to a cybersecurity incident. Focussing on increasing awareness and providing training, the *Be Cyber Aware At Sea* campaign provides a range of free and paid for courses aimed specifically at countering the cyber threat to the mercantile marine. Supported by a range of government and commercial organisations including the UK Royal Navy, it also seeks to promote knowledge sharing of maritime cyber security expertise to increase understanding of the challenges that the digital era brings to shipping and offshore organisations.[23]

Despite the recognition to improve cybersecurity at sea, the wider issue of the maritime environment and its relationship with cyberspace in the projection of cyberpower is an area that so far remains unexplored and requires further investigation. Exploiting cyberpower in the maritime environment introduces the concept of maritime cyberpower which can be seen as a facilitator of maritime power which itself is defined by the UK Ministry of Defence in its Maritime Doctrine as *the ability to project power at sea and from the sea to influence the behaviour of people or the course of events*.[24] The role of cyberspace in maintaining maritime power is acknowledged as going beyond just information systems and reaching into command and control, intelligence, surveillance and reconnaissance activities as well as the physical control of systems. This recognises the importance of cyberspace as a facilitator in the effective operation of other systems, but not as a means to exert power at sea in its own right.[25] The doctrine also highlights that the cyber environment can be used by both state and non-state adversaries as an asymmetric tactic to seek an advantage over an otherwise militarily superior force.[26]

Conclusion to chapter 3

This chapter has provided the initial foundation for the forthcoming investigation into the conduct and role of cyberpower and security within the maritime environment by examining the unique challenges and risks from securing operations at or from sea. To be able to influence people through the medium of cyberspace requires an understanding of both the nature of power and the physical environments in which the cyber related infrastructure as well as where the target population is located. Together they provide the framework for investigating the close relationship and interdependence between the maritime and cyber environments. The recognition that the maritime environment is an historically significant one for nations to exploit for power projection has resulted in the role of security becoming established as a prominent factor in preventing others from interfering with their operations. The has led to a growth in the profile of measures to protect the freedom to operate at sea and now that cyber operations have extended to complement these activities, maritime cyber security has now become an important component to consider for seafarers and those who rely on the seas for their trade and protection of national assets. This has resulted in a range of organisations seeking to provide an important range of services offering maritime cyber security advice and is an active area of university led research initiatives.

Despite the extensive research that has been conducted into analysing the nature of power and its utility in cyberspace for a range of purposes including military action, its relationship with the other operating environments and in particular the maritime arena has been shown to not yet be fully investigated. The examination of power projection and security in the maritime environment requires the inclusion of a range of new and unique factors related to the nature of operating from the sea, many of which have yet to be fully understood and form one of research objectives of this work. Cyberpower and cyber security are inextricably linked as the ability to compromise a system provides an aggressor with the ability to either disconnect their victim from the wider network thereby preventing them from being able to communicate with others or

facilitate access that would otherwise be denied. Good security can thus be regarded as a counter power strategy in cyberspace. The ability to control the information transmitted on a network to a target population provides a powerful means to project power in the form of an information campaign, which could be delivered from the sea. Maritime trade may also form part of a nation's economic wealth, but its dependence on cyberspace for shore support may render it vulnerable to both attack and the subsequent effects of a strategic power projection campaign that seeks to alter the behaviour of nation states.

Although ships may be targeted as the victims of power projection from cyberspace and so need protecting, they may also be used as the means of exerting power in the environment and this too has yet to be fully explored by scholars. Similarly, the methods, consequences, and implications of isolating a country from cyberspace by cutting cables or interfering with electromagnetic transmissions carrying communication or navigational data either as deliberate acts of war or as an accidental event have not been fully examined and remains an important area of future research. This is particularly the case as the infrastructure has developed over a period of time and has been located in areas determined by factors other than security considerations. This is one area highlighted in the next chapter, which presents a novel way to model cyberspace and includes not only the physical infrastructure, but all the constituent components that must be considered when seeking to project cyberpower or to secure an organisation from the influence of others.

Chapter 3 Endnotes

[1] Oxford English Dictionary, 2016. *Oxford English Dictionary.* [Online] Available at: http://www.oed.com/. [Accessed 12 Apr 2016].
[2] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.p78.
[3] UK Government, 2011. *The UK Cyber Security Strategy.* [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. P10. [Accessed 6 Nov 2015].
[4] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office.
[5] Ibid.
[6] HM Government, 2010. *The National Security Strategy.* 1st ed. London: Her Majesty's Stationery Office .
[7] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.2-21
[8] Development, Concepts and Doctrine Centre, 2014. *Joint Doctrine Publication 0-01 UK Defence Doctrine.* 5th ed. London: Ministry of Defence.p3
[9] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office. p.9
[10] Development, Concepts and Doctrine Centre, 2010. *Joint Doctrine Publication 04 - Understanding.* 1st ed. London: Ministry of Defence.p1-5
[11] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office. p.9
[12] Blum, A., 2012. *Tubes.* 1st ed. London: Penguin.
[13] Ibid. p.199.
[14]Starosielski, N., 2015. *THe undersea network.* 1st ed. London: Duke. pp.60-93
[15] Jones, K. D., Tam, K. & Papadaki, M., 2016. *Threats and Impacts in Maritime Cyber Security,* London: Institution of Engineering and Technology.
[16] Plymouth University, 2016. *Maritime Cyber Threats research group.* [Online] Available at: https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group. [Accessed 12 Apr 2016].
[17] Fitton, O., Prince, D., Germond, B. & Lacy, M., 2015. *The Future of Maritime Cyber Security,* Lancaster: Lancaster University.
[18] Engineering and Physical Sciences Research Council, 2011. *Scheme to Recognise Academic Centres of Excellence in Cyber Security Research.* [Online] Available at: https://www.epsrc.ac.uk/files/funding/calls/2011/scheme-to-recognise-academic-centres-of-excellence-in-cyber-security-research/. [Accessed 12 April 2016].
[19] Ibid. p.28.
[20] Ibid. p.9.
[21] NIST, 2012. *Computer Security Incident Handling Guide.* [Online] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. [Accessed 23 May 2017].
[22] BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, 2016. *The Guidelines for Cyber Security Onboard Ships,* Bagsvaerd: BIMCO.
[23] Be Cyber Aware At Sea. [Online] Available at: https://www.becyberawareatsea.com/ [Accessed 17 June 2017].
[24] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.
[25] Ibid. para 355.
[26] Ibid. page 1-2

Chapter 4: Modelling cyberspace

Introduction

To be able to fully understand and explore the relationship between the cyber and maritime environments, it is necessary to appreciate their composition and dependencies. Whereas the attributes and composition of the physical maritime environment can be observed, measured, and has defined geographic boundaries, cyberspace is a continually evolving, artificial environment and does not yet have an equivalent agreed definition or agreement as to its composition. Previous attempts to describe cyberspace have either been incomplete or by intending to highlight a single or narrow range of attributes do not represent the full range of uses for which it can be exploited in the 21st century. Instead, the environment has been viewed from within the context of achieving a particular aim and descriptions has been developed for that purpose. This chapter fulfils the initial research objective of this thesis by introduce a novel three-dimensional model of cyberspace optimised to better understand how its properties and attributes can be measured and to demonstrate that the environment does not exhibit universal characteristics but that its structure and use may differ at the source and destination of a cyberpower campaign. This chapter continues the tradition of explaining cyberspace in terms of how it used for a particular purpose by developing and validating a model that for the first time is optimised for explaining power projection within the context of the characteristics of the physical environment in which its users and infrastructure reside. Later chapters will apply it to the unique attributes of the maritime environment using Rid's three offensive cyber activities to demonstrate the close relationship between the two environments and its role in power projection at and from the sea.

Comprising five sections, this chapter initially builds on previously published literature to present a new model of cyberspace optimised to explain the relationship between the cyber and other physical environments, including the maritime. A key aspect of this model is that it emphasises that cyberspace exists in three dimensions and that its attributes may differ at the point where

information originates and where it is received and processed. Thus, the nature of cyberspace at the point where a target audience accesses the environment is more important in terms of power projection than the location where the message is composed and disseminated from. This contributes towards completing the initial objective of this research by demonstrating that the nature and properties of cyberspace are not universal, but alter depending upon the geographic location of its physical infrastructure and from where the user is accessing it.

In the first section, earlier work to characterise and define cyberspace in terms of a number of vertical layers is examined to demonstrate how attempts to explain this man-made environment have evolved and developed. Secondly, these earlier models are expanded and developed to include new aspects not previously included that are considered fundamental to understanding the cyber environment from the perspective of using it as a means of power projection. Thirdly a second dimension is introduced to present a notion of distance to cyberspace. This is significant as the often-instantaneous nature of communication through networks and the opaque nature of its routing and the lack of control over the path it follows can result in this element of the medium being disregarded. However, when considering how data travels from source to destination, particularly when it may be subject to filtering or censorship, mapping its path becomes a significant issue and this section emphasises the utility of appreciating the distance and route it follows. This is supplemented by the inclusion of a third dimension to the model of cyberspace that enables different types of power projection to be considered separately and finally the model is validated by using a qualitative assessment of six criteria to examine in detail a range of cyber-attacks recorded from 2007 to 2017 that demonstrates a correlation between their sophistication, origin, and the layer at which the attack was targeted.

Writing for the RAND Corporation in 2009, Martin Libicki acknowledged that as a virtual medium, cyberspace is much less tangible than the other physical environments of land, sea, air, space or even the Radio Frequency (RF) spectrum.[1] In describing its nature, he views it as consisting of three layers;

physical, syntactic, and semantic, which together describe the core elements of its composition, but not its use or how they can be applied in any single context. He defines the physical layer as being the hardware components and wires, which together form the part of cyberspace that is susceptible to kinetic attack and physical destruction. The syntactic layer sits above the physical and contains the code and protocols that enables the components of the physical layer to interact with each other and include such functions as device recognition, addressing and routing. The complexity of the syntactic layer is dependent upon the type of system in use and will be bespoke to the user requirement and is the layer that would be targeted remotely across the network by hackers seeking to access or manipulate the software without having physical access to the hardware. At the top of Libicki's stack is the semantic layer. This contains information that makes the totality of the system useful to the operator and includes files such as address lookup tables and process-control information that are user provided and enable the system to perform as intended.[2]

John Sheldon also describes cyberspace in terms of layers, but increases the number to four and emphasises that control of one layer does not mean control of the others.[3] Again the infrastructure at the base of the stack contains the material components such as hardware and cabling, but above it is a physical layer. This considers the properties of the electromagnetic spectrum that animate the infrastructure layer and is an important consideration as it highlights that cyberspace is not uniform and draws on a range of methods and media to transmit information from source to destination. Above the physical layer is the syntactic layer containing data formatting information and the protocols that controls cyberspace. Finally, at the top level is the semantic layer that makes information useful and comprehensible to users. Sheldon notes that when attacking a system, the layer targeted depends on what outcome is trying to be achieved; for example, stopping the system from working will involve the syntactic and infrastructure layers whereas spoofing a user will involve manipulation of the semantic layer.[4]

The evolution of these previous models demonstrates how the perspective of cyberspace has changed. Initially in his three-layer model of physical, syntactic, and semantic layers, Libicki describes the environment, but not how it could be utilised and does not consider variations in its composition or how it is reliant on external factors. His view describes it as essentially a network upon which computer code enables the transfer of information. Sheldon, however does begin to appreciate the layers as having their own very distinct characteristics and that his lowest, infrastructure layer is more complex than just consisting of hardware and wires. His physical layer, which considers the electromagnetic properties of the infrastructure layer starts to introduce the notion that the method by which the data is communicated may have a bearing on the success of its receipt and should be a consideration in the composition of cyberspace. However, like Libicki, Sheldon does not consider how cyberspace might be employed for any single purpose or how its existence depends on the physical environment for its existence.

Developing the model of cyberspace

Building on the previous work of Libicki and Sheldon, this section proposes a model of cyberspace that has evolved from previous interpretations of the environment to enable its role as a means of power projection to be fully understood and measured. In addition to building on previously identified attributes, this version also contributes to addressing the third objective of this thesis by enabling the geographic environment to be fully appreciated in terms of the planning and activities required to project cyberpower and influence through acts of intelligence gathering, sabotage, or subversion. By taking Sheldon's four-layer model and expanding it to include four additional layers, it incorporates aspects of the environment not previously included or considered, but are important when planning how to reach a target audience to achieve behavioural change. This introduces factors that emphasise the relationship that cyberspace has with the physical environment in which the infrastructure and users reside and that it is also reliant on the provision of external support and maintenance for its continued existence. Also, as previous models have not sought to examine the reason a human user or connected system engages

with cyberspace and what they hope to gain from it, which is fundamental when considering the concept of cyberpower, these are included as separate layers of the environment.

The new more comprehensive representation of cyberspace is shown graphically in figure 1 alongside the two models discussed previously and is followed by an explanation of each layer and a description of possible methods by which each attribute could be measured. This enables a comparison to be made between different systems that identifies strengths and weaknesses in each layer. The result of this analysis may also highlight aspects that might need to be defended if subject to attack or expose vulnerabilities that may be useful if planning to infiltrate a system. This measurement function is important as it enables an assessment to be made between different methods of power projection to determine which may have the best chance of success. As it also incorporates the wide range of physical and virtual components that together comprises cyberspace, it may be determined that where there is an option of several layers to target, some may be more vulnerable to attack than others.

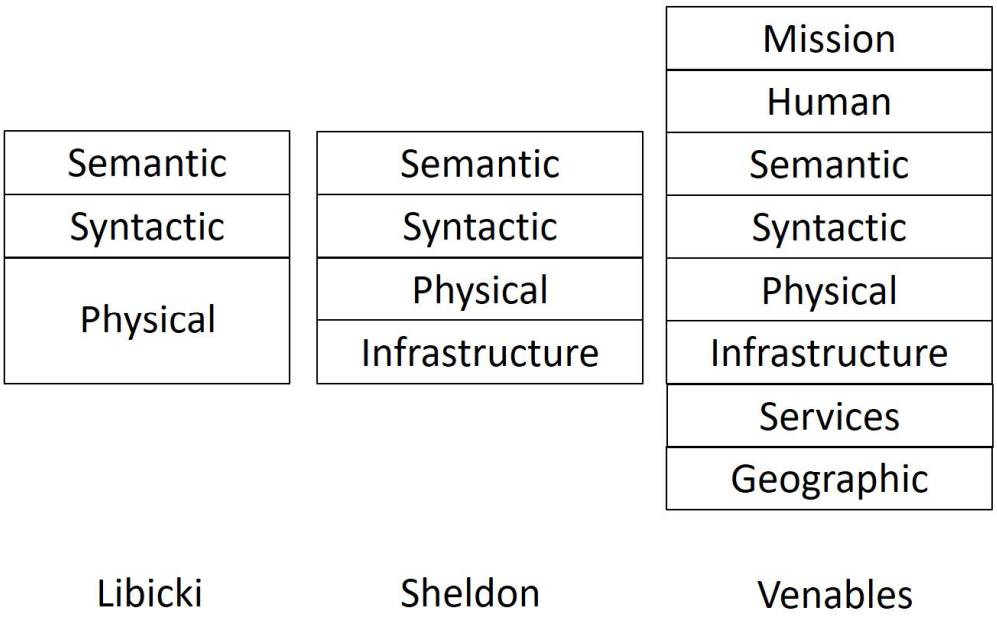

Figure 1: Comparison of different models describing cyberspace in terms of layers

Geographic Layer: At the bottom of the model a new foundation layer termed geographic has been added. This specifies the environment in which an element of cyberspace exists, be it land, maritime, air or space. This is significant when considering the properties of cyberspace in a particular area as, for example, propagation in the air or space environments can only be by Radio Frequency transmission, whereas in the land or maritime, depending on the location, it can be either wired or wireless. Regional variations in the Land environment can also be significant in that shifting desert terrain may prevent the use of mast mounted microwave links or mountainous regions may not favour buried cables. Political aspects may also be considered in this layer as some countries may not allow free passage of data across their borders without monitoring or censorship, or that they may have not invested in a widespread modern infrastructure which restricts the speed of transmission within their territory. As the means by which networks are formed and their properties are fundamental to the properties of cyberspace, a consideration of the geographic area and the path that the data may take across it may influence the type of message that can be delivered to the intended audience. For example, a congested or legacy network may not have sufficient bandwidth capacity to meet the demands of users or enable them to be reached. An understanding of the nature, capacity and reach of the infrastructure of an opponent is thus a vital component in the planning of a cyberpower campaign.

Services Layer: Above the geographic layer and below the infrastructure layer a new layer termed services has been added. This incorporates the dependencies of the other components that must be met to enable cyberspace to exist and includes utilities such as power supplies, chilled water, air conditioning and even the security of the physical buildings housing the elements that make up the infrastructure layer. Although not normally regarded as integral components of cyberspace, they emphasise its fragility and reliance upon external factors for it to function correctly. This is highlighted in that not only do all electronic components require a reliable and stable power supply, but they in turn generate heat and so additional power must be expended in cooling them.[5] Also, as the Internet was not initially designed to incorporate the level of expansion and growth that has since developed, there are some critical

locations that have become hubs for regional connectivity and single points of failure with the potential that should the services layer be compromised in these sites it could result in the disconnection of whole urban areas.[6]

Measurements of the services layer would include an assessment of a country's capability to support its critical national infrastructure (CNI) and the utilities required to maintain its cyber infrastructure including the ability to attract and train the skilled personnel to ensure its continued operation. Crime rates, particularly when considering component theft could also be included in an overall appreciation of the resilience of the services layer. In considering a hard power campaign involving physical destruction, it is the services layer that may be the most attractive to an adversary due to it being the most exposed to kinetic attack and that the after effects are the most obvious to observe and assess. These may be conducted by conventional explosive 'kinetic' weaponry, rather than cyber 'coded' payloads. This vulnerability to destructive effects may be due to it having less redundancy in case of failure or it being provided by third party organisations such as power companies that have contracted availability criteria of less than 100% and regard some level of failure as acceptable. A proportion of the components of the services layer such as electrical sub stations may also be outside the protective perimeter of an area containing the more obvious elements of the cyber infrastructure and so will be more challenging to monitor and secure. Attacking power supplies as a means of affecting a country's infrastructure has already been recognised by America's development of the so called CBU-94 *Blackout Bomb.* First used in 1999 against Serbia, this munition consists of a bomb that dispenses chemically treated carbon graphite filaments that short-circuit electrical power distribution equipment such as transformers and switching stations with minimal risk of collateral damage.[7]

Infrastructure layer: This comprises the physical embodiment of cyberspace and incorporates the hardware that stores, processes and transfers data. This includes computer clients, servers, networking components, cabling, satellites, and other elements fundamental to the operation of cyberspace. Whereas the services layer provides the supporting function to cyberspace, but carries no

data itself, the infrastructure layer is defined as the components across which information passes, be they the end points or the connecting nodes. The infrastructure layer is also the most widely dispersed element of cyberspace as it incorporates the different types of cabling through which most domestic and international communication is passed as well as including those devices that users interact with such as Personal Computers (PCs), laptops, tablets, smart phones, wearable devices, and medical implants as well as their associated wireless connectivity. An important consideration of the infrastructure layer is that every aspect is owned and therefore under the authority of an organisation, which may be a government, democratic or otherwise, or a commercial enterprise. This not only gives them control of its availability, but also how content can be filtered, censored, or prioritised and is an increasingly significant issue as the infrastructure itself is now also beginning to be owned by content providers. This has been seen in the case of *Google fiber*, which is being installed in some cities in the US and with promised speeds of up to 1000 megabits per second (MBPS) will be aligned to the company's other services such as *Google Drive's* cloud storage facility and its television service *Google Cast*.[8] In addition to investing in infrastructure within the developed world, the ambitious *Google Loon* project also seeks to connect the two thirds of the world's population that does not yet have Internet access by using balloons floating in the stratosphere to provide wireless cellular access.[9]

The infrastructure layer could be measured in terms of the proportion of the population with access to the Internet representative the potential audience of a message, speed of the network highlighting the capacity for content requiring a large bandwidth and the average time between users upgrading hardware indicating the processing capacity of their computers. The levels of smart phone ownership may also determine content type and the number of Internet Service Providers (ISPs) relative to the population show resilience as does the range of international gateways providing global connectivity. This latter component is significant as the presence of international gateways demonstrate that cyberspace is not borderless and cannot be regarded as some form of 'cloud' in which data passes without impediment and that it may be subject to filtering, censorship or blocking at national borders, which may align to the geographic

layer. As for the services layer, the infrastructure layer is also susceptible to kinetic attack with the physical destruction of components a clear indicator of a successful engagement with replacement and installation of components taking time to complete. If access to the equipment is possible, physical destruction is also the easiest to undertake to achieve an effect due to the complexity and fragility of electronic components. Importantly, this layer also includes connected industrial systems and machinery that are linked to the network, which rather than transferring data to other locations, act as end points to control and manage electro-mechanical systems. Measurement of the success of the attack can be provided by firstly observation of the results of the physical damage and then by recording the period for the equipment to be repaired or replaced. This may take some time if specialist components that are not easily acquired are damaged, or if they are particularly expensive may take time to release the required funds to the equipment manufacturer for their replacement.

Physical layer: This layer incorporates features that are governed by the laws of physics and describes the properties and techniques associated with the transfer of data across the infrastructure layer. These include the characteristics of the electromagnetic spectrum such as the passage of photons in fibre optic cables, electrons in cablings and wireless propagation from a range of systems such as mobile telephony, Wi-Fi, Bluetooth communication, point to point microwave and international satellite links. The physical layer is thus defined as the attributes of the infrastructure layer and how data is transmitted within it. Measurements of this layer involve recording the physical speed and bandwidth of transmissions across the different types of cabling and wireless transmissions. Comparisons could be made between the proportion of a nation that is served by older legacy copper cable connections compared with modern high-speed fibre-optic infrastructure, the number of Wi-Fi hotspots per head of population, type and extent of mobile phone coverage, average data consumption per subscriber and the cost of access compared with average national salary. The physical layer is important for a number of reasons; from a performance perspective, data transfer rates vary considerably depending on the medium in use with a legacy copper telephone line only having a data transfer rate of 100 MBPS compared to a fibre optic link at up to 1 gigabit per

second (GBPS).[10] Furthermore, speed may also be an issue as although faster than copper wiring, transmission through fibre optic cable is slower than a microwave link as the energy travels quicker through air than through glass. This may not be an issue for most users, but within the financial industry it is an important issue in order to serve the requirements of high speed automated trading where knowing commodity prices a millisecond in advance can make the difference in being able to secure a profit.[11] Methods to attack the physical layer should also be considered in assessing the resilience of a system and will vary according to the type of medium used with hardware components susceptible to the same type of damage as for the infrastructure layer. For pure Radio Frequency type transmissions, there are non-kinetic methods available to attack this form of communication including jamming (denial), spoofing (imitating) and hijacking (altering) data, with unencrypted data particularly vulnerable to these latter two methods.

Syntactic layer: This is a measurement of how data is formatted to facilitate communication between and within components of the infrastructure layer and how it is prepared for transmission to remote systems through the physical later. Examples of how the syntactic layer could be assessed include a comparison of the use of older Internet Protocol Version 4 (IPv4) versus the newer Version 6 communication protocols, age of software components and the efficiency of network routing algorithms. The type of software employed can be an important factor as the use of unsupported Operating Systems or applications can introduce well known vulnerabilities that have not been subject to patching and can therefore be very susceptible to attack or exploitation. Measurements of this layer could not only include the use of the latest software, but also the amount and type of encryption routinely employed and the proportion of computers protected by anti-virus software and the proportion of infected machines within a network. This information is readily available through the use of the *GlobalStats StatCounter*, which provides a breakdown by country of the type of Operating Systems and Internet browsers used.[12] *Statista* also provide information relating to the countries with the highest rate of malware infected computers.[13] Information of this type could provide an indication of how susceptible a target nation could be to exploitation of known vulnerabilities or

the amount of pirated software in use that is not subject to developer updates. Research of this type has been conducted by *Rapid7*, a provider of security data and analytics software designed to enable organisations to implement an active, analytics-driven approach to cyber security.[14] Their *National Exposure Index* uses port scanning to infer a country's Internet security posture by measuring the prevalence of clear, unencrypted services compared to similar encrypted counterparts and how this relates to their economic strength in term of their Gross Domestic Product (GDP). The results indicated that there is some correlation between internet connectivity and a region's overall economic strength as expressed by GDP and that where the overall use of encrypted communications is sporadic a league table of their level exposure to exploitation can be derived.

As well as the level of use of secure encryption algorithms, the syntactic layer can also be measured in terms of freedom of access to Internet services and the levels of censorship, content filtering and network prioritisation. This final element is known as network neutrality and refers to the principle of an agnostic network that does not discriminate against the content that travels across it and not give preference to particular applications, protocols, sites, services or users.[15] Attacks at the syntactic layer are within the realm of what nations regard as Offensive Cyber Operations (OCO) against an adversary or by non-state actors and criminals as *computer hacking* and will involve attempts at breaking encryption algorithms to access data not intended to be freely accessed or retrieving data by diverting its path within a network by changing the network configuration within routers to an area in which it can be read. Activity at this level also includes measures to prevent access entirely through the use of Denial of Service (DoS) attacks. This is method of stopping a server from delivering requested information to a genuine client by overloading its capacity to respond with high levels of malformed requests for data. This saturates the capacity of the server thereby preventing legitimate users from accessing its services. A measurement of the strength of a country's syntactic layer to recognise and resist this and other types of cyber-attack can provide an indication of how easy it may be to infiltrate and manipulate the information flows and therefore how successful a campaign of cyberpower directed at its

population may be. This information can be obtained from an assessment of how much is invested in systems to monitor information flows and what capabilities such as Intrusion Detection and Prevention Systems (IDP/IPS) or Security Information and Event Management (SIEM) software are present to mitigate for attacks.

Semantic layer: This layer forms the translation medium between the digital data used for computer communications and the users to enable them to make sense of the information and for it to be beneficial to them. It is therefore an important component in any computer system that involves a human operator to ensure that data can be correctly interpreted and acted upon. The semantic layer typically comprises computer applications and its measurement could include subjects such as the type and popularity of user interfaces, application software, as well as the linguistic, cultural, and human factor considerations employed in their design. These are all related to how a user seeks to engage with others in cyberspace to achieve their desired end state and may involve methods by which operators with different backgrounds can use similar software configured to their own unique needs.

The interpretation of the semantic layer, which provides an output that is useful and understandable to human operators, also acknowledges the specific needs of the end user. As computers become more prevalent in society, interactions that were previously purely mechanical now provide an input to software control systems and this communication also forms part of the semantic layer. An example of this is in transport systems where in some cars the amount by which the accelerator is depressed acts as a digital input to the engine management system governing the speed of the car. The output from the semantic layer in this case is twofold, both the cognitive appreciation of a difference in speed by the driver, but also the visual display from the dashboard speed indicator or audible alarm if the car is equipped with a speed limit warning system. Being software based, the semantic layer is subject to similar attack methodologies as for the syntactic layer and the more complex the application is, the more vulnerabilities may exist that are at risk from exploitation by an attacker. As this layer is designed specifically for human interaction, it can be one of the easiest

to be accessed or reverse engineered by hackers seeking to identify vulnerabilities that have the potential to be exploited. As some types of software become increasingly popular and attract worldwide use, they also become more attractive to exploit as any weaknesses found will have more widespread utility and so will be able to affect a greater number of potential victims.

The semantic layer can be measured by how intuitive it is to users and how much training is required to fully exploit its potential. This refers to both how easy it is for operators to use the software to input information as well as what skills are required to understand its output. The number of users accessing an individual application could also be regarded as a measurement of the influence of both the software itself as well as its developer. Attacking at the semantic layer may aim to achieve several objectives, which may include attempts to deny user access to their data, manipulate it to display erroneous information or exfiltrate it without authorisation for embarrassment, financial gain, or blackmail.

Human layer: Above the semantic component a human layer is added as the incorporation of the user element is considered fundamental to the nature and understanding of cyberspace and cyberpower. This is because the environment is dependent upon the people component as unlike the other environments with which it is often compared; Land, Sea, Air, and Space, it requires human intervention for its creation, maintenance, exploitation and ultimately destruction. The human layer also forms the conduit to the other environments and experiences here may affect how the operators interact with cyberspace and how they interpret the data that they are presented with. Understanding the attributes of the human layer may affect how the semantic layer is designed as it can be easier to alter a software interface once to be more intuitive and better understood by all users rather than retrain each one to be able to configure complex, specialist applications. This layer also presents a major threat to a computer system as it without doubt contains the greatest range of vulnerabilities. Human operators are open to a variety of influences that cannot be totally predicted or prevented such as by social engineering, bribery, and blackmail as well as the normal human traits of error and negligence. Although

the inclusion of security features in the software design can to some extent mitigate these issues at the semantic and syntactic layers, some of the most effective measures to prevent a successful attack are through education and supervision at the human layer. This emphasises the importance of training for users at all levels to be able to engage effectively and safely with cyberspace. Comprehensive education designed to provide an appreciation of the capabilities and limitations of the cyber environment is essential and can affect how attitudes to the technology are formed. For the generation at school today, the so called *digital natives*, their familiarity with the use of smart phones and social medial applications demonstrates the success of those designing the semantic layer to be intuitive and requiring no formal instruction to be effectively used. More worrying though is that those same users may not understand the importance of the security settings of these same applications, how encryption protects them, or indeed how to develop their own software and computing applications to suit their own unique requirements. The UK has struggled to provide sufficient teachers with the right skills to be able to deliver the computing curriculum and have realised that those who provide courses in Information Communication Technology (ICT), may not have the skills to teach computing science.[16] This is because the ICT syllabus only applies to the semantic layer, whereas computing courses tend to concentrate at the syntactic and is regarded as a separate subject for the teaching profession.[17]

The addition of a human layer, although it usually refers to an operator's interaction with the environment, also predicts a greater integration between technology and people in the future. User interfaces with cyberspace have moved from static hard-wired computers to mobile smart phones connected wirelessly through cellular networks or via Wi-Fi directly to Internet routers. 2015 saw the introduction of the Apple Watch and the next generation of wearable connected devices that have moved from being just a novelty item used by first adopters to becoming more practical and useful devices. The next logical stage in this development has already been mooted as being implants in which users have devices inserted into their bodies and interact directly with them. Examples of this have already achieved significant publicity due to the research of Kevin Warwick, former Professor of Cybernetics at Reading

University and now Deputy Vice-Chancellor of Research at Coventry University, who has been implanted with a number of devices enabling him to control external devices.[18] As an active area of research, the border between humans and cyberspace are predicted to become increasingly blurred as more methods are designed to connect the two and new ways to harness the potential of these developments are proposed.

Mission Layer: As a final addition to this expanded model of cyberspace, a capstone mission layer is included. This emphasises that cyberspace was designed and created to fulfil a specific purpose and is not a naturally occurring phenomenon. Every interaction within cyberspace, whether conducted by a person or automated function has a specific intent and consequence, whether intentional or unintentional, innocent, or malevolent. By specifying and highlighting the aim of an activity at the top of the model, the role of the layers below can be better understood and contextualised. It is important to appreciate that the mission layer itself is distinct from the other seven layers and refers to the context in which the medium is used and is not part of it. Although adjacent to the human layer, it is not directly associated with any human operator as not every activity in cyberspace requires human interaction. For example, a remote Industrial Control System (ICS) monitoring system may only utilise the layers from services to syntactic, but the mission layer can still be considered in the role performed by these lower four layers. Unlike the other layers, it is not subject to measurement or attack, but purely states the purpose that the levels below are contributing to. However, that is not to say that the mission layer cannot be manipulated – external factors may inspire users to engage with cyberspace in new or previously unforeseen ways. For example, an advertising billboard with a Quick Response (QR) code, may encourage a user to scan it with their smart phone with the aim of finding out more about the product shown illustrating the close relationship between cyberspace and the physical environments.

When viewing cyberspace as a series of layers, cyberpower can be described in terms of who has control of each one, noting that power over one layer does

not result in governance of all. Cyberpower may be exerted either over a range of layers or by targeting only one, however the aim is always the same, that of obtaining preferred outcomes through use of the electronically interconnected information resources of the cyber domain. The ability to measure one or a range of variables of the layers affected by a cyber power could be used to produce a comparative index of their power over others. These could then enable a relative position against an economic competitor or military adversary to be calculated. Specific areas that are revealed to be comparatively weak can then provide an indication of where additional effort needs to be concentrated to improve performance. An important consideration of the layers of this model is that although when combined they make up the constituent components of cyberspace, each one should be considered in isolation and that they are not necessarily intended to represent information flows from infrastructure to human layers. Thus, the borders between them may or may not be significant and indeed could have several components depending on the system being considered. There may also be circumstances in which some layers can be disregarded. For example, a self-contained and internally regulated Industrial Control System may not have a direct semantic or layer, but may be accessed indirectly through the syntactic element of a separate system that does have a human operator monitoring the system. Also, using the definition of cyberspace from chapter 2, there is no requirement for every system to be directly connected to the Internet, which may limit the definition of the physical layer to that of purely an internal network using a bespoke or commonly used Internet based communication protocols.

Adding a second dimension to the model of cyberspace

In addition to defining cyberspace in terms of the eight vertical layers, it can also be considered horizontally. A second dimension to the model of cyberspace adds a representation of distance, which increases its utility and the range of scenarios that can be investigated. The key advantage of being able to include a concept of horizontal separation between different users is that it enables the layers to be considered separately in terms of the properties of each location. To put perspective on the model, the terms of *near*, *mid*, and

far geographic operating space are used. These are described in table 4 and are based on those first publicly described in the UK Ministry of Defence's *Cyber Primer*.[19]

Environment	Description
Near Space	At a national level these are networks and systems that are considered vital to support critical national infrastructure and services and are assumed to be controlled and protected by governmental agencies. At a local level, this is the element of the network that is owned and configured by users and on which they exercise control on the type of software and devices that are installed and used.
Mid Space	These are defined as networks and systems critical to access global cyberspace but over which there is no local control or protection. Typically, these may be geographically distant and owned by a foreign commercial company or a third-party state.
Far Space	The networks and systems that, based on intelligence gathering operations, are assessed as comprising a competitor or adversary's near space. This is the target area that must be influenced or controlled, either temporarily or permanently as part of a campaign to project power and influence through cyberspace.

Table 4: Horizontal components of cyberspace

As near space defines the networks under local control, this is the area in which one's own cyber security efforts are concentrated. To achieve this, it is vital that there is a comprehensive understanding of the network infrastructure and the users who are active in it. From a national perspective, control of the near space is vital to protect the security of national or local interests from attackers and those who would wish to illicitly infiltrate it. In this two-dimensional model, an adversary or competitor also have their own near space with similar properties that needs protecting and which from the perspective of others is termed far space. However, it must be noted that the properties of far space are viewed and assessed remotely from the perspective of another's near space and that its composition is either derived from intelligence gathering operations or from what information is made publicly available. There may thus be a difference between the understanding of what far space consists of and the actual composition of an adversary's near space in cases where overall visibility is

lacking or intelligence is incomplete or not correctly interpreted. The area in between near and far space, which is under the control of a third party, is termed mid space and within the context of power projection represents the distance that must be crossed to reach the target network.

Protection of near space can be defined as being within the realm of Defensive Cyber Operations (DCO). This is defined by the UK Ministry of Defence in the second edition of their Cyber Primer as *Active and passive measures to preserve the ability to use cyberspace*.[20] Activity against an adversary in far space is the remit of Offensive Cyber Operations (OCO), described from the same source as *Activities that project power to achieve military objectives in, or through, cyberspace* and aligns to the notion of using cyberspace as a means of power projection.[21] NATO use slightly different interpretations of the terms and in drawing on a US source identify DCO as *Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems*.[22] This is significant as it refers to activities outside the defended network, which may have legal implications and be seen as escalatory by an attacker. In comparison, NATO's definition of OCO is also drawn from a US source and is very similar to the UK's in being *Cyberspace operations intended to project power by the application of force in or through cyberspace.*[23] Both organisations thus regard Offensive Operations in cyberspace as being associated with power projection, the subject which is at the core of this thesis.

A key aspect of OCO is an analysis of an opponent's strengths and weaknesses, which when based upon an understanding of far space can provide information on possible attack vectors that can be exploited to reduce their overall influence and ability to operate freely in cyberspace. This can be used to illustrate that although cyberpower may be exercised in some elements of the domain, it does not guarantee control of all and that some techniques targeting individual aspects may only have a limited overall effect against an adversary. The use of this model also enables attacks to be appreciated in

terms of their intended areas of effect and for the defender an understanding of where the greatest risk to their organisation lies.

Although others have also sought to demonstrate that cyberspace has a distance element, previous work has not also combined it with the layered model and have concentrated on showing growing global connectivity and routing paths. This is exemplified in the *Opte* Project, which produces dramatic graphics showing the Internet as a constellation of networks that have been displayed as works of art.[24] By combining the eight vertical layers with the three horizontal components of cyberspace, it is possible for the environment to be illustrated in a new way in two dimensions as shown in figure 2. It is important to note that this model may not necessarily be regarded as a map through which a path through cyberspace can be traced. Instead, each element of the environment should be considered as a separate, discrete entity that needs to be considered individually. This enables an appreciation to be made of the cyber landscape between a source and destination and highlights any unintended consequences that may arise from their use as part of a power projection plan. This analysis may provide an assessment of whether there is a threat to one's own near space from an adversary or to highlight weaknesses that can be exploited in far space that may provide an attack vector through which an effect can be created. As part of this assessment process, it may be determined that an element that presents no threat or cannot be exploited can be disregarded, or it may be concluded that it is the vital component over which both attacking and defending elements will compete for overall dominance. Control of both the vertical and horizontal layers of cyberspace is therefore fundamental to enable power and influence to be exerted. Of course, not all attempts to exert power are in far space and it may be that there is a requirement to direct a campaign within a country to target an internal population in near space. As an ability to effectively translate cyberpower into an effect in the physical domain requires a clear understanding of what objectives are desired and how success or failure can be determined, any national cyber strategy must be fully coherent with broader governmental policy. Cyberspace and cyberpower also do not exist in isolation and any

actions must be coherent with wider political objectives and an overall campaign plan.

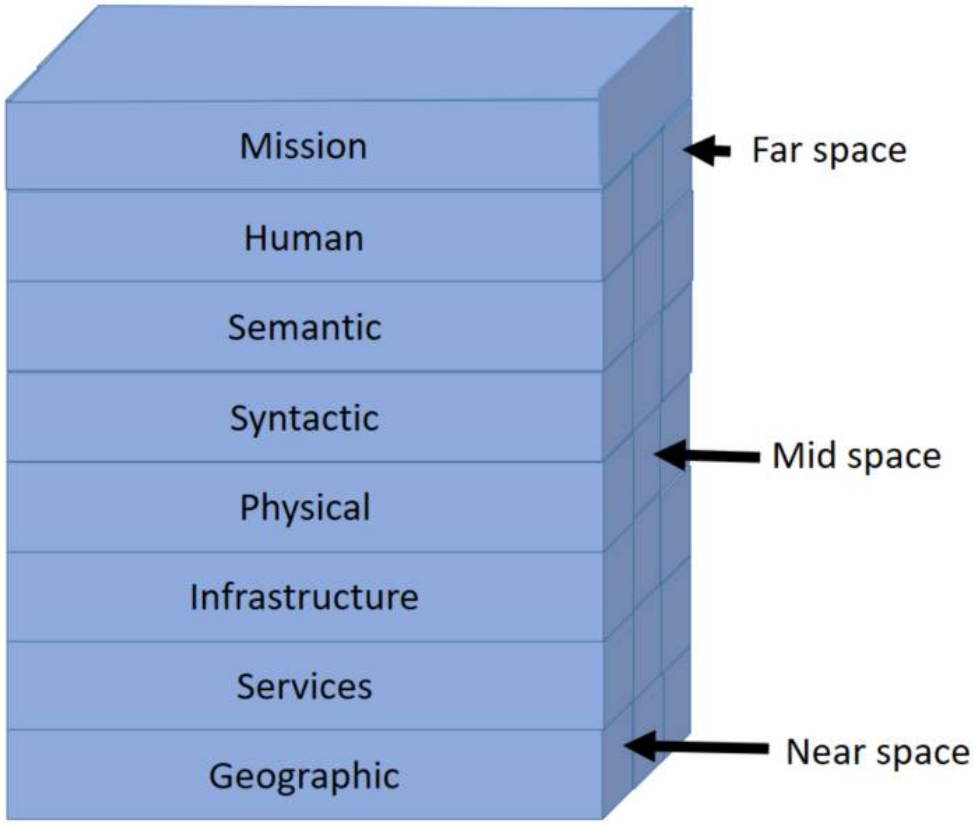

Figure 2: Two-dimensional model of cyberspace

To demonstrate how the model of cyberspace proposed in this chapter can be applied in practice, table 5 illustrates how each component can be defined in terms of a national government's strategy to use video clips on social media to influence European-born Jihadists who have travelled to the Middle East to return to the West. In this case, the targets have been identified as predominantly using mobile telephony and are active on a variety of social media platforms. Of note is the inclusion of hacktivists from the *Anonymous collective* operating in mid space who have been active in the disruption of extremist media platforms through their *#OPIsis* campaign and need to be considered as part of the assessment process.[25] Both the source and destination locations are based in the land environment with the passage between them in mid space utilising land and undersea fibre cables. Cost,

bandwidth, and latency limitations would probably preclude the use of satellite communications in the air and space environments.

Layer	Near Space	Mid Space	Far Space
Mission	Persuade UK born Jihadists to return home		
Human	Government employee	'Anonymous' hacktivist	European born Jihadist
Semantic	Video production software	Routing software	Social media application
Syntactic	MPEG-4 video format	Transmission Control Protocol (TCP)/ Internet Protocol (IP)	MPEG-4 video format
Physical	Electrons in Ethernet cable and light in fibre-optic cable	Light in fibre-optic cable and radio frequency communication within satellite and microwave links	Radio frequency communication within mobile telephone networks
Infrastructure	Video production suite, desktop computer and Local Area Network	Microwave and satellite link, fibre-optic undersea cable and ISP infrastructure	Mobile telephone network and smart phone
Services	UK infrastructure assessed as reliable and guaranteed	Routing unknown, but infrastructure assumed to be reliable	Intermittent, locally generated power supplies considered unreliable and subject to failure
Geographic	Land environment	Land and Maritime environments	Land environment

Table 5: Illustrative example of the role of the components of cyberspace

A key strength of this model is its ability to express each component of cyberspace separately in a discrete way. This emphasises the requirement that for any power projection campaign to be successful every element must be considered. This in turn may highlight potential issues that may prevent an individual activity from successfully delivering its message to the intended audience. In the example given in table 5, noting that far space is only believed

to be accessed via mobile devices with an intermittent power supply, it would suggest that messages would have to be short and optimised for transmission over a telephone network and that bandwidth limitation and download costs should be considered. Similarly, the format in which the message is produced must be compatible with and be comfortably viewed on a smaller screen with perhaps a lower resolution than that from which it was produced. This would require background knowledge of the types of device in common use in the area in which the target audience lives.

This model of cyberspace also enables its components to be regarded in new ways. Figure 3 illustrates the model with the elements in which data resides highlighted. Whereas other models may specify data as a dedicated layer, figure 3 illustrates how it permeates through five layers, any of which may exhibit a vulnerability that can be exploited or used to prevent the passage of information. At rest, it is stored in hardware devices in the infrastructure layer and is transferred between locations using the attributes of the physical layer. Identifying the geographical location may offer options as to how it can be kinetically targeted as will a knowledge of whether it uses wireless rather than a cabled routing. Protocols in the syntactic layer, which may be subject to exploitation, encapsulate the information and route it from source to destination. After passing through an application at the semantic layer and depending on the purpose of the process as specified at the mission layer, it is viewed by a human, which can also reveal methods by which an attack can be tailored to the unique attributes of the end user. Although the services layer is primarily utilised in facilitating and supporting the activity in the layers above, it is even possible that it will be involved in the production of data or require its processed output if it is part of an industrial control system. The role of boundaries between near, mid, and far space should also be considered as shown in figure 3 where a firewall offers protection. This provides a graphical representation of the weaknesses of a firewall as only being able to protect in this situation the semantic, syntactic and infrastructure layers and leaving the physical and human layers at risk.

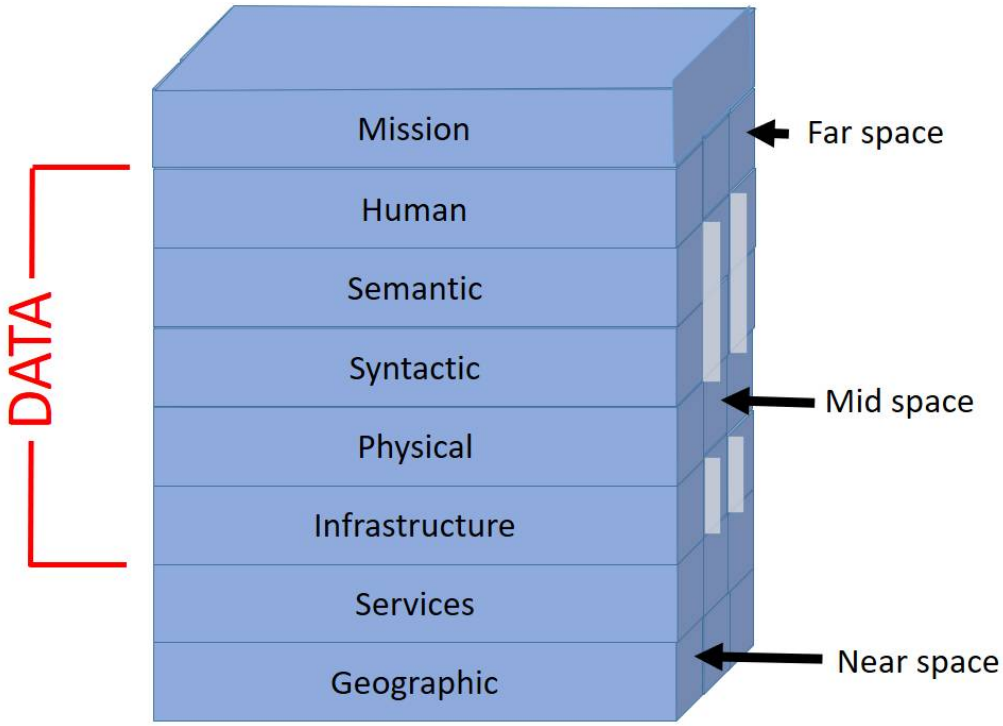

Figure 3: Two-dimensional model of cyberspace illustrating location of data and areas protected by a firewall

Analysing the threats to data at each level can provide a useful method of vulnerability analysis as shown in table 6 below, which details some generic risks to information security. By tailoring this process to each individual circumstance, it would be possible to determine where additional security measures may be required or from an attacker's perspective, which level may offer the highest likelihood of success of compromising a system.

Layer	Risk to data	Protected by Firewall
Human	Social engineering attack Human error	No
Semantic	Malware	Yes
Syntactic	Fake access points	No
	Network traffic redirection	Yes
Physical	Passive packet sniffing on wired or wireless networks	No
Infrastructure	Hardware theft	No
	Malware	Yes

Table 6: Indicative risks to data at each layer of cyberspace where it resides

Adding a third dimension to the model of cyberspace

From the two-dimensional model of cyberspace, a third element can be added to illustrate how a campaign of power projection can be planned through the spectrum of soft, hard, and smart power across cyberspace from source to destination through near, mid, and far space. This is significant as there can be major differences in the techniques used in soft or hard power projection. Soft power involves the dissemination of a message of persuasion and attraction to an individual or group, whereas hard power involves communicating coercion or intimidation. It is possible that this could utilise the same media as soft power, although the content may be less welcome, but it could also involve the transmission of malicious software code, termed *malware*, aimed not at a human target, but at a computer or Internet connected computing device. Figure 4 illustrates the now three-dimensional model showing how soft, hard, and smart power can be considered within each aspect of the model. In planning such a campaign, due consideration of each element may result in the conclusion that one type of power projection may not be appropriate or practical considering the nature of the route and attributes between near and far space. This analysis may assist the planners in deciding which strategy has the greatest chance of success and may influence the entire operation's objective. It should also be noted that the third dimension of the model does not extend to the services, mission, or geographic layers. This is because the services layer supports the entire cyber environment and is agnostic to its use or the type of data that is transmitted and the single mission statement that determines the overall purpose of the campaign of cyberpower projection. Although the geographic layer may affect the structure of cyberspace and how data passes across it, it also does not affect the content of the information or how it is interpreted.

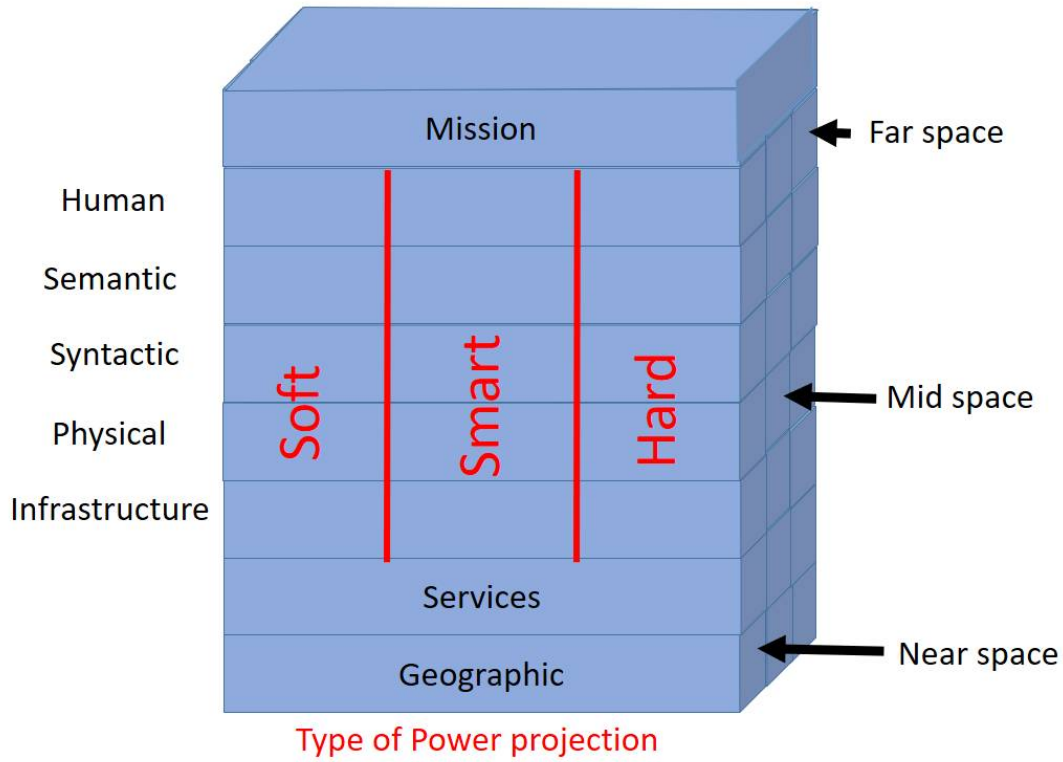

Figure 4: Three-dimensional model of cyberspace illustrating how soft, smart, and hard power can be considered in a campaign of power projection

Validating the model - Qualitative analysis of cyber-attacks

This section comprises two subsections. The first subsection seeks to characterise a cyber-attack as comprehensively as possible in terms of six discrete attributes that have for the first time been selected to provide an index of the sophistication and effect of the attack methodology. In the second subsection thirteen well publicised cyber-attacks that occurred in the land environment from 2007 - 2017 are evaluated by qualitative textual analysis in terms of these six attributes. This enables an assessment to be made of how they were reported in relation to the proposed new model of cyberspace in terms of levels of complexity. The output from this examination is then used to provide a relative measurement of the correlation between the levels of sophistication required to achieve an effect at the different layers of the model of cyberspace. The examples of cyber-attacks that have been selected have been classified on a scale of increasing complexity against the layers of cyberspace that they targeted, which together provides the ability to produce a graphical comparative scaling of the attacks. Sophistication is measured in

terms of the following six characteristics, which have been selected as they are considered to comprehensively describe a cyber-attack in terms of; persistence, propagation, novelty, precision, impact, and attribution, and are described below. These characteristics enable a differentiation to be made between types of attack and the effect it has on the target. The selection criteria are based on there being sufficient open source information for each attribute with enough expert analysis being available on each one to allow an overall assessment and score to be made.

Persistence is measured in terms of how self-sustaining an attack is with, for example a Denial of Service (DoS) attack that requires continued action from an attacker to be effective scoring less than a virus which requires human action to propagate, which scores less than a self-replicating worm that once delivered requires no further originator or target interaction to penetrate and spread through a victim network. A DoS attack is an intentional activity with the explicit aim of denying authorised users legitimate use of an information system. Typically, this involves an attacker generating more Internet traffic addressed to the target than it can handle resulting in it either shutting down or being sufficiently overloaded such that it cannot respond to genuine requests. When multiple attackers are targeting a single address, this is termed a Distributed Denial of Service (DDoS) attack and has the potential to be more effective as increased traffic can be generated from a range of source locations making attribution of the original source of the attack more challenging.

Propagation is measured in terms of how much effort is required to deliver the payload, with a successful attack on a system that is not linked to the Internet scoring higher than one that is more easily accessed through a connected machine. Similarly, an attack that is directed at a system that has higher protection such as a military or industrial system is rated more highly than a civilian public facing infrastructure.

Novelty is a measure of the uniqueness of the technique employed by the attack payload and the amount of effort that has been expended in its development. The use of previously unknown vulnerabilities, known as *Zero-*

day exploits as there is no known mitigation for them, scores particularly highly due to their exclusivity. Zero-day exploits are very valuable commodities for criminals as because there are no methods to detect or mitigate for them, they provide a more assured means to attack a system without being detected or blocked. Because of this, they can command high values on underground Internet forums, although once they have been used and recognised by the developers of the targeted software their value decreases after they have been reverse engineered and a patch is released to mitigate their effects. It is for this reason that the use of unsupported software applications is not recommended as vulnerabilities that have been identified and exploited will not be patched and could continue to be used.

Precision and accuracy is an indication of how discrete the attack is in achieving an effect against a specific target. This considers the level of collateral damage against other non-targeted systems or people and to what extent the timing of the payload being effective can be determined. An attack that has been focused to achieve a specific effect on a unique target at a precise time scores more highly than a general widespread attack with no control of timing or target as it indicates either the complexity of the objective or a concerted desire to reduce collateral damage. Additionally, more complex attacks require a greater effort to gather intelligence on the target and will take longer to develop, yet because they have a more limited wider utility is indicative of the level of financial investment that the attacker is willing to expend on compromising a single or small number of victim systems.

Impact is a measurement of the effectiveness of an attack, which can be determined by its psychological value as well as the actual effect it has on the target. Impact can also be measured in terms of the temporal effect of the attack depending on whether it is either temporary or permanent. This scoring is also influenced by the publicity the attack generated and by the assessment of cyber security commentators of the importance of the event. However, attacks may also score highly in circumstances in which the precise details of how the attacks were conducted were not released to the public domain, but generated comment and publicity due to the nature of the techniques used.

Attribution is the ability of the target of a cyberpower campaign to be able to accurately and with confidence identify its source. Although it may be that the originator aims to make its identity clear, this may not always be the case, particularly if it might be regarded as an illegal act that may result in retaliatory action. In disguising its origin, the perpetrator may seek total anonymity or attempt to imply that they are from another group or country for either deliberately political purposes or to confuse the investigative process – so called *false flag* operations. The scoring index used will depend upon the mission of the cyber-attack, although generally the greater the anonymity achieved, the higher the rating.

Each of these six attributes of a cyberattack are individually assessed to gauge the sophistication of the techniques used to achieve an effect, which are shown in table 7 below. The attributes are further divided to highlight the level of complexity used and the severity of the effect achieved with a scoring scale of 1-4 to show increasing sophistication enabling more advanced methods to be recognised and credited. Thus, an attack using readily available open source tools and methods would score less highly than a bespoke, highly targeted payload using zero-day vulnerabilities and a tool developed specifically to target a uniquely identified victim would score more highly than a generic tool over which there may be less control over its effect. Attacks on targets that are also more challenging to reach, such as military systems not directly connected to the Internet would also score more highly than a public facing web site compromise and the level of attribution is also recognised with high levels of anonymity achieving a higher rating. By giving each technique within each criterion a unique score, different attacks can be compared using the same scale, which provides a more rigorous methodological assessment than relying solely on expert option.

Score	Criteria					
	Persistence	Propagation	Novelty	Precision and accuracy	Impact	Attribution
1	No executable used	Public facing web site	Open source technique	No control over target and time	Open source technique continued activity needed	Attribution declared
2	Denial of Service attack	Target Internet connected	Scripted attack using toolkit	No target control, time specified	Bespoke technique continued activity needed	Attribution suspected – civilian actor
3	Virus/Trojan	Civilian target not connected to Internet	Single zero day vulnerability	Unique target no time control	Temporary effect	Attribution suspected – state actor
4	Worm/recode	Military target not connected to Internet	Multiple zero day vulnerabilities	Unique target and time specified	Permanent effect	Total anonymity

Table 7: Grading criteria for cyber-attack sophistication

Using the criteria outlined in table 7, the selected cyber-attacks have been characterised in terms of the layers of the model in which they were active, either as the means to compromise a system or to illustrate the layer affected by the activity. Table 8 on pages 112-114 shows the results of this investigation and while it is acknowledged that these have all taken place in the land environment and that other attacks have taken place before and since, these were selected for their significance in terms of the publicity that they generated and the level of analysis of the methods involved in industry and academic literature. By drawing on these sources and an examination of the methods used, it has been possible to assess the level of sophistication of the attack in terms of the layer of cyberspace targeted. It should also be noted that in this example the scoring criteria that have been chosen has reflected the types of methods used and it is accepted that in future should new methods of attacking computer systems be developed or a single element become more prominent that that these factors could be reassessed and their scoring realigned. In acknowledging that table 8 is a predominantly qualitative assessment of the sophistication of the attacks and that data has been drawn from a range of textual sources, figure 5 on page 115 illustrates this information graphically

indicating the overall relative sophistication of the attacks and the layers of cyberspace that they affected.

As can be seen from figure 5, there is a general trend that indicates that a less complex and technically challenging approach is often required to attack the human and semantic layers with the syntactic, infrastructure and services layer requiring a more complex approach. This is believed to be due to the upper layers being designed to be more readily accessible by users and so requiring less effort to understand their configuration to achieve a successful compromise. The human targets themselves are not only easier to access, but may also be more susceptible to external influence and change than programmed technical components, which only have a limited range of responses to the range of possible inputs. Creating an effect on the layers that are not designed for direct human interaction such as the syntactic, infrastructure, physical and services layer can be concluded to be a more complex undertaking. This is because it involves creating an effect contrary to that envisaged by the designers of the system and so requires a greater understanding of their underlying architecture and configuration. Within the graphic, a further characteristic of these attacks is indicated with those marked with a hashed, rather than solid background highlighting those events that are suspected of being conducted by state actors, rather than individuals or hacktivist groups. This also demonstrates that those with the greatest resources, both monetary and in terms of expertise are capable of more sophisticated activity and the ability to interfere with the lower levels of cyberspace. This may be the case for a number reasons; the first of which is that with greater sophistication, a more covert attack may be conducted, which would be a preferable course of action for state actors attacking other nations. Also, by employing superior resources it is possible to invest more in understanding the nature of the target, which may reveal additional areas that could be open to attack. Finally, after investing in a complex, but successful attack vector, states may wish to reuse elements of the code against other targets, which has been seen in the similar techniques used in Stuxnet, Duqu and Flamer. Non-state actors, with more limited resources, can be seen to limit their attacks to a single target, perhaps as they were then identified and

arrested or that the lower levels of complexity used in their efforts were easier to identify and mitigated by system patching or the deployment of other countermeasures. Of interest is the final example given in table 8 in which the *Wannacry* worm exhibits a combination of techniques from different sources. This is due to it being part of a leaked set of tools developed by the US National Security Agency and exposed by a hacking group known as the Shadow Brokers, which enabled it to be combined with the ransomware code and released to the Internet.[26]

It can also be seen that whereas the less sophisticated attacks caused more superficial or temporary effects, to achieve permanent damage tends to require a more complex approach requiring resources that may be only available to state actors. An attack designed to cause physical damage to a specific component or system will also have to be more carefully targeted to reduce collateral damage and limit the effect only to the intended system. However, if it is determined that should a physical effect be desired and that an attack on the lower elements of a network will require too great a degree of preparation and planning, an alternative strategy may be considered more effective. Depending on the circumstances, it may be determined that after analysing the route through cyberspace from source to destination that the most timely, economical, and effective way of achieving the desired effect will be to plan to attack the target using conventional kinetic munitions, rather than by cyber means. However, a decision in weighing up the strengths and weaknesses of the different options can only be made after a thorough intelligence led analysis of the target is undertaken and this process can be aided by assessing its properties in terms of the desired effect to be achieved through an investigation within the context of the new model of cyberspace and the methodology described above to determine the sophistication of an attack.

Name and date	Layers active	Sophistication					
		Persistence	Propagation	Novelty	Precision	Impact	Attribution
Estonia - Denial of Service attack[27] [28] 2007	Semantic Syntactic	2	1	1	4	1	3
	Coordinated Distributed Denial of Service (DDoS) attack on the public facing web sites of Estonia's national infrastructure through Near, Mid, and Far space.[29] The attack, although large scale, used relatively unsophisticated methods and was launched across the Internet at the Syntactic layer. Although it created considerable publicity, it was relatively short lived with limited long-term damage. Although not proven, this attack is thought to have foreign state acquiescence. Total score = 12						
Aurora[30] 2009	Semantic	3	2	3	3	3	3
	Targeted malware attack against Adobe and Google through Mid and into Far space. Thought to be state sponsored against at least 30 companies and employed a previously unknown zero day vulnerability in Internet Explorer at the Semantic layer that enabled computers to be controlled and data exfiltrated.[31] The effects of this attack were eventually neutralised with a browser and anti-virus update. Total score = 17.						
Stuxnet[32] 2010	Infra Syntactic	4	3	4	3	4	4
	Highly sophisticated malware suspected due to its complexity to be state sponsored, which is believed to have targeted particular industrial control systems in Far space that could not be directed accessed via the Internet. It utilised an unprecedented number of previously unknown Microsoft vulnerabilities and included deceiving the Human Computer Interface of the monitoring system. Total score = 22.						
Duqu[33] 2011	Semantic Syntactic	4	2	3	3	3	4
	Suspected state sponsored Stuxnet like malware that targeted the Windows Operating System through an infected Microsoft Word document at the Semantic and Syntactic layers with the purpose of information theft in Far space. Sought information regarding industrial control systems and exfiltrated the data back through Mid space to the originator's Near space. Total score = 19						

HBGary attack[34] 2011	Human Semantic	1	1	1	4	3	1
	Attributed to the Anonymous collective.[35] Relatively unsophisticated attack using a combination of social engineering and open source techniques against a content management system containing known vulnerabilities to exfiltrate sensitive data and conduct a Denial of Service attack. Total score = 11.						
Flamer[36 37] 2012	Syntactic	3	2	3	4	3	4
	Although unrelated and also affecting the Windows Operating System, in this case fully patched Windows 7 systems, Flamer had a complexity and similarity to both Stuxnet and Duqu. Unattributed, but thought to be state sponsored due to its complexity, this cyber espionage toolkit targeted Eastern Europe and Middle Eastern countries to exfiltrate information and data from a wide range of targets in Far space back through Mid to Near space. Total score = 19.						
Shamoon[38] 2013	Infra	4	2	2	3	4	4
	Highly targeted and widespread attack in Far space on the critical infrastructure of Saudi Aramco by means of a self-replicating worm that deleted data and rendered computers unusable. Thought to be state sponsored. Total score = 19.						
Advanced Persistent Threat (APT) 1[39 40] 2013	Semantic	3	2	2	3	3	3
	Widespread suspected state sponsored industrial espionage of western commercial enterprises in Far space. Initiated though a spear phishing campaign to entice a victim to download malware using complex and well organised procedures to compromise Semantic layer to access data. Total score = 16.						
ISIL campaign[41] 2014	Semantic Human	1	1	1	1	4	1
	Non-state sponsored campaign through social media in Mid space targeting domestic and western media using material of high production quality to publicise activities, encourage supporters and intimidate adversaries. Total score = 9.						

Sony attack[42 43] 2014	Semantic Syntactic Infrastructure	4	2	2	3	4	3
	The origin of this attack on the Sony Corporation is the subject of considerable debate, but resulted in the exfiltration and publication of sensitive data and permanent damage to storage devices causing commercial embarrassment and financial loss. Possibly state sponsored. Total score = 18.						
Juniper Firewall[44] 2015	Syntactic	4	2	2	4	2	4
	Backdoor software discovered in Tech company Juniper Networks NetScreen Firewalls enabling encrypted traffic to be read and administrative access to be gained. Patches released by Juniper to correct this suspected nation-state attack. Total score = 18.						
Talk Talk[45] 2016	Semantic	1	1	1	4	1	2
	Relatively unsophisticated non-state sponsored breach of Telecommunications provider's website database using a 'blind SQL injection' to exploit a vulnerability in a web page video. Total score = 10						
WannaCry[46] 2017	Syntactic	4	2	3	1	4	3
	Based on suspected NSA code leaked by a group of hackers known as the Shadow Brokers, this self-propagating ransomware worm exploited an unpatched vulnerability on the no longer supported Windows XP Operating System to encrypt user files including documents, images and videos, demanding payment in bitcoins for the decryption key. It also attempted to access SQL server databases and Microsoft Exchange data files. Within four days it had hijacked over 200 000 computers in 150 countries. Total score = 17						

Table 8: Characterising cyber attacks

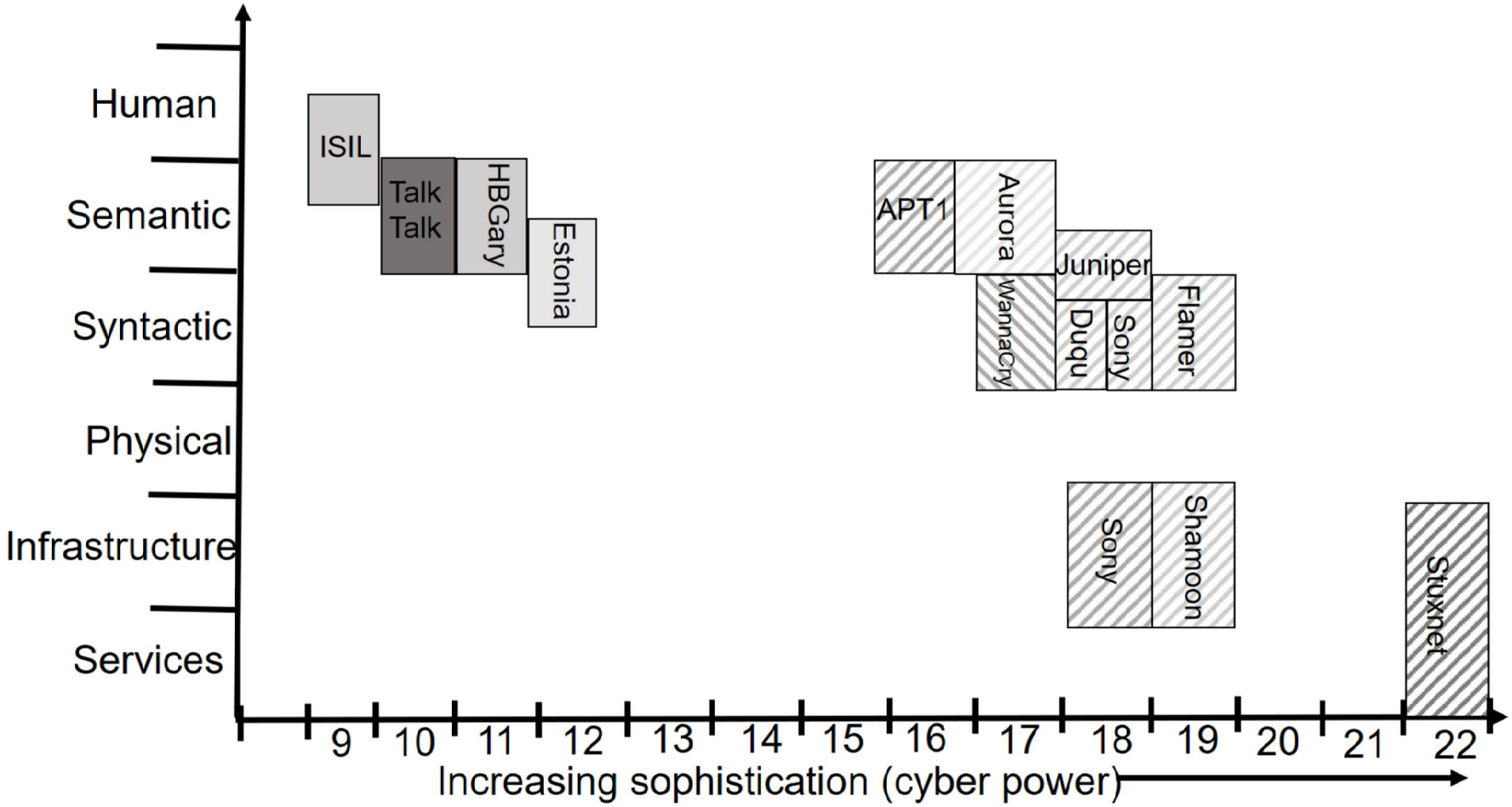

Figure 5: Graphical presentation of the sophistication of a range of cyber-attacks against the layers that they targeted

Conclusion to chapter 4

This chapter fulfils the initial objective of this thesis by introducing a novel three-dimensional model of cyberspace. The design of the model is optimised to better understand how its properties and attributes can be measured in terms of its ability project power and to demonstrate that the environment does not exhibit universal characteristics but that its structure and use may differ at the source and destination of a cyberpower campaign. This model adds an additional degree of complexity compared to previous attempts to describe cyberspace in that it includes a range of attributes not previously considered and rather than just provide a description of the components of the environment, it offers way in which they can be measured. As cyberspace and its foundation networks have developed, new and innovative ways have been developed to explore its potential. Initially, the environment was described purely in terms of the network and how it was used to transfer data from one computer system to another. This explanation was later expanded to include the properties of the network, but did not include an appreciation of the geographical factors, services providing the supporting functions, the human user and the purpose of engaging with cyberspace.

A key element of the chapter's investigation is that it has built on the well-established and recognised of work of those who were the first to have characterised cyberspace in terms of layers, each of which perform a distinct function. The advantage of this means of describing the medium is that it has enabled the properties of each one to be considered in isolation in terms of the specific role that they play in enabling information to reach the intended target in the right format and how developments in the technology and use of cyberspace has led to an evolution in their use. By separating the elements of cyberspace into distinct layers it enables an assessment to be made of the properties of each and how they contribute to the overall functioning of the medium. It also enables these attributes to be characterised and measured and for the first time enables a comparison to be made between different areas of cyberspace to determine which are better able to provide a high capacity,

secure and resilient capability to transfer information. This understanding of the properties of cyberspace at different geographical locations enables a campaign of cyberpower to be planned to ensure that the most effective methods are used to reach and influence a target audience.

The introduction of the notion of distance using the concepts of near, mid, and far space to add a second dimension to the model emphasises that not all aspects of cyberspace are under the control of the originator of a message. It also highlighted that the environment at the destination in terms of bandwidth, language, equipment used and availability of service may be very different than at the origin of a communications channel. This model of cyberspace could thus be used at the planning stage of an offensive cyberpower operation to identify aspects that could prove problematic in being able to access the planned audience and highlight alternative strategies. Similarly, in a defensive operation this model could identify areas where the local network could be open to exploitation by an adversary. The inclusion of the third dimension emphasises that the use of cyberspace for power projection may vary depending upon the characteristics of the medium at the point where the target accesses the message, but also takes into consideration the nature of the target themselves and the type of message to which they may be most receptive.

By illustrating the utility of the model through the qualitative analysis of a range of cyber-attacks, it has been shown to be a valid method of abstracting the complexity of cyberspace in terms of the unique set of attributes of each of the six layers through which power is applied. In addition to determining the usefulness of this method of describing cyberspace, a key conclusion of this method of analysing attacks has been to emphasise and confirm the difficulty in attacking the lower levels of the model and the differences in the effects that can be achieved on the target. At the higher levels, where more user interaction takes place at the human and semantic layers, it appears to be easier to achieve a successful system compromise and so is a favoured target of individuals and hacktivist groups. This is due to these layers having been designed to be engaged with and that the more user friendly and accessible they are, the more straightforward they are to attack. At the base levels, which

are designed only for system to system communication, it is harder to achieve a successful system infiltration and so becomes the realm of well-resourced state agencies to attack, for which ensuring a covert comprise is more of an issue. However, it should also be noted that the returns that can achieved from attacking at this level may be greater as it is closer to accessing the infrastructure layer where the system data, which may be the ultimate target of an attack, is stored. Attacking at the higher levels may be easier, but there are more layers to then transverse to reach the core of the system target. This knowledge can be further applied in a third dimension by considering separately how hard, soft, and smart power methods could be projected through the different layers. This would seek to examine how hard power techniques of system damage could be achieved when compared to the soft power strategy of seeking to influence the users. By comparing the ease by which these different attack methodologies could be achieve may ultimately determine which means of power projection stands the highest chance of success or will achieve the greatest impact on the target.

This novel method of examining cyberspace and how it can be exploited to affect the behaviour of a target audience offers a powerful new way to deepen our understanding of the environment and enables strategies to be developed that can estimate the chances of the success of a campaign of power projection in a range of scenarios. The next chapter starts to address the issues raised by the second research objective by investigating the close relationship and interdependence between the maritime and cyber environments within the context of power and security. This research leads to the new concept of maritime cyberspace that combines the properties of cyberspace identified in this chapter with an examination of the attributes of the maritime. This is significant as cyberspace is usually regarded in isolation, but in considering the properties of both, it lays the foundation for a more specific, nuanced analysis of how the characteristics of both can be harnessed as a means of power projection and the security issues that need to be considered to defend against the actions of adversaries.

Endnotes to chapter 4

[1] Libicki, M. C., 2009. *Cyberdeterrence and Cyberwar,* Santa Monica, CA: RAND Corporation. p.12
[2] Ibid. p.12
[3] Sheldon, J. B., 2011. Deciphering Cyberpower. *Strategic Studies Quarterly,* Issue Summer, p.98.
[4] Ibid. p.99.
[5] Balandin, A. A., 2009. Chill Out. *IEEE Spectrum*, 1 October, pp. 34-39.
[6] Strassmann, P. A., 2009. *The Internet's Vulnerabilities are built into its infrastructure.* [Online]
Available at: http://www.afcea.org/content/?q=internets-vulnerabilities-are-built-its-infrastructure [Accessed 12 July 2016].
[7] Network, M. A., 1999. *CBU-94 "Blackout Bomb" BLU-114/B "Soft-Bomb".* [Online]
Available at: http://fas.org/man/dod-101/sys/dumb/blu-114.htm [Accessed 13 July 2016].
[8] Google.com, 2016. *Google fibre.* [Online] Available at: https://fiber.google.com/about/ [Accessed 13 July 2016].
[9] Project Loon, 2016. *Balloon-powered Internet for everyone.* [Online] Available at: https://www.google.com/loon/ [Accessed 13 July 2016].
[10] McDowell, G., 2014. *Types Of Internet Access Technologies Explained, And What You Should Expect.* [Online]
Available at: http://www.makeuseof.com/tag/types-of-internet-access-technologies-explained-and-what-you-should-expect/ [Accessed 16 Mar 2016].
[11] Blum, A., 2012. *Tubes.* 1st ed. London: Penguin. p.198-199.
[12] Global Stats, 2016. *Top 7 Desktop, Tablet & Console OSs from May 2015 to May 2016.* [Online]
Available at: http://gs.statcounter.com/#os-ww-monthly-201505-201605. [Accessed 13 July 2016].
[13] Statista, 2016. *Countries with the highest rate of malware infected computers as of 1st quarter 2016.* [Online] Available at: http://www.statista.com/statistics/266169/highest-malware-infection-rate-countries/ [Accessed 13 July 2016].
[14] Rapid7, 2016. *National Exposure Index. Inferring Internet Security Posture by Country through Port Scanning.* [Online] Available at: https://information.rapid7.com/national-exposure-index.html [Accessed 13 July 2016].
[15] Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.p.149.
[16] Dickens, J., 2016. *ICT teachers struggling with transition to computing.* [Online] Available at: http://schoolsweek.co.uk/teachers-lack-confidence-in-computing-science/. [Accessed 13 July 2016].
[17] Cambridge International Examinations, 2016. *Programmes and Qualifications.* [Online] Available at: http://www.cie.org.uk/ [Accessed 13 July 2016].
[18] Warwick, K., 2015. *Kevin Warwick.* [Online] Available at: http://www.kevinwarwick.com/ [Accessed 21 Dec 2015].
[19] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence.p.1.26
[20] Ministry of Defence, 2016. *Cyber Primer.* 2nd Ed. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf. [Accessed 20 June 2017]. P.52.
[21] Ibid.p.54.
[22] CCDCOE, 2013 *Cyber Definitions.* [Online] Available at: https://ccdcoe.org/cyber-definitions.html. [Accessed 20 June 2017].
[23] Ibid.
[24] Lyon, B., 2014. *What is Opte about?.* [Online] Available at: http://www.opte.org/about/ [Accessed 13 July 2016].
[25] Sullivan, B., 2015. *Anonymous #OPIsis Attackers Take Down ISIS Twitter Accounts.* [Online]
Available at: http://www.techweekeurope.co.uk/security/cyberwar/anonymous-isis-hack-161671 [Accessed 5 Nov 2015].

[26] Naked Security, 2017. *WannaCry: the ransomware worm that didn't arrive on a phishing hook.* [Online] Available at: https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/ [Accessed 13 June 2017].
[27] McDowell, D., 2013. Understanding Denial-of-Service Attacks. [Online]
Available at: https://www.us-cert.gov/ncas/tips/ST04-015. [Accessed 5 January 2015].
[28] Richards, J., 2009. *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security,* Washington, DC. USA: International Affairs Review, George Washington University.
[29] Kozlowski, A., 2014. Comparative Analysis of the Cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal February 2014 /SPECIAL/ edition vol.3.* pp.242
[30] Sophos, 2010. Operation Aurora. What you need to know. [Online]
Available at: http://www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx. [Accessed: 1 January 2015].
[31] Sans Institute. 2011. Responding to Zero Day Threats. [Online]
Available at: http://www.sans.org/reading-room/whitepapers/incident/responding-zero-day-threats-33709. [Accessed: 1 January 2015].
[32] Symantic. 2011. W32 Stuxnet Dossier. [Online] Available at:
http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. [Accessed 1 January 2015].
[33] CrySyS. 2011. Duqu: *A Stuxnet-like malware found in the wild*. [Online]
Available at:http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf. [Accessed 1 January 2015].
[34] Bright. P., 2011. Anonymous speaks: the inside story of the HBGary hack. [Online]
Available at: http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/. [Accessed 31 December 2014].
[35] Cadwalladr. C., 2012. Anonymous: behind the masks of the cyber insurgents. [Online]
Available at: http://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents. [Accessed 5 January 2015].
[36] Symantec. 2012. Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East. [Online]
Available at: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east. [Accessed 1 January 2015].
[37] Russia Today, 2012. *'Flame' Virus explained: How it works and who's behind it.* [Online]
Available at: https://www.rt.com/news/flame-virus-cyber-war-536/ [Accessed 13 July 2016].
[38] Bronk. C., 2013. The Cyber Attack on Saudi Aramco. *Survival: Global Politics and Strategy.* Vol. 55. Ed. 2. pp. 81-96. [Online] Available at:
http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272. [Accessed 1 January 2015].
[39] Symantec. 2014. Advanced Persistent Threats: How They Work. [Online] Available at:
http://www.symantec.com/theme.jsp?themeid=apt-infographic-1. [Accessed 5 January 2015].
[40] Mandiant. 2013. APT1: Exposing One of China's Cyber Espionage Units. [Online] Available at: http://intelreport.mandiant.com/. [Accessed 1 January 2015].
[41] Irshaid. F., 2014. How ISIS is spreading its message online. *BBC Monitoring*. [Online]
Available at: http://www.bbc.co.uk/news/world-middle-east-27912569. [Accessed 1 January 2015].
[42] Federal Bureau of Investigation, 2015. *Update on Sony Investigation.* [Online]
Available at: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation [Accessed 8 May 2016].
[43] Freed. A., 2014. Norse investigation focussing on a small group, including Sony ex-employees. [Online]
Available at: http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/. [Accessed 2 January 2015].
[44] Zetter, K., 2015. *Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors.* [Online]
Available at: https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ [Accessed 13 July 2016].
[45] Price, R., 2015. *We talked to people close to the TalkTalk hack before the arrests began — and they told us why they allegedly did it.* [Online] Available at:

http://www.businessinsider.com/talktalk-hack-vamp-c-glubz-hackers-interviews-2015-11?r=UK&IR=T [Accessed 13 July 2016].

[46] Naked Security, 2017. *WannaCry: the ransomware worm that didn't arrive on a phishing hook.* [Online] Available at: https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/ [Accessed 13 June 2017].

Chapter 5: The maritime cyber environment

Introduction

This chapter begins to address the second research objective of this thesis by exploring the formerly unresearched subject of the relationship and dependencies between the maritime and cyber environments within the context of power and security. In chapters 2 and 3 the previously published literature relating to power, cyberspace and the security of the maritime environment was examined and the connection between them introduced. Historically, these three disciplines have been regarded in isolation as their roles developed separately, but they are now brought together with a focus on how the attributes of the seas and coastal regions can be exploited to project cyberpower. In chapter 4 a new model of cyberspace was developed that can be utilised in any environment and this chapter lays the framework for its application to the maritime.

Starting with a description of the maritime environment from both civilian and military perspectives, the factors and attributes that make it unique among the other operating areas are explained in terms of its role in global trade, security and as a source of fuel and food. For those nations that have an established maritime tradition or who are major trading partners with other coastal states the challenges of operating at sea or being dependent upon it will be a familiar concept. However, for other landlocked nations, the sea might be regarded as an alien and distant region and they may well have little appreciation of the close relationship that they unknowingly have with it. Due to its well-established link with power, security and the wealth that can be gained from their natural resources, the ocean and coastal regions have become highly politicised and this is explained in terms of the recognised legal boundaries that form the basis of the territorial claims made by nations for inclusion as part of their sovereign territory or areas of influence. This also includes other aspects associated with the seas such as the role played by ports and infrastructure and the terms used by military forces in defining their areas of operation and their right to transit international and territorial waters during peacetime.

The nature of maritime power is an important one for states that are either reliant on the seas or wish to have an influence in the waters surrounding their coasts. Drawing on the UK military's maritime doctrine, the concept of power at and from the sea in terms of control and denial is explained, which aim to ensure that nations maintain access to parts of the oceans for limited periods of time to enable them to operate freely within it, whilst preventing their use by adversaries. Allied to sea power is the issue of maritime security and its related tasks, which may include a cyber element that can present additional unique challenges to operating at sea or in the littoral. These are closely related to a state's wider national security objectives and are described within the context of protecting merchant shipping to ensure their freedom of access for lawful purposes. As vital components for maintaining the integrity of national borders and for establishing the safe trading conditions that contribute to a country's economic prosperity, these move beyond just conflict resolution at the state level to include other threats. These additional factors involve mitigating the effects of non-state actors such as terrorists and criminals, which may operate outside the territorial jurisdiction of nations and present a significant threat to maritime cyberspace. In assessing this threat, the range of maritime security tasks and objectives that have been identified by the UK to secure the seas are examined and where these operate across borders, include an assessment of the role of international collaboration to counter the global risks to security. In reviewing these issues, the UK's national security strategy is reviewed, a document that specifically highlights a range of maritime risks including the potential for cyber-attack, which it views as a prominent threat.

The relationship between the cyber and maritime environments is an area that has attracted little interest from scholars, yet the two have many similarities and mutual dependencies in their use for trade, communication, and in the projection of national power. Within the wider military use of cyberspace, maritime forces are shown to have a prominent role in adding to the situational awareness of an area of interest as part of a wider campaign of information operations. From this, the concept of *information superiority* is explained and how it can be used to assist in the defeat of an adversary by means of how the

quantity and quality of information processed can contribute to the instruments of national power. This link between the seas and the littoral with cyberspace is demonstrated through the introduction of the new notion of *maritime cyberspace*. By analysing how this new concept can be exploited in terms of utilising the existing theories of power at sea, the attributes of these two environments are combined and developed leading to the new terms of *maritime cyberpower* and *cyber seapower*, the latter of which comprises *cyber sea control* and *cyber sea denial*. A detailed examination of the composition and characteristics of maritime cyberspace follows and how they contribute to security and the influence of others through power projection. With the exploitation of maritime cyberspace at the core of this thesis and a key research objective, methods are examined to identify what attributes are required to be able to project maritime cyberpower and cyber seapower. This includes an assessment of how vulnerabilities within ship systems can be exploited and what security measures are required to mitigate for them.

This chapter concludes by considering its findings in terms of the arguments developed by Rid that were introduced in the previous chapter's literature review. These are used to discuss whether cyberwarfare could become a reality and how maritime cyberspace could be utilised for offensive operations as a means of national power projection. The application of Rid's analysis of what he suggests are the three categories of cyberattacks; espionage, sabotage and subversion to the other operating environments are an area of detail not covered in his earlier work. By highlighting the relationship between the maritime and cyber environments, this chapter lays the foundation for a more detailed analysis in later chapters of Rid's work within the context of maritime cyberspace. This will extend and apply his arguments in terms of how the properties of the sea and cyberspace can be used in the projection of cyberpower, demonstrating the link between the cyber environment and the physical geography of the terrain in which it resides.

Defining the maritime environment

At the heart of any definition of the maritime environment is an acceptance of its critical importance to global trade, communication, security and as a source of fuel and food. With the growth of globalisation, climate change and over population resulting in unsustainable regional pressure on natural resources, this role is not going to diminish in the foreseeable future. Indeed, it is predicted by the UK Ministry of Defence (MoD) that a high proportion of future conflicts will occur in or adjacent to a zone of maritime influence and for nations such as the UK with sovereignty of overseas territories, there is the added risk of threats and intimidation from other countries that have their own territorial claims over them.[1] From a military perspective, the sea also provides access for land and embarked air assets to contribute to achieving their government's political objectives. The maritime operating environment is one of five recognised by UK MoD doctrine; the others being Land, Air, Space, and Cyberspace. The nature of the maritime environment is described in the UK's Future Maritime Operating Concept as *providing critical access for joint assets allowing influence in support of political objectives, the conduct of a wide range of maritime security and international engagement and when necessary, the means to assemble and apply decisive combat power at a time and place of political choice.*[2] British Maritime Doctrine, the aim of which is to consistently and coherently articulate to both internal and external audiences how and why the Royal Navy performs as it does, highlights that maritime power is not an end in itself, but operates within a wider national security framework.[3] The doctrine defines the environment as comprising six discrete components described in detail in Appendix 1, noting that they are interrelated and of equal importance although the physical element provides the overarching context for all and highlights its uniqueness.

The physical aspect of the maritime environment can be regarded as comprising several separate elements, some of which are legally defined in the United Nations Convention on the Law of the Sea (UNCLOS) and others that are core to their use.[4] The importance of these legal definitions is that they limit the regions of the sea to which nation states can lay claim and the activities that

other nations can undertake within these areas. This is significant when considering the interaction between the maritime and cyber environments as geographical constraints can limit the effects that can be achieved within a campaign of power projection. The core components of the maritime environment are as follows: [5]

The High Seas: The high seas are all parts of the sea that are not included in Exclusive Economic Zones, territorial seas, internal waters of a State or the archipelagic waters of archipelagic state such as the Bahamas or Philippines.

Baseline: The normal baseline for measuring the breadth of the territorial sea is the low water line along the coast as marked on officially recognised large-scale charts.

Internal Waters: Internal waters are all water and waterways on the landward side of the baseline. Countries are responsible for setting laws and regulations for the use of these internal waters.

Territorial Seas: The territorial sea is regarded as an extension of the sovereignty of a coastal state beyond its land territory and includes the airspace above and subsoil below up to a limit not exceeding 12 nautical miles measured from the low-water line along the coast as marked on the large-scale charts officially recognised by the coastal state.

Contiguous Zone: This area, which does not exceed beyond 24 nautical miles from the baseline from which the territorial sea is measured, is an area over which a state may exercise control necessary to prevent an infringement of its laws within its territory or territorial seas. These may include such elements as ensuring the integrity of its customs, fiscal, immigration, or sanitary regulations.

The Exclusive Economic Zone (EEZ): The exclusive economic zone is an area adjacent to and beyond the territorial sea extending not beyond 200 nautical miles measured from the same baseline as that of the territorial sea. In

this area, the coastal State has sovereign rights for exploring, exploiting, managing, and conserving the natural resources in the sea, seabed and below.

Continental shelf: This area is defined as the seabed and subsoil beyond the territorial sea that may be regarded as a submerged extension of the land territory normally to 200 nautical miles but can be as much as 350 nautical miles. The continental shelf is important as the coastal state can exercise exclusive sovereign rights for exploring it and exploiting its natural resources. These rights remain such that even if a state chooses not to undertake these activities, no other state can without its express permission. It should be noted that the area beyond the EEZ to the boundary of the continental shelf refers purely to the seabed and not the seas above. The International Seabed Authority administer the seabeds of the high seas.[6]

Figure 6 below illustrates the maritime zones detailed in the United Nations Convention on the Law of the Sea (UNCLOS). However, there are several additional components that together comprise the maritime environment and these are detailed as follows:

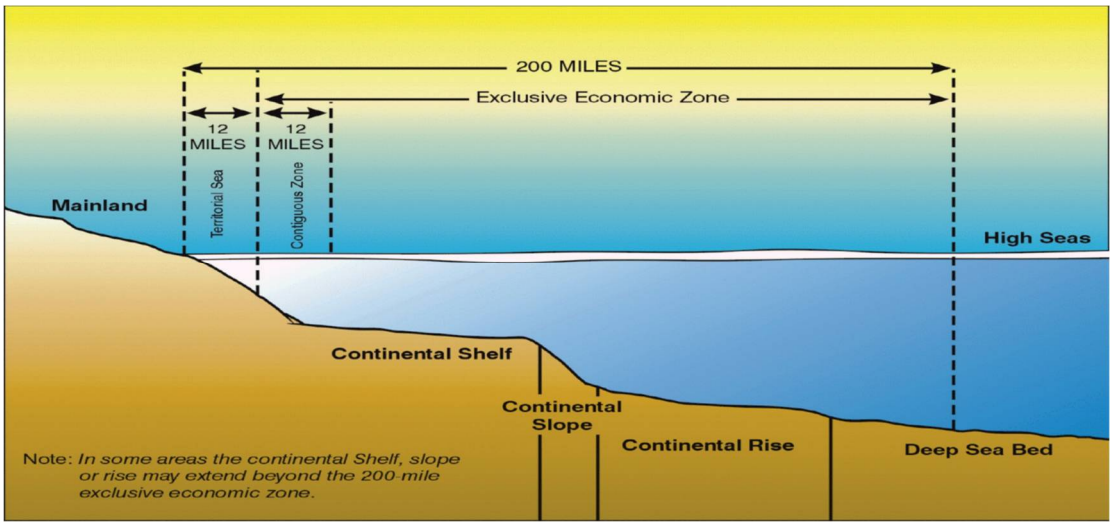

Figure 6: United Nations Convention on the Law of the Sea (UNCLOS) Zones[7]

The Littoral: This is defined as a narrow band of land, sea and airspace that are predominantly susceptible to engagement and influence from the sea.[8] As most human maritime activity such as shipping, fishing, and energy recovery such as oil exploration and wind farms is conducted within the 200-nautical mile EEZs it means that a substantial proportion of the total global economic and political activity occurs in relatively narrow strip of land and sea surrounding the earth's land masses. It is because of this that this area is a key focus for military power projection, but to totally control the littoral region requires the full spectrum of capabilities including amphibious units, naval vessels capable of delivering, protecting, and supplying the force and aircraft providing both air defence and ground attack.

Ports and Maritime Infrastructure: Ports and harbour works are important for delimiting territorial seas as their outermost permanent elements, if integral to the harbour system and not offshore structures, are treated as forming part of the coast. States can thus increase their claims to territorial waters by extending breakwaters and harbour installations out to sea. Ports can provide an important safety function with large or busy terminals such as Dover in the UK having their own Vessel Traffic Service providing radar surveillance and communications services to ships using their facilities. With 500 ships a day transiting the Dover Straits, these have the ability to identify and intercept shipping that are not complying with the procedures and are considered a threat to the safety of other users of the port.[9] [10] Ports can also have significant political significance, particularly those of neutral states during times of war when they may gain strategic importance as warships of belligerent nations are only able to visit them only once every three months and then only for 24 hours as stated in the 13th Hague convention.[11] This was seen in 1939 during the Battle of the River Plate when the German Pocket Battleship Graf Spee sought sanctuary in the neutral port of Montevideo in Uruguay following an engagement with the four cruisers of the Royal Navy South American Naval Division. Forced by the convention to leave or be impounded, the Graf Spee's Commanding Officer, Captain Hans Langsdorff, chose to scuttle his ship than face defeat by what he erroneously believed was a superior British Force awaiting him at sea.

Logistics Infrastructure: Although not formally recognised in UNCLOS, a fundamental component of the maritime environment that enables it to be accessed and exploited is the logistics infrastructure that supports seafarers. At any one time, there are around 1 500 large commercial ships off the UK coast carrying 95% of the country's trade by volume with UK ports handling 393 million tonnes of international cargo and over 4.4 million containers annually.[12] The logistics infrastructure to facilitate this ranges from the provision of fuel, engineering support and chandlery that supply the ports and enable vessels to go to sea to the food supplies that sustain the crew. Offshore platforms rely on air support from helicopters and all depend on accurate computer aided meteorological forecasts to determine when it may be too dangerous to operate at sea. There is also a fundamental reliance on technology and an increasing migration to incorporating it with the wider cyber environment. Charts are now electronic and integrate with complex automated navigation systems that enable ships to automatically follow a pre-programmed route. Navigational aids and buoyage are surveyed using the satellite based Global Positioning System (GPS) and systems devoted to ship safety such as the Automatic Identification System (AIS) and Global Maritime Distress and Safety System (GMDSS) are both fundamental components of the shipping industry. These are based on satellite and Radio Frequency (RF) data transmissions sent from and received by computer systems between ships and linking ships to shore stations.

Global Commons: A key feature of the oceans is that they can provide unhindered access to large parts of the world. Whereas transportation over land is dependent on geographical constraints such as mountains, rivers and political borders that may obstruct or hamper access, transportation via the sea does not suffer from these considerations. Accepting that they do not allow direct access to inland continental areas and adverse weather can delay access, the seas can provide entrance via amenable host countries and provide flexibility in determining the preferred route inland. Oceans, in common with the Atmosphere, Antarctica and Outer Space form what are termed the *Global Commons*, which are resources or domain areas that lie outside of the political reach of any one nation state.[13] Although originally the concept of the Global

Commons referred to those areas that could not be controlled by one state, they have recently been redefined as the set of natural resources, basic services, public services or cultural traditions that should be part of a public trust to be enjoyed by all people.[14] Using this definition there has also been an argument that cyberspace should be considered as part of the Global Commons.[15]

Freedom of Navigation: Freedom of Navigation refers to a range of rights and freedoms that warships, merchant ships, aircraft and submarines have that enable them to navigate on, over or under the world's seas. Freedom of Navigation facilitates global maritime trade and enables military forces to respond to worldwide threats to security.

The attributes of maritime power

The UK Ministry of Defence defines maritime power as *the ability to project power at sea and from the sea to influence the behaviour of people or the course of events*. As such, it is coherent with other more general descriptions of the concept of power and to achieve this, maritime forces have several unique attributes that they can exploit, which are described as follows. [16]

Access: Maritime forces can provide unparalleled geographical access to countries that would otherwise be regarded as so remote as to be outside their sphere of influence. According to *Worldbymap.org*, 202 countries out of a total of 245 have some form of coast ranging from Canada with 202 080km to Monaco with 4.1km.[17] Although all can claim 12 nautical miles of territorial waters there is also a right of transit through choke points that may be within this area and also the ability to conduct innocent passage in the territorial waters of any coastal state, which may be restricted only in very limited cases.[18] This implies than maritime forces have the potential for accessing over 80% of the world's countries either directly or indirectly and at a time of their choosing. They can also select to make their presence known by positioning themselves within sight of the coast or covertly by operating over the horizon depending on the political situation.

Mobility: As UNCLOS states that the seas are international spaces, all vessels have the right of innocent passage through territorial waters and other claimed areas. This access enables maritime forces, both civilian and military to move freely worldwide independent of any requirement for third party agreement. Ships travelling at 20 knots can travel 480 miles a day and combined with their load carrying capability can transport material much more efficiently than by land or air.

Lift Capacity: One of the major advances in the development of international trade was the introduction of containerisation. Standard size shipping containers are either 20' or 40' long and although there are a multitude of other dimensions, the acknowledged unit of measurement is a TEU standing for 'Twenty-foot equivalent unit'.[19] Whereas in the 1980s container ships had a capacity of no more than 5000 TEUs, the latest ships have a capacity of around 20 000 and with a cruising speed over of over 20 knots represent significant capital and commercial assets.[20] The size of container ships has also historically been determined by the capacity of key transit areas such as the Panama Canal. Prior to 2009, the maximum capacity of the so called *Panamax* ships was 5000 TEU, but with the construction of new locks, this was increased to 13 000 termed the *New Panamax*, which rendered large numbers of ships obsolescent as shipping companies ordered new ships to benefit from the economies of scale that could be achieved from operating larger ships.[21] The strategic importance of these vessels and their cargo is highlighted in that in 2006 the arrival in the UK of a single container ship from China in early December was reported in the national media as bringing the Christmas presents for the entire country.[22] Oil tankers have also increased in size, although the largest currently in service are smaller than the largest ever built. The current largest tanker is the *TI Asia*, which is employed as a floating production storage and offloading vessel for crude oil and at full load displaces 509 000 tons carrying over 3 million barrels of oil.[23] Large as this may appear, it does however only represent 2 days' worth of the UK's oil consumption illustrating the dependence of island nations on a reliable, regular seaborne supply.[24]

Sustained Reach: Maritime forces, suitably supported by fuel and food, can operate independently worldwide, and can therefore be used to project power for extended periods. Merchant ships taken up from trade can be used to supplement specialist support shipping that can replenish warships at sea enabling them to provide a continuous presence in an operating area. This enables blue water navies to operate worldwide and extend their influence well beyond that of their regional location.

Versatility: Although merchant ships tend to be optimised for a single purpose, warships are inherently flexible and can conduct a range of tasks both in peace and wartime. Many classes of warship can fight in multiple threat environments be it from the air, surface or sub surface and the use of an organic helicopter further increases this flexibility in being able to extend their influence beyond their immediate vicinity. Working in national or coalition forces, their design enables them to rapidly refocus from a soft power role of diplomacy and aid delivery to hard power coercion and military force. This enables a change of political posture to be immediately presented in accordance with government policy. Equipped with a comprehensive suite of communications and sensors, it is also possible to use active and passive electronic measures to establish local situational awareness and monitor a situation ashore for relaying to shore agencies for further analysis.

Poise: The ability for national flagged shipping and warships to represent a nation's interests can be a powerful political signal and represent a wiliness to deter aggression or to coerce a potential adversary. Hospital ships, vessels delivering aid, warships or those designed for specialist intelligence gathering duties can remain on station for prolonged periods as tools of soft or hard power and can enable influence to be projected inland without the need for a footprint to be established ashore.

Resilience: Warships, especially when supplemented by specialist support vessels, are designed to be capable of operating, even in a reduced capacity, after taking damage from adverse weather or enemy action. This adds to their

ability to operate reliably for extended periods in high threat or difficult conditions.

Leverage: The attributes above, when combined, can demonstrate the power of naval forces working with the merchant marine to influence events ashore. Leverage of an opponent can be used for both military or political purposes as a statement of resolve and can present a range of smart power options and a demonstration of intent to pursue them. This can only be achieved through the inherent flexibility of maritime power.

Maritime Power at sea

British Maritime Doctrine details three roles for the Royal Navy; War-fighting, Maritime Security, and International Engagement, which are inter-related and may be conducted concurrently or consecutively.[25] Although the primary focus of the UK's 2010 *National Security Strategy* was the prevention of conflict and de-escalation, there must be an ability to coerce or confront aggressors if required through deterrence or lethal combat power. Deterrence is at the cornerstone of UK defence policy with its aim being to dissuade an opponent from taking a course of action that threatens the national interest. To project the maritime power required to achieve these aims it is necessary to be able to deliver an effect at sea and from the sea. Initially the term Command of the Sea was used to be able to exploit the sea to an advantage. However, as this implied total control of the entire ocean all the time, which was impractical, other terms are now used that are described below, which refer to a more realistic aspiration of temporary control limited in time and space to that required to conduct a given task or operation.

Sea Control: Sea control is defined as the freedom to use an area of the sea for one's own purpose for a limited time and if necessary to deny its use to an opponent if it is contested. It depends upon the ability to govern the surface and sub surface environments, which includes the seabed and the air above the area in which sea control is required.[26] This may be as simple as being able to exercise the right of innocent passage in a state's territorial water or Exclusive

Economic Zone (EEZ) to using force to eliminate another naval force from challenging sea control over an area of sea. As sea control is a temporary condition it would usually be an objective to enable the conduct of a single mission or as a precursor to other operations. Depending on the threat, obtaining it may involve actual military action against an opponent at sea or their containment by blockade to prevent them from accessing the disputed area

Sea Denial: Sea Denial differs from sea control in that it occurs when one party prevents another from controlling an area, but without controlling the region itself. Historically minefields were used to deny total access to all nations or the threat of submarines was used to deter opposition surface forces from operating in a particular area. More recently and especially in littoral areas, surface to surface missile or gun batteries have been used to present an increased level of risk that may deter maritime forces from operating in coastal regions. Sea Control and Sea Denial may also be used in conjunction as denial in one region may facilitate control in another.

Other forms of sea power: In addition to Sea Control and Denial there are other forms of sea power detailed in British Maritime Doctrine. These are Fleet-in-Being, Cover and the role of Decisive Power. The concept of a Fleet-in-Being is that an inferior maritime nation withholds its forces as a deterrent against a superior opponent. By deliberately avoiding conflict, it complicates the options available to the more capable force by preventing it from achieving sea control by having to divert assets to counter a potential attack from a Fleet-in-Being. The concept of Cover provides support to vulnerable units within a force that are engaged in their own operation within an area in which sea control is held. Decisive battle requires a concentration of force such as that required for sea control. However, by concentrating force in a single area, it may be possible for a smaller force to evade it. Concentrating forces also prevents other tasks from being undertaken and reduces the element of surprise. Hence, whereas it may be argued that in the land environment a decisive battle may be worth the cost, in the maritime environment the focus should be in achieving control of the sea and then exploiting it to achieve strategic aims.[27]

Maritime power from the sea

In addition to control or denial at sea, there may be a requirement to project power from the sea such as in a littoral area. Maritime forces can exploit their right to freedom of manoeuvre and unrestricted access up to the 12-mile territorial mile limit to apply force at a time and place of their choosing to gain the initiative and attack areas that are vulnerable. Maritime power projection can also contribute to wider operations in the following ways:

Shape: In preparation for future operations, forces are used for intelligence gathering or other precursor activities.

Reassure: The presence of maritime forces can reassure a friendly state, which may then provide access to their facilities for future operations.

Deter: Early presence in a region at times of low political risk can deter future aggression.

Coerce: As forces build up, limited action can demonstrate resolve and prevent an aggressor from using force, whilst maintaining control over how a conflict escalates.

Disrupt: Prior to offensive operations, forces can shift focus from defensive to offensive by disrupting enemy activity.

Project: Manoeuvring to a position from which force projection can be threatened or applied.

Support: The full range of capabilities of maritime forces can support other friendly forces. This can include intervention, either permissive or non-permissive, to support a country as part of its rebuilding post conflict or natural disaster within a wider security sector reform and stabilisation programme.

Limit: A powerful force can limit the effect of others to project power, whilst using the same power against them.

Recover: The ability to move items from the theatre of operations and provide protection whilst doing so.

Power projection can be achieved through either proactive or reactive means. Although force projection is by nature proactive by seizing the initiative, it may not always be offensive and sea control offers both options. Offensive action forces the enemy to fight to defend their position, whereas defensive action forces the enemy to attack if they wish to engage in offensive operations to achieve influence in a contested area.

Defining the cyber environment

Although has been highlighted in Chapter 2, there is no formally accepted definition for the cyber environment, the UK Ministry of Defence's 2013 *Cyber Primer* describes it as the *interdependent network of information technology infrastructures, (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein within the information environment*.[28] At the heart of cyberspace is information and the information environment is defined by the UK Ministry of Defence as a *logical construct whereby assured information can pass unhindered from point of origin to point of need*, where assured indicates that the information can be proven as authentic and that the originator can be identified.[29] The Cyber Primer also moves beyond just describing the environment to what comprises military operations in cyberspace and defines it as *the employment of capabilities where the primary purpose is to achieve effects in, or through, cyberspace.* This has significant coherence with the definitions of maritime power projection as being able to influence the behaviour of people or the course of events. In explaining cyberspace in terms of the Information environment, the Primer describes it in terms of three domains; the physical, virtual, and cognitive as described below:

Physical Layer: The physical layer comprises the hardware elements of cyberspace and their geographical location. This includes the networking components and their connections.

Virtual Layer: The virtual layer consists of the software applications, their network coding protocols and the logical connections that enable those in cyberspace to exchange data. It also includes the information that is passed between users facilitating useful work to be done.

Cognitive Layer: This layer has three components; persona, people and social that connects users to each other through cyberspace. The persona elements are the roles that are performed by the users themselves who form the people element. The social aspects are the groups that are formed from the users that combine to fulfil a certain role.

Noting that cyberspace is a complex and dynamic environment, the Cyber Primer emphasises its importance to military operations and the reliance placed on defence communications. However, it also notes the need to use commercial off the shelf (COTS) hardware and software and civilian owned and operated infrastructure for its essential operations.[30] This requires protective measures to be conducted to enable mission critical systems and the information they carry to function with the requisite resilience such that they maintain the confidentially, integrity and availability of data. A key facet of this is its relationship and interdependency with the electromagnetic spectrum (EMS), which is an integral part of the cyber environment, particularly for mobile platforms that do not have access to a fixed infrastructure for connection. However, radio frequency transmissions have the disadvantage in that they can be received, manipulated, or interfered with by others thereby making them a valuable tool for intelligence gathering, sabotage, or subversion.

Cyber Electromagnetic Activities (CEMA)

As the definition of cyberspace has continued to develop it is accepted that although wired networks form much of the environment, there is also a

significant component that relies on wireless transmission. This has resulted in the new concept of CEMA – cyber electromagnetic activities. The US military defines this as activities *to seize, retain and exploit an advantage….. in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same…….* [31] Within the UK military, the importance of CEMA in synchronising and coordinating the related disciplines of Electronic Warfare, Signals Intelligence and Cyber is recognised in both offensive and defensive activities and resulted the formation of a dedicated Joint CEMA Group (JCG) as part of the 2015 Strategic Defence and Security Review.[32] This acceptance of the electromagnetic environment as being part of, or related to, cyberspace is an area of ongoing discussion and debate emphasising the evolving nature of the environment.

Comparing the maritime and cyber environments

British Maritime Doctrine defines Maritime Power as *The ability to project power at sea and from the sea to influence the behaviour of people or the course of events*.[33] Cyberpower has been described from a variety of perspectives, but Joseph Nye refers to it as *the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain.*[34] Combining these two definitions to investigate how the maritime environment could be used as a means to enter cyberspace in order to influence a target has yet to attract significant academic interest, but by using the concept of seapower as the basis for projecting cyberpower the notion of *Maritime Cyberpower* can be introduced as:

> **The ability to project power from the sea to influence the behaviour of people or the course of events through and within the medium of cyberspace.**

In addition to using the features of the maritime environment as means of influencing others in the wider medium of cyberspace it is also conceivable to use the properties of cyberspace develop power at sea in the conventional sense. This presents a new concept of *cyber seapower*, which can be termed:

The ability to use cyberspace to influence the behaviour of people or the course of events in the maritime environment.

There is a distinct difference between these new ideas of maritime cyberpower and cyber seapower as whereas the former seeks to achieve an effect from the sea that influences events anywhere in cyberspace, the latter seeks to use cyberspace to achieve an effect solely in the maritime environment, including the littoral. An example of maritime cyberpower would therefore be to use a maritime platform to disrupt a cyber infrastructure to prevent access or to alter the content of systems to affect the behaviour of a population ashore. Cyber seapower however would be to utilise the medium to directly affect the ability to facilitate sea control or sea denial. This would include adversely affecting the ability of ships, port, or offshore installations to operate normally. The concepts of maritime cyberpower and cyber sea power within the contexts of cyberpower and sea power are shown in figure 7 below, which emphasise their contributory nature to the wider power component:

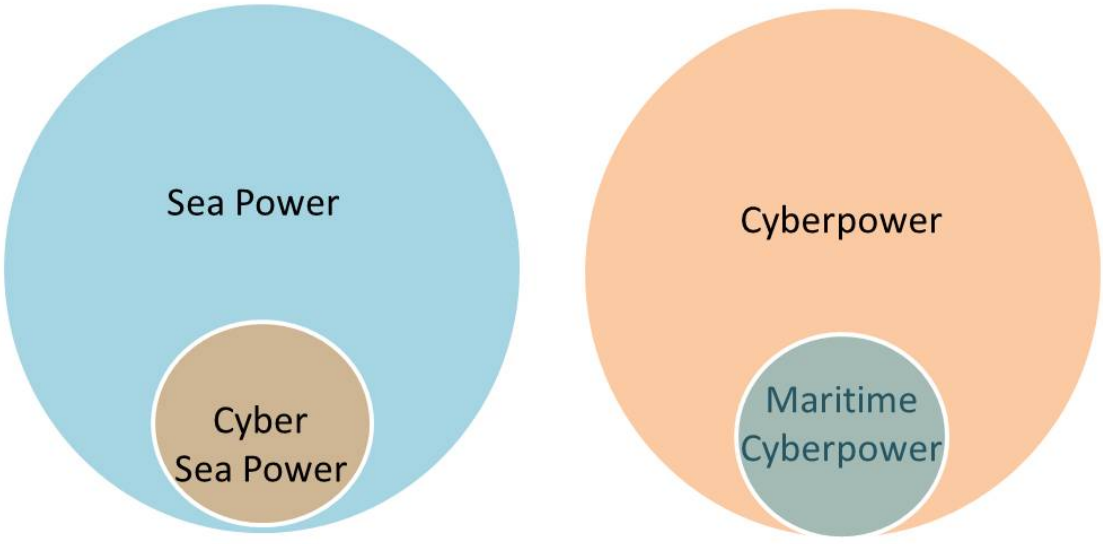

Figure 7: The relationship between Sea Power, Cyberpower, Cyber Sea Power and Maritime Cyberpower

Maritime power by itself is an important factor to be considered by any state with a seagoing tradition as its prosperity, stability and security can be

dependent on it. For nations that regard themselves as global players, they can use the maritime environment to protect and promote their national interests at home and abroad. However, the UK Ministry of Defence's Development, Concepts, and Doctrine Centre's Future Character of Conflict paper suggest that the trend towards globalisation will increase the likelihood of conflict involving state and non-state actors that have no formal affinity to any nation. In these types of conflict, it is suggested that asymmetric tactics such as the use of cyberspace will play an important part as both seek an advantage over those who are superior in conventional military capability.[35]

The increasing number of actors operating in cyberspace have the potential to confuse the cyber environment and present challenges in the ability to recognise allies from adversaries, civilians, media, and other non-governmental organisations communicating with each other as they try to influence and inform within the same operating area. The cyber component to maritime power will also become an increasingly important consideration for seagoing nations seeking to protect their shipping and for global players who seek to use their maritime assets to project power from the sea.

Although the maritime and cyber environments may appear very dissimilar at first inspection, there are a significant number of parallels that can be drawn. Many of the factors that need to be considered when operating at sea, can also apply when seeking to achieve an effect in cyberspace. For example, the size of the two environments means that they are ungovernable by a single authority, indicating that sea control and denial have equivalents in cyberspace for power projection. Also, both require manufactured devices to effectively use them, be they ships or computing devices as unlike land warfare, a human cannot enter and engage with the environment unassisted. Furthermore, they are both environments that are international in nature with ships at sea emanating from many countries and cyberspace comprised of components manufactured worldwide, even if certain countries are predominant in both. Similarities also exist with some states having larger merchant fleets or being dominant in the computer or networking markets. Similarly, to function, there are global agreements that govern both environments – UNCLOS determining

the use of the oceans and internationally accepted addressing and routing protocols controlling how data is transmitted around the networks of cyberspace. Finally, although both are fundamental to global trade and economic wealth, control over both environments is disputed in some areas with sovereignty over some coastal waters contested and networks subject to interference to exfiltrate data or to adversely affect their performance and ability to function as designed.

Components of maritime cyberspace

Maritime cyberspace can be described as those elements of the cyber environment that rely on and contribute to the effective exploitation of the maritime and where the attributes of one affect the properties of the other. The composition of maritime cyberspace and how it can be used to exert power to influence a target or in what way it employs security measures to inhibit these activities has not been well researched in the past. However, for it to function it relies on a range of technologies, some of which are unique to the maritime environment and others are widely used in all areas of cyberspace. Combined, they form the unique elements upon which shipping is now dependent for their safe and effective operation. The discrete capabilities that comprise maritime cyberspace are described as follows:

Position, Navigation, and Timing (PNT) Systems

The first of these capabilities is the use of satellite based navigation systems. The primary system in use is the Global Positioning Satellite (GPS) constellation, which is an American owned utility that provides users with positioning, navigation, and timing (PNT) services. The system consists of three segments; the space and control elements, both of which are developed, maintained and operated by the US air force's 50th Space Wing located at Schriever Air Force Base in Colorado, and thirdly the user component.[36] The space element consists of a constellation 31 operational satellites to meet the requirement of maintaining at least 24 available 95% of the time with each one orbiting the earth every 12 hours at an altitude of approximately 12 550 miles.[37]

In addition to the master control station in Colorado, the control aspect comprises a global network of 12 command and control antenna and 16 monitoring sites that track the satellites and optimise their performance by analysing their signals as they pass overhead.[38] The user component comprises the wide range of commercial receivers that utilise GPS's PNT data in a wide range of maritime, terrestrial and airborne applications. The GPS system is quoted as operating to an accuracy of a millionth of a second, velocity to within a fraction of a mile an hour and location to within 100 feet.[39]

Although GPS is the predominant satellite based PNT system, there are two others in use or development; the European Galileo and Russian Glonass systems. When fully deployed in 2020, the Galileo system will comprise 24 satellites with initial services made available from the end of 2016.[40] The Russian Glonass system also comprises 24 satellites and provides worldwide coverage, although it is optimised for northern latitudes. Initially developed for military use, it is being exploited commercially and many receivers can utilise signals from multiple systems to increase their accuracy.[41]

Automatic Identification System (AIS)

Satellite based navigation systems is a primary component of the second element of maritime cyberspace, the Automatic Identification System (AIS). This is a system introduced to enhance the safety of vessel traffic by automatically exchanging information in real time as well as being able to track and monitor ships.[42] The use of AIS transponders has been a mandatory requirement for all passenger vessels and international shipping over 300 tons.[43] The AIS comprises Very High Frequency (VHF) data transmissions and it broadcasts a range of information types including the vessel's identity, position acquired from GPS and information about its passage. It is a vital aid used by shipping for collision avoidance and for transmitting data relating to search and rescue operations, navigational aids, meteorological, hydrological and navigational safety information.[44] AIS is also used for tracking vessels within a nation's territorial waters and is fundamental to the safety of shipping in areas of high concentration such as the English Channel, where it is integral

into the Dover Straits Channel Navigation Information Service.[45] More recently, satellites have been used to receive AIS data to provide global coverage and information on shipping outside the range of shore based receivers, which is updated hourly. By accumulating this data, it is possible to show worldwide shipping and areas of high traffic concentration as shown in figure 8. This enables AIS data to be integrated not only in the maritime cyber environment, but also accessed by anyone with an Internet connection.

There are several websites such as *www.vesselfinder.com* that offer near real time AIS data overlaid on mapping software that not only indicate the position of vessels active on AIS, but enable searches to be made for individual ships and interrogate and respond to searches about the information that they are transmitting.[46] This can prove problematic for military vessels that may be obliged to transmit on AIS even though they may wish to keep their location hidden. An example of this was seen in the reporting of the recently built UK Aircraft Carrier HMS Queen Elizabeth during her initial sea trials. Operating under merchant navy regulations prior to being accepted by the Royal Navy, her precise location in the North Sea was readily available via AIS tracking data, facilitating intelligence gathering operations by other nations' navies.[47]

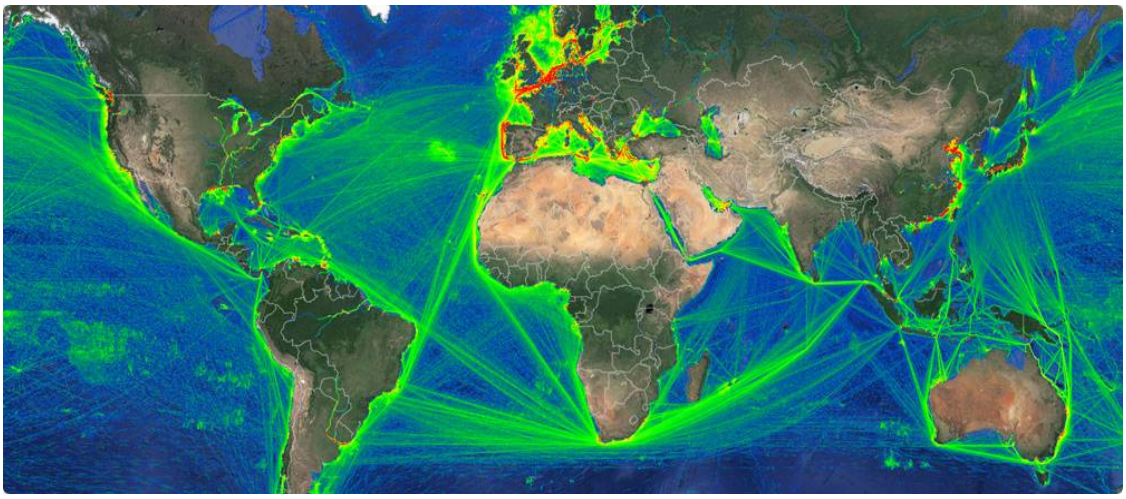

Figure 8: Global Satellite AIS Coverage[48]

Satellite Communication Systems

In addition to providing Position, Navigational or Time information and enabling the reception of AIS information transmitted from ships, satellites are also fundamental to maritime data and voice communications. There are two main systems in use; the UK based International Maritime Satellite Organisation (INMARSAT) set up by the International Maritime Organisation (IMO) in 1979 and the UAE based privately owned THURAYA network. Both provide near total global coverage, although INMARSAT has a greater footprint at extreme latitudes, but as both systems employ geostationary equatorial satellites, they are limited in coverage at the poles. INMARSAT's maritime service offers a range of telephony and broadband Internet connections providing comparable services to land based fixed infrastructures plus the option of bespoke applications tailored for shipping.[49] THURAYA also offer a specialist maritime communications service providing an option of voice and / or data services. Their data services are similar to that of a terrestrial provider, but do not offer the specialised maritime applications of INMARSAT.[50] Both systems however would enable a ship to establish a permanent connection to the cyber environment with similar functionality to a land based subscriber.

Terrestrial Communication Systems

Complementary to space based connectivity to the cyber environment, it is possible to use more traditional communication methods to transfer data using the same protocols as the Internet. These however can be more challenging to engineer and have significant restrictions; both in the limitations of the medium, but also that they are more susceptible to atmospheric conditions affecting their propagation. The propagation of radio waves depends on their frequency as shown in figure 9 below:

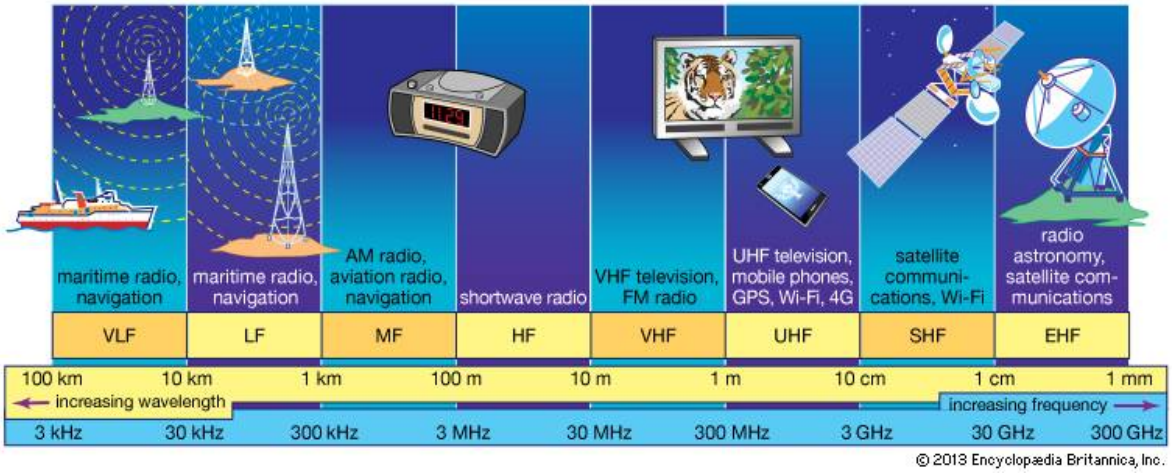

Figure 9: Commercial radio frequency spectrum[51]

Within the radio frequency spectrum, information is transmitted by changing the characteristics of the signal. The faster these attributes are changed, the more information can be passed and as frequency is a direct measurement of the rate of change in values, the higher the frequency of the signal, the more information can be passed – hence high data rate satellite communications use Super High Frequency (SHF) wavelengths.[52] Transmissions at the Very High Frequency (VHF) and above are line of sight, hence are ideal for point to point links to satellites, but using these elements of the spectrum for non-space based communications is limited in range to the visible horizon and the lower the frequency, the lower the data rate.

Below VHF, High Frequency (HF) radio transmissions have the property that they can refract off the ionosphere layer of the atmosphere back to the surface of the earth and be received over the horizon from the transmitting station. Known as *sky wave*, this range of frequencies is commonly used for long range marine radio and despite their lower frequency restricting the potential data rates of communications, they can be used for the transmission of e-mails. In addition to a compatible transceiver, this requires the use of a radio modem, computer hardware and an account with a specialist service provider such as *sailmail*.[53] It should be noted though that long-range HF communications are not as reliable as SHF based satellite communications as their hop distance is based on their frequency, atmospheric conditions, and time of day. Dead zones can occur close to the transmitter where no signal is received and ranges

achieved at night can be twice that of day time communications.[54] E-mail systems such as sailmail essentially use dedicated file transfer protocols and not the standard Internet protocols such as the Transmission Control Protocol and Internet Protocol (TCP/IP) that are required for web browsing. To be effective, TCP/IP relies on a continuous transfer of data packets, not only to exchange information, but also to check that the packets have been received correctly. The quantity of these additional data packets and the latency of the transmission if skywave is used is beyond that which can be realistically transmitted over the limited data rates of HF and packet loss due to unreliable connections could render the communications channel ineffective. There have though been some attempts at using IP over HF, particularly by the military which have developed their own standards to make the most efficient use of the limitations of the medium.[55]

Submarine Cables

The final component of maritime cyberspace is without doubt the most important as it is fundamental to existence of the cyber environment and yet is mostly invisible with the majority of its users oblivious to its existence. It is also one which the mariners themselves do not engage directly with. Despite the increasing use of wireless devices to interact with cyberspace via mobile telephony or Wi-Fi, beyond the cell phone mast or wireless router, most data communication is wired and for international communication this involves fibre optic cable laid on the ocean floor. This network of over 300 undersea cable systems stretches over 550 000 miles and transports 99% of all transoceanic digital communications. The longest single cable has 39 landing points from Germany to Korea and spans 24 000 miles.[56] Their essential role in data and voice communications has resulted in their reliability being deemed by countries as *absolutely essential for the functioning of governments and the enforcement of national security* and because of this they are regarded as part of many countries critical national infrastructure. [57]

The routing of the fibre cable network is relatively centralised and follow similar courses across the globe with some laid over 25 000 feet below the ocean's

surface.[58] This is due to the lower risk of using paths which have previously proved successful and some seabed topography being more suited to laying cables than others. Routes tend to avoid shipping lanes to reduce damage from dragging anchors and are also highly politicised with cable companies having to overcome objections from local communities for a variety of reasons including economic and environmental. This can result in their paths often being circuitous, rather than direct.[59] They also tend to terminate in or near traditional port cities following conventional trading routes.[60] Compared to satellite communication, undersea cables are cheaper to use, have a longer lifespan and have a shorter transmission time as geostationary communication satellites are placed in orbit at altitudes of 22 000 miles above the earth. This means that a signal travelling between London and New York takes one eighth the time to reach its destination by cable as by satellite.[61] As the numbers of these cables expand they offer increased redundancy of communication as well as capacity and a range of routing options leading to a greater resilience in global communications. These four elements of cyberspace; satellite based PNT, AIS and wired as well as wireless communications are now fundamental components of the maritime environment and establishes the composition of the new environment of maritime cyberspace. The relationship between them is shown in figure 10 below:

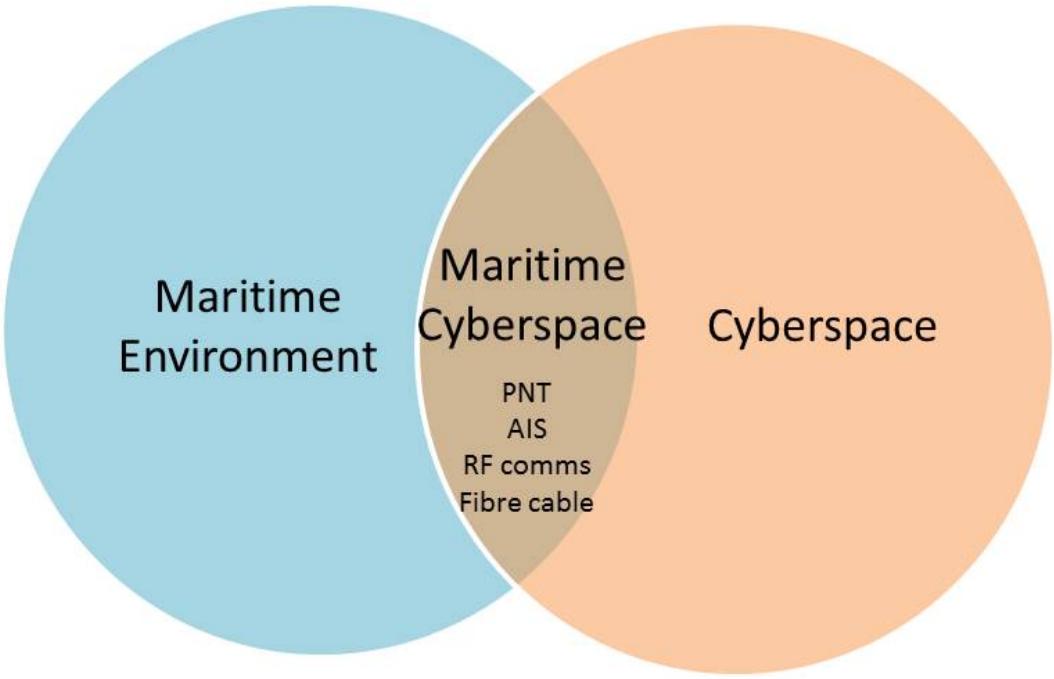

Figure 10: The composition of maritime cyberspace

Exploiting Maritime Cyberspace

Having identified the similarities between the maritime and cyber environments and their use for the projection of power in both areas, it can be seen that while the exploitation of maritime cyberspace offers significant potential for achieving national objectives, measures must be taken to ensure that its security is maintained to deter adversaries from interfering with its use or to illicitly hijack resources for their own benefit. By combining figures 7 and 10, a composite model of power projection in maritime cyberspace can be derived, which is shown in figure 11. This demonstrates that both maritime cyberpower and cyber seapower can be developed either separately or as part of a combined strategy within maritime cyberspace.

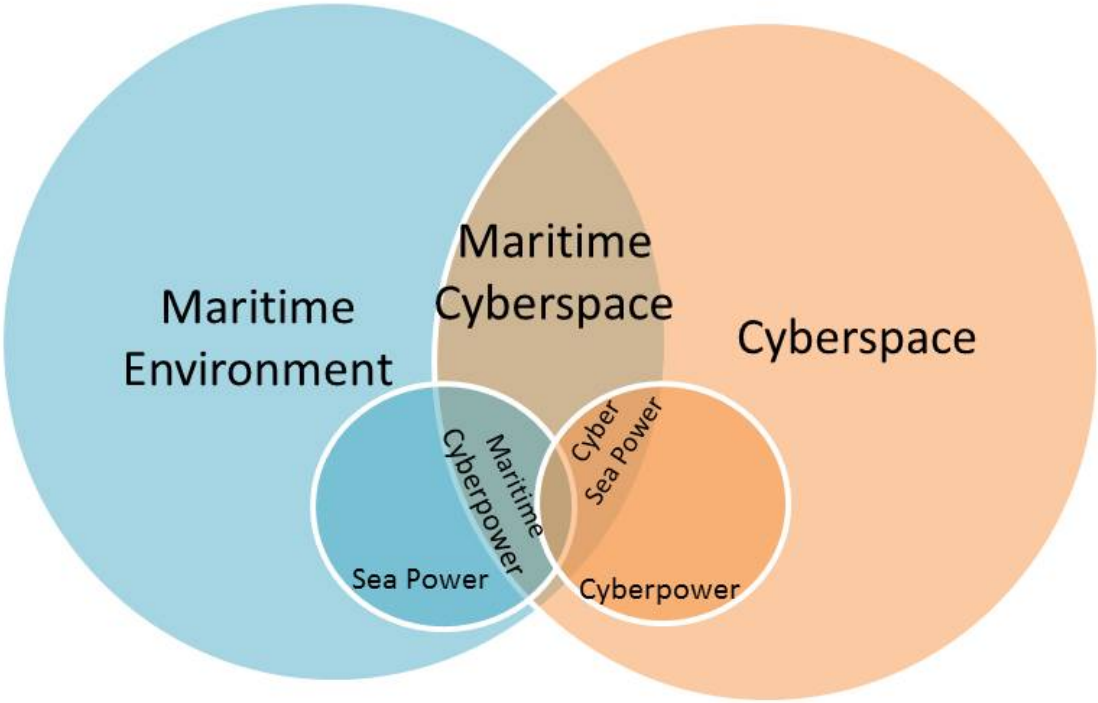

Figure 11: Power projection in the maritime and cyber environments

As sea power in the physical environment is comprised of a combination of sea control and sea denial, the same logic can be applied to maritime cyberspace to enable the new terms of *cyber sea control* and *cyber sea denial* to be derived, which can be defined as follows:

- **Cyber sea control: The freedom to use an area of maritime cyberspace for one's own purpose for a limited time and if necessary to deny its use to an opponent if it is contested.**

- **Cyber sea denial: The ability to prevent another from using an area of maritime cyberspace, but without using it itself.**

The Royal Navy has recognised the potential benefits of combining the attributes of the two environments by developing a single strategy that encompasses the full spectrum of cyber operations.[62] Their approach recognises four distinct elements to exploiting maritime cyberspace, the first of which is People and Training. This identifies the need to create, develop, and

retain cyber talent acknowledging the time required in acquiring the specialist skills needed of a cyber operator and that this expertise is highly perishable if not continually practised. Secondly, the importance of maintaining the availability of the networks is recognised, which is achieved through effective situational awareness of system activity and taking steps to ensure that they are resilient to potential threats. Thirdly, the use of maritime platforms as an integral component of a nation's cyber capability is included so that they can contribute to the full spectrum of cyber operations. Finally, the inclusion of cyber operations in the single Service and joint force planning processes is emphasised to enable the rapid employment of cyber assets as part of the full spectrum targeting process. This final point is important as it stresses that cyber should not be considered in isolation and that the maritime cyberspace is intimately linked to the rest of the maritime environment.

The challenge of preventing adversaries from exerting maritime power by compromising systems onboard ships is being addressed by several organisations, including Lancaster University. In a paper published in February 2016, the dangers of integrating previously separate systems into a single integrated network, which are then connected to the Internet, were raised. The practice of automating the control and management of these systems is becoming increasingly common with commercial providers offering Integrated Platform Management Systems (IPMS) that oversee all aspects of a vessel's propulsion plant and systems, whilst interfacing with navigation and communication suites on a single network. This provides a remote monitoring and control capability via satellite link that reduces the number of personnel needed onboard to check systems *in situ* and enables the rapid detection and response to maintenance issues as they occur. Suppliers of IPMS reduce risk and cost by relying on well-established technologies such as operating systems and networking components that would be familiar in a home or office environment. Reliability is ensured by incorporating proven Commercial Off The Shelf (COTS) components that have been used in a range of environments and designed using open architectures and industry standard protocols. This enables systems to be easily configured, reconfigured, and upgraded with a range of software packages to suit the individual needs of the customer.

Although using commonly available products and software that are proven and reliable provides reassurance that a system will work, they also present a range of vulnerabilities that may be exploited by those of malicious intent or through negligent action. Software that is in widespread use is also the most frequent to be targeted by malevolent parties as their efforts in understanding and learning how to alter the computer code will be rewarded by any exploits that are developed being able to be reused effectively against a broad range of targets. An appreciation of what type of technology is used in ships and then being able to easily acquire copies to work on will also make their task easier. Similarly, systems that are intended to be upgraded are designed to be easily accessible, which further increases their vulnerability to malicious interference. Ships that are frequently at sea and subject to reduced Internet bandwidth may also fail to update their Operating Systems with the latest security patches leaving them susceptible to exploitation by known vulnerabilities. Operating Systems themselves may also not be updated when they are no longer supported by their developers as to do so will incur costs including that of a possible hardware upgrade if needed to run the new software. Ship owners may also choose to accept the risk of using obsolescent software if they are running specialist applications that are not compatible with the latest version that would need additional investment to ensure their continued use.

There is no shortage of methods available by which a ship's system integrity can be compromised, either intentionally or by accident. A direct connection to the network by an infected laptop or USB connected memory drive may be the easiest method, but wireless networks or remote access logins via an Internet connection may also be a convenient means to access the system. A vessel in port with a network that is unencrypted or protected by a weak password would present an attractive and easily accessible target. In addition, the use of multifunctional control terminals also presents another system weakness as once compromised, they could provide access to the entire network and its subsystems.[63] This threat to the shipping and the maritime environment through activities in cyberspace i.e. *cyber seapower*, has been recognised by being the subject of regular conferences and seminars hosted by or aimed at the global

shipping industry. The purpose of these conferences can range from increasing the general awareness of the threat and offering some vendor neutral advice to those sponsored by the providers of specialist security products or maritime insurance services.

Exploiting maritime cyberspace for power projection at a state level brings into focus the issues that are discussed in later chapters of whether the environment can be used to conduct warfare in its true sense or whether its role is restricted to purely soft power means of using non-coercive methods of persuasion and using the powers of attraction to alter behaviour. Power projection by one state against another may involve offensive activities that may be regarded as hostile, but fall short of warfare in its accepted sense. In arguing that warfare must be violent, potentially lethal, and instrumental in achieving an end state, Thomas Rid suggests that it cannot be achieved solely by actions in cyberspace, which exhibit only the consequences, not the characteristics of conflict.[64] He also emphasises that warfare must be political, rather than criminal in nature and has been described as an act of force to compel an adversary for one nation to exert its will over another with clear attribution of the aggressor by the defender. In proposing that offensive acts in cyberspace cannot be categorised as warlike; Rid suggests instead that they fall into one of the three categories of espionage, sabotage and subversion, which provides an important classification of where the attack is to be targeted and what effect is intended to be achieved. [65] However, it should be noted that regardless of how the attacker may wish their intentions to be understood, the significant aspect in all international relationships is not the act itself, but how their victim perceives it, which if misunderstood may lead to a rapid escalation of events. [66]

Although cyberwar has attracted much comment and analysis, previous work has viewed cyberspace as a single entity and that cyber related attacks have an equal effect across it. Rid's examination of the nature of cyber-attacks is agnostic of the environment from which it emanates or the nature of the target. The implications of how the source and destination of offensive cyber operations can affect its efficacy or method of implementation is worthy of study both from the perspective of both attackers and defenders. Based on Rid's work

and depending on the results of this analysis, it may be determined that the unique attributes of the maritime environment may favour one type of attack over another or that it may be concluded not to be an appropriate means to attack an opponent at all. Similarly, the same work may inform a defender of where their systems and networks are most vulnerable and from where an attack will emanate. This may then enable decisions to be made as to where to review or reinforce network defences.

Conclusion to chapter 5

This chapter has begun to address the second question posed by this research by highlighting the relationship between the maritime and cyber environments and that in the area where the properties of both coincide dependencies exist in terms of power projection and security. To explain this relationship, it has introduced the concept of *maritime cyberspace*, which can be described as those elements of the two environments that rely on each other to be fully utilised and where the attributes of one affect the properties of the other. The maritime environment is complex both in terms of its role to society and how changes in its physical attributes can determine how operations can be conducted within and from it. All nations, even landlocked ones rely on maritime trade for the transport of fuel, raw materials and manufactured goods and the global economy is dependent upon sea lanes and choke points being available for shipping and safe from maritime crime. Water depths, weather, tides, currents, and density of shipping combine to make the maritime environment a dynamic and at times dangerously unpredictable one in which to operate and access cannot always be guaranteed. The attributes of maritime cyberspace can assist in making the use of the seas a safer and a more productive and therefore economical place to operate and is therefore an important component in maintaining global trade. This may result in maritime cyberspace becoming a contested environment as control or denial of its constituent components could become an important aspect in a future conflict.

The seas are often an area of dispute as neighbouring nations compete for limited resources in adjacent waters and their importance as a source of food,

fuel or means of transportation is such that when access is interrupted it can result in matters that would otherwise be regarded as being solely foreign policy concerns rapidly becoming domestic issues. These legal, political, and diplomatic disputes can quickly become militarised as nations seek to protect access to what they regard as their own waters, while exerting influence on those claimed by other nations that are disputed.

To explain cyberpower at sea, this chapter has introduced the two distinct but related terms of *maritime cyberpower* and *cyber seapower*. In the former, the maritime cyber environment is used to contribute to the ability to project power from the sea to achieve an effect that may be local or at range. This involves the use of techniques and methods explained in later chapters to exploit the medium of cyberspace to alter the behaviour of a target individual, group, or population. Cyber seapower however uses the cyber environment to facilitate cyber sea control or cyber sea denial that is used either to establish the free use of an area of the sea or maritime cyberspace for a period of time or to deny its use to an adversary. The comparable properties of the cyber and maritime environments enable parallels to be made as to how these different forms of power can be exercised. A key conclusion from investigating the properties of maritime cyberspace is the demonstration of the link between security and power projection. For an adversary, whether a state actor or criminal, to be able to exert influence on the target system, there is a need to be able to access it. Effective cyber security measures will prevent or limit the access that an aggressor will have and therefore restrict the effect that they hope to achieve. This highlights that there may be potential vulnerabilities within a component of maritime cyberspace that a threat actor may be able exploit. To understand and mitigate the risk of compromise it is essential to understand that the environment should be seen as a hostile one from the perspective of a defender and that protection strategies should be developed. After measures have been put in place to secure maritime cyberspace, these should be regularly re-assessed to determine whether the level of protection continues to be sufficient in an ever-changing threat landscape.

Academic institutions have only recently become aware of the issues that have arisen from combining elements of the maritime and cyber environments and how this may affect operations from a security context. More recent work has recognised and highlighted the role of the operator in maintaining system integrity. This is coherent with one of the most significant elements of both environments; that to fully engage with them the users must understand and interact with manufactured elements whether these are ships or computing devices. Indeed, cyberspace itself as an artificial environment created by humans seeking to harness the properties of the electronic components to create the networks and infrastructure required for it to function.

This chapter has highlighted that maritime cyberspace is unique in both comprising of and relying on several discrete capabilities. These are space based systems for position, navigation and time information, the Automatic Identification System for a range of navigational safety based capabilities and wireless communication from either space or terrestrial Radio Frequency based systems. The final element of maritime cyberspace comprises the hundreds of miles of fibre optic cables that cross the ocean floor connecting continents. The maintenance of these cables is crucial to the very existence of cyberspace. Combining the attributes from both environments is a complex undertaken and according to the Royal Navy required four elements. These are the people and training, maintaining network availability, incorporating maritime platforms into the wider planning and targeting process and finally not to consider the cyber component in isolation, but integrating it into the maritime and joint cyber environments. With the increasing trend to combine previously separate ship systems onto a single network controlled by an Integrated Platform Management System, which may be connected via satellite to shore based networks, whole vessels can now be considered part of maritime cyberspace and must be protected from attackers wishing to influence the behaviour of the ship’s company by compromising their systems.

The dependence upon the electromagnetic spectrum by maritime cyberspace highlights the importance of the emerging term of CEMA as combining Cyber and Electromagnetic Activities as it can be seen that they are inextricably

linked. Shipping can only engage with cyberspace by means of the electromagnetic spectrum across a range of frequencies and both contribute to and receive information from the wider cyber environment. It is acknowledged though that whereas the cyber environment draws on the electromagnetic environment as a communications medium to enable digital data to pass between nodes in a wider network, the radio frequency spectrum is also utilised for a wide variety of other purposes. This includes radar used for surveillance as well as the tracking and identification of targets for weapon systems, voice communications and for one-way broadcast media such as radio and television. The analysis of these different types of transmission, which may be on similar frequencies, is a discrete discipline that should encompass all the electromagnetic spectrum with its use by the cyber environment being a significant aspect.

This chapter has shown that the relationship between maritime cyberspace, cyber warfare and power projection can contribute to the enduring debate of whether conflict in cyberspace meets the accepted criteria for what defines warfare. However, what is important is the context of how the defending nation interprets a potentially hostile act, regardless of the intent of the attacker. Thomas Rid's conclusion that offensive action in cyberspace can be described in terms of espionage, sabotage, or subversion provides a useful baseline from which to consider ways by which the development of power in the maritime environment can be achieved, but also how it can be applied and importantly measured in maritime cyberspace.

To fully explore the relationship between maritime cyberspace and Rid's three activities, it is necessary to apply the model of cyberspace developed in chapter 4 to a campaign of power projection in the maritime environment. This model will allow Rid's three categories to be applied in a more nuanced way focused on power projection and concentrates on how they can each contribute to achieving the end state of altering the behaviour of a target individual, group, or population. This enables the activities themselves to be regarded as the ways and means and not the objective itself. Therefore, although for example subversion has a direct application to altering a target's mindset, the role of

sabotage is viewed not from the aspect of attempting to cause damage for its own sake, but as a means to demoralise an adversary as part of a process to alter their behaviour.

Endnotes to chapter 5

[1] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre. P.v
[2]Development, Concept and Doctrine Centre, 2007. *Future Maritime Operating Concept.* 1st ed. London: Ministry of Defence. Para 123
[3] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre. P.iii
[4] United Nations, 1982. *United Nations Convention on the Law of the Sea.* [Online] Available at: http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf. [Accessed 12 Apr 2016].
[5] United Nations, 1982. *TERRITORIAL SEA AND CONTIGUOUS ZONE.* [Online] Available at: http://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm. [Accessed 12 Apr 2016].
[6] International Seabed Authority, 2014. *International Seabed Authority.* [Online] Available at: https://www.isa.org.jm/. [Accessed 12 Apr 2016].
[7] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office. P.9
[8] Development, Concepts and Doctrine Centre, 2010. *Future Character of Conflict,* London: Ministry of Defence.p40.
[9] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office.p17
[10] Port of Dover, 2016. *Operations / Vessel Traffic Service.* [Online] Available at: http://www.doverport.co.uk/operations/vessel-traffic-service/. [Accessed 12 Apr 2016].
[11] Lillian Goldman Law Library, 2008. *Laws of War : Rights and Duties of Neutral Powers in Naval War (Hague XIII); October 18, 1907.* [Online] Available at: http://avalon.law.yale.edu/20th_century/hague13.asp [Accessed 12 Apr 2016].
[12] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office. P.17
[13] United Nations Environment Programme, 2016. *IEG of the Global Commons.* [Online] Available at: http://www.unep.org/delc/GlobalCommons/tabid/54404/. [Accessed 12 Apr 2016].
[14] Other Worlds, 2016. *Defending the Global Commons.* [Online] Available at: http://www.otherworldsarepossible.org/defending-global-commons. [Accessed 12 Apr 2016].
[15] Dataquest, 2012. *Cyberspace as Global Commons: The Challenges.* [Online] Available at: http://www.dqindia.com/cyberspace-global-commons-the-challenges-1/. [Accessed 12 Apr 2016].
[16] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.
[17] World by Map, 2015. *http://world.bymap.org/Coastlines.html.* [Online] Available at: http://world.bymap.org/Coastlines.html. [Accessed 12 Apr 2016].
[18] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.1-4
[19] BillieBox, 2016. *Facts about Shipping containers.* [Online] Available at: https://www.billiebox.co.uk/facts-about-shipping-containers/. [Accessed 12 Apr 2016].
[20] BBC News, 2015. *On board the world's biggest ship.* [Online] Available at: http://www.bbc.co.uk/news/magazine-31813045. [Accessed 12 Apr 2016].
[21] Maritime Connector, 2017. *Panamax and New Panamax.* [Online] Available at: http://maritime-connector.com/wiki/panamax/. [Accessed 2 June 2016].
[22] The Guardian, 2006. *How world's biggest ship is delivering our Christmas - all the way from China.* [Online] Available at: http://www.theguardian.com/uk/2006/oct/30/christmas.shopping. [Accessed 12 Apr 2016].
[23] Marine Insight, 2011. *The TI Class Super Tankers: The Fantastic Four.* [Online] Available at: http://www.marineinsight.com/types-of-ships/the-ti-class-super-tankers-the-fantastic-four/. [Accessed 12 Apr 2016].
[24] Global Firepower, 2015. *Oil Consumption data.* [Online] Available at: http://www.globalfirepower.com/oil-consumption-by-country.asp. [Accessed 11 Apr 2016].
[25] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre. P.2-7

[26] NATO, 2014. *Allied Joint Doctrine for Air Maritime Coordination AJP-3.3.3.* 1st ed. Brussels: NATO.
para 0303
[27] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.2-13
[28] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence. p1-1
[29] Ministry of Defence, 2013. *Defence Information and Communications Technology Strategy.* 1st ed. London: Ministry of Defence. P8
[30] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence. p1-3
[31] Department of the Army, 2014. *Field Manual 3-38 Cyber Electromagnetic Activities,* Washington DC: Department of the Army.
[32] HM Government, 2015. National Security Strategy and Strategic Defence and Security Review, London: Her Majesty's Stationery Office.
[33]Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.iii
[34] Nye, J. S., 2011. *The Future of Power.* 1st ed. New York: Public Affairs.p.123.
[35] Development, Concepts and Doctrine Centre, 2010. *Future Character of Conflict,* London: Ministry of Defence.
[36] GPS.gov, 2014. *What is GPS?.* [Online] Available at: http://www.gps.gov/systems/gps/. [Accessed 12 Apr 2016].
[37] GPS.gov, 2016. *Space Segment.* [Online] Available at: http://www.gps.gov/systems/gps/space/. [Accessed 12 Apr 2016].
[38] GPS.gov, 2015. *Control Segment.* [Online] Available at: http://www.gps.gov/systems/gps/control/. [Accessed 12 Apr 2016].
[39] US Air Force, 2015. *Global Positioning System.* [Online] Available at: http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104610/global-positioning-system.aspx. [Accessed 12 Apr 2016].
[40] European Space Agency, 2016. *Galileo navigation.* [Online] Available at: http://www.esa.int/Our_Activities/Navigation/The_future_-_Galileo/What_is_Galileo. [Accessed 12 Apr 2016].
[41] Beebom, 2015. *What is GLONASS And How It Is Different From GPS.* [Online] Available at: http://beebom.com/2015/05/what-is-glonass-and-how-it-is-different-from-gps. [Accessed 12 Apr 2016].
[42] Balduzzi, M., Wilhoit, K. & Pasta, A., 2014. *A Security Evaluation of AIS,* Texas, USA: Trend Micro.
[43] International Maritime Organisation, 2016. *AIS Transponders.* [Online] Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx. [Accessed 12 Apr 2016].
[44] HM Government, 2014. *Mapping UK shipping density and routes from AIS (MMO 1066).* [Online]
Available at: https://www.gov.uk/government/publications/mapping-uk-shipping-density-and-routes-from-ais-mmo-1066. [Accessed 12 Apr 2016].
[45] Maritime and Coastguard Agency, 2014. *Dover Strait crossings: channel navigation information service (CNIS).* [Online] Available at: https://www.gov.uk/government/publications/dover-strait-crossings-channel-navigation-information-service/dover-strait-crossings-channel-navigation-information-service-cnis#how-cnis-works. [Accessed 12 Apr 2016].
[46] Vessel Finder, 2016. *Real-Time AIS Data.* [Online] Available at: https://www.vesselfinder.com/. [Accessed 12 Apr 2016].
[47] Nichol, M., 2017. *Big Lizzie's location is top secret, says MoD (But anyone – including Mr Putin – can track her on this FREE smartphone app!).* [Online} Available at: http://www.dailymail.co.uk/news/article-4658082/Free-app-showing-location-HMS-Queen-Elizabeth.html . [Accessed 16 Jul 2017].
[48] Marine Source, 2016. *Satellite AIS Data.* [Online] Available at: http://www.marinetraffic.com/en/p/satellite-ais. [Accessed 12 Apr 2016].
[49] Inmarsat, 2016. *Fleet Broadband.* [Online] Available at: http://www.inmarsat.com/service-collection/fleetbroadband/. [Accessed 12 Apr 2013].
[50] Thuraya, 2016. *Marine Comms.* [Online] Available at: http://www.thuraya.com/marine-comms. [Accessed 12 Apr 2016].

[51] Encyclopaedia Britannica, 2016. *Transmission media and the problem of signal degradation.* [Online] Available at: http://www.britannica.com/topic/telecommunications-media. [Accessed 12 Apr 2016].
[52] Computernetworkingsimplified.com. *Relationship between Bandwidth, Data Rate and Channel Capacity.* [Online] Available at: http://computernetworkingsimplified.com/physical-layer/relationship-bandwidth-data-rate-channel-capacity/. [Accessed 12 Apr 2016].
[53] Sailcom Marine, 2016. *HF shortwave SSB radio email systems.* [Online] Available at: http://www.sailcom.co.uk/pactor/. [Accessed 12 Apr 2016].
[54] yachtcom, 2016. *Long Distance Communications Made Clear and Simple.* [Online] Available at: http://info.yachtcom.co.uk/HF/. [Accessed 12 Apr 2016].
[55] Isode, 2016. *Why IP over HF Radio should be Avoided.* [Online] Available at: http://www.isode.com/whitepapers/ip-over-stanag-5066.html. [Accessed 12 Apr 2016].
[56] Business Insider Science, 2015. *Animated map shows the undersea cables that power the internet.* [Online] Available at: https://www.youtube.com/watch?v=llAJJI-qG2k. [Accessed 12 Apr 2016].
[57] Starosielski, N., 2015. *The Undersea Network.* 1st ed. Durham and London: Duke. p.1
[58] Business Insider Science, 2015. *Animated map shows the undersea cables that power the internet.* [Online] Available at: https://www.youtube.com/watch?v=llAJJI-qG2k. [Accessed 12 Apr 2016].
[59] Starosielski, N., 2015. *The Undersea Network.* 1st ed. Durham and London: Duke.p.31
[60] Blum, A., 2012. *Tubes - Behind the scenes at the Internet.* 1st ed. London: Penguin. p.194
[61] Starosielski, N., 2015. *The Undersea Network.* 1st ed. Durham and London: Duke.p.9
[62] Royal Navy. *Cyber Strategy.* Portsmouth. 2016.
[63] Venables, A., 2016. Protecting Ships - The Threat of Hackers. *Port Technology*, 69 Edition, pp. 30-31.
[64] von Clausewitz, C., 1832 (1980). *Vom Kriege.* 1st ed. Berlin: Ullstein. p.27.
[65] Rid, T., 2013. *Cyberwar will not take place.* 1st ed. London: Hurst.
[66] Gray, C. S., 2005. *Another Bloody Century.* 1st ed. London: Orion. p.294.

Chapter 6: Intelligence gathering in maritime cyberspace

Introduction

This chapter is the first of three that contribute to all three research objectives of this thesis. Previous chapters explained the composition of cyberspace in three dimensions in a manner that was optimised for power projection and highlighted the intimate nature of the relationship between the maritime and cyber environments, leading to the introduction of the notion of maritime cyberspace and how it relates to the new model of cyberspace. This new analysis of cyberspace illustrates which elements of the maritime cyber environment can be exploited as a means to project power and what techniques could be used to achieve a desired end state. By combining the conclusions from these previous chapters, the next three chapters provide an in-depth analysis of how different types of cyberpower can be projected within and from the maritime environment, highlighting that the properties of cyberspace differ depending upon the environment in which its infrastructure and users are located.

The concept of power can be described as altering the behaviour of people, either willingly or under coercion, and the work of Rid is used here as the basis for describing its different forms and is used to explain how operations can be utilised within maritime cyberspace to influence a target. In his argument that *cyberwar has not and will not happen*; Rid proposes that political cyber-attacks can be classified as just sophisticated versions of three activities; espionage, sabotage, and subversion.[1] What he does not seek to do is expand on is how the different components of cyberspace can be harnessed to achieve these effects and how different aspects of the environment can be levered in a range of ways. In terms of power projection, Rid also does not discuss in detail the challenges of creating the desired effect in far space at range from a source in an adversary's near space and how the properties of cyberspace can differ between them.

Although espionage, sabotage, and subversion were used by Rid to classify what he regarded as the different types of offensive cyber activity, they also provide an indication of the different methods that can be employed in order to facilitate power projection, either on their own or coordinated with the others to maximise their impact. Espionage, as part of the broader discipline of intelligence gathering is a function that is continually conducted during a campaign of power projection. Its purpose is to acquire information about or directly from an opponent, either as a precursor activity for acts of sabotage or subversion or to determine the nature and intent of an adversary's own power projection activities. Sabotage is a hard power activity that seeks to target people indirectly by attacking the systems upon which they rely and can do this in several ways depending on the desired effect to be achieved or the ease by which it can be undertaken. For example, it can be coercive to alter behaviour through force after a conflict has started or it can be used as an anticipatory measure prior to the start of hostilities to prevent the adversary being able to conduct their own pre-emptive attacks. The final method, subversion, is the purest form of power projection as it attempts to engage directly with humans to alter their behaviour through soft power by persuasion, hard power coercion or by a combination of these techniques as part of a hybrid strategy. In this section, the link between subversion, propaganda, and the military discipline of Psychological Operations (PSYOPS) is made as they can be regarded as being closely aligned in operational planning. The connection between a cyber-attack and power projection is also emphasised throughout in that both require an intimate knowledge of the target that can only be achieved through intelligence gathering followed by the implementation of active measures to achieve the intended effect. It is the very nature of both sabotage and subversion that they are not accidental, but are deliberate, planned actions that seek to cause an alteration of behaviour by the target. Thus, by categorising power projection in terms of these three types of activity a link can be made with other offensive actions and what they hope to achieve.

In addition to referring to the research of Rid, these next three chapters also draws on the work of the scholars and military doctrinal publications that were first introduced in chapters 2 and 3 that contribute to the overall understanding

of cyberpower in the maritime environment. These enable for the first time offensive activities in cyberspace to be assessed in terms of the unique attributes of maritime cyberpower and cyber seapower within the context of the new model of cyberspace proposed in chapter 4. The unique attributes and role of each element of the cyberspace model allows these three offensive activities to be viewed from the perspective of the layer which they affect and how, when they are combined, form the foundation of this investigation of cyberpower projection.

The characteristics that make the cyber maritime environment distinct from land, air and space relate primarily to the bearers used for the transmission of information. Whereas in the land environment a choice can often be made between wired or wireless communications, this is not the case at sea where only a single option may be available. To be most cost effective, efficient and provide capacity to meet demand, transoceanic communication between continents relies on fibre optic cable, but there is also a dependence on the element of the electromagnetic spectrum used for radio frequency communications for shipping as well as some fixed installations such as off shore oil platforms that do not have access to a wired network to exchange information. It should also be noted that both wired and wireless types of communications medium have vulnerabilities. Although the fixed, physical links are for the most part safe from most types of interference at depth, their routes are well known, which can make them susceptible to interference in shallower waters. Wireless communications may not be subject to physical attack, but do have weaknesses in that despite being able to facilitate mobile global connectivity, data exchange via radio frequency transmissions can be intercepted. This means that unless encrypted their contents can be subject to collection for analysis, manipulation or interference by state agencies or persons other than the intended recipient thereby making them a valuable target for intelligence gathering, sabotage or for subverting their users. At sea, very nature of shipping means that effective communications from shipping uniquely relies upon wireless communications and the need to have the correct, serviceable equipment and the facilities and resources to connect to use maritime cyberspace to connect to the wider cyber environment.

Information, Espionage, and Intelligence

Although Rid specified ‘espionage’, rather than ‘intelligence’ in his triptych of attack types, the latter term in used here as it encompasses the full range of techniques that can be employed to collect information from a target within cyberspace. Rid defines cyber espionage as an *attempt to penetrate an adversarial computer network or system for the purpose of extracting sensitive or protected information,* but the deliberate infiltration into computer systems to find and collect data is only one way of gathering information and there is just as much and possibly more data of value that can be retrieved from searches of freely available repositories and websites.[2] There must also be a careful delineation in defining information, intelligence and espionage as doctrinally there are significant differences between them that have implications in how the data is handled and interpreted.

Information is the raw product of cyberspace and can be defined as *unprocessed data of every description that may be used in the production of intelligence*.[3] Within cyberspace there are four distinct types of information, which are distinguished by the methods by which they are collected and highlight the nature of the environment as being one that is information based. The first type of information is that which is made freely available on line by the originator and of which they are aware. Social media postings, blogs, journals, company and organisation web sites and news agencies are ready sources of this type of information. However, as this type of information is designed to be retrieved, it may be deliberately erroneous as part of a campaign of deception.

The second type of information is related to the first in that it is freely available to access but was either planned for a limited audience or not intended for publication at all. Examples of this include individuals not properly configuring their social media postings to be viewed by only known acquaintances and consequently being available to all, or inadvertent disclosures on websites or other online media that may be of interest to a competitor or adversary. An example of this was the 2012 disclosure of Norwich City Football Club’s new team clothing by a fan who discovered an unpublished page on their website

by examining the freely accessible source code.[4] In this situation, although the material was uploaded onto the football club's web server, there were no direct links to it from the Internet facing web site with the intention that it would be added when the new clothing line was formally released. Although initially regarded as a criminal matter, the case was dropped after it was determined that there was no malicious intent, but it does emphasise the danger of making information unintentionally available to the curious or to those with a malicious disposition.

The third type of information that may be readily available but of which the originator may be unaware is meta data. This is *data about data* and includes a range of information types included within documents and files and may include its author, time of creation, version history and even location data. This can prove to be a valuable source of information and has been used to even catch out governments. In April 2015, Russian President Putin announced *I can tell you outright and unequivocally that there are no Russian troops in Ukraine*.[5] Yet in an Instagram posting, a Russian Army Sergeant posted a photograph of himself which was geotagged with GPS derived metadata embedded into the picture that revealed that he was in Ukrainian territory in an area controlled by pro-Russian separatists.[6]

To take advantage of this type of data, a range of specialist search engines and software have been developed to conduct in depth analysis of this *open source* information. These include *Creepy*, which extracts location data from pictures on social media that may have been added to the image file by the camera.[7] *The Harvester* is another readily available tool that searches public sources such as search engines and name servers for e-mail addresses, names and website configuration information.[8] With the increasing trend to connect industrial control systems and webcams to the Internet, a dedicated search engine, *Shodan*, has been developed to identify these devices and provide information related to their installation and security settings, which has highlighted the importance of properly configuring new devices and changing the factory default settings for passwords and access features. The ease by which unsecured Internet connected devices can be accessed has been

highlighted in a number of recent articles including one in which instructions were provided as to how to find vulnerable web cameras and access them without authorisation.[9] Notwithstanding the privacy concerns of voyeurs accessing webcams, more concerning is Shodan's ability to detect Supervisory Control and Data Acquisition (SCADA) or Industrial Control Systems (ICS), which in the maritime environment may form part of a port or marine infrastructure.[10] Once, identified, these may then be subject to further techniques to discover any security vulnerabilities, which may lead an attacker to gain total control of the system. As ships themselves become more connected, their use of the same components as shore based systems means that there is a danger that they too may come to the attention of applications such as Shodan and be susceptible to attack, which may have immediate consequences for a vessel at sea.

The final type of information is that which is intended to be private and accessed only by the originator or by those who have been specifically approved by them. Access to this type of information may be restricted as its contents might be sufficiently sensitive to be of commercial benefit to a competitor or in the case of state information, of military benefit to an adversary. To protect it, this type of information may be encrypted, require a password to access its location or be contained within a network infrastructure that cannot be directly accessed from the global Internet. Due to its content, this material can be very valuable and this makes it an ideal target for an adversary who may benefit from its knowledge directly or for a criminal who although themselves may not profit from it may hope to gain financially from selling it on to another interested party. As methods have been taken to prevent ready access to this material by unauthorised personnel, to do so requires special measures and techniques and this falls within the realm of espionage. According to the UK's Secret Service, commonly known as MI5, espionage is the *process of obtaining information that is not normally publicly available*.[11] As espionage, or spying, involves the acquisition of information that is intended to remain hidden, cyberspace as part of the information environment is an ideal medium in which to conduct this activity as it can be conducted remotely with less risk to the agent and possibly with a lower risk of detection and attribution. Rid notes that

this activity is usually covert in nature and this is for two reasons, the first being that the techniques used to access the restricted material itself are of value and would need to be protected to stop the victim taking mitigation measures to stop them being used again in the future. This is particularly significant where an encryption system has been successfully compromised or bypassed, perhaps after significant time and effort. Knowledge of this compromise would simply result in a change of encryption method, rendering the previous work nugatory. Secondly, as the victim has intended the material to be restricted, if it becomes known to have been compromised, it may alter their behaviour resulting in the attacker losing the advantage from having the information.

Having acquired information from an adversary from one of the four sources described above, it must be analysed to be of value. Data on its own is of little use unless it is viewed in context and applied to a particular scenario or course of events. This process converts information to intelligence, which is defined by the UK Ministry of Defence as *the directed and coordinated acquisition and analysis of information to assess capabilities, intent, and opportunities for exploitation by leaders at all levels.*[12] Information gathering and its conversion to usable intelligence is a complex process and is dependent to a large extent on the method by which it was gathered and its source. For this reason, it is divided into several different types, which although distinct in their own right, may be combined for the purpose of achieving a particular mission and some of which have a role in the cyber environment. The key types of intelligence sources and their relationship with maritime cyberspace are described in Appendix 2.

The role of intelligence operations in cyberpower projection

Intelligence operations by themselves will not alter the perceptions or behaviour of a target group. Indeed, if carried out properly, they may not even be aware that they are being subject to surveillance in anticipation of a future operation against them. However, without an intelligence campaign, methods of power projection may not work or have limited success. By gaining as much relevant information on an adversary as possible through effective intelligence

gathering, the optimal means of constructing and delivering an effect on a target can be identified and conducted. It is for this reason that having comprehensive intelligence on every layer of an adversary's' near space can be regarded as an essential precursor and supporting activity to any power projection activity and should be included in all aspects of planning a cyberpower campaign. Understanding the totality of an attacker's near space from what type of message the human target is most liable to be receptive to down to understanding the availability and reliability of their infrastructure and services leads to a comprehensive *cyber situational awareness* of the target. This must be as complete as possible for the power projection plan to be designed with the best available information to give it the greatest chance of success.

Where information about an individual layer is not complete, this is regarded as an *intelligence gap*, leading to an *intelligence requirement*, which an *intelligence agency* will be tasked to fill using the resources at their disposal.[13] Obtaining the information to fill this knowledge gap may not necessarily come from cyber means at all, but may call on any of the types of intelligence listed above. What is important is that the process is methodological and properly coordinated with the risk of compromising the operation weighed against the potential benefits that can be obtained from exploiting the information sources available. Information gathering and intelligence analysis does not cease at the start of an operation against a target, but continues throughout to gauge its success and how opinions of the target group may be affected and changed to the advantage of an attacker. To achieve this, measures of effectiveness will be identified early in a campaign and key indicators highlighted in determining whether it is working and if it is being completed in accordance with the time scale of the campaign plan. This requires a careful assessment to determine whether the effect recorded is caused by the campaign, is the result of other external factors, or maybe purely coincidental.

The conduct of intelligence operations through the medium of maritime cyberspace enables its unique attributes to be harnessed to facilitate the collection of information that would otherwise be unavailable to the collector. At the core of this ability is access to the seas or coastal regions and be able to

retrieve the information being transmitted through maritime cyberspace. This level of access may be directly related to being able to locate a collector in close proximity to the near space of the target within range of their transmissions or it may be that the flexibility offered by a collector afloat enables it to position in an area that a terrestrial collection would not be able to retrieve the target signal. It should also be noted that although much of this information may be specifically related to sea going activities, it may be that strategic information not related to the conduct of maritime operation may be collected. This may have wider significant to influence national policy and emphasises the importance of maritime cyberspace and a maritime collector in being able to retrieve intelligence information that cannot be obtained through other means over an extended period whilst operating at sea.

Espionage in the pursuit of maritime cyberpower

The maritime environment can offer nations a unique and powerful means to obtain information on an adversary's use of cyberspace due to the levels of access that can be achieved. If the analysis of the data collected exposes vulnerabilities that can be exploited, it can be an important element in the planning of an overall cyberpower campaign. This essentially involves using a range of maritime vessels to collect intelligence on the high seas and in the littoral and since the end of the second world war, there has been a tradition of nations using specially equipped ships as Signals Intelligence (SIGINT) platforms able to collect a range of voice communications and electronic emissions. Intelligence gathering need not be completely covert, particularly if the ships are operating in international waters. For example, the spy ships of European nations tend to leave no doubt as to their purpose as demonstrated by the Norwegian *Marjata*, shown in figure 12, which has a distinctive wedge shape design for increased stability in high seas.[14]

Figure 12: The Norwegian spy ship Marjata[15]

Russia and America also have a fleet of vessels suspected of intelligence gathering, although in the past they have chosen to nominally disguise their roles. Since the 1950s Russia has used trawlers for intelligence gathering with their hull design enabling them to operate in all weathers and which as noted by Judson Knight are designed with large compartments for fish, but could be converted for 'other activities'.[16] Despite nominally having the same design as fishing vessels, as shown in figure 13, the surfeit of aerials reveals their true purpose. More recently though, Russia has adopted the European model and has operated ships designed specifically for collection tasks that are overt in nature such as the *Yantar*, which although officially termed a Research ship, has been suspected of being employed for espionage tasking.[17]

Figure 13: Cold War Russian Spy Ship Linza[18]

The US currently appear not to operate publicly declared dedicated SIGINT collection vessels and it is suspected that this capability is part of the equipment fit of the nation's warships. This policy may be because of two well publicised historical incidents in which lightly armed specialist intelligence gathering vessels were attacked with significant loss of life. The first of these was the USS LIBERTY, which was attacked in international waters by Israeli forces during the 1967 6-day war with Egypt, which resulted in the loss of 34 American crewmen and 171 wounded. As a result of the attack, the damage to the ship was so extensive that it was later scrapped.[19] The second incident occurred 7 months later when the USS PUEBLO was attacked and captured by North Korean forces with a crew member killed. The remainder of the crew were held captive for 11 months and to this day the ship remains on display as a museum ship in Pyongyang as shown in figure 14.[20]

Figure 14: USS Pueblo today[21]

In the past, these types of intelligence gathering ships were tasked to collect and analyse radio and other electronic transmissions. Unencrypted communications provided immediate real-time intelligence benefit, but those that had been encoded were recorded for later non-real time analysis. With the advent of the increased use of digital data communications, the capabilities of these vessels could now be diverted to collect non-voice transmissions, which could be of strategic, rather than tactical significance. Although most of what comprises cyberspace consists of cabled connections, wireless transmissions are still widely utilised, most notably in the use of point to point microwave links and for data exchange via mobile telephony, which could be collection targets for ships operating outside territorial waters. Microwave transmitters are typically placed approximately 50km apart and so a link perpendicular to a coast may have spill over and be capable of being received at sea.[22] Mobile telephones can connect with towers between 22 – 45 miles away and so their emissions would also be able to be received by a suitable equipped vessel at sea.[23]

Although the reception of these radio transmissions requires a ship to be positioned in international waters relatively close to the coast, it is also possible to conduct some types of collection operations on the high seas. These other sources of information collection are illustrated by the French ship *Monge*, shown in figure 15, which is officially is a missile range instrumentation ship used for space surveillance but is reported to be also capable of satellite tracking and monitoring.[24] The US Navy also operates a satellite tracking ship, the *USS Howard O. Lorenzen*, which has been linked to a previously demonstrated capability to destroy a satellite in orbit.[25] The Chinese have also been active in this area with the deployment of the *Yuan Wang* class. Although details of their specification and employment have not been released by the Chinese authorities, the ships' configuration is such that it can be deduced that it can also be used for space tracking and surveillance tasks.[26]

Figure 15: French Ship Monge Missile Range Instrumentation Ship [27]

As well as surface ships, submarines are ideally suited for intelligence collection tasks. Their covert nature enables them to penetrate territorial waters and with a collection antenna that just breaks the surface of the water, the chance of detection is small, particularly at night. These masts may be covered in radar absorbent material that further reduces their chance of being discovered by

surveillance systems.[28] Submarines from many nations have historically been employed for intelligence collection tasks and in this respect, what may be regarded as the older, less sophisticated technology of diesel electric propulsion can be a better intelligence collection platform in coastal regions than nuclear submarines due to their smaller size, lower acoustic signature, and ability to operate in shallower waters.[29]

The final component of maritime cyberpower to be discussed is the most challenging to accomplish by maritime units, yet has the potential to be most productive in terms of intelligence collection opportunities. Although the development of maritime cyberpower so far has concentrated on the interception of wireless transmissions, be they from satellites, cellular networks, or microwave links, they only form a small element of cyberspace and usually only the final stages of a communications link to the end user. The majority of cyberspace is wired and in addition to the domestic national infrastructures, ninety-nine percent of international data is transmitted by fibre optic cables that transverse the ocean. In 2015 there were 300 undersea cable systems covering 550 000 miles globally, enough to circumvent the world 22 times.[30] The challenge of laying and maintaining these cables is significant with some laid over 25 000 feet below the ocean's surface. The cables themselves are less than 3" thick and comprise a cluster of several smaller cables providing a degree of redundancy and greater capacity. With so much information crossing the oceans within these lines, they are a very attractive target for intelligence gathering operations, particularly as once clear of territorial waters on the High Seas these activities can continue unimpeded by national forces.

The potential vulnerability of undersea cables to interference by intelligence agencies has a historical precedent in 1971 with *Operation Ivy Bells*, in which the specially converted US Submarine *Halibut* laid a tap on the telephone lines connecting the Soviet Union's missile submarine base at Petropavlovsk to the Pacific Fleet Headquarters in Vladivostok under the Sea of Okhotsk.[31] Initially, the equipment recorded telephone calls on analogue tapes that were changed monthly, but later nuclear powered devices could store a year's worth of data from dozens of telephone lines. The operation was highly successful and

continued until compromised in 1980 by NSA employee Ronald Pelton, who revealed details of the multi-million dollar mission for $35 000 in an attempt to mask his own bankruptcy.[32]

The network of undersea cables that form the world's Internet communication by linking the near space of different countries through mid space presents a tempting target for intelligence agencies and 33 years after the exposure of the telephone tapping of Operation Ivy Bells, another NSA employee, Edward Snowden revealed details of how the advent of the digital age had purportedly led to a combined NSA and GCHQ operation to tap the fibre optic cables that joined continents. A significant difference between tapping telephone and fibre optic cables that carry Internet traffic is that the capacity of fibre is much greater and that the routing infrastructure of the Internet is such that world-wide traffic can be collected from a single location. Snowden revealed details of the alleged *Tempora* program that supposedly collected information from cables as they came ashore in the UK and that advances in technology had transformed intelligence collection.[33] Whereas *Ivy Bells* collected in non-real time with the submarine placing recording devices that had to be retrieved at regular intervals and returned to the US for analysis. *Tempora*, it was reported, could collect in real time with computer aided searches identifying key words that identified communications of interest. The quantity of data that could be retrieved also differed with *Ivy Bells* stored on tape that could be retained indefinitely whereas information from fibre could only be kept for up to 30 days due to the quantity of material passing through the cables.[34] A significant feature of the *Tempora* program was that although it supposedly tapped undersea cables, it did so as they came ashore in near space on UK and US soil and, controversially, with the apparent acquiescence of their domestic telecommunications companies. More challenging would be to achieve the same effect in mid or far space without the knowledge of those maintaining or owning the cables, but clearly that would enable traffic that was not routed through friendly countries to also be monitored.

In 2005, it was reported in the Associated Press that the US Navy was developing this very capability and that a submarine, the *USS Jimmy Carter*

had been converted to carry specialist personnel and equipment to tap cables. It was suggested that this may be conducted at the regeneration points where signals are amplified and retransmitted as the cables are unbundled and laid out individually. [35] This could be achieved using optical splitters that divert a small amount of the light away from its intended path.[36] Although the depths at which modern nuclear submarines such as the *Jimmy Carter* can operate are a closely guarded secret, depending upon the seabed topography of a target nation, this depth may be in international waters outside the sovereign seas of the target nation enabling it to operate with impunity. More recently in 2016, open source tracking information of the Russian Research ship *Yantar* acquired from *www.marinetraffic.com* revealed that it had been noted loitering in the vicinity of underwater cables connecting Syria and Cyprus in the Eastern Mediterranean. Analysis of the vessel's search pattern and speed led to speculation that she may had deployed manned or unmanned submersibles that she is known to carry to conduct intelligence gathering operations on the cables.[37] This is not the first time that Yantar has been suspected of this type of activity as in 2015 she was located operating off the coast of the US where undersea cables from Guantanamo Bay land.[38]

Espionage and cyber seapower

Establishing and maintaining seapower is a complex, time consuming and expensive undertaking. The oceans are large and with unpredictable weather it can be challenging to maintain forces in the right location at the right time that are properly equipped and supplied for an extended period. Should conflict arise, any advantage that one of the belligerents can lever from intelligence gathering operations can make the difference between victory and defeat. In the pre-Internet, Cold War period, the US Navy was unquestionably the most powerful and technologically advanced in the world. With its nuclear-powered aircraft carrier fleet and large numbers of surface ships and submarines, it was assumed to be able to project seapower globally. However, due to the activities of what has become known as the *Walker-Whitworth spy ring*, it has been argued that material passed to the Russians during this time could have given their navy a winning edge in a war with NATO.[39] Motivated by money, former

US navy Chief Warrant Officer John Walker, his brother Arthur, son John and fellow senior rating Jerry Whitworth passed sensitive military material including cryptographic keys to the Russians. Using the communications equipment captured from the USS Pueblo, it became possible for the Soviets to decrypt US and NATO communications providing them with intelligence that could have been invaluable during a conflict between NATO and the Warsaw Pact nations at sea.

The impact on the balance of seapower by being able to intercept and decipher enemy naval communications had previously been demonstrated during the Battle of the Atlantic where the size of the ocean and difficulty in locating enemy submarines presented challenges unique to the maritime environment. It was the work of Alan Turing in being able to break the German Naval *Enigma* codes that gave the allies an enormous advantage in being able to determine the location of U-boats and direct convoys away from them.[40] It is estimated that the ability to read the Enigma codes shortened the war in Europe by as many as two to four years, during which time greater fortifications could have been built along the French coastline making invasion more difficult and larger numbers of V1 and V2 missiles could have been launched against southern England with great loss of life.[41]

In the Internet age, not only are military communications potential targets for intelligence gathering operations, but the increased use of commercial off the shelf (COTS) products also presents a valuable target. In particular, vulnerabilities in commercial satellite communication systems onboard both naval and commercial vessels that may not have been subject to the same design rigor as military systems may exist, which could be exploited for intelligence gathering. Although the space based segments of commercial satellite systems are currently regarded as being resilient to common forms of attack and as yet there have been no reports of successfully compromising a satellite, recent research has revealed a range of vulnerabilities in the end terminals used by users. These included hardcoded credentials common to all devices, the use of insecure protocols and backdoors that could be exploited by an attacker in a range of scenarios.[42] Hardcoded credentials would enable

anyone with a knowledge of them to access any similar device and using protocols with known weaknesses would also enable a knowledgeable attacker to monitor communications. Backdoors are methods by which security can be bypassed to gain control of a system and although often included by developers in the system production process, they can remain in place in the final products. Although the researchers that discovered these issues did not publicly release them and only informed the manufacturers of their findings to enable software patches to be developed, they emphasise that notwithstanding the investment in communication infrastructure and end user devices, software can still be the weak point in any computer based system.

Being able to exercise seapower against an adversary, particularly a technologically superior one, requires as much of an understanding of their military capabilities as possible through intelligence gathering. In the past, this included the use of the type of tradecraft employed by the *Walker-Whitworth* spy ring of physically copying or removing documentation, but if data is stored electronically in far space on systems accessible through mid space and able to be exfiltrated, different methods can be employed. These techniques have the advantage of presenting little physical risk to the aggressor and may be achieved covertly with the victim only aware of the event after their data has been lost. Edward Snowden's leaks of classified US data has revealed the significance of China's cyber espionage campaign and its potential impact on the seapower of the US and UK navies. By targeting employees of the victim companies using cleverly crafted e-mails that looked genuine, but in fact contained attachments that when opened released malware, the Chinese could obtain unauthorised and undetected access to the computer networks. These *spear-phishing* campaigns proved remarkably successful in being able to gain access to a number of companies' data repositories.

Although China's alleged espionage did not directly involve the maritime environment, the impact on it may be considerable as it involved, among others, the new F35 fighter. This aircraft is the most expensive ever developed at a cost of around $400 billion and the vertical take-off F35B version will form the offensive capability of the new aircraft carriers being delivered for the Royal

Navy.[43] Indeed, as these ships do not have catapults or arrester wires, more commonly fitted to aircraft carriers of this size, they are totally dependent upon these highly specialised and costly aircraft for providing the air component of their maritime power projection capability. With as much as 50 terabytes of data stolen including information on radar tracking systems, this information could be used to develop countermeasures to their weapon systems and there is even evidence that this information has been used to influence the design of more recent Chinese fighters. Figure 16 illustrates the similarities between the US F-35 and the later Chinese J-31 aircraft.[44] Significantly, the attackers did not target military computer systems for this information, but those of the manufacturers with the prime contractor Lockheed Martin reported as suffering the most significant compromise. However, it was also reported that the systems of British Aerospace were breached emphasising that in the western nations, the development of complex weapon systems such as fighters are often multinational enterprises requiring commercially sensitive data to be duplicated in multiple networks across the globe.[45] This increases the number of threat vectors that an attacker can attempt to compromise and that it only needs a single one to be successfully exploited to reveal the information held by all.

Figure 16: Comparison between the US F-35 and Chinese J-31 fighters

A final example of cyber seapower is the role that non-state actors play in influencing the use of the sea by global shipping companies. Although operating at the at the other end of the technological spectrum from national maritime forces, their effects can have a global impact as has been seen from the

activities of pirates operating off the Somali and Yemini coasts. Pirates have a long history of hijacking ships for ransom or for stealing their cargo with the intention of selling it on and previously have used sea going vessels to patrol commonly used shipping lanes looking for suitable targets. More recently, however it has been reported that information transmitted by the Automatic Identification System (AIS) has been exploited by Somalis and Yeminis, who would normally earn a living as coastal fishermen, using their small craft to identify and intercept target ships transiting close to the coast.[46] With AIS receivers cheap, portable, easily procured and able to provide information on ships that included their name, position, course, speed and the type of cargo carried, these fishermen when armed with automatic weapons have been able to select their victims at will. After identifying a suitable ship, they have then used their AIS receivers to intercept their targets and subsequently board them, taking the crews hostage whilst diverting the vessel into coastal waters. The result of this was that ships that considered themselves vulnerable to attack altered their routes further south so as to be out of the range of the pirates' own boats and that the International Maritime Organisation (IMO) issued guidance suggesting that Masters of ships should consider turning off AIS completely if they considered it represented a threat to their vessels.[47]

The use by pirates of the freely available AIS data to conduct their activities and the resulting actions of the ship owners emphasises the effective use of maritime cyberspace as an intelligence tool without having recourse to the subterfuge which would normally be regarded as a facet of espionage to gain the information that was required. This use of the data from AIS, combined with cheap, low technology boats and weaponry led to what was in effect sea denial of the shipping lanes around the Yemini and Somali coasts. The rerouting of ships further south resulted in an increase in time and shipping costs, including a rise in insurance premiums to cover the risk of hijacking. Ultimately this threat was successfully mitigated with increased patrols from a coalition of nations deploying warships to the area and shipping better protecting themselves with physical barriers and barbed wire around the decks to counter any attempts at boarding.[48]

Conclusion to chapter 6

In a quote often attributed to Francis Bacon, it is said that *Knowledge itself is power* and as an extension it could be suggested that knowledge of cyberspace leads to cyberpower.[49] Collecting intelligence of all types ranging from that which is openly available to accessing a target's most closely guarded secrets is fundamental in generating that power. To be useful, intelligence must be relevant, timely and optimised to meet the needs of the collector. The maritime environment demands tailored intelligence to meet the requirements necessary to achieve sea control and sea denial and as navies increase their reliance on cyberspace to operate, this environment becomes more important as a source of critical information. Similarly, as nations themselves become more connected, both internally and externally, globally accessing these links to gather information becomes more attractive. Ideally achieving this locally within the collectors' near or mid space reduces the probability of detection but intelligence gathering in the near space of the target may enable them to circumvent security measures placed at a nation's boundary to prevent just such activities. Table 9 illustrates the main targets of maritime cyber intelligence operations and demonstrates the advantage of the maritime environment in being able to access the far space of the collector as ultimately that is where the networked data of an adversary resides. In this respect, the collector may be ashore collecting information on a target afloat or utilising a maritime platform to collect on a target ashore. It is also of note that as intelligence gathering is primarily concerned with retrieving data, whether protected or not, it is at the syntactic layer, which controls the access to the information and the infrastructure layer that stores it that are the main targets. Ideally, that access could be achieved from the safety of the attacker's near space, but to do so requires interaction initially with the higher human and semantic layers, which is harder to achieve as it requires successful contact with users who must inadvertently compromise their own systems to enable illicit access to the their information. Although not a provider of information related to an adversary's future intentions, intelligence operations may also seek to understand the nature of an adversary's services layer either directly or via other sources. This

could provide valuable information exposing their vulnerabilities, which could provide information to inform future sabotage activities.

Layer	Near Space of collector	Mid Space of collector & target	Far Space of collector / near space of target
Mission	Intelligence gathering		
Human			Phishing campaign to access systems
Semantic			Exploitation of vulnerabilities in software
Syntactic	Shipping detection through global AIS reporting	SIGINT collection by ship or submarine	SIGINT collection by submarine
Physical	Light in fibre optic cables/Radio Frequency transmissions	Light in fibre optic cables/Radio Frequency transmissions	Light in fibre optic cables/Radio Frequency transmissions
Infrastructure	Fibre optic cables at landing point	Seabed submarine operations	Seabed submarine operations
Services			Understanding the reliance on and vulnerabilities of supporting services.
Geographic	Maritime/Land	Maritime	Maritime/Land

Table 9: Targets of maritime cyber intelligence gathering

The role of intelligence within the context of power projection is to acquire and analyse information to predict the capabilities and intent of an adversary to enable decision makers to identify the optimum strategy to alter their behaviour in an advantageous manner. Although intelligence gathering operations can involve espionage, it need not necessarily require covert techniques as useful information may be readily available from open sources and retrievable with the use of specialist search engines or tools. As it is of fundamental importance in the development of an influence campaign to ensure that the most effective and efficient techniques are used and that the audience interprets and acts on them in the manner for which they were intended, intelligence can provide the crucial

information in this process. However, although intelligence is of vital importance in the planning of an operation, it is not intended itself to directly alter perceptions and acts as a continuous background activity to support other tasking that does cause an effect on the target. These are the subject of the next two chapters that investigate the nature of sabotage and subversion as a means of power projection.

Endnotes to chapter 6

[1] Rid, T., 2013. Cyberwar will not take place. 1st ed. London: Hurst. pp. xiv
[2] Ibid. P. 81
[3] Ministry of Defence, 2011. Joint Doctrine Publication 2-00 Understanding and Intelligence Support to Joint Operations Third Edition. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf [Accessed 14 August 2016]. p.1-9
[4] BBC News Norfolk, 2012. Norwich City FC apologises over handling of kit internet posting. [Online] Available at: http://www.bbc.co.uk/news/uk-england-norfolk-17780084 [Accessed 14 August 2016].
[5] Czuperski, M. et al., 2015. Hiding in Plain Sight. Putin's War in Ukraine. [Online] Available at: http://www.atlanticcouncil.org/images/publications/Hiding_in_Plain_Sight/HPS_English.pdf [Accessed 14 August 2016].
[6] Mills, R., 2014. Russian soldier's 'selfies' show he was inside Ukraine. [Online] Available at: http://www.krmg.com/news/news/local/russian-soldiers-selfies-show-he-was-inside-ukrain/ngtTF/ [Accessed 14 August 2016].
[7] Kakavas, Y., 2016. Creepy. [Online] Available at: http://www.geocreepy.com/ [Accessed 14 August 2016].
[8] Edge-Security, 2016. The Harvester. The Information Gathering Suite. [Online] Available at: http://www.edge-security.com/theharvester.php [Accessed 14 August 2016].
[9] OccupyTheWeb, 2016. How to Find Vulnerable Webcams Across the Globe Using Shodan. [Online] Available at: http://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-webcams-across-globe-using-shodan-0154830/ [Accessed 14 August 2016].
[10] OccupytheWeb, 2016. SCADA Hacking: Finding SCADA Systems using Shodan. [Online] Available at: http://www.hackers-arise.com/#!SCADA-Hacking-Finding-SCADA-Systems-using-Shodan/c112t/577152d10cf2e26a9983f701 [Accessed 14 August 2016].
[11] Security Service, 2016. Espionage. [Online] Available at: https://www.mi5.gov.uk/espionage [Accessed 14 August 2916].
[12] Ministry of Defence, 2011. Joint Doctrine Publication 2-00 Understanding and Intelligence Support to Joint Operations Third Edition. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf [Accessed 14 August 2016]. P.1-9
[13] Ministry of Defence, 2011. *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations.* 3rd Change 1 ed. Shrivenham, UK: Development, Concepts and Doctrine Centre.
[14] Russia Today, 2015. 'Russian spy ships' loitering off UK coast, claims ex-Navy chief. [Online] Available at: https://www.rt.com/uk/241901-spy-ships-russia-espionage/ [Accessed 14 August 2016].
[15] Abovetopsecret.com, 2015. *The New Spearhead Spy Ship Marjata IV; Norway Navy Intelligence.* [Online] Available at: http://www.abovetopsecret.com/forum/thread1074090/pg1 [Accessed 13 Oct 2016].
[16] Knight, J., 2016. Ships Designed for Intelligence Collection. [Online] Available at: http://www.faqs.org/espionage/Se-Sp/Ships-Designed-for-Intelligence-Collection.html [Accessed 14 August 2016].
[17] Gertz, B., 2015. Russian Spy Ship Makes Port Call in Caribbean. [Online] Available at: http://freebeacon.com/national-security/russian-spy-ship-makes-port-call-in-caribbean/ [Accessed 14 August 2016].
[18] Cryptome.org, 1986. Soviet Okean class intelligence collection ship LINZA underway. [Online] Available at: http://cryptome.org/eyeball/ssv/ccb-linza.htm [Accessed 14 August 2016].
[19] Committee for Accuracy in Middle East Reporting in America, 2007. USS Liberty. [Online] Available at: http://www.sixdaywar.org/uss-liberty.asp [Accessed 14 August 2016].
[20]Schumacher, S., 2012. *USS Pueblo (AGER-2).* [Online] Available at: http://www.usspueblo.org/Welcome.html [Accessed 14 August 2016].

[21] Photoblog, 2013. North Korea's Cold War prize, USS Pueblo, set to be displayed for 'Victory Day'. [Online]
Available at: http://www.nbcnews.com/news/other/north-koreas-cold-war-prize-uss-pueblo-set-be-displayed-f6C10760692 [Accessed 14 August 2016].
[22] study.com, 2016. Wide-Area Wireless Communication: Microwave, Satellite, 3G, 4G & WiMAX. [Online]
Available at: http://study.com/academy/lesson/wide-area-wireless-communication-microwave-satellite-3g-4g-wimax.html [Accessed 14 August 2016].
[23] Markgraf, B., 2016. How Far Can a Cell Tower Be for a Cellphone to Pick Up the Signal? [Online]
Available at: http://smallbusiness.chron.com/far-can-cell-tower-cellphone-pick-up-signal-32124.html [Accessed 14 August 2016].
[24] Military-today.com, 2016. Monge Missile range instrumentation ship. [Online]
Available at: http://www.military-today.com/navy/monge_ship.htm. [Accessed 13 Oct 2016].
[25] warisboring.com, 2016. The Pentagon Just Got a New Ship That Can Track Satellites … And Help Destroy Them. [Online] Available at: https://warisboring.com/the-pentagon-just-got-a-new-ship-that -can-track-satellites-and-help-destroy-them-67a1bbd70102#.ivfn3gkfb [Accessed 14 August 2016].
[26] defenceforumindia.com, 2010. China's Yuan Wang class tracking ships. [Online]
Available at: http://defenceforumindia.com/forum/threads/chinas-yuan-wang-class-tracking-ships.14326/ [Accessed 14 August 2016].
[27] Military-today.com, 2016. Monge Missile range instrumentation ship. [Online]
Available at: http://www.military-today.com/navy/monge_ship.htm [Accessed 13 Oct 2016].
[28] Freedberg, S. J., 2015. *Cyber Subs: A Decisive Edge For High-Tech War?.* [Online]
Available at: http://breakingdefense.com/2015/03/cyber-subs-a-decisive-edge-for-high-tech-war/ [Accessed 15 August 2016].
[29] naval-technology.com, 2015. *Kockums A26 Submarine, Sweden.* [Online]
Available at: http://www.naval-technology.com/projects/kockums-a26-submarine/ [Accessed 15 August 2016].
[30] BI Science, 2015. Animated map shows the undersea cables that power the internet. [Online]
Available at: https://www.youtube.com/watch?v=llAJJI-qG2k [Accessed 14 August 2016].
[31] Sontag, S., Drew, C. & Drew, A. L., 1998. Blind Man's Buff. 1st ed. London: Hutchinson. p158
[32] Ibid. P250
[33] Shubber, K., 2013. A simple guide to GCHQ's internet surveillance programme Tempora. [Online]
Available at: http://www.wired.co.uk/article/gchq-tempora-101 [Accessed 14 August 2016].
[34] MacAskill, E., Borger, J., Hopkins, N. & Ball, J., 2013. GCHQ taps fibre-optic cables for secret access to world's communications. [Online] Available at: https://www.theguardian.com/uk/2013 /jun/21/gchq-cables-secret-world-communications-nsa [Accessed 14 August 2016].
[35] The Associated Press, 2005. New Nuclear Sub Is Said to Have Special Eavesdropping Ability. [Online]
Available at: http://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html [Accessed 14 August 2016].
[36] The Fiber Optic Association, 1999. How To Tap Fiber Optic Cables. [Online]
Available at: http://www.thefoa.org/tech/ref/appln/tap-fiber.html [Accessed 16 August 2016].
[37] Sutton, H.I., 2016. Russian ship loitering near undersea cables. [Online] Available at: http://www.hisutton.com/Yantar.html. [Accessed 27 August 2017].
[38] Sanger, D. E. & Schmitt, E., 2015. Russian Ships Near Data Cables Are Too Close for U.S. Comfort. [Online]
Available at: http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0 [Accessed 27 August 2017].
[39] Ballantyne, I., 2014. Brothers in Treachery. [Online]
Available at: http://iainballantyne.com/brothers-in-treachery/ [Accessed 14 August 2016].
[40] Clements, K., 2016. How Alan Turing Cracked The Enigma Code. [Online]
Available at: http://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code [Accessed 14 August 2016].
[41] Copeland, J., 2012. Alan Turing: The codebreaker who saved 'millions of lives. [Online]

Available at: http://www.bbc.co.uk/news/technology-18419691 [Accessed 14 August 2016].
[42] Santamarta, R., 2014. A wake-up call for SATCOM Security. [Online]
Available at: http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf [Accessed 23 July 2016].
[43] Paganini, P., 2015. Snowden's documents reveal China stole designs for the US-built F-35 Fighter jet, and provides details also a counter-intelligence operation run by the NSA. [Online]
Available at: http://securityaffairs.co/wordpress/32437/intelligence/china-stole-plans-f-35-aircraft.html [Accessed 14 August 2016].
[44] NWO Report, 2015. Confirmation that China stole F35, F22 and B2 stealth bomber secrets as early as 2007. [Online]
Available at: https://nworeport.me/2015/01/29/confirmation-that-china-stole-f35-f22-and-b2-stealth-bomber-secrets-as-early-as-2007/ [Accessed 14 August 2016].
[45] Leppard, D., 2012. Chinese steal jet secrets from BAE. [Online] Available at: http://www.thesundaytimes.co.uk /sto/news/uk_news/National/article991581.ece [Accessed 14 August 2016].
[46] Idarat Maritime, 2009. New Tactics and Equipment in the Somali Pirates' Campaign. [Online]
Available at: http://www.idaratmaritime.com/wordpress/?p=156 [Accessed 14 August 2016].
[47] westpandi.com, 2011. Piracy - Revised Guidance on the use of AIS in the High Risk Area off Somalia. [Online]
Available at: http://www.westpandi.com/Publications/News/Archive/Piracy---Revised-Guidance-on-the-use-of-AIS-in-the-High-Risk-Area-off-Somalia/ [Accessed 14 August 2016].
[48] Rood, P., 2015. Gulf of Aden HRA Reduced. [Online] Available at: https://www.shephardmedia.com/news/imps-news/gulf-aden-hra-reduced/ [Accessed 23 November 2016]/
[49] Oxford University Press, 1981. *The Oxford Library of Words and Phrases Volume 1 - The Concise Oxford Dictionary of Quotations.* 2nd ed. London: Guild Publishing. P.14

Chapter 7: Sabotage in maritime cyberspace

This chapter is the second of three that further explores Rid's analysis of the activities that he proposes comprise offensive cyber operations. By applying these elements to chapter 4's model of cyberspace within the context of the maritime cyber environment introduced in chapter 5, it contributes to the research objectives of this thesis by demonstrating the depth and nature of the relationship between the two environments within the context of power projection.

Whereas intelligence operations in cyberspace seek to access information systems to extract data from them for later analysis, the aim of Rid's second activity, sabotage, is to target the same systems with the intention of deliberately degrading or altering their intended mode of operation. He defines sabotage as *the deliberate attempt to weaken or disable an economic or military system* and notes that although it is predominantly technical in nature, there may well be social enablers to facilitate access.[1] Sabotage is described as exhibiting four features; first and foremost, it is technical in nature and secondly, it can range from simple to highly complex activities. Thirdly, it can be undertaken by either groups or individuals and will be conducted to involve the minimum danger to the perpetrator of detection, attribution, and reprisal, and finally it is the skilled insider who potentially presents the greatest threat to the target.

In referring to sabotage as an indirect form of attack, Rid notes that it may not always result in physical destruction or overt violence and may just be planned to create a temporary effect. Although the intention of an act of sabotage may be that it contributes to a wider campaign that will be instrumental in causing a change in behaviour of a decision-maker, Rid asserts that by itself, it will only be able to achieve a local tactical effect. Thus, he argues that the outcome of a single act of sabotage will not have a wider operational or strategic impact on an overall campaign. He also refers to sabotage as on its own not qualifying as an armed attack as their perpetrators may deliberately avoid open violence and political attribution. Lastly, he refers to it as not being focused on the human

body, but intended to impair a technical or commercial system and aims to achieve a particular effect by means of damaging that system.

It is important to emphasise that there is a significant link between intelligence and sabotage operations. In order to be able to understand the how a system can be successfully attacked and what effects can be expected to be achieved from what action, it is necessary to conduct a comprehensive reconnaissance of the intended target. This will include an assessment of determining what access can be gained, what type of payload can be successfully delivered, what the probable effects are, how likely it is that the attacker will be discovered and how long it will take to recover from the sabotage. If it is determined that the time, cost, and resources needed to achieve only limited results does not represent good value, the operation may not be worth the effort. However, value must be considered more than in just terms of physical effect as the psychological effect of the operation may make a large investment for an apparently small return worthwhile. Examples of this are the *Doolittle raid* on Tokyo following the Japanese attack on Pearl Harbour and the *Black Buck* bombing mission on the Falkland Islands during the Argentinian occupation. In the first of these examples, sixteen *B-25 bombers* were flown on a one-way mission, from the *USS Hornet* to attack targets on mainland Japan on 18 April 1942 in a symbolic gesture four months after the Japanese attack on Pearl Harbour that brought the US into the Second World War.[2] Forty years later, single *Vulcan* aircraft successfully attacked the runway and other targets in Port Stanley, the capital of the Falklands, in four separate raids in what was then the longest non-stop bombing missions of its type in history with each requiring the support of 14 airborne tankers.[3] Although both these operations had limited military effect, both had a significant psychological impact for both the attacking and defending forces.

A further issue to be taken into consideration when planning an intelligence led sabotage operation intended to change the behaviour of the target is the potential loss of the source that informed the mission. This may be because if the source itself is the target, once the attack has taken place it may become clear how the operation was planned and what information must have been

available to the attacker. This may be particularly the case if the target is a compromised communications system, which may result in the victim either changing their method of communicating or using it to relay false information in the knowledge that its content is known to an adversary. Similarly, an attempt to sabotage a system in cyberspace may require the deployment of previously unknown techniques or *zero day* vulnerabilities, so called as the victim has no time to counter them and which at the time were only known to the attacker. As *one-shot weapons*, once deployed their existence will be revealed and they can be forensically examined and then reverse engineered to identify which system vulnerability they had exploited. This could result in them either being used back against the attacker in their original or an amended form, or software patches developed to mitigate for their effects and so rendering them of no further use as an offensive technique.

Rid's description of sabotage was written in the context of trying to argue that it was non-violent in nature as part of a wider justification that cyber-attacks do not meet the academic and legal definitions of warfare. It is in this setting that he makes the assertion that it is an indirect form of attack that may not always lead to physical destruction or overt violence and just be intended to disable. Furthermore, he suggests that it is only a tactical and not a strategic act and so can only achieve a limited effect, and finally that it may not qualify as an armed attack if the saboteurs avoid open violence or political attribution. He also refers to sabotage as differing in the use of 'conventional' weapons that are focused on attacking humans, as by definition they target technical or commercial systems and influence leaders through the indirect effect of damaging capability, not people. However, away from the cyber environment, sabotage may be wider than this narrow definition and that it could meet Rid's definition only because there were no other options available to create a greater physical impact.

An example of an effective campaign of sabotage is the case of the *Special Operations Executive* (SOE) of the Second World War. Formed by Prime Minister Winston Churchill with the direction to 'set Europe ablaze', their mission was sabotage and subversion behind enemy lines in may what be

described as the Nazi near space.[4] SOE sabotage involved the physical destruction of trains, bridges and factories and included acts of subversion in fostering revolt against the German forces in occupied Europe.[5] These actions could most definitely be regarded as an armed attack, yet they were restricted by a number of factors in what methods they could employ and what effects could be achieved. These included having limited number of agents and resistance fighters that could be recruited and trained and using only the types of weapons and explosives that could be covertly dropped by parachute flying from the UK and with tactics optimised to fighting against a superior military force. Although the SOE and the Resistance fighters they worked with could only achieve limited military effect compared to other weapons of the war such as the heavy bomber force, their psychological effect was considerable in creating uncertainty as to where they would strike next and requiring significant numbers of enemy forces to be employed in detecting them through their radio transmissions and then searching for them after they had been localised.[6]

In accepting that sabotage is an accurate term for actions that are intended to affect the operation of a system in cyberspace as part of a coercive cyberpower projection strategy, a comparison with the actions of SOE can be regarded as a more appropriate model to use rather than the more restricted definition used by Rid. By considering hard power in cyberspace in much the same context as the operations of the SOE several parallels can be drawn. The most significant of these is that both operate in what can be regarded as the near space of an adversary and so require access to a potentially protected and monitored environment. This is unlike some other intelligence gathering operations, which may be conducted remotely beyond the reach of the target.

To communicate between one's own near space and the near space of an adversary requires a reliable and preferably encrypted communications channel back to the attacker's controlling authority. SOE agents used radios disguised to look like suitcases and *one-time pads* to provide an unbreakable encryption and an equivalent exists in the use of *covert channels* in communication networks and Session keys used in Secure Socket Layer (SSL) cryptology.[7] A covert channel is a stealthy communication method used

between computers employing processes that would not normally be permitted, thereby bypassing normal security measures such as Firewalls. Figure 17 illustrates encryption using a paper one-time pad used by the SOE and the contents of a computer file displaying one-time Session keys used by the Chrome browser.[8] The browser actually generates two randomly generated session keys, which are required as part of the two-stage process that SSL uses to first establish a connection between Client and Server and then to securely exchange data.[9]

Figure 17: SOE One-time pad and SSL Session Keys[10]

Sabotage operations in cyberspace may also be restricted in what can be achieved, not through intent, but by what capability is available. The level of access to the target system and the tools that can be utilised in the circumstances may be the deciding factor in determining the effect that can be realised. The SOE for example were mostly restricted to the use of easily concealed and maintained small arms and equipment that were used to attack targets that had only light or no protection such as railways or factories as they could not match the firepower of a defending professional military force. Similarly, cyber sabotage may be limited to systems that have poor or incomplete cyber security and the level of protection combined with the technical proficiency of the attacker may also dictate the techniques and choice of target. Likewise, the covert nature of both the SOE and cyber sabotage is a factor in determining attribution. SOE operatives worked in an extremely high risk and vulnerable environment with identification or capture not only exposing

themselves and their associates, but under interrogation running the risk of revealing important information of value to the enemy.

Attribution in cyberspace is also a significant issue and if it is suspected that a defender may be able to determine the source of an attack, obscuration techniques such disguising the originator or suggesting that someone else is responsible may need to be included in the planning of an operation. The final parallel between sabotage conducted by the SOE and in cyberspace is the role of insiders. A key objective of the SOE was to recruit and train selected members of the local population into resistance units who would be equipped to perform sabotage operations. Their knowledge of the area and language skills that enabled them to integrate into the local community were recognised as key attributes in being more effective than outsiders who would have to learn about the environment before becoming operationally effective and would in the meantime be more likely to arouse suspicion.

The ability of an insider with unique information to cause a devastating attack on a cyber target was evidenced from the case of *Vitek Boden* who in 2000 attacked the computer and radio-controlled sewage equipment in Maroochy Shire Council in Queensland, Australia. As a disgruntled former employee who had probably been involved in the initial installation of the system, he used stolen equipment to issue radio commands to sewage equipment causing 800 000 litres of raw effluent to spill in local parks and rivers.[11] This case emphasises the distinct advantage of being able to directly enter the target's near space, particular when security measures prevent access from the safety of the attacker's near space or when, as in this case, the sewage system did not have a networked connection to wider cyberspace that could be exploited remotely.

The capability to conduct sabotage operations in cyberspace is acknowledged as an aspiration by both the armed forces and intelligence agencies. The US Air Force announced in 2012 that it was interested in developing these methods, which were to be available at the tactical level and used as a precursor to warfare such that an adversary would enter the conflict *in a*

degraded state.[12] Even before then in 2010 according to US Marine Corps Lt Gen Richard Mills, cyber-attacks were being made during the Afghanistan conflict against the Command and Control systems of the insurgents, illustrating that sabotage in cyberspace has become an increasingly mainstream activity.[13] In planning the effects of a campaign of sabotage in cyberspace in support of a power projection strategy and depending on the target organisation, the attacker may seek to achieve one or more of a range of outcomes. GCHQ's *Joint Threat Research Intelligence Group* (JTRIG), the existence of which was included in Edward Snowden's allegations, describes the purpose of its activity as *using online techniques to make something happen in the real or cyber world*.[14] These activities encompass what is known in military organisations as *Information Operations* and encompass a range of disciplines including influence or disruption. These may in turn be regarded as *power projection* and *technical disruption*, the latter of which may include *sabotage*.[15] What effect is selected as the objective of the activity will depend on a variety of factors including what is assessed to be the most effective in altering the behaviour of the target. Other issues will include the knowledge, access, techniques, and time available to the attacker with this final element often being the determining factor in the method used.

Within NATO, actions taken to disrupt, deny, degrade, or destroy information comes under the remit of *Computer Network Attack (CNA)*.[16] Deception is not included in CNA, but is incorporated within the wider concept of *Command and Control Warfare (C2W)* and is intended to deny accurate information to an adversary and is covered under the heading of subversion in the next chapter. However, all are included within the overarching remit of Information Operations; which NATO defines in its Allied Joint Doctrine publication (AJP) 3-10 as:

> *A staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries…..*[17]

A key aspect of this definition is that there is no specific reference to these actions only occurring as part of military operations, implying that it can take place during times of tension, or even peacetime operations. This is notably different from US doctrine that highlights that Information Operations are *the integrated employment, during **military operations**, of information related capabilities…*[18] Within AJP 3-10, NATO defines the '4Ds' of Information Operations as:

Destroy: *To damage an object…so that it is rendered useless to the enemy until reconstituted*. This is the most extreme form of sabotage as it results in the physical destruction of the target. It is also the most challenging to perform through cyber means as it will require the injection of software into the target system that controls an integrated Supervisory Control and Data Acquisition (SCADA) or Industrial Control Systems (ICS). To be effective, this new code will reprogram physical components to perform in such a way that they function outside their designed parameters so that permanent damage occurs rendering them useless until repaired or replaced.

Deny: *To prevent the enemy use of a specific thing*. In Information Operations, this means preventing the target from accessing or using critical information, systems and services and can be either permanent or temporary. Denial differs from destruction as it can be performed by software so that although physical damage does not occur, it is still prevented from performing as designed. Within the cyber environment, denial can be permanent if the saboteur causes the victim's data to be encrypted, deleted, or corrupted, but it can also be temporary if it requires continual action from the attacker, such as in a Denial of Service (DoS) attack, to be effective. A DoS attack involves saturating the target with data beyond its capacity to cope, such as in sending malformed requests to a web server or continual texts or calls to a telephone.[19]

Degrade: *To lower the character or quality of.* In cyberspace, this refers to reducing the performance of an adversary command and control system, communications infrastructure, or information collection effort. It can also be referred to in the context of degrading the morale of the target through cyber

means. It is a less severe form of sabotage than destruction or denial as it will result in the target still operating but at a reduced effectiveness and efficiency than it was designed to do. As noted by GCHQ's JTRIG, this effect can be subtler, with its effects less likely to be detected and it can therefore enable a more sustainable effect to be achieved over a longer period if the target becomes used to lower performance standards and accepts them as the norm.[20]

Disrupt: *To disturb or interrupt.* This applies to capabilities being used to interfere with information flow and so by definition is a temporary effect. Within the cyber context, this could be a short-term DoS attack conducted at a critical time in operations when the target's use of its information system is most critical. It can also involve changing or corrupting databases or reconfiguring systems to temporarily cause them to malfunction or fail and requiring remediation measures ranging from a simple reboot to major system restore from a backup.

Sabotage and maritime cyberpower

Many of the activities that were discussed within the theme of intelligence gathering operations within the context of maritime cyberpower may be used to facilitate sabotage operations in the same environment. Therefore, if signs that these precursor reconnaissance operations have taken place are detected, they may provide evidence of an increased risk of attack. This is particularly pertinent in the situation where unusual military activity is detected near undersea fibre optic communication cables forming the infrastructure layer of cyberspace. These cables' essential role in facilitating the global Internet infrastructure function is well recognised and is particularly important for the UK as shown in Figure 18 where they carry 99% of all transoceanic digital communications and which is the primary termination point for many transatlantic cables and acts as an intermediate hub for traffic routed to mainland Europe and beyond.[21]

Cables are a potential target for sabotage throughout their route between continents, although the danger and threat actor does vary along their path. The relatively shallow depth of the UK continental shelf of less than 100m and their potential vulnerability from this ease of access is an increasing cause of concern. This is particularly so as there have been reports that Russian submarines have been detected operating near them, raising fears that they are either engaged in monitoring activities or planning to cut them in times of tension.[22] In the UK's near space at shallower depths the greatest threat from state actors with the technological capability come from monitoring communications rather than cutting them as although it is physically easier to do, should the cables be cut, they are more easily repaired. Non-state actors however who would be unable to access the cables at greater depth may seek to damage them in shallow waters using divers or dragging anchors over them if their paths are not being protected or monitored. However, in the deeper waters of mid space and in the open ocean outside the reach of non-state actors, deploying monitoring capabilities is a more challenging undertaking. At these depths, severing cables in deep water by deploying remote submersibles armed with cutting devices or explosives would be a more attractive option for more technological advanced adversaries as repair would be a more challenging and time consuming process. Making several cuts in a single cable at irregular intervals may even make it impossible or uneconomic to repair at all.

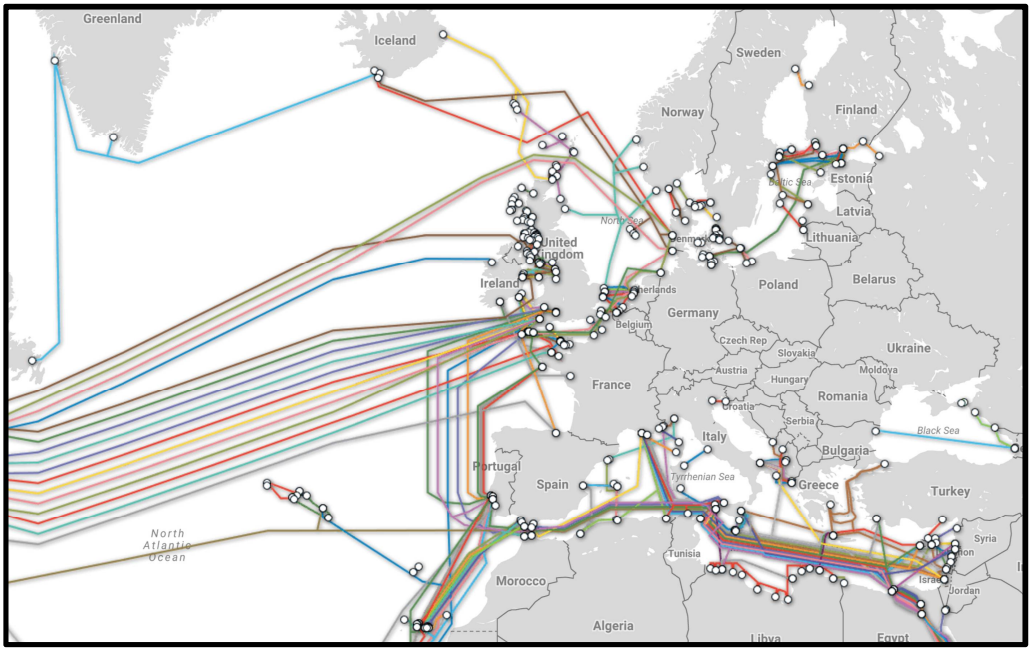

Figure 18: Submarine cable map of the Atlantic [23]

The threat of cuttings undersea cables should not be underestimated as there is a historical precedence for this activity. By the time of the First World War in 1914, there was already an expansive worldwide network of telephone cables as shown in figure 19.[24]

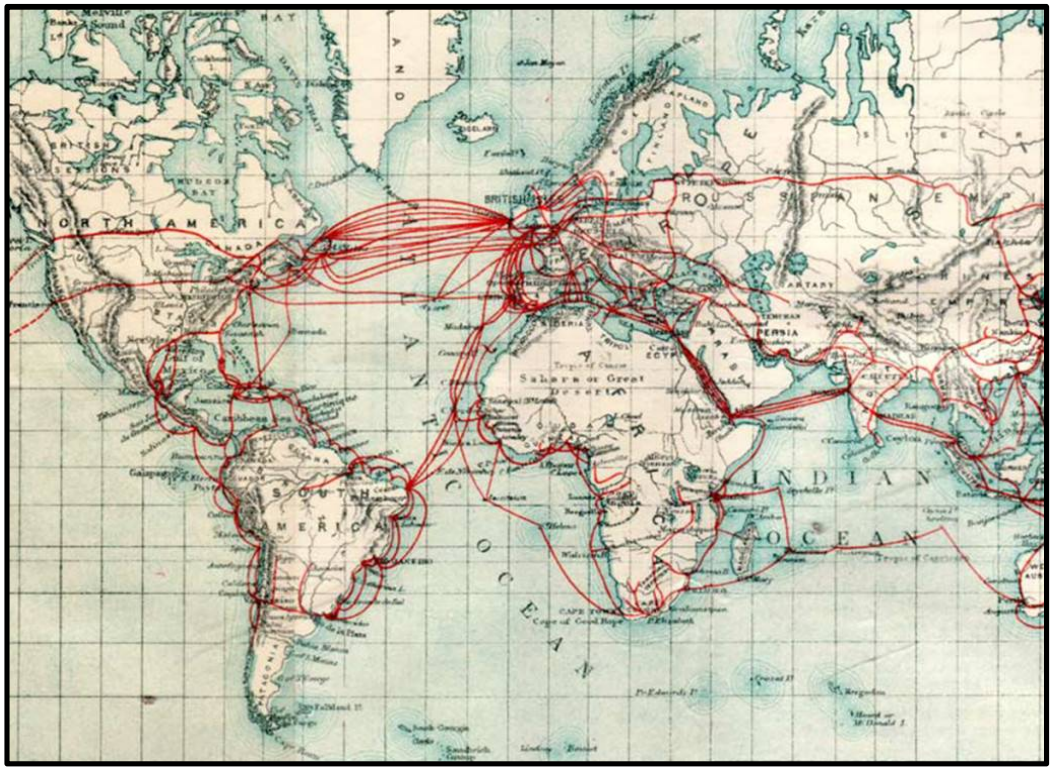

Figure 19: 1901 map of submarine telephone cables

On 5 August 1914, soon after war was declared, the British General Post Office (GPO) cable ship *Alert* cut five German overseas underwater cables linking Enden to Vigo, Tenerife, the Azores and the USA via the English Channel.[25] Not only did this sever direct German telegraph links to destinations outside Europe, but it also meant that international communications across the Atlantic had to be sent via the UK where they were being monitored.[26] Although these were encrypted, the code was broken and through this early COMINT, Britain intercepted the so called *Zimmerman Telegram* sent from the German Foreign Minister Arthur Zimmermann to the German Ambassador in Mexico. It promised that if the then neutral USA went to war with Germany, an alliance would be offered with Mexico with the promise that should Germany win, Mexico would receive Texas, New Mexico and Arizona in return.[27] After the decrypted telegram was passed to the US Embassy in London and subsequently released to the media in the US, its content plus the impact of increased German submarine warfare against shipping in the Atlantic resulted in a change in US government and public opinion that eventually led to a declaration of war on Germany and its allies on 6 April 1917.[28]

It is of significance that cutting fibre optic cables today also has the potential to create a similar situation to that which facilitated the intercept of the Zimmerman telegram. As undersea cables are expensive to lay and maintain with a cost of up to $28 000 per kilometre, investment decisions have traditionally been based on the demand for increased capacity, whilst keeping costs as low as possible.[29] However, in the light of the Snowden revelations exposing US and UK monitoring of cables landing on their shores, nations such as Brazil that discovered that they were subject to surveillance are now laying new cables that are outside the reach of foreign intelligence agencies. An example of this is their proposed new direct link from Fortaleza to Lisbon avoiding the US.[30] It is quite feasible to assume that as in 1914, there may well be work by several nations to identify particularly significant cables that are outside the reach of their intelligence agencies and plans being prepared to cut them in times of tension and conflict to force traffic to be diverted to other routes that are subject to monitoring and analysis. The strategic importance of undersea cables and

their acknowledgement that they form part of a nation's critical national infrastructure means that should they be cut, the effects may be more than just the tactical impact proposed by Rid, but may have strategic consequences. This emphasises the connected nature of cyberspace and its reliance on these cables to link nations. [31]

As well as targeting undersea cables, coastal wireless networks may also present a target for sabotage as a means of projecting maritime cyberpower. Significantly, noting the relatively short range of some of these transmitters, this could only be conducted within close proximity to the shore deep in the near space of the target. This type of operation could thus only be undertaken by a submarine submerged within territorial waters using specialist antennas raised above the surface in what would be regarded as a particularly aggressive or even hostile act by the target nation if detected. Despite these physical, technical, and indeed legal challenges, it has been suggested that this type of capability is already in service within the US Navy. During a live streamed discussion on the future of submarine warfare at the Center for Strategic and International Studies on 8 July 2016, Rear Admiral Michael Jabaley, Program Executive Officer for Submarines, in discussing offensive cyber-attacks, referred to an *offensive capability* that was *prized very highly* and that there are submarines involved *at the highest technical level, doing exactly the kind of thing that you would want them to do*.[32] This capability perhaps refers to the *USS Annapolis*, a submarine that has been alleged to possess a *computer network exploitation (CNE)* toolkit using antennas that can intercept and manipulate communications data on networks that either have no or weak security measures in place.[33] This is also coherent with material leaked by Snowden and published by the German newspaper *Spiegel* that revealed trials with the *Annapolis* had successfully connected to computer wireless networks at a range of several miles.[34]

Sabotage and cyber seapower

Sabotage in cyber seapower presents a particularly danger to shipping as they become more automated and their complex systems are increasingly becoming

reliant upon cyberspace for their routine operations. This was recognised in the 2014 UK national strategy for maritime security that specifically identified cyber-attack as a risk within the context of a strike on both infrastructure and shipping.[35] The role of cyber saboteurs is also made easier by the systems that ships use being of an open standard with their specifications freely accessible and able to be analysed. In particular, the GPS and AIS signal format that are used by the majority of vessels and are relied upon by merchant shipping are very vulnerable to sabotage due to the weak signal strength of data received from satellites.

A nation wishing to exercise cyber sea denial of its local waters may seek to jam or spoof both GPS and AIS, which would result in automatic navigation and collision avoidance systems being unable to function correctly. Spoofing is the injection of false data into a system with the intention that the users act on the erroneous information. In these circumstances ships would normally revert to using other electronic navigation methods such as radar or traditional visual navigation techniques. However should a nation be determined to make passage through their waters as challenging as possible, commercial radar frequencies could also be jammed or false targets injected into radar systems using techniques already commonly used by practitioners of the well-established discipline of electronic warfare.[36] Although military GPS receivers do employ techniques such as advanced aerial design and encryption to defeat jamming and spoofing, civilian commercial GPS receivers would be more susceptible to interference.[37] The significance of GPS jamming and its potential impact has been highlighted in a recent US military test in June 2016 in which aircraft were warned of a jamming exercise centred at the Naval Air Weapons Station at China Lake, California which had an effective radius of over 250 miles at 50 feet above ground level.[38] Exercises of this sort are not just designed to practise for theoretical events as it has been reported that North Korea has on several occasions jammed GPS receivers near its border with the South. In a recent event in April 2016, cyber sea denial was exerted when about 70 fishing vessels and 52 other ships were affected with the former having to return to port.[39]

Although GPS denial can have serious effects, once receivers lose lock or show erroneous data, the jamming can be recognised and mitigation measures put in place. More dangerous though is spoofing an electronic system, which can be regarded as a form of sabotage by deception. This activity can be more dangerous than purely denying a system as the victim may be unaware that it is taking place and may act on the false information potentially leading a vessel off its planned track and into danger. The effects of GPS spoofing were demonstrated in 2013 as part of an experiment conducted by the University of Texas when a custom-made device was used to transmit GPS type signals towards the antennas of a target ship at sea in international waters. By overpowering the genuine signals, control over the ship's navigation system was achieved and course alterations made, even though the electronic chart showed that no corrections had been made.[40] Although in this trial the cyber sabotage device was located onboard the target vessel, as a proof of concept it does emphasise the potential of cyber seapower to affect ships in disputed waters.

As well as GPS, AIS signals have also been subject to successful spoofing attacks and has been the subject of debate within the maritime community as to its potential impact. Manipulation of data has been demonstrated on the *MarineTraffic.com* website, which receives information from multiple sources for public display. As a demonstration, a vessel was 'moved' from the Missouri River to appear in the middle of Texas and another vessel's track was shown to spell out 'PWNED' – a corruption of the word *owned* and used as a hacking term for successfully taking control of a system, as shown in figure 20.[41]

Figure 20: Spoofing AIS

The researchers from *Trend Micro* who investigated these issues were also able to deny AIS communications to shipping as well as triggering safety alerts that could be used to lure vessels to navigate into hostile waters. Furthermore, it was shown that it was possible to generate false potential collision situations to cause automatic navigation systems to alter a ship's course. In response, the shipping industry noted that AIS is designed primarily for collision avoidance and therefore must be an open and not a secure system and so by nature will be to some extent be vulnerable to manipulation. However, back up measures do exist using radar or visual observation and that this type of open data should not be used as the sole information source for making safety critical decisions. The issue of spoofing though, is regarded as a significant challenge to navigational safety where subtle changes in data could result in a ship altering course towards danger or into an adversary's territorial waters where it could be subject to boarding or even impounding.[42]

Although systems such as AIS and those providing Position, Navigation and Timing information, including GPS, are very susceptible to sabotage due to their low signal power and open standards, the same is not true of some of the other components of cyber seapower. Encryption is available for both military and commercial satellite communication systems to prevent an adversary using the

same frequency to imitate legitimate users. Denial of a satellite signal is however possible, although its effectiveness is dependent on the power and range of the jammer and the sophistication of the aerial used by the terrestrial base station. Examples of jamming satellite television have been reported in countries such as Iran and Cuba where exposure to outside cultural influences is regarded as a threat to the state's power and where Internet access is also heavily filtered.[43] Satellite jamming can take two forms, orbital and terrestrial. Orbital jamming involves transmitting signals directly to the satellite via a rogue uplink station, which either overrides legitimate transmissions or combines with and confuses the channels available for all users and possibly in the case of satellite television, over a very wide area. Terrestrial jamming however targets the users and takes place in a specific location. These jammers transmit at the same frequencies as the satellites and confuse the receiving equipment thereby corrupting the original signal. Depending on the frequency used, this type of equipment can also interfere with terrestrial radio transmissions, thereby denying a range of different types of communications medium.[44]

In situations where jamming devices are ground based, there are methods by which ships at sea can mitigate their effects. Aerial design is a primary factor as through careful construction and increasing its diameter the direction from which it concentrates its reception can be concentrated upwards towards the satellite and less horizontally from where the jamming signal emanates.[45] Manoeuvring the ship so that the superstructure can shield the aerial from the jammer can also reduce its effects. Finally, the ship can position itself further out to sea beyond the range of a shore based transmitter, but that may achieve the aim of the jamming nation by achieving sea denial through the effects of cyber sea power. Another possible denial method is to use airborne jammers flying between the ships and communications satellite. This can be very effective as it enables the interfering signals to be concentrated in the main beam of the aerial and the higher the altitude of the jammer, the greater its effective range. This method is restricted though by the endurance of the aircraft and would make a very attractive target in times of conflict.

The final example of cyber sabotage that could be used a means of exerting sea denial is one that may not be directly associated with the vessels themselves, but is of fundamental importance in ensuring that ships can operate and project maritime power. Ships at sea have always been dependent upon logistics support for food, supplies and since the introduction of steam and diesel propulsion, fuel, and ensuring that ships are properly provisioned is a major consideration in planning and supporting operations. Sabotaging military logistics has historically been recognised as having the potential for smaller forces to defeat militarily superior ones and disrupting German rail activity in France during the occupation was a major role for the SOE. Although the physical destruction of railway infrastructure provided a very visual demonstration of capability, it relied on a supply of explosives, risked capture and affected the civilian population. A subtler means of sabotage was to switch the routing labels on railway wagons, which sent supplies to the wrong destination. Although this did not actually destroy the material, it caused delay, congestion, and inconvenience with the further advantage that it did not require the storage, maintenance, or training in the use of dangerous explosives.[46]

With modern logistics organisations now reliant upon cyberspace for the inventory management and transport of goods, they present a very attractive target, particularly as the military now also rely on civilian supply chains for items that do not require special handling such as ammunition or cryptographic material.[47] As civilian organisations supplying the military will use commercial software on computers connected to the Internet for their communication, they may well have vulnerabilities that could be exploited by compromising these systems. An example of attacking a maritime logistics system was exposed by *Verizon* in their 2016 data breach digest.[48] A shipping company had reported incidents of piracy in which its ships had been intercepted on the high seas. The attacks were targeted and well timed with the pirates forcing the crew into a single area of the ship before searching for and using each container's unique bar code to identify and open a single one containing a high value cargo before quickly leaving. Research by Verizon established that the computer systems of the shipping company had been breached and that their Content Management System (CMS) consisting of a user interface and database was being accessed

by the criminals. By searching shipping records, the 'pirates' were able to access the cargo inventories and future routing details of each ship and so were able to plan their attacks accordingly to be the most profitable and with minimal risk of capture. In this incident, the criminals were better pirates than computer hackers as they left sufficient forensic evidence to enable the shipping company to secure their systems. It does however emphasise the high value cargo that ships carry and that once at sea, they may be unable to protect themselves from armed and determined adversaries and that they may be beyond the immediate reach of law enforcement authorities.

The case of the *cyber pirates* illustrates the wider vulnerabilities of the maritime environment beyond the immediate vicinity of the ships themselves to include shore infrastructure. The ability to predict a ship's future position could leave it vulnerable to attack or by altering commercial data could result in shipping containers being misdirected or the ship's passage plan being altered prior to sailing. In the future, should the vessels themselves become part of the maritime cyber environment, the potential to illicitly access data held onboard and sabotage records to change a ship's plan once it has sailed cannot be discounted. In addition, should the objective of a cyber saboteur be to cripple a ship remotely as part of a campaign of sea denial, the practice of automating the control and management of ship systems may expose vulnerabilities that could make this a potential risk in the future.

Commercial providers are now offering *Integrated Platform Management Systems* (IPMS) that oversee all aspects of a vessel's propulsion plant and systems and which interface with navigation and communication suites on a single network.[49] This provides a remote monitoring and control capability that reduces the number of personnel needed onboard to check systems *in situ* and enables the rapid detection and response to maintenance issues as they occur. Suppliers of IPMS reduce risk and cost by relying on well-established technologies such as commonly used operating systems and networking components that would be familiar in a home or office environment. Reliability is ensured by incorporating proven commercial off the shelf (COTS) products that have been used in a range of environments and are designed using open

architectures and industry standard protocols. This enables systems to be easily configured, reconfigured, and upgraded with a range of software packages to suit the individual needs of the customer. It is unfortunate that although using commonly available components and software that are proven and reliable provides reassurance that a system will work, it also presents a range of vulnerabilities that may be exploited through malicious intent or negligent action. Software that is in widespread use is also the most frequent to be targeted by saboteurs as their efforts in understanding and learning how to alter the computer code will be rewarded by it being able to be reused effectively against a broad range of targets. An appreciation of what type of technology is used in ships and then being able to easily acquire copies to work on will also make a criminal's task easier. Similarly, systems that are intended to be upgraded are designed to be easily accessible, which further increases their vulnerability to sabotage.

Conclusion to chapter 7

In assessing the role of sabotage in cyberspace, Rid was correct in his assertion that these attacks do not have to be violent. However, a caveat should be added that attacks in the cyber environment *may* be violent and importantly have to demonstrate the potential to be violent in order than lesser acts can have deterrent value by implying that a capability exists that in future could do harm.[50] Sabotage, by its very nature of altering the performance of a target system in such a way that it changes the behaviour of people is likely to be perceived as a hard power activity. The examples given here of how to achieve maritime cyberpower and cyber seapower are naturally coercive in nature by demonstrating an ability to override the normal operation of a system to the detriment of the target. This is particularly the case when the systems attacked are those concerned with the ability maintain communications or when concerned with shipping safety. As well as demonstrating a power over the ability of an adversary to operate, it illustrates the potential to interfere with systems upon which they depend for normal operations at sea, which may be sufficient to deter them from their current course of action.

The activities of the SOE in the Second World War provides an example of sabotage in the physical domain for which cyber activities can be compared. Their operatives would be in no doubt that some of their acts were violent, although others such as the diversion of railway wagons might well have been regarded as subordinate acts of sabotage to blowing up the railways themselves. Sabotage is defined by its target; systems rather than humans, and this lends itself to the manufactured, machine dependent environment of cyberspace. Like SOE's operations, sabotage in the maritime cyber environment aligns with Rid's assertion of its technical nature, being conducted by groups or individuals, employing attribution avoidance and being most productive when accomplished by an insider. Acts of sabotage though may be restricted by the art of the possible, not by what is desirable as limitations in access and capability may limit what can be accomplished. They may also be undertaken, not for their material impact, but for the psychological effect on both the target and sympathisers.

Table 10 summarises the range of possible targets that could be the identified as candidates for maritime cyber sabotage. This emphasises its role in targeting infrastructure, the protocols and systems that enable it to operate correctly, including the services that enable a system to function. Its potential use in projecting cyberpower from and within the maritime environment demonstrates the potential vulnerability of national assets such as undersea cables and those parts of the electromagnetic spectrum used for transmitting digital information relating to ship safety. These should be regarded as being just as important a part of a nation's critical national infrastructure as power generation and other utilities and afforded similar protection. Denying access to the components of maritime cyberspace can be relatively easily achieved through physical or electronic interference as part of an offensive cyberpower campaign and would have an immediate impact upon a nation's economic wellbeing.

It is of note that British Maritime Doctrine specifically mentions the role of the Royal Navy in protecting Oil and Gas installations but does not include patrolling and securing the nation's maritime communications infrastructure, which is as important a contributor to the nation's wealth.[51] The capability of

advanced nations to use the sea as a means of access to local networks is also significant. Radio networks, and indeed spies, do not recognise national boundaries and these must be included when considering critical infrastructure protection. Finally, logistic support to maritime operations is an essential component in gaining and maintaining power at sea and from the sea. It may also be one of the most vulnerable aspects if its importance is not recognised and they are not properly secured. Maritime cyberspace is a wide ranging and diverse environment and the challenge of protecting it from different types of sabotage should not be underestimated.

Layer	**Near Space of saboteur**	**Mid Space of saboteur & target**	**Far Space of saboteur / near space of target**
Mission	Sabotage		
Human			
Semantic			Spoofing GPS/AIS Hacking maritime logistics systems
Syntactic			Jamming GPS/AIS/Communications
Physical		Light in fibre optic cables	Light in fibre optic cables/ Radio Frequency transmissions
Infrastructure		Cutting fibre optic cables	Cutting fibre optic cables
Services			Disrupting electricity or heat dissipating cooling services.
Geographic		Maritime	Maritime / Land

Table 10: Targets of maritime cyber sabotage

The planning and conduct of sabotage operations in both the physical as well as cyber environments can use parameters that are relatively easy to define and measure. Initially, a target system or capability is identified and a desired effect to be achieved against it is selected and planned. In conjunction with these, indicators that the operation has been successful will be determined and the planning processes commenced. Noting that the preparation and conduct of such an operation both in maritime cyberspace and elsewhere may be fraught with difficulties, the nature of the target and its location may be

constants that provide the basis for determining the chances of success. However, the greatest element of doubt in any sabotage operation within a campaign of power projection is whether it will have the desired effect of altering the behaviour and attitudes of the people who are being indirectly targeted. This is undoubtedly the most complex element of the planning process as the unpredictable nature of human behaviour is a challenging subject to model. This leads on to the third and final activity of power projection to be discussed; subversion, which is arguably the most demanding activity to plan, conduct and measure the effectiveness of as it seeks to directly target the source of power; those individuals with the ability to influence the policy and direct the activities of an adversary.

Chapter 7 Endnotes

[1] Rid, T., 2013. Cyberwar will not take place. 1st ed. London: Hurst. P. 57
[2] EyeWitness to History, 2007. The Doolittle Raid, 1942. [Online] Available at: http://www.eyewitnesstohistory.com/doolittle.htm [Accessed 23 August 2016].
[3] Royal Air Force, 2016. Operation Black Buck. [Online] Available at: http://www.raf.mod.uk/history/OperationBlackBuck.cfm [Accessed 23 August 2016].
[4] Special Forces Club, 2010. SOE History. [Online] Available at: http://www.sfclub.org/history.htm [Accessed 23 August 2016].
[5] Morris, N., 2011. The Special Operations Executive 1940 - 1946. [Online] Available at: http://www.bbc.co.uk/history/worldwars/wwtwo/soe_01.shtml [Accessed 23 August 2016].
[6] Crowdy, T., 2016. SOE: Churchill's Secret Agents. 1st ed. Oxford: Bloomsbury. P.27.
[7] Kliarsky, A., 2010. Covert Channels, Swansea, UK: SANS Instiute InfoSec Reading Room.
[8] spymuseum.org, 2016. One-time pad (Silk). [Online] Available at: http://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/one-time-pad-silk/ [Accessed 23 August 2016].
[9] Vandeven, S., 2013. SSL/TLS: What's Under the Hood, Swansea, UK: SANS Institute.
[10] Shaver, J., 2015. Decrypting TLS Browser Traffic With Wireshark - The Easy Way. [Online] Available at: https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/ [Accessed 23 August 2016].
[11] Abrams, M. & Weiss, J., 2008. Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia. [Online] Available at: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf [Accessed 23 August 2016].
[12] Shachtman, N., 2012. 'Degrade, disrupt, deceive': US talks openly about hacking foes. [Online] Available at: https://www.wired.com/2012/08/degrade-disrupt-deceive/ [Accessed 23 August 2016].
[13] Satter, R., 2012. US general: We hacked the enemy in Afghanistan. [Online] Available at: https://www.yahoo.com/news/us-general-hacked-enemy-afghanistan-161426332.html?ref=gs [Accessed 23 August 2016].
[14] LeakSource, 2014. Destroy, Deny, Degrade, Disrupt, Deceive: GCHQ “Effects” Operations Revealed. [Online] Available at: https://leaksource.info/2014/02/07/destroy-deny-degrade-disrupt-deceive-gchq-effects-operations-revealed/ [Accessed 23 August 2016].
[15] NATO, 2015. AJP-3-10 Allied Joint Doctrine for Information Operations. Edition A Version 1 ed. Brussels, Belgium: NATO.
[16] NATO, 2012. AAP-06. 2012 Version 2 ed. Brussels, Belgium: NATO.
[17] NATO, 2015. AJP-3-10 Allied Joint Doctrine for Information Operations. Edition A Version 1 ed. Brussels, Belgium: NATO.
[18] Bodeau, D. & Graubart, R., 2013. Characterizing Effects on the Cyber Adversary, Bedford, MA: MITRE.
[19] CESG, 2016. Mitigating Denial of Service (DOS) Attacks. [Online] Available at: https://www.cesg.gov.uk/guidance/mitigating-denial-service-dos-attacks [Accessed 23 August 2016].
[20] LeakSource, 2014. Destroy, Deny, Degrade, Disrupt, Deceive: GCHQ “Effects” Operations Revealed. [Online] Available at: https://leaksource.info/2014/02/07/destroy-deny-degrade-disrupt-deceive-gchq-effects-operations-revealed/ [Accessed 23 August 2016].
[21] Miller, G., 2015. Undersea Internet Cables Are Surprisingly Vulnerable. [Online] Available at: http://www.wired.com/2015/10/undersea-cable-maps/ [Accessed 23 August 2016].
[22] Sanger, D. E. & Schmitt, E., 2015. Russian Ships Near Data Cables Are Too Close for U.S. Comfort. [Online] Available at: http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0 [Accessed 23 August 2016].
[23] TeleGeography, 2016. Submarine Cable Map. [Online] Available at: http://www.submarinecablemap.com/#/ [Accessed 23 August 2016].

[24] Miller, G., 2015. Undersea Internet Cables Are Surprisingly Vulnerable. [Online] Available at: http://www.wired.com/2015/10/undersea-cable-maps/ [Accessed 23 August 2016].
[25] The National Archives, 2016. Fighting Talk: First World War telecommunications. [Online] Available at: http://www.nationalarchives.gov.uk/first-world-war/telecommunications-in-war/ [Accessed 23 August 2016].
[26] Gibson, M., 2016. Britain Cuts German Cable Communications 5 August 1914. [Online] Available at: https://warandsecurity.com/2014/08/05/britain-cuts-german-cable-communications-5-august-1914/ [Accessed 23 August 2016].
[27] Alexander, M. & Childress, M., 1981. The Zimmermann Telegram. [Online] Available at: http://www.archives.gov/education/lessons/zimmermann/ [Accessed 23 August 2016].
[28] Ibid.
[29] Neal, R., 2014. Underwater Internet Cables: 'Submarine Cable Map' Shows How The World Gets Online. [Online] Available at: http://www.ibtimes.com/underwater-internet-cables-submarine-cable-map-shows-how-world-gets-online-1559604 [Accessed 23 August 2016].
[30] Thomas, A., 2014. Brazil Laying Their Own New Internet Cables. [Online] Available at: http://www.gadgethelpline.com/brazil-laying-internet-cables/ [Accessed 23 August 2016].
[31] Starosielski, N., 2015. *The Undersea Network.* 1st ed. Durham and London: Duke. p.1
[32] Center for Strategic and International Studies, 2016. Delivering on the Future of Submarine Warfare. [Online] Available at: https://www.youtube.com/watch?v=yfrrYcphFBo [Accessed 23 August 2016].
[33] Fung, B. & Peterson, A., 2016. America uses stealthy submarines to hack other countries; systems. [Online] Available at: https://www.washingtonpost.com/news/the-switch/wp/2016/07/29/america-is-hacking-other-countries-with-stealthy-submarines/ [Accessed 23 August 2916].
[34] Spiegel.de, n.d.. NIOC Maryland Advanced Computer Network Operations Course. [Online] Available at: http://www.spiegel.de/media/media-35657.pdf [Accessed 23 August 2016].
[35] HM Government, 2014. The UK National Strategy for Maritime Security. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/310323/National_Strategy_for_Maritime_Security_2014.pdf [Accessed 23 August 2016]. P.33.
[36] Naval Air Warfare Center Weapons Division, 2013. Electronic Warfare and Radar Systems. [Online] Available at: http://www.navair.navy.mil/nawcwd/ewssa/downloads/NAWCWD%20TP%208347.pdf [Accessed 23 August 2016].
[37] Cole, S., 2015. Securing military GPS from spoofing and jamming vulnerabilities. [Online] Available at: http://mil-embedded.com/articles/securing-military-gps-spoofing-jamming-vulnerabilities/ [Accessed 23 August 2016].
[38] Thomson, I., 2016. US military tests massive GPS jamming weapon over California. [Online] Available at: http://www.theregister.co.uk/2016/06/07/us_military_testing_gps_jamming/ [Accessed 23 August 2016].
[39] BBC News, 2016. North Korea 'jamming GPS signals' near South border. [Online] Available at: http://www.bbc.co.uk/news/world-asia-35940542 [Accessed 23 August 2016].
[40] The University of Texas at Austin, 2013. UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. [Online] Available at: http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea [Accessed 26 August 2016].
[41] Trend Micro, 2014. A Security Evaluation of AIS. [Online] Available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf [Accessed 26 August 2016].
[42] Browning, P., 2014. Spoofing AIS - The Debate Continues. [Online] Available at: http://blog.exactearth.com/blog/bid/339822/Spoofing-AIS-The-Debate-Continues [Accessed 26 August 2016].
[43] Waller, J. M., 2003. Iran, Cuba zap US Satellites. [Online] Available at: http://www.wnd.com/2003/08/20157/ [Accessed 26 August 2016].
[44] Small Media, 2012. Satellite Jamming in Iran: A war over airwaves. [Online]

Available at: https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf [Accessed 26 August 2016].
[45] Srinivas, S., 2012. Defeating the jamming battle. [Online]
Available at: http://www.satelliteprome.com/tech-features/defeating-the-jamming-battle/ [Accessed 30 October 2016].
[46] YouTube, 2013. Gladiators of World War II - SOE. [Online]
Available at: https://www.youtube.com/watch?v=Bkl4Qz07WrI [Accessed 26 August 2016].
[47] Defence and Security Systems International, 2013. In it together: a collaborative approach to warfare logistics. [Online]
Available at: http://www.defence-and-security.com/features/featurein-it-together-a-collaborative-approach-to-warfare-logistics/ [Accessed 26 August 2016].
[48] Verizon, 2016. Data break digest. [Online]. Available at: http://www.verizonenterprise.com/resources /reports/rp_data-breach-digest_xg_en.pdf [Accessed 26 August 2016].
[49] ship-technology.com, 2016. *Avio - Integrated Platform Management System (IPMS) for Commercial Vessels.* [Online] Available at: http://www.ship-technology.com/contractors/controls/avio-propulsion1/ [Accessed 29 August 2016].
[50] Rid, T., 2013. Cyberwar will not take place. 1st ed. London: Hurst. P. 56.
[51] Ministry of Defence, 2011. *Joint Doctrine Publication 0-10 British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.2-17.

Chapter 8: Subversion in maritime cyberspace

Subversion is the final element of cyberpower projection in maritime cyberspace to be investigated and it differs from intelligence and sabotage in that it involves a direct approach to reach the ultimate target of power – people. Of Rid's two previous examples of what constitutes offensive operations in cyberspace, intelligence gathering seeks to gain information that supports the planning and conduct of operations and sabotage acts indirectly to affect people through the systems they use, but it is the third, subversion, that targets them directly and presents an opportunity to deploy a soft power campaign. However, whereas the processes used by systems such as GPS and AIS can be analysed and understood to develop methods and techniques to alter their behaviour, people are much more complex to comprehend. Differences in nationality, language, culture, attitudes, and family traditions all potentially play a part in determining the unique make up of an individual or social group and what influences them requiring bespoke strategies to be developed for each one. Rid recognises this complexity, commenting that it has not received much scholarly attention in the past and in examining historical and more current examples of protest and political violence, he notes that they display the common attributes of seeking to undermine the authority of an existing order.[1] He also highlights how protest movements throughout history have benefited from, and taken advantage of, new communicating technologies that were outside the control of the establishment that they were seeking to undermine.

Cyberspace is just the latest medium through which subversive activities can be undertaken. However, it differs from its predecessors in that it not only offers the ability to penetrate further into a society, but it also enables global information exchange between activists, which can facilitate a distributed and geographically dislocated structure. For the first time, this also includes the maritime environment as with satellite communications ships can be on a par with the land environment in terms of the immediacy and content of the material available. Subversive activity can be originated and conducted either from the near space of the target or from another location, but to reach and influence

them they must have regular, unfettered access for the activity to be effective. Thus, a mass communications medium such as cyberspace can both lower the threshold for conducting subversive activity, but it also raises the bar for success as it competes with other conflicting messages and campaigns, which may distract supporters.[2]

The ability for large numbers of potential subversives to enter cyberspace with their own ideals and campaigns to promote leads Rid to suggest that subversion is now more cause driven than ever. However, as technology has made it easy to gain information about a political movement with little effort, supporters do not have to make much commitment to be nominally involved. This has resulted in what Rid terms membership-mobility as supporters may drift out of campaigns if their attention is drawn to another cause. Finally, he suggests that the nature of cyberspace as a participant driven medium does not encourage or facilitate high levels of centralised, organisational control. This results in the overall success of any campaign depending on a range of factors including the political environment and society in which it operates.[3] In returning to his core argument that cyber-attacks need not use hard power to threaten violence, he points out that subversion does not have to include the threat of force, but can be a soft power focussed, persuasive campaign, although as with all power projection, the threat of coercion may always exist as an option.

Subversion can be described as *the deliberate attempt to undermine the trustworthiness, integrity, and the constitution of an established authority or order.*[4] However, as Rid suggests, it can be designed to have limited objectives, such as undermining an organisation and eroding its social bonds and beliefs to change its behaviour without necessarily replacing it. Therefore, as a concept, it may cover a broad range of activities short of violent insurrection and its activities may remain entirely within the law. However, within the context of power it is only one element of a spectrum of activities that may be used to target people directly to alter their behaviour without causing them harm, many of which, such as those requiring physical interaction, cannot be achieved through cyber means alone. Whatever technique is employed, its aim though is

always to undermine the authority or credibility of an organisation that exercises control, but the method by which it aims to achieve this may vary depending on the circumstances.

Although the ultimate ambition of subversion may be regime change, a subversive activity may be just to discredit a key leader or organisation by establishing a feeling of distrust or doubt as to their trustworthiness or credibility.[5] Making a figure of authority appear less worthy of loyalty to undermine their position so that their supporters no longer believe in them or their ideals can be a very personal issue. Targeting an individual, rather than a set of principles can therefore be a powerful method of undermining a cause, particularly if the they are strongly associated with its ideology, and may convince the uncommitted that they are not worthy of their support. What makes subversion such a powerful tool is that, depending on the moral perspective of the perpetrator, success is measured in the opinions and attitudes of the target audience and the methods used to form those views need not necessarily be honest or truthful. In this respect cyberspace and the ease by which content can be produced and accessed is an ideal medium to peddle half-truths or unfounded rumours. At times, all that is required is a scent of a scandal to be sufficient to undermine the credibility of a person in authority. In domestic politics, this sort of activity is often termed a *smear campaign* and can bear all the hallmarks of subversive activity. It is most often seen in the approach to elections in which by the time the truth is acknowledged, the votes have been cast.[6] In law, redress from this type of activity can be possible though legal measures where defence from the written word can be sought though libel and from the spoken word by accusations of slander.[7]

A key element in the success of a campaign of subversion is being able to gain the backing of sufficient numbers of people to demonstrate enough popular support such that it exerts an influence against an established order. To do this requires the dissemination of a compelling message using the mass media of the time. Figure 21 shows two examples of this separated by 180 years; the *Chartist Movement* of the 1830s and the *Anonymous Collective* of 2010.[8] The

Chartists were a popularist movement campaigning for electoral reform at a time when only 18% of the adult male population could vote and its manifesto stated that it sought to *use legal means to place all classes of society in possession of their equal, political and social rights.*[9] Information was spread using print media including newspapers & pamphlets, mass meetings and speeches, but when their demands were rejected, there were calls within the organisation to use more coercive means resulting in some civil unrest that was swiftly quelled by the authorities.[10]

The Anonymous group are a decentralised collective of hacktivists who although have no specific formalised political goals, seek in general terms to subvert the control exercised by states and large corporations through combating censorship and promoting freedom of speech.[11] *Operation Payback* was a Distributed Denial of Service (DDoS) attack on a range of government and commercial websites following the Swedish government's decision to prosecute the founder of *WikiLeaks*, Julian Assange, on rape charges.[12] Rather than print media, the activities were coordinated via posts on the bulletin board *4Chan*, which encouraged individuals to download and run a script that would generate malformed requests to a range of government and commercial websites with the aim of preventing their normal operation. Although they achieved some success, their campaign has since faltered and like the Chartists, their cause ceases to attract the popular support or publicity that it once did, although it should be noted that over time all but one of the Chartists demands, that of annual elections, were eventually met.

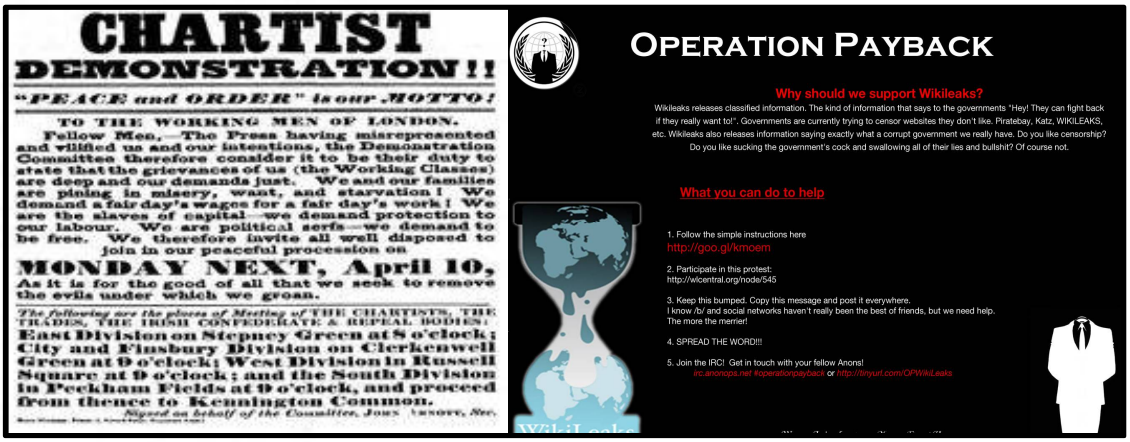

Figure 21: Subversion through mass media – The Chartists and Anonymous

Within a military context, the aim of subversion remains the same as in a civilian environment; targeting people to act in such a way that it inspires a change in the established order, and it is referred to by the term *psychological operations* (PSYOPS). These activities are coordinated through an *Information Operations campaign*, which was introduced in the previous chapter discussing sabotage, as part of an overall information strategy. Noting that the US use the term *military information support operations* (MISO), in NATO Joint Doctrine PSYOPS is described as:

Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes, and behaviour, affecting the achievement of political and military objectives.[13]

In the conduct of PSYOPS, two additional 'Ds' are added to the four of Information Operations, which can be used to contribute to a campaign of subversion as follows:[14]

Deceive: *To deliberately cause (someone) to believe that something that is not true.* Deception in Information Operations seeks to mislead adversary decision-makers by manipulating their perception of reality and persuading them to adopt a course of action advantageous to the attacker.

Discredit: *To harm the good reputation of.* In Information Operations, this includes the reputation, credibility, and/or the authority of a target. Within the cyber environment, this can include deleting their online presence, changing their online information, sending, or posting incriminating material in e-mails or blogs on their behalf and leaking personal or business information that will adversely affect their professional or personal life.

A key element of PSYOPS doctrine is that although it may be conducted to achieve both long and short-term objectives, to be effective and avoid unintended second and third order effects, an intelligence led comprehensive understanding of the audience is necessary. This is achieved through a Target Audience Analysis (TAA), which is a *systematic study of people to enhance understanding and identify accessibility, vulnerability, and susceptibility to behavioural and attitudinal influence.*[15] TAA thus seeks to determine and exploit a target where a target may be psychologically weakest and an example of this is shown in figure 22 of a leaflet air dropped and fired from artillery by the Germans at Ardennes during the Battle of the Bulge in December 1944. This can be regarded as a mass media campaign disseminated by the latest technology of the time in an attempt to undermine the morale and fighting spirit of the US troops on the front line. The message is clear in the text of the leaflet that suggested that while away fighting in a foreign land, the young wives of American soldiers at home were being unfaithful.[16]

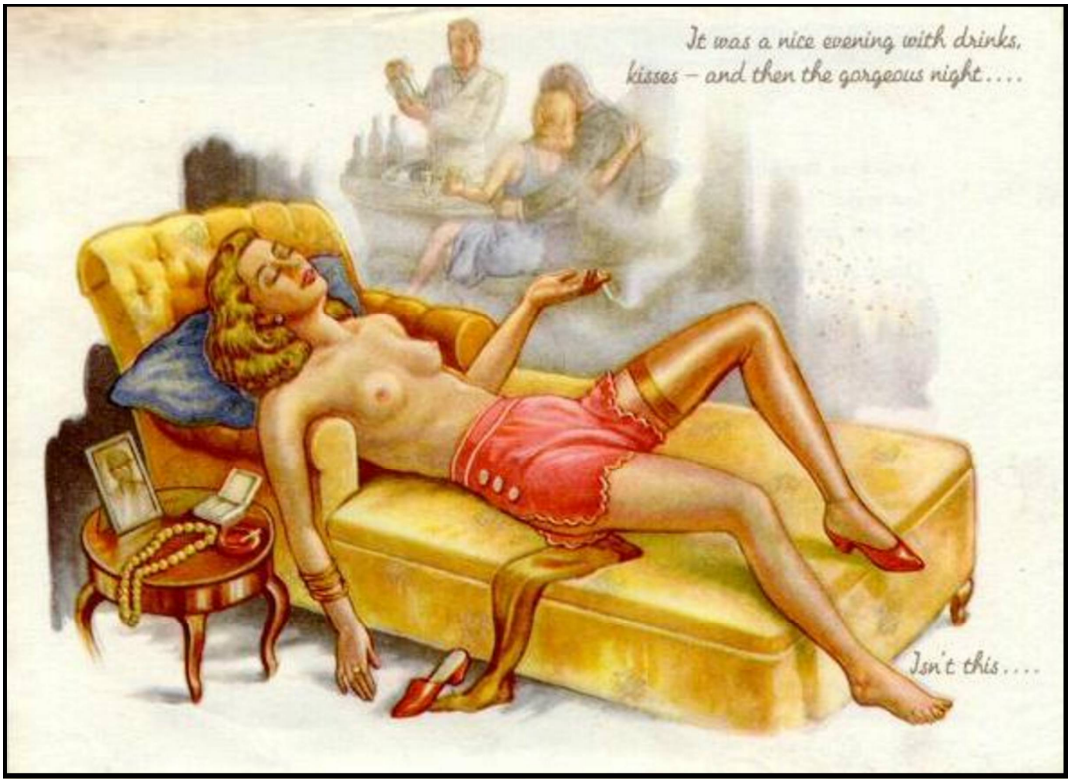

Figure 22: Example of a military PSYOPS campaign leaflet

The advent of the information age and mass communication through electronic means has enabled sophisticated PSYOPS and subversion campaigns to harness multi-media technology to its full extent in targeting both civilian and military audiences. In particular, the use of cyberspace as a means of intimidation and coercion to exert power has been ably demonstrated by the *Islamic State in Iraq and the Levant* (ISIL) through its media presence.[17] Their prominent videos of beheadings and the promotion of an extremist ideology through the Internet have been widely disseminated and with mainstream news organisations broadcasting images of their latest atrocity around the world their message has been further disseminated through social media and blogs. This effectively increases their exposure beyond their initial audience with the opportunity to reach potential converts to their cause. Images censored by traditional media are readily available online in their original format and may be seen to play a role in effectively inspiring the radicalised at home and abroad, while demonstrating the consequences of dissent to those already living under its regime. The quantity of images published online may also act to normalise these acts of terror, desensitising potential perpetrators from considering these

actions abnormal and extreme. The potential impact of extremist material being disseminated online and its contribution in radicalisation was recognised by the UK Prime Minister Theresa May in June 2017 in which she called on Internet companies to eradicate what she termed ‘safe spaces’ that allow terrorism to ‘breed’.[18] However, such calls for what is in essence is censorship of material raised concerns regarding the right to free speech online and the difference of what can be regarded as extremist and what is legitimate political dissent.[19]

At the other end of the spectrum and although not normally classed as PSYOPS or subversion, but with a similar aim of causing a change in the existing political order, albeit through legal means, are democratic election campaigns that now also harness the power of cyberspace. This has the advantage in its ability for politicians to reach a wide audience through advertising and media coverage to gain access to opposition supporters who would not normally seek out their message in order to discredit their policies and their leaders. These tactics usually involves presenting them as less trustworthy in key policy areas such as managing the economy or national defence or at a more personal level by attacking the integrity or competence of individual politicians. This *negative campaigning* can be combined with a soft power campaign promoting the strengths of the favoured candidates and there are already examples of how effective this technique can be on a receptive audience that is technologically literate and with a wide individual ownership of devices capable of receiving the message.

Barak Obama’s use of social media as a tool of soft power proved particularly noteworthy in the 2008 presidential campaign. In the previous 10 years prior to his election US broadband Internet access had doubled to 55 per cent and social networking applications had matured; technology which Obama’s team fully exploited and placed at the centre of their strategy. Although all the candidates hoping for the Democratic party nomination had websites, he made better use of Twitter, text messages and Facebook to proactively engage with his supporters in publicising his message, gaining supporters and fund raising, whilst attacking his opponents through this new medium.[20]

An integral component of any campaign to influence behaviour is an understanding by the target of the originator of the message and their intentions. This may be clear when faced with military force or a radio broadcast announcing its origin, but may be erroneous if it is part of a deception plan. Within cyberspace, attribution may not be straightforward and misinformation is rife. Social media in particular has been noted as providing an environment in which individuals have been deceived, sometimes with devastating personal consequences.[21] Established media organisations and democratic governments with an online presence strive to ensure the credibility of all information that they broadcast and that it is not perceived as state-sponsored propaganda. To achieve this, it must be truthful and open to corroboration, clearly attributable to the source and sensitive to local cultures and religions.[22]

Despite the efforts of reputable news organisations to disseminate information, which to the best of their knowledge is unbiased and neutral, the mass of conflicting information online can be problematic. It has been shown that what people believe to be true and what they wish to be true can be very different with audiences evaluating evidence in a biased manner. Examples demonstrated that where political convictions are challenged by scientific studies, people interpret the results to fit their preconceived beliefs.[23] According to NATO doctrine, campaigns to alter perceptions, attitudes and behaviour have a greater chance of success if they are seen as credible and from the target's perspective spread a consistent message. The use of indisputable facts that can survive scrutiny will build the confidence of the audience who may then be able to accept more unpalatable information.[24] Similarly, it may be advantageous to present an opposition's information campaign as untruthful or even to confuse the attribution of certain messages. According to UK Doctrine, PSYOPS are categorised according to their attributability as follows:[25]

White: White PSYOPS involve products disseminated and acknowledged by the sponsor or accredited agency.

Grey: Grey PSYOPS involve products that do not specifically reveal their source.

Black: Black PSYOPS involve products that appear to emanate from a source other than the true one.

The Doctrine also notes that the UK's PSYOPS are predominantly white, as historically it has been found that black campaigns are generally less successful. Consequentially, its products are generally attributable to the UK or to a partner nation or organisation, even if they are part of an overall strategic deception plan or strategy to discredit an adversary.

Whereas sabotage is an innately coercive activity associated with hard power, subversion may adopt either a hard or soft strategy and what method is used will depend upon how it is perceived that the target audience will most favourably respond to. Although hard power may be used when nations are openly engaged in hostile acts; soft and the softer aspects of smart power may be employed in hybrid operations or in the period prior to offensive actions taking place. This initial state of operations prior to military engagement is referred to as 'Phase 0' during which the aim is to shape the battlespace and ideally prevent or deter armed conflict.[26] It is during this stage that a soft power message may be predominant and subversive activities will take place to persuade an adversary to adopt a preferred course of action, which may be different from that originally intended. It is at this time that 'The mission is the message, and the message is the mission.'[27]

Subversion and maritime cyberpower

Subversion in the pursuit of maritime cyberpower can present some difficulties as the environment is based on machine to machine communications that do

not directly interface with the human users who are the target of a campaign of subversion. This is especially the case for fibre optic cables that carry vast amounts of data that are aggregated at terminal points prior to their undersea passage with individual users unable to engage with the product until it has been separated and routed to their personal electronic devices. There has been no evidence to suggest that data can or has been added or manipulated at the cables themselves to subvert a target and to date they are purely used as a means of data transmission or as a target of intelligence gathering or sabotage. The same issue occurs with two of the other components of maritime cyberspace; the position, navigation and timing signals from GPS or other similar satellite navigation systems and AIS that only provide data, rather than the type of information that could undermine beliefs or behaviour. The key element, however which could have a major contribution to the delivery of maritime cyberpower are the parts of the radio frequency spectrum that are used for the transmission of human readable information within cyberspace.

As has been seen from chapter 2, many countries are very active in filtering the content of cyberspace from their populations, which would make any direct attempt at a campaign of subversion or PSYOPS very challenging. Where this censoring takes place at the border between near and mid space the only way to be able to successfully access a local audience would be to engage directly with them by entering their near space. Whereas penetrating wireless networks for the purpose of sabotage can only be achieved at the relative short ranges of Wi-Fi and well within the 12-mile limit of territorial waters, to be able to achieve power projection into the near space of a target country from international waters would be a distinct advantage. The versatility of maritime units to provide global access, mobility, and poise in an area of influence enables them to remain on station for extended periods providing an enduring presence and means to display both a very visible sign of intent and source of a soft power message. To take advantage of the attributes of the maritime environment, a proposed method of projecting cyberpower by influencing a target population through subversion or PSYOPS would be to harness the growing ownership of smart phones in the key demographic of young adults

who use mobile networks to access web based content. This is significant as in some areas smart phones are now becoming the predominant means to access the Internet with ownership in developing nations rising from 21% in 2013 to 37% in 2015.[28]

Whereas domestic carriers might impose significant charges and restrict content, a vessel at sea in international waters, but within communication range would be able to act as a mobile telephony base station enabling users ashore to download a range of otherwise censored material for free. This would entail ships having their own web servers containing a range of informative and entertaining content that would not be available to users in their own country. Although intended to be subversive by undermining the authority of the target government and circumventing Internet filtering and censorship, this material could also contain a soft power message of attraction and promoting alternative cultural values as part of a PSYOPS campaign. A ship operating 13nm off the coast of a target country would require a transmitter placed 45m above sea level to be within line of site of a receiver at ground level. [29] With rising ground inland or a higher transmitter, further ranges could be met until limited by topography, handset power or the technology in use. This technique could also be used to pass information to local mariners working in fishing fleets or vessels operating in coastal waters who have their mobile devices turned on when at sea. This has the added advantage in that if the warship or vessel transmitting the message is within sight, the origin of the message is clearly attributed and will allay fears that it is part of a campaign orchestrated by their own government to locate and identify opposition supporters. Using established techniques to capture the unique International Mobile Subscriber Number (IMSN) of mobile phones within range, text messages could be sent advertising the service offered.[30] Subscribers would then be able to connect directly to the broadcasting ship's transmitter and access material that has been optimised for viewing on mobile devices.

As well as including multimedia files disseminating a soft power message; tools, applications, and advice on the use of Virtual Private Networks (VPN) or third

parties, known as *proxies*, could be included to enable users to access otherwise restricted material outside their country's borders. Downloading such material via a mobile data connection would be very attractive as typical data rates of 14Mbps could be achieved using a 4G connection and with the latest generation of devices capable of 4G LTE-Advanced connections this speed could be increased to around 42Mbps.[31] Once downloaded, material can then be shared within the target population either by transferring the files via a personal computer, laptop or directly between mobile devices using a peer to peer file sharing application. Attempts to block the signals through electronic jamming are possible, but would have the side effect of also blocking domestic network traffic and the transmitting ship can respond by simply relocating to an uninterrupted area. Although mobile telephony is required when operating at range, the use of Wi-Fi could also be considered when ships are alongside in ports or harbours. Typically, this could be used to pass information to a local population where the host nation would be amenable to this type of activity, such as in a disaster relief operation. This would of course assume that electricity for charging mobile devices are available, or if not that hand wound or solar chargers are provided as part of a wider aid package.

Subversion and cyber seapower

The difficulties of using a predominately people focussed activity such as subversion to create the effects of sea control or sea denial through either hard and soft power means is undoubtedly challenging. As for maritime cyberpower, many of the components of maritime cyberspace that do not have direct human interaction cannot be used for subversion. This includes the undersea cables, PNT systems and AIS, but the communications media of RF transmissions and satellites do offer possibilities. The role of intelligence is important in this respect as it would be a key requirement to know what type and levels of access the target ships and their personnel have to cellular and satellite telephones, television receivers and radio. If they are available, direct telephone calls to the Commanding Officers of the ships may prove useful, particularly if there is no cost to receive a call. This may be particularly productive if intelligence can

determine whether a Commanding Officer might be susceptible to subversion and if so whether a soft or hard power approach should be used. If the ships' crew are known to have smart phones and are able to connect to a ship equipped with a mobile telephone transmitter arrangement described earlier, this may also be a useful method to engage with them directly. However, this method would only be practicable if the ships were within visual range and the crew could use their devices. In a hostile environment, this activity may result in the transmitting ship being regarded as a target and whilst active would be easily identified, tracked by electronic warfare sensors, and possibly even jammed or attacked if considered a threat.

As part of a strategic PSYOPS campaign and depending upon the level of access an adversary has to social media ashore, a campaign directed at the families of target personnel as well as other military organisations may also provide a method to indirectly influence personnel at sea by spreading dissent or doubt as to the validity of their cause or the strength of military opposition that they may encounter. The nature of the campaign and message that is promulgated would rely upon an in-depth Target Audience Analysis to determine whether such a campaign of subversion would be effective. The use of PSYOPS directed ashore as a means to subvert naval personnel and influence a maritime campaign has a very successful historical precedence in 1939 at the beginning of the Second World War. Having sought temporary sanctuary in Uruguay following an inconclusive engagement with the British South American Naval Division, Captain Hans Langsdorff made the decision to scuttle his ship, the *Graf Spee,* in the entrance of Montevideo harbour rather than face what he believed was a superior allied naval force. Although British reinforcements were over 1000 miles refuelling in Rio de Janeiro, a story was leaked to the Germans via the Argentine media that they were in fact much closer and about to refuel at the Argentine naval base in Mar Del Plata.[32] By subverting Lansdorff's commitment to the authority of the Nazi regime and appealing instead to the welfare of his crew by not sending them to what he believed to be certain defeat, sea control within the South Atlantic was ceded

to an inferior naval force and this represents a powerful example of the use of the mass media communication of the day in support of military operations.

Measuring subversion

A key challenge of projecting any type of power in cyberspace is determining not only how best to deploy it, but also how to measure its effect. Conventional military hard power campaigns are violent in nature and results in physical damage to targets and casualties among the enemy. Post engagement battle damage assessment (BDA) would then be conducted to determine the effect of the activity and gauge its success with conflict in the physical environment ultimately measured in terms of territorial gain or control over an area. Compared to hard power campaigns, activities involving subversion, PSYOPS and indeed soft power generally are very difficult to quantify as behavioural changes, influence and affinity cannot easily be calculated. Instead, measurements or indicators are normally expressed in terms of an increase or decrease in a specified activity of a target audience.[33] However, there is a danger that attempts to gauge success may only result in recording those aspects that can be more easily identified as discrete variables and not the more abstract elements such as how the message is perceived in terms of established cultural norms.

Some matrices can however be identified such as within the social media applications employed in Obama's successful Presidential election campaign. In addition to the previously used comparisons of monetary donations between the other candidates, these included comparing the numbers of Twitter followers of each candidate, which provided a direct indication of relative popularity as did MySpace 'friends' and Facebook supporters.[34] In addition to purely just measuring the number of followers in Twitter, other methods have been used to determine the spread and impact of a message. Research has shown that the use of Twitter hashtags that identify certain topics as well as mentions and retweets can provide a more reliable indication of the influence of the originator than just comparing the number of followers.[35] Since July 2014,

Twitter has also provided a powerful facility to investigate the use of its platform with its own analytics function that allows users to discover who has viewed their Tweets and provides an overview of their profiles.[36]

Although the use of social media in which users actively interact with the application by posting their own messages and engaging with others readily lends itself to quantitative analysis, methods also exist to measure user engagement with other means of communication such as websites in which there may be no direct data input. The proposed method of projecting maritime cyberpower by using shipping as mobile transmitters for users to connect, access and download otherwise prohibited web based content presents a powerful method not only to disseminate the material, but also to measure what is popular and as importantly, what is not. This activity is directed solely at creating an effect at the human layer of the model of cyberspace and the difficulty that this entails demonstrates that the higher up the model away from the lower infrastructure and syntactic layers, the more challenging it becomes to create and measure an impact in maritime cyberspace. By owning the web servers and content, analysis could be conducted to identify trends in web traffic and searches of content to provide indicators as to how an overall information campaign was progressing.

Many of the techniques that can be applied to determining the effectiveness of a subversive or soft power message can be taken from the domain of Internet commerce in which website visits are recorded and analysed with the aim of optimising the user experience and increasing sales. *Google analytics* is a facility that provides information about a website's traffic and measures the number of visits that results in actual sales. It can record in real time for later analysis how and from where the user accessed the site, such as directly or through other links, and tracks their interaction with the pages while logging what material is downloaded.[37] Also commonly used by websites to aid their analysis of user activity are the use of *cookies*, which are small non-executable harmless text files, downloaded by web servers onto the devices accessing their websites. These can then be used to provide user identification of the

machine, record revisits, track browsing habits and tailor the user experience accordingly. By measuring the number of visits and their interaction with the range of pages contained within the site, ongoing and repeat interest in its contents can then be gauged.[38]

Although both widely used, Google analytics and cookies do require the acquiescence of the user in allowing the use of scripting languages embedded in the websites to be executed by their browser and permitting cookies to be downloaded. An alternative method, which is purely server based, utilises monitoring software that tracks the mouse clicks and information requests of visitors to a website.[39] This software records which pages have been most accessed, what type of information is of most interest and the path that users take as they navigate its pages and the time spent on each one. This type of *web analytics software* places no information onto the visitors' computers and no personal information is collected. It is becoming regarded as an essential component of those with a commercial web presence and although designed and primarily used as a method of optimising the web experience of potential customers, it has a potential use as a means of measuring the reaction to material designed to spread a soft power message.

In addition to the methods used in optimising online commerce, there are also other means available that could theoretically be used to project and measure the spread of soft power. These originate from techniques used by the creators of malware and involve activities that could be regarded as straying into the realm of hard power and would have significant legal and ethical constraints in their use. These draw on the methods used by *botnets* to deliberately infect a target computer with executable code, which would then report back to a command and control server. This could be achieved by the victim clicking on a link within a website to download the code, or even by conducting a *driveby* attack by just visiting a specifically designed page containing the malware using a browser configured to grant access to scripting languages.[40] This spyware's role could be as simple as reporting usage such as sites visited and material downloaded, but it could also be used for a range of other activities more

commonly associated with malware, such as harvesting user credentials and directing users to fake websites feeding false information or even rendering the machine itself inoperable. These different tracking methods are summarised in table 11 below.

Tracking method	Where hosted	Active or Passive	Invasive	Site redirection
Google analytics	Client/Server	Active	Yes	No
Cookies	Client/Server	Passive	Yes	Yes
Web analytics	Server	Passive	No	No
Spyware	Client	Active	Yes	Yes

Table 11: Methods of measuring web site interaction

All these methods are mature technologies and their ongoing development and current use would be driven by the commercial need to understand how users interact with online commerce or, in the case of the final method, for illicit purposes. Botnets were first recorded in 1999 and have increased in complexity and sophistication to avoid detection and as a result end users may not even be aware of their existence within their computers. This may particularly be the case if their signatures are not included within the anti-virus software in use and the communication to their command and control server remains unnoticed.[41]

The techniques used in commercial advertising to attract customers and increase revenue have distinct parallels with the desire of both state and non-state actors to influence the behaviour of a population as part of a strategy to project cyberpower. Both are intended to alter the perception of their targets in order to conduct activities to the benefit of the originator. Advertising is the ultimate in soft power – the power of attraction and imitation with coercion and deterrence being an option used by those with an extremist culture, doctrine, or religion to promote. However, if detected, the employment of malware to harvest information or direct users to alternate sites would be seen as a provocative action by the target and depending on the nature of the information

disseminated and the political situation at the time may be seen as an aggressive or possibly even a hostile act.

Conclusion to chapter 8

Subversion is at the core of any power projection campaign as it is directly focussed at altering the behaviour of people to act in a way that is advantageous to the attacker by undermining the trustworthiness, integrity, and the constitution of an established authority or order. As such, it can only be deployed in the far space of an attacker as it needs to engage in the near space of the target in which they access cyberspace. However, the additional effort required to enter far space can be beneficial as targeting an individual directly can be a powerful method of undermining a cause, particularly if the they are strongly associated with its ideology, and may convince the uncommitted that they are not worthy of their support. Significantly though, the message does not have to necessary be truthful as it can be part of a wider campaign of psychological campaign designed to deceive or discredit an opponent.

Table 12 illustrates how the use of subversive measures in maritime cyberspace targets the higher levels of chapter 4's model of the cyberspace and seeks to interact with the human and semantic layers. This demonstrates that subversion relates to the values of people and to be effective must target them through their beliefs directly or through the systems that they use to gain information rather than via the raw, factual data associated with the lower levels. Subversion, does not naturally lend itself to maritime cyberspace and so by implication neither are maritime cyberpower or cyber seapower the optimum aims of this type of power projection. This is because they are by nature technical domains supporting the manufactured ships that are used to exploit and control the maritime environment. However, using techniques derived from Information Operations using Psychological Operations it may be possible to target humans as in other ways and then use the components of maritime cyberspace as the delivery mechanism to subvert them. These techniques may draw on either cohesive hard power using threats or intimidation or the

attractive qualities of soft power depending on the nature of the operation and how it is perceived that the target audience will most favourable respond to in order to achieve the desired behavioural change.

Layer	Near space of subversive	Mid space of subversive & target	Far space of subversive & near space of target
Mission	Subversion		
Human			Mariners operating in coastal waters or ashore Families of mariners with influence over them Local population living in coastal regions
Semantic			Using allied shipping as platforms for mobile telephone base stations with access to PSYOPS product Exploiting popular media such as social networking or news sites
Syntactic			
Physical			Radio Frequency transmissions
Infrastructure			
Services			
Geographic			Maritime

Table 12: Targets of maritime cyber subversion

These last three chapters have built on the previous five to fulfil the research objectives of this thesis by demonstrating the interdependency of the maritime and cyber environments in the projection of power at sea within the context of the new model of cyberspace. Initially, in considering the use of power projection activities within the context of the new three-dimensional model of cyberspace it demonstrated not only the utility of the model and how it can be applied, but that cyberspace does not exhibit universal characteristics and that its structure and use may differ at the source and destination of a cyberpower campaign. By building on and expanding Rid's work by applying it to maritime cyberspace, it achieved the second research objective by indicating the link

between the maritime and cyber environments by demonstrating how maritime cyberpower and cyber sea power can be exerted through Rid's three offensive activities against an adversary. This confirm Rid's assertion that cyber-attacks can be regarded as just sophisticated versions of these activities, although intelligence is an expansion of his original example of espionage and subversion has been extended to include Psychological Operations and in doing so fulfilled the third objective by developing a more nuanced and complex appreciation of how power can be projected in maritime cyberspace to reach a target audience. Throughout this analysis, Rid's work has been used as providing the context of what techniques can be applied to achieve cyberpower. These have extended his original work to include additional details not previously considered such as how his three activities can be directed through different areas of cyberspace, both vertically through the different layers and horizontally through near, mid and far space.

The relevance of maritime cyberpower is emphasised by the extent to which nations censor or filter traffic thereby preventing cyberpower projection from outside their borders. Using the attributes of the maritime environment it may be possible to access the target's mid or near space to bypass these restrictions and engage directly with a target system or population through maritime cyberspace. Cyber seapower however exploits the increasingly technical nature of ships' systems and their dependence on a range of technologies and communications media that originate both externally and internally from the ship to influence their activities. The acknowledgement that the environment can play a role in being able to achieve cyberpower fulfils the third objective of this research by demonstrating that cyberspace does not exhibit the same properties globally and a consideration of the geographic setting in which its infrastructure and users are located will affect how cyberspace can be effectively employed to achieve a desired end state.

From table 13 below, it can be seen that sabotage affects the lower, more technical elements of the cyber environment. These layers contain manufactured components that can be directly accessed to adversely affect

their operation to the advantage of the attacker. As subversion is directed at people, as would be expected, it is the higher levels of the model that are targeted with a greater emphasis on influencing the user directly. Of interest is the semantic layer, which forms the link between the human users and the technical components of cyberspace and can be used for both sabotage and subversion. Intelligence activities, or to use Rid's term of espionage, also covers all layers of cyberspace. This is necessary to gain a comprehensive understanding of the totality of the cyber environment and also to support both the sabotage and subversion elements, emphasising its essential role in underpinning all military operations.

By demonstrating the coherence between the model of cyberspace developed in chapter 4 with Rid's three cyber activities and their relationship with the new concepts of maritime cyberpower and cyber seapower, the key findings of the previous chapters can be brought together. These show how these three distinct contributions to cyberpower projection can combine with the utility of regarding the maritime environment as having unique properties when considering how best to alter the behaviour of a target through cyberspace. The next, and final, chapter will conclude with the results of this research and will propose how nations can exploit the conclusions of this work to be able to exploit maritime cyberspace for power projection most effectively.

Layer	**Cyberpower activity**		
Mission	Intelligence	Sabotage	Subversion
Human	Phishing campaign to access systems		Mariners operating in coastal waters or ashore Families of mariners with influence over them Local population living in coastal regions
Semantic	Exploitation of vulnerabilities in software	Spoofing GPS/AIS Hacking maritime logistics systems	Using allied shipping as platforms for mobile telephone base stations with access to PSYOPS product Exploiting popular media such as social networking or news sites
Syntactic	SIGINT collection by submarine Shipping detection through AIS	Jamming GPS/AIS/ Communications	
Physical	Light in fibre optic cables/Radio Frequency transmissions	Light in fibre optic cables/Radio Frequency transmissions	Radio Frequency transmissions
Infrastructure	Seabed submarine operations Fibre optic cables at landing point	Cutting fibre optic cables	
Services		Interrupting power and supporting services	
Geographic	Maritime/Land	Maritime/Land	Maritime/Land

Table 13: Components of cyberspace used for power projection in the maritime environment

Chapter 8 Endnotes

[1] Rid, T., 2013. Cyberwar will not take place. 1st ed. London: Hurst. P. 114.
[2] Ibid. P.115.
[3] Ibid. P.115.
[4] Ibid. P.116.
[5] Ibid. P.114.
[6] Bell, I., 2015. Essay of the week: a brief history of the political smear. [Online] Available at: http://www.heraldscotland.com/opinion/13209481.Essay_of_the_week__a_brief_history_of_the_political_smear/ [Accessed 29 August 2016].
[7] Oxford Reference, 2016. http://www.oxfordreference.com/. [Online]
Available at: http://www.oxfordreference.com/ [Accessed 29 August 2016].
[8] Responses to Liberalism, 2016. Chartists (chartism). [Online]
Available at: https://responsestoliberalism-period2.wikispaces.com/Chartists+(chartism) [Accessed 29 August 2016].
[9] British Library, 2016. Chartism (Summary). [Online] Available at: http://www.bl.uk/learning/histcitizen/21cc/struggle/chartists1/summary/chartism.html [Accessed 29 August 2016].
[10] UK Parliament, 2016. Chartists. [Online] Available at: http://www.parliament.uk/about/living-heritage/transformingsociety/electionsvoting/chartists/overview/chartistmovement/ [Accessed 29 August 2016].
[11] Sands, G., 2016. What to Know About the Worldwide Hacker Group 'Anonymous'. [Online] Available at: http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302 [Accessed 29 August 2016].
[12] Addley, E. & Halliday, J., 2010. Operation Payback cripples MasterCard site in revenge for WikiLeaks ban. [Online] Available at: https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks [Accessed 29 August 2016].
[13] Ministry of Defence, 2014. Allied Joint Doctrine for Psychological Operations - Allied Joint Publication 3.10.1. Edition B Version 1 with UK National Elements ed. Brussels: NATO.
[14] NATO, 2015. AJP-3-10 Allied Joint Doctrine for Information Operations. Edition A Version 1 ed. Brussels, Belgium: NATO.
[15] Ibid. P.1-3
[16] Friedman, H., 2016. Sex and Psychological Operations. [Online]
Available at: http://www.psywarrior.com/sexandprop.html [Accessed 29 August 2016].
[17]Lister, C., 2014. *Profiling the Islamic State.* [Online]
Available at: http://www.brookings.edu/research/reports2/2014/12/profiling-islamic-state-lister [Accessed 5 Nov 2015].
[18] Maidment, J., 2017. *Theresa May calls on internet companies to eradicate 'safe spaces' for extremism in wake of London Bridge terror attack.* [Online] Available at: http://www.telegraph.co.uk/news/2017/06/04/theresa-may-calls-internet-companies-eradicate-safe-spaces-extremism/ [Accessed 17 Jun 2015].
[19] Land, M., 2017 *The UK's plan to deny terrorist 'safe spaces' online would make us all less safe in the long run.* [Online] Available at: http://theconversation.com/the-uks-plan-to-deny-terrorists-safe-spaces-online-would-make-us-all-less-safe-in-the-long-run-79323 [Accessed 17 Jun 2015].
[20] Talbot, D., 2008. *How Obama Really Did It.* [Online]
Available at: http://www.technologyreview.com/featuredstory/410644/how-obama-really-did-it/ [Accessed 5 Nov 2015].
[21] Tsikerdekis, M. & Zeadally, S., 2014. *Online Deception in Social Media.* [Online]
Available at: http://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1013&context=slis_facpub [Accessed 5 Nov 2015].
[22] Nye, J. S., 2008. Public diplomacy and soft power. *The Annuals of the American Academy of Political and Social Science,* 616(1), pp. 98.
[23] Bastardi, A., Uhlmann, E. L. & Ross, L., 2011. Wishful Thinking: Belief, Desire, and the Motivated Evaluation of Scientific Evidence. *Psychological Science,* 22(6), pp. 731-732.
[24] NATO, 2015. AJP-3-10 Allied Joint Doctrine for Information Operations. Edition A Version 1 ed. Brussels, Belgium: NATO. P.1-9

[25] Ibid. P.1-6
[26] Joint Operations. 2017. *Joint Publication 3-0*. P. V-14 [Online]. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf [Accessed 16 Jul 2017].
[27] As quoted by Captain Rory Bryan OBE, Chief of Staff to Rear Admiral Alex Burton, Commander UK Maritime Battle Staff during Exercise Joint Venture 2017.
[28] Pew Research Centre, 2016. *Smartphone ownership and Internet usage continues to climb in emerging economies.* [Online] Available at: http://www.pewglobal.org/files/2016/02/pew_research_ center_global_technology_report_final_february_22__2016.pdf [Accessed 23 February 2016].
[29] Kruger, B., 2000. *Distance of the horizon.* [Online] Available at: http://www.cactus2000.de/uk/unit/ masshor.shtml [Accessed 23 February 2016].
[30] Gallagher, R., 2013. *Meet the machines that steal your phone's data.* [Online] Available at: http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ [Accessed 24 February 2016].
[31] 4g.co.uk, 2015. *How fast is 4G.* [Online] Available at: http://www.4g.co.uk/how-fast-is-4g/ [Accessed 24 February 2016].
[32] Trueman, C. N., 2016. *The Graf Spee in Montevideo.* [Online] Available at: http://www.historylearningsite.co.uk/world-war-two/war-in-the-atlantic/the-graf-spee-in-montevideo/ [Accessed 30 August 2016].
[33] Ministry of Defence, 2014. *Allied Joint Doctrine for Psychological Operations. AJP-3.10.1* Edition B Version 1 + UK National Elements. P.Lex-6
[34] Talbot, D., 2008. *How Obama Really Did It.* [Online] Available at: http://www.technologyreview.com/featuredstory/410644/how-obama-really-did-it/ [Accessed 5 Nov 2015].
[35] Cha, M., Haddadi, H., Benevenuto, F. & Gummadi, 2010. *Measuring User Influence in Twitter: The Million Follower Fallacy.* Washington, D.C., The AAAI Press, Menlo Park, California.
[36] Twitter, 2015. *Twitter Analytics.* [Online] Available at: https://analytics.twitter.com/about [Accessed 5 Nov 2015].
[37] Google, 2015. *Google Analytics.* [Online] Available at: http://www.google.com/analytics/ [Accessed 5 Nov 2015].
[38] Jegatheesan, S., 2013. Cookies – Invading Our Privacy for Marketing, Advertising and Security Issues. *International Journal of Scientific & Engineering Research,,* 4(5), pp. 926-928.
[39] Kent, M. L., Carr, B. J., Husted, R. A. & Pop, R. A., 2011. Learning web analytics: A tool for strategic communication. *Public Relations Review,* Volume 37, pp. 536-543.
[40] Barwinski, M. A., 2005. *Taxonomy Of Spyware And Empirical Study Of Network Drive-by downloads.* 1st ed. Monterey, CA: Naval Postgraduate School.
[41] Gassen, J., Gerhards-Padilla, E. & Martini, P., 2012. Current Botnet-Techniques and Countermeasures. *Praxis der Informationsverarbeitung und Kommunikation,* 35(1), pp. 3-10.

Chapter 9: Conclusion

This thesis has addressed three distinct research objectives that together define the relationship between the maritime and cyber environments within the context of power projection and security. Power in the context of this research has been defined as the ability to affect the behaviour of *people* such that A can be regarded as having power over B to the extent that they can get B to do something that they would not otherwise do.[1] Security is regarded as the means by which a power projection strategy can be neutralised or inhibited. This ability to be able to alter the activities of a target individual, group, or population to the benefit of the perpetrator and possibly to the detriment of the target is at the heart of a campaign of power projection in any environment and this thesis drew on several methods by which this can be achieved by combining the attributes of the maritime and cyber.

The first objective was to introduce a novel three-dimensional model of cyberspace optimised to better understand and explain how its properties and attributes can be measured in terms of power projection and to demonstrate that the environment does not exhibit universal characteristics, but that its structure and use may differ at the source and destination of a cyberpower campaign. This emphasises that the view of cyberspace often portrayed as some form of 'cloud' is unhelpful and that its attributes will vary depending upon a range of factors including technical, political, and geographic. Essentially there is no 'cloud', it's just part of cyberspace owned by somebody else.

The second objective was to investigate the close relationship and interdependence between the maritime and cyber environments within the context of power and security leading to the new concept of maritime cyberspace. This enabled direct parallels to be drawn between well-established notions of how power at sea is derived and can be applied to the cyber environment.

Finally, by classifying cyberattacks as acts of intelligence gathering operations, sabotage, or subversion, the third objective built on the outcomes of previous two to develop a more nuanced and complex appreciation of how power can be projected in maritime cyberspace to reach a target audience and better understand the types of effect that can be achieved and which component of cyberspace is utilised to achieve a particular outcome.

As political and military activity extended initially from the land to include maritime, air and now also to encompass space, previous literature has tended to overlook their relationship with the cyber environment. This was despite historical precedents of combining the attributes of the physical environments, as demonstrated by the employment of specialist amphibious warfare units, shipborne aviation and the use of satellite derived communications and intelligence illustrating how naval forces can combine their distinctive qualities in the projection of seapower. The rationale for conducting this research now is that previously ships have been disconnected from the wider cyber environment and were regarded as autonomous vessels with only minimal interaction using external data communication systems. This has now changed in that they have increasingly become reliant upon cyberspace for their navigation, safety, logistic support and for coordinating their movements with other vessels, particularly when operating in congested coastal waters. In addition, onboard management systems are becoming more dependent upon computer based networks for their operation and when connected digitally to a shore based infrastructure have become an integral part of the global cyber environment. That, and the ability for a nation's ships and submarines to engage with the shore based infrastructure of another country to extend their influence into another state has raised the profile of the relationship between the two environments.

In considering the first research objective it was important that the new model of cyberspace could encompass the characteristics of the environment in such a way that all aspects of an operation to project cyberpower could be considered as well as how such a campaign could be disrupted. Integral to this

was a recognition of the geographic differences that may exist in the environment at the source and destination of a power projection campaign and how that could affect the properties of cyberspace and the ways in which the information could be accessed. The model was used to demonstrate that cyberspace does not exist in isolation and must incorporate and consider the physical and supporting elements that enable it to function, including the environment in which its infrastructure is located and through which it transits. Furthermore, it needed to be able to account for the variety of communicating media used by both state and non-state actors and that the path followed by data may not be under the control of either the transmitting or receiving locations. This is significant as the methods and degree of sophistication used by different organisations and individuals to target an audience may differ and yet the impact of a successful campaign may be very similar.

A key aspect of this model was that it expanded on and combined the work of others who have been prominent in this area of research. Previous literature has sought to explain of nature of cyberspace in terms of layers with each one having distinct attributes and properties. Viewing cyberspace in this way has evolved from initially a three-layer model to four and this thesis builds on both to propose an eight-layer structure. This involved including for the first-time factors such as its relationship with the geographic environment through which it passes, supporting services, the human user, and an inclusion of the purpose for the user engaging with cyberspace. Together these provide a comprehensive understanding of all elements of the environment that combined can effectively project power through cyberspace.

As the new model of cyberspace was designed with the intention of understanding cyberpower, its initial layered format was further developed to enable it to be interpreted in three dimensions. This included combining its eight layers with an appreciation of distance through near, mid, and far space taken from the UK Ministry of Defence's Cyber Primer and making it possible for each aspect of the environment to be assessed as part of an overall cyberpower campaign. These enabled differences in the properties of cyberspace to be

identified at the source and target of a cyberpower campaign as well as the components between them. To this two-dimensional view, a third component was added by enabling a differentiation to be made between the techniques used for hard, soft, and smart power projection. This enabled a consideration to be made as to the type of message to be promulgated and that the properties of cyberspace at the point where the target accesses it may determine which has the greatest chance of achieving the desired behavioural change. By combining these elements from previously published work, the resultant three-dimensional model drew on their strengths and expanded its overall utility to enable cyberspace to be viewed in a new and more comprehensive manner.

A key aspect in the development of this model was its successful validation in the qualitative analysis of a range of cyber-attacks, which enabled a range of incidents to be modelled in terms of their sophistication and the layers that they targeted. The results of this study enabled it to be concluded that the further away from the human interface that the attack sought to target, the greater the level of sophistication needed. This is due to the additional complexities of interacting with elements of a systems that are not intended to be directly accessed and therefore require bypassing the intended user interface. From the endorsement of this new representation of cyberspace, it was seen that it has the potential for it be used for planning offensive activities in cyberspace. This would include modelling a cyberpower campaign and analysing a range of potential attack methodologies. From a defensive perspective, it could also be used to identify security weaknesses in a system that may need to be addressed to counter a cyber-attack. As such the model can be regarded as being of use to anyone who wishes to understand how the elements of cyberspace that they control interfaces with the wider environment and can also highlight the threats and opportunities that it presents.

A distinct aspect of the qualitative analysis of the model was that by referring to the conclusions of industry commentators of each cyber-attack it was possible to demonstrate that generally the more sophisticated types of attack were attributed to state actors with the resources and expertise available to invest in

more complex attack methodologies. This can be used to analyse the attributes of new cyber-attacks as they are detected to determine how they align with those previously detected to provide an indication of their possible source.

The second objective of this research was to investigate how the attributes of the maritime and cyber environments can be combined, which resulted in the new concept of maritime cyberspace being developed. An understanding of the relationship between the natural physical attributes of the sea and coastal areas and the artificial manufactured technologically based cyberspace is important as it raises significant security implications for all seafarers who engage with them. This is due to the potential opportunities it presents to those nations that regard themselves both as maritime powers and also to understand the importance of the cyber environment and how they can both be exploited to fulfil their national foreign policy aspirations. This includes nations that not only have significant military assets afloat, but also those that exploit the seas for economic purposes by harvesting its resources or for the global transportation of cargo.

The relationship between the maritime and cyber environments, particularly within the context of influencing others, is an area that is unexplored in terms of research and understanding as the two environments are usually studied in isolation and their mutual dependencies not considered. However, when combined, their unique characteristics can be harnessed both to alter behaviour and through the implementation of security measures used as a counter power strategy, to limit the influence of others. The research strategy used in addressing this issue initially involved an appreciation of the two environments with the aim of understanding how their properties affected each other and how they are used for power projection. This drew on a range of literature sources including international legal agreements and national policy and doctrinal documents as well as technical material related to the construction of cyberspace and the protocols that enable data exchange to take place. Combined, this investigation confirmed the following important similarities in the attributes of the maritime and cyber environments:

- Despite one being a natural environment and the other artificial, both require manufactured means to exploit them, be it a vessel of some description for the maritime or a computer and coded software applications for cyberspace.

- Both environments have areas that are legally recognised as owned by identifiable parties or countries such as national territorial waters or an organisation's local area network and other parts that are not under the close supervision of any entity such as the high seas or the traffic within the Internet's large capacity backbone networks or undersea cables.

- It is not possible to for one country to totally control everywhere, all the time, the activities that take place either across the world's oceans or in cyberspace.

- However, influence or local control is possible in some areas, some of the time through the predominance of the number of ships owned or operated by a single nation or in the amount of hardware and software that originates in one country or produced by a single company.

- There are a range of international agreements that dictate the use of both environments, be it the United Nations Convention on the Law of the Sea or the Internet's routing and addressing protocols.

- Both environments are fundamental to global trade and are essential elements of a modern economy and require freedom of access and the confidence to operate securely without external interference.

- Control over both maritime and cyber environments can be contested with disputed areas of the sea subject to tension where sovereignty is challenged, which may result in the presence of warships attempting to exert dominance. Areas of cyberspace can also be contested in which state and non-

state actors seek to gain control of the infrastructure of another's to exfiltrate data or to adversely affect its performance or routing protocols.

Combining the features of these two environments led the development of the concept of *maritime cyberspace*. This consists of those aspects where a mutual dependency exists between the maritime and cyber environments. Currently, maritime cyberspace has been defined as comprising four components; satellite derived position, navigation, and timing (PNT) data, the Automatic Identification System (AIS) that contributes to maritime safety, terrestrial Radio Frequency data communications and finally the undersea fibre optic cables that carry transoceanic digital communications. By considering the composition of maritime cyberspace and relating British Maritime Doctrine to the attributes of cyber environment, a direct association can be drawn between power at sea and power in cyberspace. This enabled the concepts of *maritime cyberpower*, which is comparable to *maritime power* and *cyber seapower*, which has similar attributes to the notion of *seapower* in the physical environment to be developed. The difference between these is that whereas maritime cyberpower seeks to achieve an effect from the sea that influences events anywhere in cyberspace, cyber seapower seeks to use cyberspace to achieve an effect solely in the maritime environment, including the littoral. Cyber seapower itself is comprised of *cyber sea control* and *cyber sea denial*, which would enable a maritime cyber power to have similar influence over aspects of maritime cyberspace as a maritime power would have in the physical environment.

In addressing the issue of how to investigate the nature of power projection and security within maritime cyberspace this research examined the evolution of the debate through the work of Arquilla and Rid. Whereas Arquilla suggested that cyberwar may be used as an alternative to a conventional destructive campaign, Rid countered this suggestion by offering a more pragmatic and evidenced based approach and that by nature cyberspace is inherently non-violent with only limited capacity for inflicting force on others. To address the tension between these author's viewpoints, this research used the more refined and, at the time of its publication, contentions conclusions of Rid as the basis

on which to develop the unexplored area of how offensive cyber activities can be conducted from and within the maritime environment. To provide the foundation on which to expand the work of Rid, this study also drew on the work of Nye and his classification of hard, soft, and smart power types. This provided the theoretical background as to how cyberspace could be used as the medium by which targets can be influenced through either one or a combination of attraction, persuasion or coercion.

The first of Rid's activities to be examined was what he termed espionage. This was expanded to encompass the full range of techniques that could be employed to collect information from a target within cyberspace, which after analysis could produce actionable intelligence. This is significant as there is a considerable amount of information that is freely available, released either intentionally or unintentionally by its originator and that it may not be necessary to revert to covert, intrusive techniques that if discovered may be regarded as hostile if discovered by the system owner.

The second activity, sabotage was examined to determine how maritime cyberspace could be used to project power and influence both in and from the sea by adversely affecting maritime systems' intended mode of operation. This indirect form of power projection seeks to alter the behaviour of people by targeting the technology that they use. This aims to either limit an adversary's ability to engage with cyberspace or to manipulate the content of the material they interact with to change their perceptions and opinions of events. The role of sabotage is significant as it implies a physical effect on a computer network or connected device through the use of computer code. Achieving an effect equivalent to a conventional kinetic attack, but which is conducted remotely and possibly with ambiguous attribution, is one which modern highly connected nations are now becoming acutely aware of, particularly in terms of when a cyber-attack can be regarded as a warlike act and result in retaliatory action from land, air or maritime forces.

Rid's third activity involves the use of subversion as a means of power projection in maritime cyberspace. Subversion differs from the information gathering activities of intelligence operations and the targeting of systems in cyberspace by seeking to directly influence the ultimate target of power, the human users by undermining their trust in the established order or to persuade them to act in a different way by offering a more attractive option. As the filtering and censorship of cyberspace by nations at their borders and internally within its networks can interfere with a campaign reaching its intended target, the properties of maritime cyberspace can be ideally suited to a soft power campaign as well as the more subversive activities of deception and false attribution by directly accessing individual users through their personal devices. The ability to influence behaviour through non-kinetic means is already recognised, in the military by the discipline of psychological operations (PSYOPS), which seeks to influence perceptions as part of a wider campaign of information operations. However, although maritime cyberspace offers the potential to use these techniques, to be most effective they must be coordinated with a broader strategic communications plan to ensure that the message is coherent with the overall campaign strategy.

By combining the results of this study and analysing the attributes of Rid's three offensive cyber activities of espionage, sabotage, and subversion with Nye's differentiation between hard, soft, and smart power within the overall context of the new model of cyberspace the relationship between them can be shown. This has resulted in the development of a new and readily repeatable means by which an operation can be planned and conducted based on figure 23 below, which illustrates the road to cyber conflict. By demonstrating that the path from peace to war consists of a spectrum of activities ranging from peacetime diplomacy through to rising tension and ultimately to high level conflict, it highlights that there is a middle ground, the so called *grey zone* when hybrid warfare is the predominant activity during which a combination of both diplomatic and warlike actions can take place in cyberspace. This spectrum of political activities aligns with the types of power projection proposed by Nye with soft power chiefly a peacetime activity and hard power gaining precedence

during warfare with both elements being employed as part of a hybrid strategy. Linking this to cyber operations, soft power aligns to a non-violent campaign of subversion that seeks to undermine the authority of an adversary and presents an alternative cultural norm as being more attractive and beneficial than that offered by the current regime. This would involve targeting the human layer of cyberspace directly via the applications that they use to interact with the semantic layer. Subversion is also only targeted in the far space of the perpetrator as that is where the adversary's population is located.

Once increasing tension leads to more aggressive activities being conducted, figure 23 recognises that a smart power strategy may be employed leading to the employment of both subversive and sabotage operations in equal measure. This would be the most complex to plan and conduct and requires a careful intelligence led assessment of the target set to identify those who would be most responsive to threats rather than persuasion.

Should a smart power campaign fail to achieve all its strategic aims, an operation focused more on hard power may be considered. In this situation, there would be a greater focus on sabotage operations, possibly in coordination with subversion, but persuasion would now take a subordinate role as the political direction would now favour a strategy based on a more threatening posture. Coercion and intimidation in cyberspace can be employed across a wider range of the layered model as it can employ a more technical, rather than human focus. In conducting sabotage operations, a campaign planner has a larger target set in that as well as targeting the semantic layer that was initially used in the soft power phase, they can also include the layers below as far as the supporting services layer that provide the power, cooling, and the physical security of the environment. Again, sabotage operations can be focussed at the far space of the aggressor in the near space of the victim, but actions may occur in mid space if engaging with these systems will also adversely affect the target. The final action, intelligence gathering, is an expansion on the more restrictive activity of espionage proposed by Rid and is a reoccurring activity throughout the road to conflict. This includes acquiring data from all sources within

cyberspace and not just those that are protected and requires precursor operations to compromise security measures before they can be accessed. The requirement to conduct intelligence mirrors every other operation in the physical environment of the sea, land, air, and space where a knowledge of the adversary and an assessment of their intentions is fundamental to inform the planning process. The global nature of cyberspace and the mostly passive act of intelligence collection means that this activity takes place throughout the environment where useful information can be collected and so will include all levels and locations defined in the model.

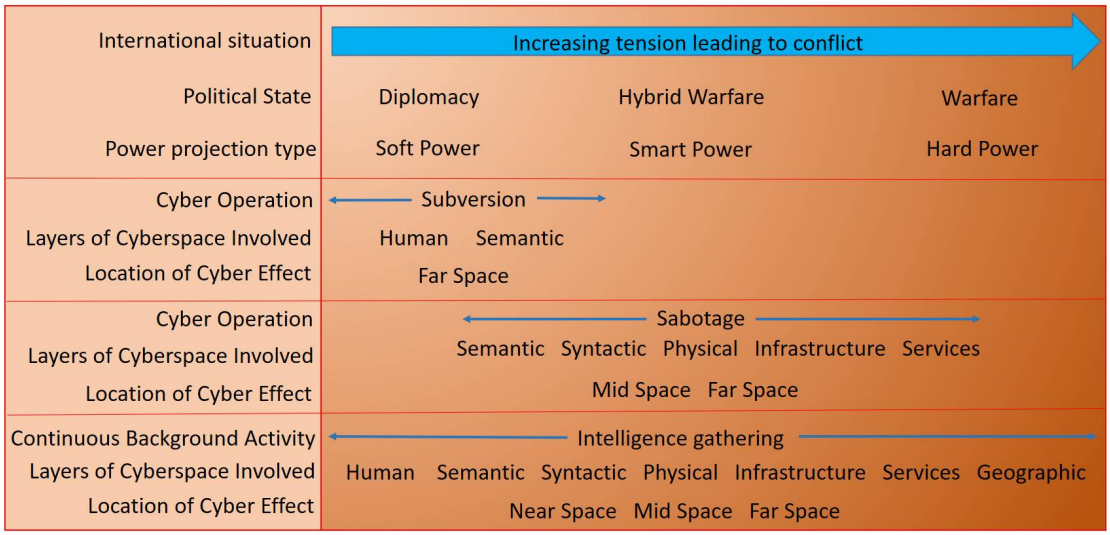

Figure 23: The road to cyber conflict

This thesis has combined a range of concepts and research subjects that have not previously been considered together to determine how power and influence can be projected within the maritime environment and what security measures are required to inhibit it. Using its conclusions in conjunction with the model of cyberspace and the graphical illustration of the road to cyber conflict shown in figure 23, a new military doctrine could be derived based on the ability to achieve a more comprehensive understanding of the nature of cyberspace as a means of power projection. This doctrine would be based on mapping a path from source to destination in cyberspace and highlighting the preferred route as well as highlighting those elements that may prevent its successful passage. This would also include an assessment of the geographic region through which

the infrastructure of cyberspace is located. As well as tracing a route, this allows the methods to be identified that may be successful in projecting the three types of power; hard, soft, or smart. These may in turn influence the decision as to which one is to be used based on the international situation, political intent, and available access.

As a result of this research, potentially new areas of investigation have emerged to further examine the properties of maritime cyberspace and how they could be expanded to be applicable not only in terms of power projection, but also in other contexts. For example, its third dimension highlighted the different characteristics of hard, soft, and smart power and how they could provide the foundation for the creation of a planning tool to assess how effective different power strategies might be. This was not examined in detail in this research, but could be a subject area for further investigation to include the use of the model with real world data to validate its utility in presenting a range of options to a decision maker. To be most effective, this would require access to a range of data sources, many of which may be nationally sensitive and so outside the scope of this work, but could be of benefit to government agencies.

Although this thesis focussed on international relationships, there is also potential to use the new model of cyberspace as a means to assess the security of an organisation or domestic user. This could involve the production of templates to address a range of security issues to enable an appreciation of each element of an enterprise to be assessed with its strengths and weaknesses analysed and highlighted. The different properties of near, mid, and far space and how they interact could provide a useful insight into how to protect the boundaries between networks owned and maintained by different organisations and for mapping routes between them. This would be of interest to those engaged with both domestic and international partners to identify how differences in the properties of cyberspace affect communications across a range of jurisdictions and whether alternative business strategies and security measures should be used when trading with other nations.

An important consideration in any further work and an issue that became apparent when reflecting on the research objective was the fluid and continually evolving nature of cyberspace. Investigating the nature of the environment using the model is not an activity to be conducted once only, but one that should be constantly reassessed to determine how any changes in the elements of the model of cyberspace may affect its properties and how they can be exploited to maximum effect. As cyberspace changes, the model itself should be regularly reviewed to ensure that it remains relevant and fit for purpose and that as new technologies and uses are found for the environment that its layers remain applicable or whether they should be redefined, sub-divided or removed.

Although this research has concentrated on the maritime environment, the methodology could also be applied to the land and air environments. The relationship between of hard, soft, and smart power types with intelligence gathering, sabotage and subversion within the context of the model of cyberspace developed as part of this research is not only relevant to operations at sea but could be equally of use in other warfare disciplines. Used in conjunction with a nation's army and air force doctrines, their combined findings would be of benefit in the planning of a joint warfare campaign of cyberpower projection deployed across an adversary's battlespace. This would be particularly relevant where a campaign's area of operations encompasses a range of geographic areas, each with their own distinct properties that may affect cyber power projection. Space, as an unmanned environment would not at present be a valid area for this application of all aspects of this research, but the hijacking and sabotage of satellite systems may prove to be a important subject as a supplementary activity.

Allied to any action offensive action conducted by a nation outside its own near space in the near space of other states' networks is the issue of legality and the applicability of the laws of war. Although state on state espionage is not deemed illegal in international law, it would be governed by each country's own domestic law with authorisation given to limit the extent of the activity and the target. However, as highlighted in the Tallinn Manual, activities in cyberspace that

result in similar effects to that of a kinetic weapon would be considered as such under the International Law of Armed Conflict and be subject to the same constraints and restrictions. As this research has demonstrated, offensive actions in cyberspace are often conducted covertly, which limits public scrutiny, academic discussion, and the development of international agreements. Should further evidence of what may be regarded as incidents of cyber warfare enter the public domain, there may be a greater demand for research leading to the establishment of international agreements to regulate and formalise its conduct.

In terms of a broader cyber security perspective, this research has highlighted that the role of cyber security is to prevent access and protect assets from unauthorised interference within cyberspace. Although normally regarded in terms of protecting infrastructure and data from theft or damage; that is, intelligence gathering and sabotage, this thesis has shown that assets can also include human users. Thus, using security measures to prevent an adversary from using cyberspace to gain access to a target population in order to alter their behaviour may be a valid objective of a plan to counter cyber power. Although, this sort of restriction to material is normally regarded as censorship, which has generally negative connotations, this research has shown that it may also be regarded as a legitimate activity to protect national interests from perceived unwanted or unwarranted external interference.

In reflecting on the experience of conducting this research, the most significant lesson that has been identified is that power and projection in cyberspace is a complex and multifaceted discipline. Although cyberspace is an artificial medium based on technology and governed by well understood computer protocols that perform in a known matter, its content is generated, accessed, and interpreted by humans who are unpredictable. Although behaviour can to a certain extent be predicted based on culture, gender, age, background, and education, it cannot be forecast with certainty. The range of elements included in this research; the properties of the cyber and maritime environments, the elements of cyberspace identified in the model and the three types of power

projection and offensive cyber activities all represent its complexity and highlight the importance of the three research objectives of this work. These also illustrate the close relationship and interdependence between the maritime and cyber environments in terms of power projection and the need to develop a model of cyberspace to extend the work of significant contributors such as Nye and Rid to fully understand how it can be applied. Finally, this research has demonstrated that cyberspace is not universal or unique, but needs to be explored in different contexts or environments, which can vary depending upon the terrain or geographic location.

Chapter 9 Endnotes

[1] Dahl, R., 1957. The concept of power. *Behavioral Science,* 2(3), pp. 201-215.

Appendix 1: The six dimensions of the maritime environment

Physical: The sea covers approximately 72% of the earth's surface and 80% of the world's population lives within 100 miles of it – a figure that is rising with population growth and climate change.[1] Its physical characteristics are hugely variable with significant ranges of air and sea temperature, salinity, humidity, and depth affecting how it can be exploited for its resources. Oceanographic currents and regional weather conditions can also have a significant impact on transiting vessels with all seafarers acknowledging that it is an unforgiving and at times a difficult operating environment. Such variations affect both the users of the seas and the propagation of electromagnetic waves that can alter the performance of communication and radar systems upon which the safety of shipping depends.

Economic: The waters that border a state can be an important source of national wealth. This is recognised in that all coastal nations can lay claim to an area adjacent to their borders by declaring territorial waters of 12nm and an Exclusive Economic Zone (EEZ) that can extend to as far as 200nm out to sea. This can be used for fishing, natural resource extraction or more recently as the base for renewable energy initiatives.[2] The protection of this area from the financial cost of illegal access is regarded as an important role for a country's government. The UK for example has 6,444 registered vessels in its fishing industry employing 12 400 people and in 2010 supported a market worth £5.84 billion. With seafood consumed by four out of five UK households at least once a month, overfishing and depletion of this important natural resource can be a significant political issue.[3]

As a means of facilitating commerce, cargos carried by sea are at the forefront of the world economy with around 90% of world trade carried by the international shipping industry. Globally, there are at least 50 000 merchant ships registered in over 150 countries and manned by over a million seaman of virtually every nationality moving cargo between more than 3 000 major commercial ports.[4] There are three major types of merchant ships at sea;

container ships carrying manufactured goods, bulk carriers transporting dry raw materials and tankers containing oil, chemicals and petroleum products with merchant traffic of all types predicted to rise as developing economies in the middle and Far East mature. With most trade dominated by three economic centres in North America, Europe and Asia, London is currently the world's principal centre for a wide variety of maritime industries including the Baltic Exchange, whose members are responsible for arranging a large proportion of dry cargo and tanker trade.[5] The UK maritime industry directly contributes up to £13.8 billion to the UK economy and indirectly contributes a further £17.9 billion. Overall the sector accounts for over 2% of the entire UK economy and creates £8.5 billion in taxes each year.[6] London's financial centre is at the heart of the international maritime insurance industry through the specialist service that Lloyds of London performs and has a prominent stake in the development of maritime law, and banking.[7] Finally, exploration of the seas for the recovery of fossil fuels or using shallow waters as the base for off shore wind farms has become an important consideration in many coastal states' economic planning and has increased the potential for international disputes to arise. In some areas, such as the North Sea, nations with a stake in the wealth that can be derived from oil exploration are engaged in collaborative ventures whereas in other locations, such as those surrounding the Falkland Islands, it has increased the already tense relationship between the UK and Argentina over the sovereignty of the Islands and the rights to exploit its surrounding waters.[8]

Political: Although over three quarters of the member states of the United Nations are coastal nations, the seas are mostly ungoverned as no country may subject any part of the high seas beyond its EEZ to its sovereignty.[9] However, some sea areas are politically very sensitive such as those which are choke points for maritime trade or where sovereignty is disputed for economic or political purposes. These include the Straits of Hormuz, which are near the coast of Iran and areas of the South China Sea where China has claimed areas of sovereignty despite objections from the neighbouring states.[10] This has resulted in the militarisation of several regions where conflicting national interests arise and the extension of national sovereignty out to the maximum

possible distance has become a contentious issue. These conflicting claims can be very challenging to resolve if there are cultural or historical precedents to the ownership of disputed areas. This may be particularly so over islands, ownership of which may also then extend rights over their surrounding waters and associated natural resources.

Diplomatic: Allied to the political dimension of states seeking to expand their national sovereignty out to sea for economic purposes are the diplomatic consequences of where claims to the same area of water arise. Existing diplomatic agreements and international bodies such as the United Nations can help diffuse complex situations, but only where both sides agree to abide by their judgements. This has been brought into sharp focus by the Chinese government's refusal to participate in or accept arbitration with the Philippines over territorial sovereignty disputes in the South China Sea.[11] This is significant as should the Philippines continue to pursue their claim in the international arena and maintain international support, China's refusal to yield could have international diplomatic consequences. However, China's vastly superior military forces and aggressive expansionism in the region, coupled with a reluctance by the rest of world to intervene will result in it achieving its aims with the resulting loss of credibility of the United Nations and other international bodies.

Legal: Notwithstanding China's policy of choosing to disregard international agreements and arbitration when it suits their domestic political agenda, there is a substantial body of important legal conventions to which many nations have agreed to abide. The most important of these is the 1982 UN Convention of the Law of the Seas (UNCLOS), which as of 2 January 2015, had been ratified by 167 nations, including China, but notably not the United States.[12] This Convention contains a range of legal rights and obligations for both coastal states and those nations that have flagged vessels. Its most important is that although all states can claim maritime zones, including territorial waters and EEZs, they are to be regarded as international spaces and vessels of any nation can transit through them on innocent passage. In addition, warships may

exercise and operate in the EEZs of other nations, although there are restrictions on their activities in territorial waters. All states, even landlocked ones, have the right to operate flagged vessels and where they do, have exclusive jurisdiction over them. Any nation's vessels can thus operate worldwide without interference and may only be subject to inspection by other country's warships in very limited circumstances such as if they are suspected of being engaged in piracy or slavery.

Military: The seas have been used for military purposes and the projection of power for many thousands of years; the first organised invasion by sea of the British Isles being by the Romans in 55BC. Today there are estimated to be over 150 navies world wide ranging from the worldwide global reach of the United States Navy to small coastal forces operated by third world nations.[13] Although not all navies have ocean going, so called *blue water,* aspirations and seek to operate for extended periods in international waters away from home, smaller forces have the potential to conduct local sea denial operations that can constrain the conduct of larger navies. For example the use of three conventional submarines by the Iranian navy has been a cause for concern for their ability to threaten the passage of shipping through the Straits of Hormuz.[14] The use of mines has also been used as a means to close shipping lanes and the Royal Navy has four minehunters permanently based in Bahrain to mitigate this threat to regional shipping.[15] This threat is taken particularly seriously as demonstrated by a 34 ship anti-mine exercise that took place in 2013 following threats made at the time by the Iranian government that it would respond to sanctions or attempts to stop its nuclear programme.[16]

Appendix 1 Endnotes

[1] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre. p.1-6.
[2] Seavision, 2016. *Fisheries and Aquaculture.* [Online] Available at: http://www.seavision.org.uk/about/fisheries-aquaculture. [Accessed 11 April 2016 Apr 2016].
[3] Seavision, 2016. *Seavision Home Page.* [Online] Available at: http://www.seavision.org.uk/fisheries-aquaculture/home. [Accessed 11 Apr 2016].
[4] International Chamber of Shipping, 2015. *Shipping and World Trade.* [Online] Available at: http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade. [Accessed 11 Apr 2016].
[5] The Baltic Exchange, 2016. *The Baltic Exchange.* [Online] Available at: http://ww.balticexchange.com/. [Accessed 11 Apr 2016].
[6] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office.p.7.
[7] LLoyds, 2016. *About Lloyds.* [Online] Available at: http://www.lloyds.com/lloyds. [Accessed 11 Apr 2016].
[8] BBC News, 2015. *Argentina judge orders asset seizure of Falklands oil firms.* [Online] Available at: http://www.bbc.co.uk/news/world-latin-america-33301540. [Accessed 11 Apr 2016].
[9] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.1-6
[10] BBC News, 2015. *Q&A: South China Sea dispute.* [Online] Available at: http://www.bbc.co.uk/news/world-asia-pacific-13748349. [Accessed 11 Apr 2016].
[11] The Diplomat, 2014. *Why China Won't Accept International Arbitration in the South China Sea.* [Online]
Available at: http://thediplomat.com/2014/12/why-china-wont-accept-international-arbitration-in-the-south-china-sea/. [Accessed 11 Apr 2016].
[12] United Nations, 2016. *Chronological lists of ratifications of, accessions and successions to the Convention.* [Online] Available at: http://www.un.org/depts/los/reference_files/chronological_lists_of_ratifications.htm. [Accessed 11 Apr 2016].
[13]Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre.p.1-12
[14] Nuclear Threat Initiative, 2015. *Iran Submarine Capabilities.* [Online] Available at: http://www.nti.org/analysis/articles/iran-submarine-capabilities/. [Accessed 11 Apr 2016].
[15] Royal Navy, 2016. *Dhabi meeting as British and UAE minehunters train in Gulf.* [Online] Available at: http://www.royalnavy.mod.uk/news-and-latest-activity/news/2016/march/10/160310-dhabi-meeting-as-british-and-uae-minehunters-train-in-gulf. [Accessed 11 Apr 2016].
[16] The Telegraph, 2016. *World's biggest anti-mine naval exercise after Iranian threats to close Gulf.* [Online]
Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10052612/Worlds-biggest-anti-mine-naval-exercise-after-Iranian-threats-to-close-Gulf.html. [Accessed 11 Apr 2016].

Appendix 2: Intelligence sources and their relationship with maritime cyberspace[1]

ACINT: Acoustic Intelligence involves the analysis of sonar or radiated noise from shipping and is of use in identifying individual types of vessel or underwater weapons from their noise signature. As these frequencies are below those used for data transmission, it has no relevance for maritime cyberspace.

GEOINT: Geospatial intelligence uses information derived from mapping and the analysis of terrain data. This will have relevance in tracing the routes of undersea cables and their landing points as well as predicting the ranges at which signals can be intercepted.

HUMINT: Human Intelligence employs agents in the field to gather information and has a role to play in all intelligence based operations. Although predominantly a technology based environment, maritime cyberspace is created, maintained, and exploited by humans who may provide useful intelligence. Although HUMINT sources are often portrayed as covert intelligence operatives engaged in espionage, they could also be researchers, academics or engineers who may be open about their role in supporting maritime cyberspace or include users who have unwittingly downloaded malware to their computers and whose activities online are being covertly monitored by intelligence agencies or criminal groups.

IMINT: Imagery Intelligence uses sensors to capture still or moving representations of a target across a range of wavelengths including the visual spectrum, infrared or radar. As a medium used in the production of images, it has a similar use as for GEOINT in terrain analysis and identifying significant infrastructure such as coastal masts used for transmitting data or the areas where undersea cables come ashore.

MASINT: Measurement and Signature intelligence derives information from the analysis of the distinctive signatures of a target, which may be physical, thermal, or electronic. As this refers to the investigation of a physical object, it may have relevance in locating and identifying active infrastructure installations.

OSINT: Open Source intelligence is the compilation of material freely available without recourse to covert measures for its collection. As cyberspace is a concept based on information in which users can access their own and other's data worldwide, OSINT is at the heart of all aspects of the environment. However, OSINT collection can have two significant issues; ensuring the material is truthful and not part of a deception plan, and where quantity is an issue, being able to filter and sort the data to discover the significant elements.

SIGINT: Signals Intelligence gathered from electromagnetic transmissions. This form of intelligence is at the heart of maritime cyberspace where fixed communication links between ships and to shore are not possible and is further subdivided into two forms, COMINT and ELINT:

COMINT: Communications Intelligence draws information directly from the contents of a communication channel such as from unencrypted radio transmissions and may also involve the decryption of secure media.

ELINT: Electronic Intelligence that analyses the attributes of a radio transmission. This includes deriving useful intelligence from frequency, amplitude, signal strength, modulation type and for data communications the type of transmission, including the protocols, data rate, or network of users. This can prove to be a valuable source of information if the contents of the transmission themselves are unreadable due to strong encryption.

TECHINT: Technical intelligence draws together information gathered on a piece of material to draw conclusions as to its purpose and performance. This can determine from, for example an aerial design, the power, modulation,

frequency, or direction of the transmission, which can cue other intelligence techniques such as ELINT onto a target.

URINT: A phrase used by Intelligence analysts to describe a *feeling in the water* and is based on the experience and training of the analyst. It is often associated with the final type of intelligence, HINTELL.

HINTELL: Deductions drawn from hints and the opinion of the analyst, rather than evidence gathered from all available sources. It must be treated with caution and the weight given to it can depend upon the reputation and experience of the analyst.

Appendix 2 Endnotes

[1] NATO, 2012. AAP-06. 2012 Version 2 ed. Brussels, Belgium: NATO.

Bibliography

4g.co.uk, 2015. *How fast is 4G.* [Online] Available at: http://www.4g.co.uk/how-fast-is-4g/ [Accessed 24 February 2016].

Abovetopsecret.com, 2015. *The New Spearhead Spy Ship Marjata IV; Norway Navy Intelligence.* [Online] Available at: http://www.abovetopsecret.com/forum/thread1074090/pg1.

Abrams, M. & Weiss, J., 2008. Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia. [Online] Available at: http://csrc.nist.gov/groups/SMA/fisma/ics/ documents/Maroochy-Water-Services-Case-Study_report.pdf. [Accessed 23 August 2016].

Adams, J., 2001. Virtual Defence. Foreign Affairs, 80(3).

Addley, E. & Halliday, J., 2010. Operation Payback cripples MasterCard site in revenge for WikiLeaks ban. [Online]
Available at: https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks. [Accessed 29 August 2016].

Alexander, M. & Childress, M., 1981. The Zimmermann Telegram. [Online] Available at: http://www.archives.gov/education/lessons/zimmermann/. [Accessed 23 August 2016].

Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is coming. Comparative Strategy, 12(2), pp. 141-165.

Arquilla, J., 2012.*Cyberwar Is Already Upon US.* [Online] Available at: http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ [Accessed 07 Dec 2016].

Balandin, A. A., 2009. Chill Out. IEEE Spectrum, 1 October, pp. 34-39.

Balduzzi, M., Wilhoit, K. & Pasta, A., 2014. A Security Evaluation of AIS, Texas, USA: Trend Micro.

Ballantyne, I., 2014. Brothers in Treachery. [Online] Available at: http://iainballantyne.com/brothers-in-treachery/. [Accessed 14 August 2016].

Barwinski, M. A., 2005. Taxonomy Of Spyware And Empirical Study Of Network Drive-by downloads. 1st ed. Monterey, CA: Naval Postgraduate School.

Bastardi, A., Uhlmann, E. L. & Ross, L., 2011. Wishful Thinking: Belief, Desire, and the Motivated Evaluation of Scientific Evidence. Psychological Science, 22(6), pp. 731-732.

BBC News Norfolk, 2012. Norwich City FC apologises over handling of kit internet posting. [Online] Available at: http://www.bbc.co.uk/news/uk-england-norfolk-17780084. [Accessed 14 August 2016].

BBC News, 2015. Argentina judge orders asset seizure of Falklands oil firms. [Online] Available at: http://www.bbc.co.uk/news/world-latin-america-33301540. [Accessed 11 Apr 2016].

BBC News, 2015. On board the world's biggest ship. [Online] Available at: http://www.bbc.co.uk/news/magazine-31813045. [Accessed 12 Apr 2016].

BBC News, 2015. Q&A: South China Sea dispute. [Online] Available at: http://www.bbc.co.uk/news/world-asia-pacific-13748349. [Accessed 11 Apr 2016].

BBC News, 2016. North Korea 'jamming GPS signals' near South border. [Online] Available at: http://www.bbc.co.uk/news/world-asia-35940542 [Accessed 23 August 2016].
Beebom, 2015. What is GLONASS And How It Is Different From GPS. [Online] Available at: http://beebom.com/2015/05/what-is-glonass-and-how-it-is-different-from-gps. [Accessed 12 Apr 2016].

Bell, I., 2015. Essay of the week: a brief history of the political smear. [Online] Available at: http://www.heraldscotland.com/opinion/13209481.Essay_of_the_week__a_brief_history_of_the_political_smear/. [Accessed 29 August 2016].

Betz, J. D. & Stevens, T., 2011. Power and cyberspace. In: D. J. Betz & T. Stevens, eds. Cyberspace and the state. London: Routledge, p. 36.

BI Science, 2015. Animated map shows the undersea cables that power the internet. [Online] Available at: https://www.youtube.com/watch?v=IlAJJI-qG2k. [Accessed 14 August 2016].

BillieBox, 2016. Facts about Shipping containers. [Online] Available at: https://www.billiebox.co.uk/facts-about-shipping-containers/. [Accessed 12 Apr 2016].

Billings, L., 2015. War in Space May Be Closer Than Ever. [Online] Available at: http://www.scientificamerican.com/article/war-in-space-may-be-closer-than-ever/. [Accessed 15 May 2016].

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, 2016. The Guidelines for Cyber Security Onboard Ships, Bagsvaerd: BIMCO.

Blum, A., 2012. Tubes - Behind the scenes at the Internet. 1st ed. London: Penguin.

Bodeau, D. & Graubart, R., 2013. Characterizing Effects on the Cyber Adversary, Bedford, MA: MITRE.

Bond, M. S., 2007. *Hybrid War: A new paradigm for stability operations in failing states.* US Army War College, Pennsylvania.

Bright. P., 2011. Anonymous speaks: the inside story of the HBGary hack. [Online]
Available at: http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/. [Accessed 31 December 2014].

British Library, 2016. Chartism (Summary). [Online] Available at: http://www.bl.uk/learning/histcitizen/21cc/struggle/chartists1/summary/chartism.html. [Accessed 29 August 2016].

Broadside, 2012. www.nelsonsnavy.co.uk. [Online] Available at: http://www.nelsonsnavy.co.uk/traf-signals.html. [Accessed 26 October 2015].

Bronk. C., 2013. The Cyber Attack on Saudi Aramco. Survival: Global Politics and Strategy. Vol. 55. Ed. 2. pp. 81-96. [Online] Available at: http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272. [Accessed 1 January 2015].

Browning, P., 2014. Spoofing AIS - The Debate Continues. [Online] Available at: http://blog.exactearth.com/blog/bid/339822/Spoofing-AIS-The-Debate-Continues. [Accessed 26 August 2016].

Business Insider Science, 2015. Animated map shows the undersea cables that power the internet. [Online] Available at: https://www.youtube.com/watch?v=IlAJJI-qG2k. [Accessed 12 Apr 2016].

Cadwalladr. C., 2012. Anonymous: behind the masks of the cyber insurgents. [Online] Available at: http://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents. [Accessed 5 January 2015].

Cambridge International Examinations, 2016. Programmes and Qualifications. [Online] Available at: http://www.cie.org.uk/ [Accessed 13 July 2016].

Carr, M., 2016. US Power and the Internet in International Relations. Basingstoke, UK: Palgrave MacMillan.

Cavelty, M. D., 2008. Cyber-Security and Threat Politics. 1st ed. Oxford: Routledge.

CCDCOE, 2013 *Cyber Definitions.* [Online] Available at: https://ccdcoe.org/cyber-definitions.html. [Accessed 20 June 2017].

Center for Strategic and International Studies, 2016. Delivering on the Future of Submarine Warfare. [Online]. Available at: https://www.youtube.com/watch?v=yfrrYcphFBo. [Accessed 23 August 2016].

CESG, 2016. Mitigating Denial of Service (DOS) Attacks. [Online]. Available at: https:// www.cesg.gov.uk /guidance/mitigating-denial-service-dos-attacks. [Accessed 23 August 2016].

Cha, M., Haddadi, H., Benevenuto, F. & Gummadi, 2010. Measuring User Influence in Twitter: The Million Follower Fallacy. Washington, D.C., The AAAI Press, Menlo Park, California.

Charap, S., 2015. The Ghost of Hybrid War. Survival - Global Politics and Strategy, 23 Nov.

Chauvin, J., 2013. [Review Essay] Rid, Thomas. Cyber War Will Not Take Place. London: Hurst & Company, 2013.. [Online] Available at: https://www.academia.edu/7493468/_Review_Essay_Rid_Thomas._Cyber_War_Will_Not_Take_Place._London_Hurst_and_Company_2013 [Accessed 7 May 2016].

Chong, A., 2010. Small state soft power strategies: virtual enlargement in the cases of the Vatican City State and Singapore. Cambridge Review of International Affairs, 23(3), pp. 282-405.

Clark, D. D. & Landau, S., 2010. Untangling Attribution. In: Proceedings of a Workshop on deterring cyberattacks. Washington, DC: The National Academies Press, pp. 25-41.

Clarke, R. A. & Knake, R. K., 2010. Cyber War. 1st ed. New York, NY: Harper Collins.

Clements, K., 2016. How Alan Turing Cracked The Enigma Code. [Online] Available at: http://www.iwm.org.uk /history/how-alan-turing-cracked-the-enigma-code. [Accessed 14 August 2016].

Cole, S., 2015. Securing military GPS from spoofing and jamming vulnerabilities. [Online] Available at: http://mil-embedded.com/articles/securing-military-gps-spoofing-jamming-vulnerabilities/. [Accessed 23 August 2016].

Committee for Accuracy in Middle East Reporting in America, 2007. USS Liberty. [Online] Available at: http://www.sixdaywar.org/uss-liberty.asp. [Accessed 14 August 2016].

Computernetworkingsimplified.com, 2016. Relationship between Bandwidth, Data Rate and Channel Capacity. [Online] Available at:

http://computernetworkingsimplified.com/physical-layer/relationship-bandwidth-data-rate-channel-capacity/ [Accessed 12 Apr 2016].

Copeland, J., 2012. Alan Turing: The codebreaker who saved 'millions of lives. [Online] Available at: http://www.bbc.co.uk/news/technology-18419691. [Accessed 14 August 2016].

Coventry University, 2017. *Maritime Security MA.* [Online] Available at: http://www.coventry.ac.uk/course-structure/arts-and-humanities/postgraduate/maritime-security-ma/. [Accessed 3 June 2017].

Crowdy, T., 2016. SOE: Churchill's Secret Agents. 1st ed. Oxford: Bloomsbury.

Cryptome.org, 1986. Soviet Okean class intelligence collection ship LINZA underway. [Online] Available at: http://cryptome.org/eyeball/ssv/ccb-linza.htm [Accessed 14 August 2016].
CrySyS. 2011. Duqu: A Stuxnet-like malware found in the wild. [Online] Available at:http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf. [Accessed 1 January 2015].

Czuperski, M. et al., 2015. Hiding in Plain Sight. Putin's War in Ukraine. [Online] Available at: http://www.atlanticcouncil.org/images/publications/Hiding_in_Plain_Sight/HPS_English.pdf. [Accessed 14 August 2016].

Dahl, R., 1957. The concept of power. Behavioral Science, 2(3), pp. 201-215.

Dataquest, 2012. Cyberspace as Global Commons: The Challenges. [Online] Available at: http://www.dqindia.com/cyberspace-global-commons-the-challenges-1/. [Accessed 12 Apr 2016].

Defence and Security Systems International, 2013. In it together: a collaborative approach to warfare logistics. [Online] Available at: http://www.defence-and-security.com/features/featurein-it-together-a-collaborative-approach-to-warfare-logistics/. [Accessed 26 August 2016].

defenceforumindia.com, 2010. China's Yuan Wang class tracking ships. [Online] Available at: http://defenceforumindia.com/forum/threads/chinas-yuan-wang-class-tracking-ships.14326/. [Accessed 14 August 2016].

Deibert, R., Palfrey, J., Rohozinski, R. & Zittrain, J., 2008. Access Denied - The Practice and Policy of Global Internet Filtering. 1st ed. Cambridge, Massachusetts: MIT Press.

DeNardis, L., 2014. The Global War for Internet Governance. 1st ed. New Haven: Yale University Press.

Department of Defense, Joint Chiefs of Staff, 2014. Joint Publication 3-13 - Information Operations, Washington, DC: Department of Defense.

Department of the Army, 2014. Field Manual 3-38 Cyber Electromagnetic Activities, Washington DC: Department of the Army.

Development, Concepts and Doctrine Centre, 2007. Future Maritime Operating Concept. 1st ed. London: Ministry of Defence.

Development Concepts and Doctrine Centre, 2007. Joint Doctrine Note 2/07 "Countering Irregular Activity within a Comprehensive Approach". 1st ed. London: Ministry of Defence.

Development, Concepts and Doctrine Centre, 2010. Future Character of Conflict, London: Ministry of Defence.

Development, Concepts and Doctrine Centre, 2010. Joint Doctrine Publication 04 - Understanding. 1st ed. London: Ministry of Defence.

The Development, Concepts and Doctrine Centre , 2011. United Kingdom Supplement to the NATO Terminology Database. 8th ed. London: Ministry of Defence.

Development, Concepts and Doctrine Centre, 2013. Cyber Primer. 1st ed. London: Ministry of Defence.

Development, Concepts and Doctrine Centre, 2016. Cyber Primer. 2nd ed. London: Ministry of Defence.

Development, Concepts and Doctrine Centre, 2014. Joint Doctrine Publication 0-01 UK Defence Doctrine. 5th ed. London: Ministry of Defence.

Dewar, R. S., 2014. The "Triptych of Cyber Security": A Classification of Active Cyber Defence. Tallinn, NATO CCD COE.

Dickens, J., 2016. ICT teachers struggling with transition to computing. [Online] Available at: http://schoolsweek.co.uk/teachers-lack-confidence-in-computing-science/. [Accessed 13 July 2016].

DigitalWatch Observatory, 2017. UN GGE [Online] Available at: https://dig.watch/processes/ungge [Accessed 20 June 2017].

Economist Intelligence Unit, 2011. Cyber Power Index. [Online]. Available at: https://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf. [Accessed 03 Mar 2016].

Edge-Security, 2016. The Harvester The Information Gathering Suite. [Online] Available at: http://www.edge-security.com/theharvester.php. [Accessed 14 August 2016].

Electronic Frontier Foundation, 2016. Net Neutrality. [Online] Available at: https://www.eff.org/issues/net-neutrality [Accessed 13 July 2016].

Encyclopaedia Britannica, 2016. Transmission media and the problem of signal degradation. [Online] Available at: http://www.britannica.com/topic/telecommunications-media. [Accessed 12 Apr 2016].

Engineering and Physical Sciences Research Council, 2011. Scheme to Recognise Academic Centres of Excellence in Cyber Security Research. [Online] Available at: https://www.epsrc.ac.uk/files/funding/calls/2011/scheme-to-recognise-academic-centres-of-excellence-in-cyber-security-research/. [Accessed 12 April 2016].

European Commission, 2013. Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace. [Online] Available at: http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace. [Accessed 6 Nov 2015].

European Space Agency, 2016. Galileo navigation. [Online] Available at: http://www.esa.int/Our_Activities/Navigation/The_future_-_Galileo/What_is_Galileo [Accessed 12 Apr 2016].

European Union Agency for Network and Information Security, 2013. National Cyber Security Strategies in the World. [Online] Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world. [Accessed 6 Nov 2015].

EyeWitness to History, 2007. The Doolittle Raid, 1942. [Online] Available at: http://www.eyewitnesstohistory.com/doolittle.htm. [Accessed 23 August 2016].

Fallon, M., 2017. *Defence Secretary's speech at Cyber 2017 Chatham House Conference* [Online] Available at: https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference. [Accessed 12 July 2017].

Federal Bureau of Investigation, 2015. Update on Sony Investigation. [Online] Available at: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation [Accessed 8 May 2016].

Fitton, O., Prince, D., Germond, B. & Lacy, M., 2015. The Future of Maritime Cyber Security, Lancaster: Lancaster University.

Freed. A., 2014. Norse investigation focussing on a small group, including Sony ex-employees. [Online] Available at: http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/. [Accessed 2 January 2015].

Freedberg, S. J., 2015. Cyber Subs: A Decisive Edge For High-Tech War?. [Online] Available at: http://breakingdefense.com/2015/03/cyber-subs-a-decisive-edge-for-high-tech-war/. [Accessed 15 August 2016].

Friedman, H., 2016. Sex and Psychological Operations. [Online] Available at: http://www.psywarrior.com/sexandprop.html. [Accessed 29 August 2016].

Fung, B. & Peterson, A., 2016. America uses stealthy submarines to hack other countries; systems. [Online] Available at: https://www.washingtonpost.com/news/the-switch/wp/2016/07/29/america-is-hacking-other-countries-with-stealthy-submarines/. [Accessed 23 August 2916].

Gady, F.-S., 2015. 'Little Blue Men:' Doing China's Dirty Work in the South China Sea. [Online] Available at: www.thediplomat.com [Accessed 2 May 2016].

Gallagher, R., 2013. *Meet the machines that steal your phone's data.* [Online] Available at: http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ [Accessed 24 February 2016].

Gartzke, E., 2013. The Myth of Cyberwar. International Security, 38(2), p. 49.

Gassen, J., Gerhards-Padilla, E. & Martini, P., 2012. Current Botnet-Techniques and Countermeasures. Praxis der Informationsverarbeitung und Kommunikation, 35(1), pp. 3-10.

Gertz, B., 2015. Russian Spy Ship Makes Port Call in Caribbean. [Online] Available at: http://freebeacon.com/national-security/russian-spy-ship-makes-port-call-in-caribbean/. [Accessed 14 August 2016].

Ghernaouti, S., 2013. Cyberpower. 1st ed. Lausanne: CRC Press.

Gibson, M., 2016. Britain cuts German Cable Communications 5 August 1914. [Online] Available at: https://warandsecurity.com/2014/08/05/britain-cuts-german-cable-communications-5-august-1914/. [Accessed 23 August 2016].

Gibson, W., 1994. Neuromancer. 1st ed. London: Harper Collins.

Global Firepower, 2015. Oil Consumption data. [Online] Available at: http://www.globalfirepower.com/oil-consumption-by-country.asp. [Accessed 11 Apr 2016].

Global Stats, 2016. Top 7 Desktop, Tablet & Console OSs from May 2015 to May 2016. [Online] Available at: http://gs.statcounter.com/#os-ww-monthly-201505-201605. [Accessed 13 July 2016].

Gomez, M. A., 2013. Identifying Cyber Strategies vis-a-vis Cyber Power. Palo Alto, CA, World Cyberspace Cooperation Summit IV (WCC4), 2013.

Google, 2015. Google Analytics. [Online] Available at: http://www.google.com/analytics/. [Accessed 5 Nov 2015].

Google.com, 2016. Google fibre. [Online] Available at: https://fiber.google.com/about/. [Accessed 13 July 2016].

GPS.gov, 2014. What is GPS? [Online]. Available at: http://www.gps.gov/systems/gps/ [Accessed 12 Apr 2016].

GPS.gov, 2015. Control Segment. [Online] Available at: http://www.gps.gov/systems/gps/control/ [Accessed 12 Apr 2016].

GPS.gov, 2016. Space Segment. [Online] Available at: http://www.gps.gov/systems/gps/space/ [Accessed 12 Apr 2016].

Greenwald, A., 2010. The Soft-Power Fallacy. Commentary, July/August, pp. 75-80.

Gray, C. S., 2005. Another Bloody Century. 1st ed. London: Orion.

Hachigian, N., 2001-133. China's cyber-strategy. Foreign Affairs, 80(2), p. 118.

Hallams, E., 2011. From Crusader to Exemplar: Bush,Obama and the Reinvigoration of America's Soft Power. European journal of American studies, Volume 1, pp. 1-21.

Hall, I. & Smith, F., 2013. The Struggle for Soft Power in Asia: Public Diplomacy and Regional Competition. Asian Security, 9(1), pp. 1-18.

Hansen, L., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, Volume 53, p. 1159.

Hare, F., 2010. The cyber threat to national security: why can't we agree?. Tallinn, Estonia, NATO Cooperative Cyber Defence Centre of Excellence.

HM Government, 2010. The National Security Strategy. 1st ed. London: Her Majesty's Stationery Office .

HM Government, 2014. Mapping UK shipping density and routes from AIS (MMO 1066). [Online] Available at: https://www.gov.uk/government/publications/mapping-uk-shipping-density-and-routes-from-ais-mmo-1066 [Accessed 12 Apr 2016].

HM Government, 2014. The UK National Strategy for Maritime Security. [Online] Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/310323/National_Strategy_for_Maritime_Security_2014.pdf [Accessed 23 August 2016].

HM Government, 2014. UK National Strategy for Maritime Security, London: Her Majesty's Stationery Office.

HM Government, 2015. National Security Strategy and Strategic Defence and Security Review, London: Her Majesty's Stationery Office.

Hoffman, F. G., 2007. Conflict in the 21st Century: The Rise in Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies.

House of Lords Select Committee on Soft Power and the UK's Influence, 2014. Persuasion and power in the modern world, London, UK: The House of Lords.

http://cryptome.org, 1986. Soviet Okean class intelligence collection ship LINZA underway. [Online] Available at: http://cryptome.org/eyeball/ssv/ccb-linza.htm [Accessed 14 August 2016].

Idarat Maritime, 2009. New Tactics and Equipment in the Somali Pirates' Campaign. [Online] Available at: http://www.idaratmaritime.com/wordpress/?p=156 [Accessed 14 August 2016].

Inkster, N., 2010. China in Cyberspace. Survival: Global Politics and Strategy, 52(4), pp. 55-66.

Inmarsat, 2016. Fleet Broadband. [Online] Available at: http://www.inmarsat.com/service-collection/fleetbroadband/ [Accessed 12 Apr 2013].

International Chamber of Shipping, 2015. Shipping and World Trade. [Online] Available at: http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade
[Accessed 11 Apr 2016].

International Maritime Organisation, 2016. AIS Transponders. [Online] Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx. [Accessed 12 Apr 2016].

International Seabed Authority, 2014. International Seabed Authority. [Online] Available at: https://www.isa.org.jm/. [Accessed 12 Apr 2016].

Internet Live Stats, 2014. Internet Users by Country. [Online] Available at: http://www.internetlivestats.com/internet-users-by-country/. [Accessed 31 Oct 2015].

Irshaid. F., 2014. How ISIS is spreading its message online. BBC Monitoring. [Online] Available at: http://www.bbc.co.uk/news/world-middle-east-27912569. [Accessed 1 January 2015].

Isode, 2016. Why IP over HF Radio should be Avoided. [Online] Available at: http://www.isode.com/whitepapers/ip-over-stanag-5066.html. [Accessed 12 Apr 2016].

Jegatheesan, S., 2013. Cookies – Invading Our Privacy for Marketing, Advertising and Security Issues. International Journal of Scientific & Engineering Research, 4(5), pp. 926-928.

Joint Operations. 2017. *Joint Publication 3-0*. P. V-14 [Online]. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf [Accessed 16 Jul 2017].

Jones, K. D., Tam, K. & Papadaki, M., 2016. Threats and Impacts in Maritime Cyber Security, London: Institution of Engineering and Technology.

Kakavas, Y., 2016. Creepy. [Online] Available at: http://www.geocreepy.com/. [Accessed 14 August 2016].

Kent, M. L., Carr, B. J., Husted, R. A. & Pop, R. A., 2011. Learning web analytics: A tool for strategic communication. Public Relations Review, Volume 37, pp. 536-543.

Kliarsky, A., 2010. Covert Channels, Swansea, UK: SANS Instiute InfoSec Reading Room.

Klimburg, A., 2011. Mobilising Cyber Power. Survival: Global Politics and Strategy, 53(1), pp. 41-60.

Knight, J., 2016. Ships Designed for Intelligence Collection. [Online] Available at: http://www.faqs.org/espionage/Se-Sp/Ships-Designed-for-Intelligence-Collection.html. [Accessed 14 August 2016].

Kozlowski, A., 2014. Comparative Analysis of the Cyberattacks on Estonia, Georgia and Kyrgyzstan. European Scientific Journal February 2014 /SPECIAL/ edition vol.3. pp.242.

Kramer, F. D., 2009. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In: F. D. Kramer, S. H. Starr & L. K. Wentz, eds. Cyberpower and National Security. Dulles, Washington: Potomac, p. 4.

Kramer, F. D. & Wentz, L. K., 2009. Cyber Influence and International Security. In: 1st, ed. Cyberpower and National Security. Dulles: Potomac, pp. 343-362.

Kroenig, M., McAdam, M. & Weber, S., 2010. Taking Soft Power Seriously. Comparative Strategy, 29(5), p. 412.

Kruger, B., 2000. *Distance of the horizon.* [Online] Available at: http://www.cactus2000.de/uk/unit/ masshor.shtml [Accessed 23 February 2016].

Kuehl, D., 2009. Cyberspace to Cyberpower: Defining the Problem. In: F. D. Kramer, S. H. Starr & L. K. Wentz, eds. Cyberpower and National Security. 1st ed. Dulles (Virginia): Potomac, pp. 24-42.

Land, M., 2017 *The UK's plan to deny terrorist 'safe spaces' online would make us all less safe in the long run.* [Online] Available at: http://theconversation.com/the-uks-plan-to-deny-terrorists-safe-spaces-online-would-make-us-all-less-safe-in-the-long-run-79323 [Accessed 17 Jun 2015].

LeakSource, 2014. Destroy, Deny, Degrade, Disrupt, Deceive: GCHQ "Effects" Operations Revealed. [Online] Available at: https://leaksource.info/2014/02/07/destroy-deny-degrade-disrupt-deceive-gchq-effects-operations-revealed/. [Accessed 23 August 2016].

Leppard, D., 2012. Chinese steal jet secrets from BAE. [Online] Available at: http://www.thesundaytimes.co.uk/sto/news/uk_news/National/article991581.ece. [Accessed 14 August 2016].

Libicki, M. C., 2009. Cyberdeterrence and Cyberwar, Santa Monica, CA: RAND Corporation.

Lillian Goldman Law Library, 2008. Laws of War: Rights and Duties of Neutral Powers in Naval War (Hague XIII); October 18, 1907. [Online] Available at: http://avalon.law.yale.edu/20th_century/hague13.asp. [Accessed 12 Apr 2016].

Lin, H., 2016. *NATO's Designation of Cyber as an Operational Domain of Conflict.* [Online] Available at: https://www.lawfareblog.com/natos-designation-cyber-operational-domain-conflict [Accessed 19 June 2017].

Lister, C., 2014. Profiling the Islamic State. [Online] Available at: http://www.brookings.edu/research/reports2/2014/12/profiling-islamic-state-lister. [Accessed 5 Nov 2015].

[1]Livezey, W. E., 1985 *Mahan on Sea Power*. 1st ed. Oklahoma: University of Oklahoma Press.

LLoyds, 2016. About Lloyds. [Online] Available at: http://www.lloyds.com/lloyds. [Accessed 11 Apr 2016].

Lyon, B., 2014. What is Opte about?. [Online] Available at: http://www.opte.org/about/. [Accessed 13 July 2016].

MacAskill, E., Borger, J., Hopkins, N. & Ball, J., 2013. GCHQ taps fibre-optic cables for secret access to world's communications. [Online] Available at: https://www.theguardian.com/uk/2013/jun /21/gchq-cables-secret-world-communications-nsa. [Accessed 14 August 2016].

Maidment, J., 2017. *Theresa May calls on internet companies to eradicate 'safe spaces' for extremism in wake of London Bridge terror attack.* [Online] Available at: http://www.telegraph.co.uk/news/2017/06/04/theresa-may-calls-internet-companies-eradicate-safe-spaces-extremism/ [Accessed 17 Jun 2015].

Mandiant, 2013. APT1: Exposing One of China's Cyber Espionage Units, Milpitas, CA: Mandiant.

Marine Insight, 2011. The TI Class Super Tankers: The Fantastic Four. [Online] Available at: http://www.marineinsight.com/types-of-ships/the-ti-class-super-tankers-the-fantastic-four/. [Accessed 12 Apr 2016].

Marine Source, 2016. Satellite AIS Data. [Online] Available at: http://www.marinetraffic.com/en/p/satellite-ais. [Accessed 12 Apr 2016].

Maritime and Coastguard Agency, 2014. Dover Strait crossings: channel navigation information service (CNIS). [Online] Available at: https://www.gov.uk/government/publications/dover-strait-crossings-channel-navigation-information-service/dover-strait-crossings-channel-navigation-information-service-cnis#how-cnis-works. [Accessed 12 Apr 2016].

Maritime Connector, 2017. *Panamax and New Panamax.* [Online] Available at: http://maritime-connector.com/wiki/panamax/. [Accessed 2 June 2016].

Markgraf, B., 2016. How Far Can a Cell Tower Be for a Cellphone to Pick Up the Signal?. [Online] Available at: http://smallbusiness.chron.com/far-can-cell-tower-cellphone-pick-up-signal-32124.html. [Accessed 14 August 2016].

McDowell, D., 2013. Understanding Denial-of-Service Attacks. https://www.us-cert.gov/ncas/tips/ST04-015. Accessed 5 January 2015.

McDowell, G., 2014. Types Of Internet Access Technologies Explained, And What You Should Expect. [Online]
Available at: http://www.makeuseof.com/tag/types-of-internet-access-technologies-explained-and-what-you-should-expect/. [Accessed 16 Mar 2016].

Miller, G., 2015. Undersea Internet Cables Are Surprisingly Vulnerable. [Online] Available at: http://www.wired.com/2015/10/undersea-cable-maps/. [Accessed 23 August 2016].

Mills, R., 2014. Russian soldier's 'selfies' show he was inside Ukraine. [Online] Available at: http://www.krmg.com/news/news/local/russian-soldiers-selfies-show-he-was-inside-ukrain/ngtTF/. [Accessed 14 August 2016].

Ministry of Defence, 2008. JDP 6-00 3rd Edition: Communications and Information Systems Support to Joint Operations. [Online] Available at: https://www.gov.uk/government/publications/jdp-6-00-3rd-edition-communications-and-information-systems-support-to-joint-operations. [Accessed 26 10 2015].

Ministry of Defence, 2011. British Maritime Doctrine. 1st ed. London: Development, Concepts and Doctrine Centre.

Ministry of Defence, 2011. Joint Doctrine Publication 2-00 Understanding and Intelligence Support to Joint Operations Third Edition. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf. [Accessed 14 August 2016].

Ministry of Defence, 2011. Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations. 3rd Change 1 ed. Shrivenham, UK: Development, Concepts and Doctrine Centre.

Ministry of Defence, 2013. Defence Information and Communications Technology Strategy. 1st ed. London: Ministry of Defence.

Ministry of Defence, 2013. Joint Doctrine Note 2/13 Information Superiority. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/239342/20130813_JDN_2_13_Info_Super.pdf. [Accessed 12 Apr 2016].

Ministry of Defence, 2014. Allied Joint Doctrine for Psychological Operations - Allied Joint Publication 3.10.1. Edition B Version 1 with UK National Elements ed. Brussels: NATO.

Monagham, A., 2016. *The 'War' in Russia's 'Hybrid warfare'.* [Online] Available at: http://www.strategicstudiesinstitute.army.mil/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf [Accessed 13 Jan 17].

Morris, N., 2011. The Special Operations Executive 1940 - 1946. [Online] Available at: http://www.bbc.co.uk/history/worldwars/wwtwo/soe_01.shtml. [Accessed 23 August 2016].

Mudrinich, E. M., 2012. Cyber 3.0: The Department of Defense Stratrgy for Operating in Cyberspace and the Attribution Problem. Air Force Law Review, Volume 68, pp. 167-206.

Muravska, J., 2013. Book Review: Cyber War Will Not Take Place. [Online] Available at: http://blogs.lse.ac.uk/politicsandpolicy/book-review-cyber-war-will-not-take-place/ [Accessed 07 May 2016].

Naked Security, 2017. *WannaCry: the ransomware worm that didn't arrive on a phishing hook.* [Online] Available at: https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/ [Accessed 13 June 2017].

NATO Cooperative Cyber Defence Centre of Excellence, 2012. National Cyber Security Framework Manual. [Online] Available at: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. [Accessed 6 Nov 2015].

NATO Cooperative Cyber Defence Centre of Excellence, 2013. Tallinn manual on the international law applicable to cyber warfare. 1st ed. Cambridge, UK: Cambridge University Press.

NATO Cooperative Cyber Defence Centre of Excellence, 2015. Cyber Definitions. [Online]
Available at: https://ccdcoe.org/cyber-definitions.html. [Accessed 22 October 2015].

NATO Parliamentary Assembly, 2009. 173 DSCFC 09 E bis - NATO and Cyber Defence. [Online] Available at: http://www.nato-pa.int/default.asp?SHORTCUT=1782. [Accessed 5 Nov 2015].

NATO, 2012. AAP-06. 2012 Version 2 ed. Brussels, Belgium: NATO.

NATO, 2014. Allied Joint Doctrine for Air Maritime Coordination AJP-3.3.3. 1st ed. Brussels: NATO.

NATO, 2015. AJP-3-10 Allied Joint Doctrine for Information Operations. Edition A Version 1 ed. Brussels, Belgium: NATO.

NATO, 2015. Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar. [Online] Available at: http://www.nato.int/cps/en/natohq/opinions_118435.htm [Accessed 3 May 2016].

Naval Air Warfare Center Weapons Division, 2013. Electronic Warfare and Radar Systems. [Online] Available at: http://www.navair.navy.mil/nawcwd/ewssa/downloads/NAWCWD%20TP%208347.pdf. [Accessed 23 August 2016].

Naval-technology.com, 2015. Kockums A26 Submarine, Sweden. [Online] Available at: http://www.naval-technology.com/projects/kockums-a26-submarine/. [Accessed 15 August 2016].

Military-today.com, 2016. Monge Missile range instrumentation ship. [Online] Available at: http://www.military-today.com/navy/monge_ship.htm.

Neal, R., 2014. Underwater Internet Cables: 'Submarine Cable Map' Shows How The World Gets Online. [Online] Available at: http://www.ibtimes.com/underwater-internet-cables-submarine-cable-map-shows-how-world-gets-online-1559604. [Accessed 23 August 2016].

Network, M. A., 1999. CBU-94 "Blackout Bomb" BLU-114/B "Soft-Bomb". [Online]
Available at: http://fas.org/man/dod-101/sys/dumb/blu-114.htm [Accessed 13 July 2016].

News, B., 2016. North Korea 'jamming GPS signals' near South border. [Online] Available at: http://www.bbc.co.uk/news/world-asia-35940542. [Accessed 23 August 2016].

Nichol, M., 2017. *Big Lizzie's location is top secret, says MoD (But anyone – including Mr Putin – can track her on this FREE smartphone app!).* [Online} Available at: http://www.dailymail.co.uk/news/article-4658082/Free-app-showing-location-HMS-Queen-Elizabeth.html . [Accessed 16 Jul 2017].

Nuclear Threat Initiative, 2015. Iran Submarine Capabilities. [Online] Available at: http://www.nti.org/analysis/articles/iran-submarine-capabilities/. [Accessed 11 Apr 2016].

NWO Report, 2015. Confirmation that China stole F35, F22 and B2 stealth bomber secrets as early as 2007. [Online] Available at: https://nworeport.me/2015/01/29/confirmation-that-china-stole-f35-f22-and-b2-stealth-bomber-secrets-as-early-as-2007/. [Accessed 14 August 2016].

Nye, J. S., 1990. Bound To Lead: The Changing Nature Of American Power. 1st ed. New York, NY: Basic Books.

Nye, J. S., 2004. Power in the Global Information Age. 1st ed. New York, NY: Routledge.

Nye, J.S., 2004. Soft Power. 1st ed. New York, NY: Public Affairs.

Nye, J. S., 2008. Public diplomacy and soft power. The Annuals of the American Academy of Political and Social Science, 616(1), pp. 94-109.

Nye, J. S., 2009. Obama's Smart Power. Non-profit quarterly, Volume Spring, pp. 7-9.

Nye, J. S., 2010. Cyberpower. [Online] Available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. [Accessed 19 10 2015].

Nye, J. S., 2011. The Future of Power. 1st ed. New York: Public Affairs.

Nye, J. S., 2014. The Information Revolution and Soft Power. Current History, 113(759), pp. 19-22.

OccupyTheWeb, 2016. How to Find Vulnerable Webcams Across the Globe Using Shodan. [Online] Available at: http://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-webcams-across-globe-using-shodan-0154830/. [Accessed 14 August 2016].

OccupytheWeb, 2016. SCADA Hacking: Finding SCADA Systems using Shodan. [Online] Available at: http://www.hackers-arise.com/#!SCADA-Hacking-Finding-SCADA-Systems-using-Shodan/c112t/577152d10cf2e26a9983f701. [Accessed 14 August 2016].

Open Net Initiative, 2014. Open Net Initiative. [Online] Available at: https://opennet.net/. [Accessed 31 Oct 2015].

Other Worlds, 2016. Defending the Global Commons. [Online] Available at: http://www.otherworldsarepossible.org/defending-global-commons. [Accessed 12 Apr 2016].

Oxford English Dictionary, 2016. Oxford English Dictionary. [Online] Available at: http://www.oed.com/. [Accessed 12 Apr 2016].

Oxford Reference, 2016. http://www.oxfordreference.com/. [Online] Available at: http://www.oxfordreference.com/. [Accessed 29 August 2016].

Oxford University Press, 1981. The Oxford Library of Words and Phrases Volume 1 - The Concise Oxford Dictionary of Quotations. 2nd ed. London: Guild Publishing.

Paganini, P., 2015. Snowden’s documents reveal China stole designs for the US-built F-35 Fighter jet, and provides details also a counter-intelligence operation run by the NSA. [Online] Available at: http://securityaffairs.co/wordpress/32437/intelligence/china-stole-plans-f-35-aircraft.html. [Accessed 14 August 2016].

Palmer, D., 2013. Syrian Electronic Army hacks US Marines website. [Online] Available at: http://www.computing.co.uk/ctg/news/2292226/syrian-electronic-army-hacks-us-marines-website#. [Accessed 7 Nov 2015].

Panetta, L., 2012. US Department of Defense. [Online] Available at: http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136. [Accessed 9 May 2016].

Pew Research Centre, 2016. *Smartphone ownership and Internet usage continues to climb in emerging economies.* [Online] Available at: http://www.pewglobal.org/files/2016/02/pew_research_

center_global_technology_report_final_february_22__2016.pdf [Accessed 23 February 2016].

Pezzoni, F. et al., 2013. Why Do I Retweet It? An Information Propagation Model for Microblogs. Social Informatics, Volume 8238, pp. 360-369.

Photoblog, 2013. North Korea's Cold War prize, USS Pueblo, set to be displayed for 'Victory Day'. [Online] Available at: http://www.nbcnews.com/news/other/north-koreas-cold-war-prize-uss-pueblo-set-be-displayed-f6C10760692. [Accessed 14 August 2016].

Plymouth University, 2016. Maritime Cyber Threats research group. [Online] Available at: https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group. [Accessed 12 Apr 2016].

Port of Dover, 2016. Operations / Vessel Traffic Service. [Online] Available at: http://www.doverport.co.uk/operations/vessel-traffic-service/. [Accessed 12 Apr 2016].

Portland Group, 2015. The Soft Power 30 - A Ranking of Global Soft Power. [Online] Available at: http://softpower30.portland-communications.com/. [Accessed 11 Nov 2015].

Powers, S. M. & Jablonski, M., 2015. The Real Cyber War. 1st ed. Illinois: University of Illinois.

Price, R., 2015. We talked to people close to the TalkTalk hack before the arrests began — and they told us why they allegedly did it. [Online] Available at: http://www.businessinsider.com/talktalk-hack-vamp-c-glubz-hackers-interviews-2015-11?r=UK&IR=T [Accessed 13 July 2016].

Project Loon, 2016. Balloon-powered Internet for everyone. [Online] Available at: https://www.google.com/loon/. [Accessed 13 July 2016].

Rapid7, 2016. National Exposure Index. Inferring Internet Security Posture by Country through Port Scanning. [Online] Available at: https://information.rapid7.com/national-exposure-index.html [Accessed 13 July 2016].

Raska, M., 2015. Hybrid Warfare with Chinese Chacteristics, Singapore: S. Rajaratnam Schol of International Studies.

Rattray, G. J., 2009. An Environmental Approach to Understanding Cyberpower. In: F. D. Kramer, S. H. Starr & L. K. Wenz, eds. Cyberpower and National Security. Dulles, Virginia: Potomac, pp. 253-274.

Responses to Liberalism, 2016. Chartists (chartism). [Online] Available at: https://responsestoliberalism-period2.wikispaces.com/Chartists+(chartism). [Accessed 29 August 2016].

Reuters, 2014. Ukrainian authorities suffer new cyber attacks. [Online] Available at: http://www.reuters.com/article/2014/03/08/us-ukraine-cricis-cyberattack-idUSBREA270FU20140308. [Accessed 26 10 2015].

Richards, J., 2009. Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security, Washington, DC. USA: International Affairs Review, George Washington University.

Rid, T. & McBurney, P., 2012. Cyber-Weapons. The RUSI Journal, 157(1), pp. 6-13.

Rid, T., 2013. Cyberwar will not take place. 1st ed. London: Hurst.

Rood, P., 2015. Gulf of Aden HRA Reduced. [Online] Available at: https://www.shephardmedia.com/news/imps-news/gulf-aden-hra-reduced/ [Accessed 23 November 2016]/

Roubaix Interactive, 2011. Binary to Text (ASCII) Conversion. [Online] Available at: http://www.roubaixinteractive.com/PlayGround/Binary_Conversion/Binary_To_Text.asp. [Accessed 26 10 2015].

Rowland, J., Rice, M. & Shenoi, S., 2014. The anatomy of a cyber power. International Journal of Critical Infrastructure Protection, 7(1), pp. 3-11.

Rowland, J., Rice, M. & Shenoi, S., 2014. Whither cyberpower?. International Journal of Critical Infrastructure Protection, 7(1), pp. 124-127.

Royal Air Force, 2016. Operation Black Buck. [Online] Available at: http://www.raf.mod.uk/history/OperationBlackBuck.cfm. [Accessed 23 August 2016].

Royal Navy. 2016. *Cyber Strategy.* Portsmouth.

Royal Navy, 2016. Dhabi meeting as British and UAE minehunters train in Gulf. [Online] Available at: http://www.royalnavy.mod.uk/news-and-latest-activity/news/2016/march/10/160310-dhabi-meeting-as-british-and-uae-minehunters-train-in-gulf. [Accessed 11 Apr 2016].

Russia Today, 2012. ‘Flame’ Virus explained: How it works and who’s behind it. [Online]
Available at: https://www.rt.com/news/flame-virus-cyber-war-536/ [Accessed 13 July 2016].

Russia Today, 2015. ‘Russian spy ships’ loitering off UK coast, claims ex-Navy chief. [Online] Available at: https://www.rt.com/uk/241901-spy-ships-russia-espionage/. [Accessed 14 August 2016].

Sailcom Marine, 2016. HF shortwave SSB radio email systems. [Online] Available at: http://www.sailcom.co.uk/pactor/. [Accessed 12 Apr 2016].

Sands, G., 2016. What to Know About the Worldwide Hacker Group 'Anonymous'. [Online] Available at: http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302. [Accessed 29 August 2016].

Sanger, D. E. & Schmitt, E., 2015. Russian Ships Near Data Cables Are Too Close for U.S. Comfort. [Online] Available at: http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0. [Accessed 23 August 2016].

Sans Institute. 2011. Responding to Zero Day Threats. http://www.sans.org/reading-room/whitepapers/incident/responding-zero-day-threats-33709. Accessed: 1 January 2015.

Santamarta, R., 2014. A Wake-up Call for SATCOM Security. [Online] Available at: http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf. [Accessed 14 August 2016].

Satter, R., 2012. US general: We hacked the enemy in Afghanistan. [Online] Available at: https://www.yahoo.com/news/us-general-hacked-enemy-afghanistan-161426332.html?ref=gs. [Accessed 23 August 2016].

Schmidt, E. & Cohen, J., 2013. The New Digital Age. 1st ed. London: John Murray.

Schmitt. M. N., 2013. Tallinn Manual On The International Law Applicable to Cyber Warfare. 1st ed. Cambridge: Cambridge University Press.

Schmitt. M. N., 2017. Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations. 1st ed. Cambridge: Cambridge University Press.

Schneier, B., 2010. The Internet: Anonymous Forever. [Online] Available at: http://www.forbes.com/2010/05/12/privacy-hackers-internet-technology-security-anonymity.html. [Accessed 1 Nov 2015].

Schumacher, S., 2012. USS Pueblo (AGER-2). [Online] Available at: http://www.usspueblo.org/Welcome.html. [Accessed 14 August 2016].

Seavision, 2016. Fisheries and Aquaculture. [Online] Available at: http://www.seavision.org.uk/about/fisheries-aquaculture. [Accessed 11 April 2016].

Seavision, 2016. Seavision Home Page. [Online] Available at: http://www.seavision.org.uk/fisheries-aquaculture/home. [Accessed 11 Apr 2016].

Security Service, 2016. Espionage. [Online] Available at: https://www.mi5.gov.uk/espionage. [Accessed 14 August 2916].

Servaes, J., 2013. The many faces of (soft) power, democracy and the Internet. Telematics and Informatics, Volume 30, pp. 322-330.

Shachtman, N., 2012. 'Degrade, disrupt, deceive': US talks openly about hacking foes. [Online] Available at: https://www.wired.com/2012/08/degrade-disrupt-deceive/. [Accessed 23 August 2016].

Shaver, J., 2015. Decrypting TLS Browser Traffic With Wireshark - The Easy Way. [Online] Available at: https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/. [Accessed 23 August 2016].

Shaw, J., 2015. Defence Review: The rules of conflict have changed. The Financial Times, 24 November, p. Online.

Sheldon, J. B., 2011. Deciphering Cyberpower. Strategic Studies Quarterly, Issue Summer 2011.

Shevchenko, V., 2014. "Little green men" or "Russian invaders"?. [Online] Available at: "Little green men" or "Russian invaders"? [Accessed 3 May 2016].

ship-technology.com, 2016. Avio - Integrated Platform Management System (IPMS) for Commercial Vessels. [Online] Available at: http://www.ship-technology.com/contractors/controls/avio-propulsion1/. [Accessed 29 August 2016].

Shubber, K., 2013. A simple guide to GCHQ's internet surveillance programme

Tempora. [Online] Available at: http://www.wired.co.uk/article/gchq-tempora-101. [Accessed 14 August 2016].

Singel, R., 2008. Pakistan's accidential YouTube re-routing exposes trust flaw in net. [Online] Available at: www.wired.com/2008/02/pakistans-accid/. [Accessed 18 Dec 2015].

Singer, P. W. & Friedman, A., 2014. Cybersecurity and Cyberwar. 1st ed. Oxford: Oxford University Press.

Small Media, 2012. Satellite Jamming in Iran: A war over airwaves. [Online] Available at: https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf. [Accessed 26 August 2016].

Smith, E., 2014. ICANN Goes It Alone: What's Next for the Internet?. [Online] Available at: http://associationsnow.com/2014/03/icann-goes-it-alone-whats-next-for-the-internet/. [Accessed 26 10 2015].

Sontag, S., Drew, C. & Drew, A. L., 1998. Blind Man's Buff. 1st ed. London: Hutchinson.

Sophos, 2010. Operation Aurora. What you need to know. http://www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx. Accessed: 1 January 2015.

Special Forces Club, 2010. SOE History. [Online] Available at: http://www.sfclub.org/history.htm. [Accessed 23 August 2016].

Spiegel.de, n.d.. NIOC Maryland Advanced Computer Network Operations Course. [Online] Available at: http://www.spiegel.de/media/media-35657.pdf. [Accessed 23 August 2016].

spymuseum.org, 2016. One-time pad (Silk). [Online]
Available at: http://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/one-time-pad-silk/. [Accessed 23 August 2016].

Srinivas, S., 2012. Defeating the jamming battle. [Online] Available at: http://www.satelliteprome.com/tech-features/defeating-the-jamming-battle/. [Accessed 30 October 2016].

Starosielski, N., 2015. The Undersea Network. 1st ed. Durham and London: Duke.

Starr, S. H., 2009. Toward a Preliminary Theory of Cyberpower. In: 1st, ed. Cyberpower and National Security. Dulles, VA: Potomac, pp. 43-91.

Statista, 2016. Countries with the highest rate of malware infected computers as of 1st quarter 2016. [Online] Available at:
http://www.statista.com/statistics/266169/highest-malware-infection-rate-countries/
[Accessed 13 July 2016].

Stone, J., 2013. Cyber War Will Take Place!. Journal of Strategic Studies, 36(1).

Strassmann, P. A., 2009. The Internet's Vulnerabilities are built into its infrastructure. [Online]
Available at: http://www.afcea.org/content/?q=internets-vulnerabilities-are-built-its-infrastructure [Accessed 12 July 2016].

study.com, 2016. Wide-Area Wireless Communication: Microwave, Satellite, 3G, 4G & WiMAX. [Online] Available at:

http://study.com/academy/lesson/wide-area-wireless-communication-microwave-satellite-3g-4g-wimax.html. [Accessed 14 August 2016].

Sullivan, B., 2015. Anonymous #OPIsis Attackers Take Down ISIS Twitter Accounts. [Online] Available at: http://www.techweekeurope.co.uk/security/cyberwar/anonymous-isis-hack-161671. [Accessed 5 Nov 2015].

SunTzu, 1994. The art of war. 1st ed. Cambridge, MA: Westview.

Sutton, H.I., 2016. Russian ship loitering near undersea cables. [Online] Available at: http://www.hisutton.com/Yantar.html.

Symantec. 2011. W32 Stuxnet Dossier. [Online] Available at: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. [Accessed 1 January 2015].

Symantec. 2012. Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East. [Online]
Available at: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east. [Accessed 1 January 2015].

Symantec. 2014. Advanced Persistent Threats: How They Work. [Online] Available at: http://www.symantec.com/theme.jsp?themeid=apt-infographic-1. [Accessed 5 January 2015].

Talbot, D., 2008. How Obama Really Did It. [Online] Available at: http://www.technologyreview.com/featuredstory/410644/how-obama-really-did-it/. [Accessed 5 Nov 2015].

Talbot, D., 2014. Watching for a Crimean Cyberwar Crisis. [Online] Available at: https://www.technologyreview.com/s/525336/watching-for-a-crimean-cyberwar-crisis/. [Accessed 3 May 2016].

TeleGeography, 2016. Submarine Cable Map. [Online] Available at: http://www.submarinecablemap.com/#/. [Accessed 23 August 2016].

Tellis, A. J., Bially, J. & Layne, C., 2000. Measuring Power in the Postindustrial Age. 1st ed. Santa Monica, CA: RAND.

The Associated Press, 2005. New Nuclear Sub Is Said to Have Special Eavesdropping Ability. [Online] Available at: http://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html. [Accessed 14 August 2016].

The Baltic Exchange, 2016. The Baltic Exchange. [Online] Available at: http://www.balticexchange.com/. [Accessed 11 Apr 2016].

The Diplomat, 2014. Why China Won't Accept International Arbitration in the South China Sea. [Online] Available at: http://thediplomat.com/2014/12/why-china-wont-accept-international-arbitration-in-the-south-china-sea/. [Accessed 11 Apr 2016].

The Fiber Optic Association, 1999. How To Tap Fiber Optic Cables. [Online] Available at: http://www.thefoa.org/tech/ref/appln/tap-fiber.html. [Accessed 16 August 2016].

The Guardian, 2006. How world's biggest ship is delivering our Christmas - all the way from China. [Online] Available at: http://www.theguardian.com/uk/2006/oct/30/christmas.shopping. [Accessed 12 Apr 2016].

The National Archives, 2016. Fighting Talk: First World War telecommunications. [Online] Available at: http://www.nationalarchives.gov.uk/first-world-war/telecommunications-in-war/. [Accessed 23 August 2016].

The Telegraph, 2016. World's biggest anti-mine naval exercise after Iranian threats to close Gulf. [Online] Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10052612/Worlds-biggest-anti-mine-naval-exercise-after-Iranian-threats-to-close-Gulf.html. [Accessed 11 Apr 2016].

The University of Texas at Austin, 2013. UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. [Online] Available at: http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea. [Accessed 26 August 2016].

The White House, 2011. International Strategy for Cyberspace. [Online] Available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. [Accessed 6 Nov 2015].

Thomas, A., 2014. Brazil Laying Their Own New Internet Cables. [Online] Available at: http://www.gadgethelpline.com/brazil-laying-internet-cables/. [Accessed 23 August 2016].

Thomson, I., 2016. US military tests massive GPS jamming weapon over California. [Online] Available at: http://www.theregister.co.uk/2016/06/07/us_military_testing_gps_jamming/. [Accessed 23 August 2016].

Thuraya, 2016. Marine Comms. [Online] Available at: http://www.thuraya.com/marine-comms. [Accessed 12 Apr 2016].

Trend Micro, 2014. A Security Evaluation of AIS. [Online] Available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf. [Accessed 26 August 2016].

Treverton, G. F. & Jones, S. G., 2005. Measuring National Power. [Online] Available at: http://www.rand.org/pubs/conf_proceedings/CF215.html#download. [Accessed 19 10 2015].

Trueman, C. N., 2016. The Graf Spee in Montevideo. [Online] Available at: http://www.historylearningsite.co.uk/world-war-two/war-in-the-atlantic/the-graf-spee-in-montevideo/. [Accessed 30 August 2016].

Tsagourias, N., 2012. Cyber attacks, self-defence and the problem of attribution. Journal of Conflict and Security Laws, 17(2), pp. 229-244.

Tsikerdekis, M. & Zeadally, S., 2014. Online Deception in Social Media. [Online] Available at: http://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1013&context=slis_facpub. [Accessed 5 Nov 2015].

Twitter, 2015. *Twitter Analytics.* [Online] Available at: https://analytics.twitter.com/about [Accessed 5 Nov 2015].

UK Government, 2011. The UK Cyber Security Strategy. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. [Accessed 6 Nov 2015].

UK Government, 2013. New cyber reserve unit created. [Online] Available at: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit. [Accessed 5 Nov 2015].

UK Parliament, 2016. Chartists. [Online] Available at: http://www.parliament.uk/about/living-heritage/transformingsociety/electionsvoting/chartists/overview/chartistmovement/. [Accessed 29 August 2016].

United Nations Environment Programme, 2016. IEG of the Global Commons. [Online] Available at: http://www.unep.org/delc/GlobalCommons/tabid/54404/. [Accessed 12 Apr 2016].

United Nations, 1982. TERRITORIAL SEA AND CONTIGUOUS ZONE. [Online] Available at: http://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm. [Accessed 12 Apr 2016].

United Nations, 1982. United Nations Convention on the Law of the Sea. [Online] Available at:

http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf . [Accessed 12 Apr 2016].

United Nations, 2016. Chronological lists of ratifications of, accessions and successions to the Convention. [Online] Available at: http://www.un.org/depts/los/reference_files/chronological_lists_of_ratifications.htm. [Accessed 11 Apr 2016].

University of Greenwich, 2016. Greenwich Maritime Centre - about us. [Online] Available at: http://www.gre.ac.uk/ach/gmc/about. [Accessed 12 Apr 2016].

US Air Force, 2015. Global Positioning System. [Online] Available at: http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104610/global-positioning-system.aspx. [Accessed 12 Apr 2016].

US Army War College. 2016. Outplayed: Regaining Strategic Initiative in the Gray Zone. Carlisle barracks, PA.

US Computer Emergency Readiness Team, 2012. National Strategy to Secure Cyberspace. [Online] Available at: https://www.us-cert.gov/security-publications/national-strategy-secure-cyberspace. [Accessed 6 Nov 2015].

US Department of Defense, 2011. Department of Defence Strategy for Operating in Cyberspace. [Online] Available at: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. [Accessed 6 Nov 2015].

US Department of State, 2010. Internet Freedom in the 21st Century: Integrating New Technologies into Diplomacy and Development. [Online] Available at: http://www.state.gov/r/pa/scp/fs/2010/136702.htm. [Accessed 1 Nov 2015].

Valeriano, B. & Maness, R., 2015. Cyber War versus Cyber Realities. 1st ed. Oxford: Oxford University Press. p.15

Vandeven, S., 2013. SSL/TLS: What's Under the Hood, Swansea, UK: SANS Institute.

Venables, A., 2016. Protecting Ships - The Threat of Hackers. Port Technology, 69 Edition, pp. 30-31.

Verizon, 2016. Data break digest. [Online] Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf. [Accessed 26 August 2016].

Vessel Finder, 2016. Real-Time AIS Data. [Online] Available at: https://www.vesselfinder.com/. [Accessed 12 Apr 2016].

Von Clausewitz, C., 1832 (1980). Vom Kriege. 1st ed. Berlin: Ullstein.

Waller, J. M., 2003. Iran, Cuba zap US Satellites. [Online] Available at: http://www.wnd.com/2003/08/20157/. [Accessed 26 August 2016].

warisboring.com, 2016. The Pentagon Just Got a New Ship That Can Track Satellites … And Help Destroy Them. [Online] Available at: https://warisboring.com/the-pentagon-just-got-a-new-ship-that-can-track-satellites-and-help-destroy-them-67a1bbd70102#.ivfn3gkfb. [Accessed 14 August 2016].

Warwick, K., 2015. Kevin Warwick. [Online] Available at: http://www.kevinwarwick.com/. [Accessed 21 Dec 2015].

westpandi.com, 2011. Piracy - Revised Guidance on the use of AIS in the High Risk Area off Somalia. [Online] Available at: http://www.westpandi.com/Publications/News/Archive/Piracy---Revised-Guidance-on-the-use-of-AIS-in-the-High-Risk-Area-off-Somalia/. [Accessed 14 August 2016].

Wilkie, R., 2009. Hybrid Warfare. Air and Space Power Journal, Winter, pp. 13-17.

Wilson, E. J., 2008. Hard Power, Soft Power, Smart Power. The ANNALS of the American Academy of Political and Social Science, 616(110), pp. 110-124.

World by Map, 2015. http://world.bymap.org/Coastlines.html. [Online] Available at: http://world.bymap.org/Coastlines.html. [Accessed 12 Apr 2016].

yachtcom, 2016. Long Distance Communications Made Clear and Simple. [Online] Available at: http://info.yachtcom.co.uk/HF/. [Accessed 12 Apr 2016].

YouTube, 2013. Gladiators of World War II - SOE. [Online] Available at: https://www.youtube.com/watch?v=Bkl4Qz07WrI. [Accessed 26 August 2016].

Zetter, K., 2015. Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors. [Online]
Available at: https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ [Accessed 13 July 2016].

Zhang, W., 2010. China's cultural future: from soft power to comprehensive national power. International Journal of Cultural Policy, 16(4), pp. 383-402.