Maritime Cyberpower Projection

Author: Adrian Venables, Lancaster University
Date: 23 November 2016

Abstract

UK military doctrine recognises five operating environments; Maritime, Land, Air, Space and Cyberspace. These are not regarded as totally separate warfighting arms as demonstrated by the role of amphibious troops, maritime aviation and the use of satellite derived communications and intelligence illustrating how naval forces can utilise the distinctive attributes of other environments in the projection of seapower. This paper examines the as yet unexplored area of how cyberspace can be used as a mechanism by which the maritime environment can generate cyberpower to influence a target population afloat or ashore. The maritime and cyber environments have many similar characteristics such as their dependence on manufactured resources to exploit their potential and that their size prevents them from being under the total control of a single power, but that temporary regional control is vital for trade, communication or to achieve an effect on an adversary's behaviour. By examining the components of cyberspace that are dependent upon the maritime environment, methods to identify the components that can project the new concepts of maritime cyberpower and cyber seapower are explored with particular emphasis on addressing the potential cyber vulnerabilities of ship systems.

Introduction

The maritime operating environment is one of five recognised by UK Ministry of Defence (MoD) doctrine, the others being Land, Air, Space and Cyberspace. This paper describes the relationship between the maritime and cyber environments and introduces the concept of *maritime cyberspace* in terms of cyberpower projection. The nature of maritime power is an important one for states that are either dependent on the seas for trade or security or wish to have an influence in the areas surrounding their coasts. Drawing on UK maritime doctrine, the concept of power at sea and from the sea in terms of control and denial is explained in which free access to areas of the oceans are required to be maintained by nation states. Allied to sea power is the issue of maritime security and its related tasks, which may include a cyber element that will present additional unique challenges of operating at sea or in coastal regions. The link between the maritime and cyber environments is a subject that is poorly researched, yet the two have many similarities and have mutual dependencies in their use for trade, communication and the projection of national power. Current doctrinal definitions are explained and the two environments are compared leading to the introduction of the new terms of *Maritime Cyberpower* and *Cyber Seapower*. This is followed by an examination of the composition of maritime cyberspace and its characteristics to show how they contribute to security and the influence of others through power projection. The paper concludes with methods to identify the components of maritime cyberspace to project maritime cyberpower and cyber seapower with particular emphasis on the need to address the potential cyber vulnerabilities of ship systems.

Defining the maritime environment

At the heart of any definition of the maritime environment is an acceptance of its critical importance to global trade, 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 that a high proportion of future conflicts will occur in or adjacent to a zone of maritime influence.[1] From a military perspective, the sea also provides access for amphibious, land and embarked air forces to embark on expeditionary operations as part of a coordinated strategy to achieve their government's strategic objectives. The maritime operating environment is described in UK Ministry of Defence (MoD) doctrine 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] The Doctrine highlights that maritime power is not an end in itself, but operates within a wider national security framework and that the environment comprises six dimensions; Physical, Economic, Political, Diplomatic, Legal, and Military. These are noted as being interrelated and of equal importance although the physical element provides the overarching context for all and highlights its uniqueness.[3]

Cyberpower and the maritime environment

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.*[4] As such, it is coherent with other more general descriptions of the concept of power and to achieve this maritime forces have a number of unique attributes that they can exploit such as Access, Mobility, Lift Capacity, Sustained Reach, Versatility, Poise, Resilience and Leverage.[5] Although cyberspace is viewed as a unique environment alongside land, air, sea and space, these are not regarded in isolation as operating areas. This is demonstrated in the UK by the coordinated use of the Royal Marines amphibious troops, the Royal Navy's Fleet Air Arm and the deployment of satellite supported communications and intelligence capabilities illustrating how naval forces can utilise the distinctive attributes of the other environments in the projection of seapower. However, although the dependencies between these physical elements are well recognised, each one's unique link to cyberspace is not and the concept of how the projection of cyberpower could be conducted from the sea has not attracted much, if any, discussion and requires further investigation. 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. What effort has been devoted to the subject has been concentrated on the related security aspects of shipping, which in 2016 is now gaining increased interest from both the mercantile industry and suppliers of cyber security products.

The maritime environment and its relationship with cyberspace in the projection of power introduces the concept of *maritime cyberpower* as an enabler of maritime power. The role of cyberspace in contributing to 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. Thus, the importance of the cyber environment is recognised as a facilitator in the effective operation of other systems, but not as a means to exert power at sea in its own right.[6] However, the use by both state and non-state actors of cyberspace as an asymmetric means to seek an advantage over an otherwise militarily superior force is also recognised. This is significant as it implies that the maritime community afloat is no longer platform centric and detached from cyberspace, but is an integral part of it if connected via satellite, mobile telephony or by the radio transmission of digitised navigation or other maritime related information. Although this bring advantages, it also exposes the maritime community to the same risks and vulnerability to attack as their land based counterparts. This is exacerbated by the issue of software aging in which a ship's lifespan may 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 any vulnerabilities in their systems, 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.[7] This may well also be combined with increased automation and the integration of different functions into a single network to reduce the manpower required afloat, which further limits its ability to operate without the aid of the computer systems. Ocean going vessels are also increasingly reliant upon a robust logistics organisation to provide global support – a system that itself is dependent upon Internet based communications and disruption of such networks may have a significant effect on the seaworthiness or ability of a ship to embark on transcontinental passages. This emphasises the integrated nature of cyberspace and that cyberattacks experienced 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 their resolution.[8]

Maritime Power at sea

To project maritime power, 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 environment to an advantage. However, as this implied total control of the entire ocean all of the time, which was impractical, other terms are now used that 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 is defined as the freedom to use an area of the sea for one's own purpose for a period of time and if necessary to deny its use to an opponent if it is contested and requires dominance of the surface and sub surface environments including the seabed and the air above.[9] This may range from being able to exercise the right of innocent passage in a state's territorial water or Exclusive Economic Zone to using force to eliminate another naval threat from challenging control over an area of sea. As Sea Control is a temporary condition, it would usually be an objective in order to conduct a particular 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. The concept of 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 or the threat of submarines were used to deny access to an area or threaten opposition surface forces. 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.

Maritime security

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 it is detrimental to a 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*.[10] Effective security can thus be used to counter the effects of a campaign of power projection or influence – it is a counter power strategy. 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 state sponsored or criminally motivated. These may range from efforts to exercise power through Sea Control or Denial to protecting fisheries or maintaining the operation of offshore oil platforms from the adverse influence of others. The UK National Strategy for Maritime Security defines it 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.[11]

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. The former of these counter the threat of invasion, attack or blockade and the latter includes the dangers from terrorism, subversion, civil disorder, criminality, insurgency, sabotage and espionage.[12] The role of cyberspace is referred to within the context of an attack on the country's critical national infrastructure. This document 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.[13]

Defining the cyber environment

Although there is no formally accepted international definition for the cyber environment, the UK Ministry of Defence's *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*.[14] 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,* with *assured* meaning that the information can be proven as authentic and that the originator can be identified.[15] The Cyber Primer also moves beyond just describing cyberspace to what comprises military operations in the environment, defining them 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 and security in being able to influence the behaviour of people or the course of events. In attempting to explain cyberspace as part of the Information environment, the Primer describes it in terms of three domains; the Physical (hardware, location and networking components), Virtual (software, networking protocols and information), and Cognitive (people, their roles and groupings).

Noting that cyberspace is a complex and dynamic environment, the Cyber Primer emphasises its importance to military operations and the reliance it places on defence communications. However, it also notes the need to use Commercial Off The Shelf (COTS) hardware, software and civilian owned and operated infrastructure for its essential operations.[16] This requires protective measures to be implemented to enable mission critical systems and the information they carry to function with the requisite resilience in order to maintain the same confidentially, integrity and availability of data as military systems. A key facet of this is its relationship and interdependency with the electromagnetic spectrum, which is an integral part of the cyber environment, particularly for mobile platforms that do not have access to a fixed infrastructure for communication. However, data exchange via radio frequency transmissions have a significant disadvantage in that they can be intercepted and unless encrypted can be subject to collection for analysis, manipulation or

interference by persons other than the intended recipient thereby making them a valuable target for espionage, sabotage or subversion.

Comparing maritime and cyber environments

Although the maritime and cyber environments may appear very dissimilar at first inspection, there are a significant number of parallels that can be drawn between them and 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, although control of some elements may be contested, the totality of the two environments are both ungovernable by a single authority, indicating that sea control and denial may have equivalents in cyberspace for power projection. Both also 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 unaided. Furthermore, the maritime and cyber environments are international in nature with ships at sea originating from many countries and cyberspace comprised of components manufactured worldwide, with no single country having total dominance in either. However, influence can be exerted as seen by some states having large warship or merchant fleets or being dominant in the computer or networking markets. Similarly, in order to function, there are global agreements that govern both environments – The United Nations Convention on the Law of the Sea (UNCLOS) in regulating the use of the oceans and the use of internationally accepted addressing and routing protocols that control how data is exchanged in the networks of cyberspace. Finally, both environments are essential mediums for global commerce with physical goods transported by sea and financial services and intellectual property traded in cyberspace.

By adapting the UK's definition of 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* and 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 cyberpower at sea and from the sea to influence the behaviour of people or the course of events through and within the medium of cyberspace. [17]

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

The ability to use cyberpower to project power at sea and from the sea to influence the behaviour of people or the course of events in the maritime environment.

There is a distinct difference in these new concepts of *maritime cyberpower* and *cyber seapower* in that 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 or influence a cyber infrastructure at sea or ashore 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, ports 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 1 below, which emphasise their contributory nature to the wider power component and their role in circumventing the security of the defender:

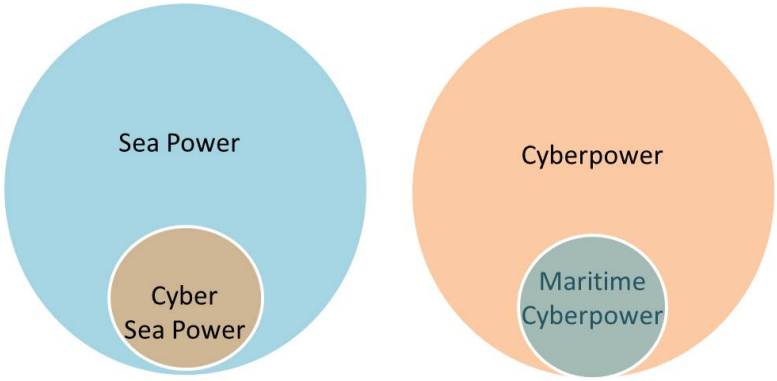

Figure 1: The relationship between Sea Power, Cyberpower, Cyber Sea Power and Maritime Cyberpower

Characteristics of maritime cyberspace

Maritime cyberspace relies on a range of technologies to function with some unique to the environment, but others widely used in all areas of cyberspace. Combined, they form the elements upon which shipping is now dependent for their safe and effective operation with the use of satellite based navigation systems arguably the most significant. The primary system in use is the Global Positioning Satellite (GPS) constellation, which is an American owned capability that provides users with position, navigation and timing (PNT) services. The 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.[18] It should also be noted that although GPS is the predominant satellite based PNT system, there are two others in use; the European Galileo and Russian Glonass systems. When fully deployed in 2020, the Galileo system will comprise 24 satellites with initial services available from the end of 2016.[19] 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 now being exploited commercially and many devices can receive signals from multiple systems to increase their accuracy.[20] Although primarily regarded as an aid to navigation, satellite based PNT systems are fundamental to ensuring maritime platforms remain connected to cyberspace by providing network and cryptographic system timing, altitude and azimuth information to enable receivers to acquire the satellites. They are however very vulnerable to a variety of attacks including spoofing (imitating), hijacking (altering) and corrupting the transmissions, which interfere with the data due to the relative weakness of the signals received from space being easily overwhelmed by malicious terrestrial based transmitters.[21] Although illegal to own or use in many countries, jammers are widely available with well documented examples of their use denying maritime and port services.[22]

Satellite based navigation systems are also 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.[23] The use of AIS transponders is a mandatory requirement for all passenger vessels and international shipping over 300 tons and comprises Very High Frequency (VHF) data transmissions broadcasting a range of information types including the platform's identity, position acquired from GPS and information about its passage. [24] It is a vital aid used by shipping for collision avoidance and for transmitting data relating to search and rescue operations, meteorological, hydrological and navigational safety information.[25] 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 in the Dover Straits Channel

Navigation Information Service.[26] More recently, satellites have been used to receive global AIS data to provide worldwide coverage of information on shipping outside the range of shore based receivers. By accumulating this data, it is possible to track international shipping and areas of high traffic concentration as shown in figure 2. 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 the information that they are transmitting.[27] However, as an open standard using unencrypted message formats and with data accessible via the Internet, it has also been found to be vulnerable to a range variety of attacks including spoofing, hijacking and jamming.[28]

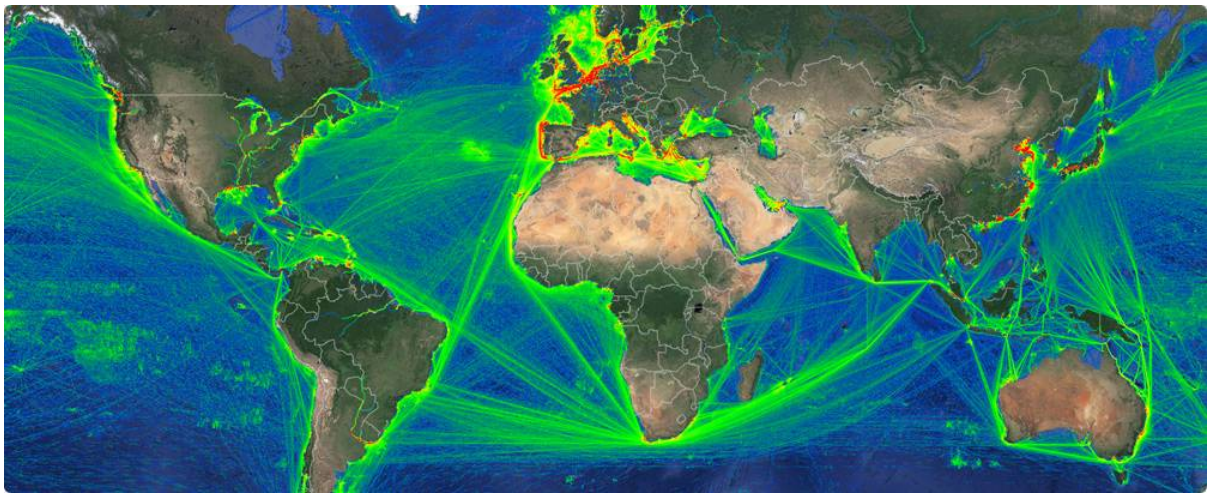

Figure 2 – Global satellite AIS coverage[29]

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 mains 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 performance at the poles. INMARSAT's maritime service offers a range of telephony and broadband Internet connections providing comparable services to land based fixed infrastructures and provide the option of bespoke applications tailored for shipping.[30] THURAYA also offer a maritime communications service with an option of voice and data services. Their data services are similar to that of a terrestrial provider, but do not offer the specialised maritime applications of INMARSAT.[31] Both systems do however enable ships to establish a permanent connection to the cyber environment with similar functionality to a land based subscriber. Despite the space based segments of commercial satellite systems being regarded as resilient to common forms of cyber-attack, recent research has revealed a range of vulnerabilities in the user terminals. These include 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.[32] Although details of these weaknesses were made known to the manufacturers 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.

In addition to space based connectivity to the cyber environment, it is possible to use more traditional radio frequency (RF) 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 and their sensitivity to changes in atmospheric conditions. The propagation of radio waves depends on their frequency as shown in figure 3 below:

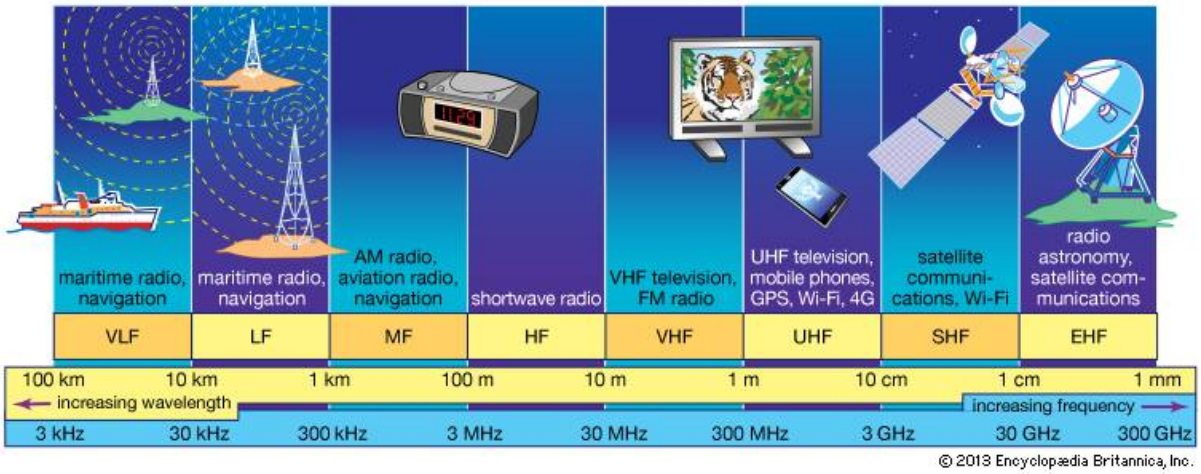

Figure 3 - Commercial radio frequency spectrum[33]

Within the RF spectrum, information is transmitted by changing the value of the signal. The faster the signal is 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 the use of Super High Frequency (SHF) transmissions for high data rate satellite communications. [34] Transmissions at the Very High Frequency (VHF) and above are line of sight and so 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 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*.[35] It should be noted though that long range HF communications are not as reliable as SHF based satellite communications as reception depends on frequency, atmospheric conditions and time of day. Dead zones can also occur close to the transmitter where no signal is received and ranges achieved at night can be twice that of day time communications.[36] RF based E-mail systems such as sailmail use bespoke file transfer protocols in addition to the standard Internet protocols of 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. However, there have 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.[37] As with all RF transmissions, communications are open to interception and measures must be taken to ensure their security. Communications denial is also possible, although depending on the distances and transmitted power, the jamming station may be required to be either within the line of sight of the target or close by.

The final component of maritime cyberspace is without doubt the most important and yet is mostly out of sight with most of its users of oblivious to its existence. 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 more than 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.[38] Their essential role in data and voice communications has resulted in its reliability being deemed by some countries as absolutely essential for the functioning of governments and the enforcement of national security and because of this they are regarded by many as being part of their critical national infrastructure.[39] This network is also relatively centralised and follow similar routes across the globe with some laid over 25 000 feet below the ocean's surface.[40] This routing pattern 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 avoid damage from dragging anchors and are also highly politicised with cable companies often having to overcome objections from local communities for a variety of reasons including economic and environmental concerns, resulting in their paths often being circuitous rather than direct.[41] They also tend to terminate in or near traditional port cities following conventional trading routes.[42] Compared to satellite communication, undersea cables are cheaper to use, enjoy a longer lifespan and have shorter transmission times 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 than by satellite.[43] 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. The combination of their known approximate location, quantity of traffic that they carry and importance to national communications has not been lost on governments who have taken a keen interest in the cables used by their adversaries. In the 1970s the US National Security Agency conducted *Operation Ivy Bells* against Russian telephone cables off the Kuril Islands to the east of the country. Divers operating from submarines positioned recording pods on the lines, which would then be retrieved after a period of time for later examination.[44] More recently, both US and Russian submarines and spy ships have been reported operating near undersea fibre optic cables leading to fears that they might be able to either tap into them to intercept the data or be planning to attack them in times of tension or conflict.[45] [46] The ability to monitor or even sever direct communications with their trading partners and military allies would significantly degrade a nation's cyberpower and may result in data having to be rerouted across other networks that may have increased latency or already be subject to monitoring activities.

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 together form the new concept of maritime cyberspace. The relationship between them is shown in figure 4 below:

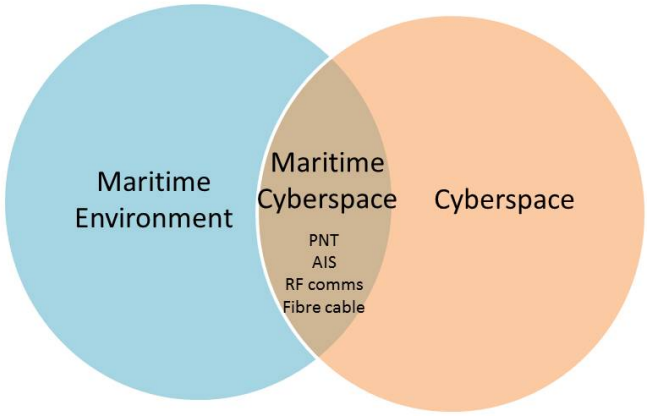

Figure 4 – The composition of maritime cyberspace

Exploiting Maritime Cyberspace

Having identified the similarities and dependencies between the maritime and cyber environments and their use for the projection of power, the exploitation of maritime cyberspace offers significant potential for developing national power, whilst emphasising the importance of maintaining its security from potential adversaries. By combining figures 1 and 4, a composite model of power projection in maritime cyberspace can be derived, which is shown in figure 5. This demonstrates that both maritime cyberpower and cyber seapower can be developed either separately or as part of a combined strategy.

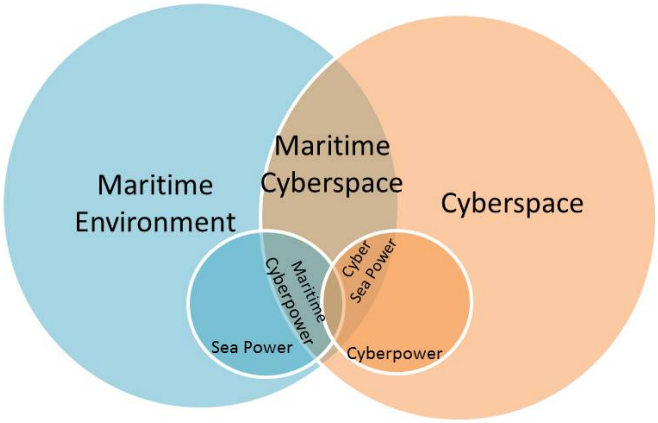

Figure 5 – Power projection in the maritime and cyber environments

The challenge of preventing adversaries from using maritime cyberspace to exert maritime power by compromising ships' systems is now being acknowledged with a greater understanding of the risks of integrating previously separate components into a single integrated network, which is then connected to the Internet. The practice of automating the control and management of different capabilities 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 communication suites and PNT systems. This provides a remote monitoring and control capability that reduces the number of personnel needed 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 including operating systems and networking components that would be familiar in any home or office. Reliability is ensured by incorporating proven COTS components that have already been used in a range of operating

environments and using open architectures with 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. However, although using commonly available products and software that are proven and reliable provides reassurance that a system will work, they may also introduce a range of vulnerabilities caused by a failure to properly secure and patch systems that can be exploited by those of malicious intent. Software that is in widespread use is also the most frequent to be targeted by malevolent parties as their efforts in understanding and developing techniques to access and alter computer code will be rewarded by them being effective 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, components that are intended to be upgradable are designed to be easily accessible, which further increases their potential vulnerability to malicious interference. There is no shortage of methods available by which a ship's system integrity can be compromised by a human operator, either intentionally or by accident. A direct connection to the network by an infected laptop or USB stick may be the easiest means, but wireless networks or remote access logins via an Internet connection may also be a convenient way to access the system. A vessel in port with a network that is unencrypted or protected by a weak password would also offer an attractive and easily accessible target. In addition, the use of multifunctional control terminals presents another system weakness as once compromised they could provide access to the entire network and its subsystems.[47] The use of cyber seapower as a means to threaten shipping and the maritime environment is now being recognised as the subject of several conferences and by the UK shipping industry, which offers guidance to ship owners and operators on how to assess their networks and put in place the necessary procedures and actions to maintain the cybersecurity of their ships.[48]

Conclusion

This paper has introduced the concept of the maritime cyber environment by bringing together the individual attributes of both elements to highlight their importance and mutual dependence. Understanding the maritime environment is vital both in terms of appreciating its role to society in supporting trade and in the projection of political power and influence. The seas are often a source of conflict as neighbouring nations compete for limited resources in adjacent waters and seek to control their use for transporting essential materials. This results in issues that could previously be regarded as being matters of foreign policy quickly becoming of domestic importance as legal and diplomatic disputes can quickly become militarised as nations seek to protect what they regard as their own, while exerting influence in those areas claimed by other nations. By developing the two distinct but related terms of *maritime cyberpower* and *cyber seapower,* the maritime environment can be seen to contribute to the ability to project national cyberpower, which may have global impact. Whereas the former utilises the maritime environment to lever the properties of cyberspace to alter the behaviour of a target individual, group or population, the latter uses the cyber environment to facilitate Sea Control or Denial to establish the free use of an area of sea for a period of time or to deny its use to an adversary. In this way, the comparable properties of both environments enable parallels to be drawn as to how these different forms of power can be exercised. A key conclusion from investigating maritime cyberspace is the link between security and power projection. In order for an adversary, whether a state or non-state actor, to be able to exert a cyber influence on a target, they have to be able to access it either directly or indirectly. Cyber security measures will prevent or limit the access that an attacker will have and therefore restrict the effect that they hope to achieve. This highlights the need to understand the potential vulnerabilities that may exist in maritime cyberspace and the need to be self-critical in how this environment can be seen from the perspective of both attackers and defender and how offensive and defensive strategies can be developed.

Academic institutions are now becoming 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 and the importance of the role of the user in maintaining system integrity. This is coherent with one of the most significant elements of both environments; that to fully engage with them, operators have to understand and interact with manufactured elements whether these are ships or computing devices. Maritime cyberspace is unique in both comprising and relying on a number of discrete capabilities including 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 consists of the thousands of miles of fibre optic cables that cross the ocean floor connecting continents and which are crucial to the very existence of the environment. With the increasing trend to combine previously separate ship systems onto a single network controlled by an IPMS, which may be connected via satellite to shore based networks, whole vessels can now be considered part of maritime cyberspace. These must be protected from those wishing to influence the behaviour of nations by compromising the systems upon which their shipping depends.

---

[1] Ministry of Defence, 2011. *British Maritime Doctrine.* 1st ed. London: Development, Concepts and Doctrine Centre. P.v

[2]Ibid. Para 123

[3] Ibid. P.iii

[4] Ibid.

[5] Ibid.

[6] Ibid. para 355.

[7] Fitton, O., Prince, D., Germond, B. & Lacy, M., 2015. *The Future of Maritime Cyber Security,* Lancaster: Lancaster University. p.9.

[8] Ibid. p.28.

[9] NATO, 2014. *Allied Joint Doctrine for Air Maritime Coordination AJP-3.3.3.* 1st ed. Brussels: NATO. para 0303

[10] Oxford English Dictionary, 2016. *Oxford English Dictionary.* [Online]
Available at: http://www.oed.com/ [Accessed 12 Apr 2016].

[11] HM Government, 2014. *UK National Strategy for Maritime Security,* London: Her Majesty's Stationery Office.

[12] Development, Concepts and Doctrine Centre, 2014. *Joint Doctrine Publication 0-01 UK Defence Doctrine.* 5th ed. London: Ministry of Defence.p3

[13] Ibid. p.9

[14] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence. p1-1

[15] Ministry of Defence, 2013. *Defence Information and Communications Technology Strategy.* 1st ed. London: Ministry of Defence. P8

[16] Development, Concepts and Doctrine Centre, 2013. *Cyber Primer.* 1st ed. London: Ministry of Defence. p1-3

[17]Ibid. p.iii

[18] 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].

[19] 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].

[20] 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].

[21] Hayes, G.,2016 *GPS can be jammed and 'spoofed'--just how vulnerable is it? Part 2*. Available at http://www.marineelectronicsjournal.com/content/newsm/news.asp?show=VIEW&a=129 [Accessed 24 July 2016]

[22]Ibid.

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

[24] International Maritime Organisation, 2016. *AIS Transponders.* [Online]
Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx [Accessed 12 Apr 2016].

[25] 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].

[26] 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].

[27] Vessel Finder, 2016. *Real-Time AIS Data.* [Online] Available at: https://www.vesselfinder.com/ [Accessed 12 Apr 2016].

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

[29] Marine Source, 2016. *Satellite AIS Data.* [Online] Available at: http://www.marinetraffic.com/en/p/satellite-ais [Accessed 12 Apr 2016].

[30] Inmarsat, 2016. *Fleet Broadband.* [Online]
Available at: http://www.inmarsat.com/service-collection/fleetbroadband/ [Accessed 12 Apr 2013].

[31] Thuraya, 2016. *Marine Comms.* [Online] Available at: http://www.thuraya.com/marine-comms [Accessed 12 Apr 2016].

[32] 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].

[33] 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].

[34] Computernetwor (Balduzzi, et al., 2014)kingsimplified.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].

[35] Sailcom Marine, 2016. *HF shortwave SSB radio email systems.* [Online]
Available at: http://www.sailcom.co.uk/pactor/ [Accessed 12 Apr 2016].

[36] yachtcom, 2016. *Long Distance Communications Made Clear and Simple.* [Online]
Available at: http://info.yachtcom.co.uk/HF/ [Accessed 12 Apr 2016].

[37] 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].

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

[39] Starosielski, N., 2015. *The Undersea Network.* 1st ed. Durham and London: Duke. p.1

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

[41] Starosielski, N., 2015. *The Undersea Network.* 1st ed. Durham and London: Duke.p.31

[42] Blum, A., 2012. *Tubes - Behind the scenes at the Internet.* 1st ed. London: Penguin. p.194

[43] Starosielski, N., 2015. *The Undersea Network.* 1st ed. Durham and London: Duke.p.9

[44] http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/

[45] Sanger, D. E. & Schmitt, E., 2015. Russian Ships Near Data Cables Are Too Close for U.S. Comfort. The New York Times, 26 October, p. A1.

[46] 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 4 August 2016].

[47] Venables, A., 2016. Protecting Ships - The Threat of Hackers. *Port Technology*, 69 Edition, pp. 30-31.

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