Lancaster University

The Future of Maritime Cyber Security

Mr Oliver Fitton, Dr Daniel Prince,
Dr Basil Germond and Dr Mark Lacy

Foreword

Contents

Introduction 1

Framework 2

Extension of the Littoral 2

Information 4

Technology 7

People 15

Key Traits 16

Maritime cyber security logistics: 2035 24

Key Trends 25

Future Fiction –Scenarios for Maritime Logistics in 2035 26

Conclusion 27

Conclusion 28

Writing Team 30

Bibliography 31

The Maritime environment is not immune to the radical ability of modern digital communications and computing to be disruptive. In order to gain the advantages of modern technology those operating in the maritime must also become aware and develop strategies to handle the inevitable security issues that modern computing systems bring with them.

This report presents a first step on the road to this understanding by presenting the findings from a joint workshop run by Security Lancaster and the Developments, Concepts and Doctrine Centre with participants from a range of government and commercial stakeholders. Here we present the salient points that we discussed within a framework that underpins a repeatable approach to scenario planning based on assessing key traits and trends in three key elements of the cyber maritime domain: Information, People and Technology.

This report identifies how the use of technology is extending the scope for maritime security far beyond traditional littoral boundaries and the key influences shaping the cyber maritime environment.

Introduction

This report will build upon the Global Strategic Trends series developed by Development, concepts and Doctrine Centre (DCDC). The latest Global Strategic Trends document (Global Strategic Trends - Out to 2045, published in 2014) takes a wide ranging approach to all aspects of the global future, this report will drill down into one aspect of that future to explore the cyber threat within the maritime environment against the backdrop of British Maritime Doctrine, the National Strategy for Maritime Security and commercial maritime operators.

Cyber operations and cyber security have been a high priority for the UK Government since the 2010 Strategic Defence and Security Review listed cyber security as a top tier threat to national security. Our current reliance on digital communication, automation and the interconnectedness of the global economy make cyber security not only an issue of national security but of global security. Emerging cyber threats including destructive malware, cybercrime and data leaks impact governments and industry alike.

In today's inextricably connected world the maritime domain plays a central role. The seas constitute tremendous lanes of communication, vital for trade, all the more in a globalised world. They also grant states' navies an almost unrestricted access to distant territories. However, as a vast, shared and largely ungoverned space, the maritime domain is prone to the proliferation of criminal non-state actors that benefit from the porosity of maritime borders: piracy and robbery at sea, illegal, unreported and unregulated fishing (IUUF), drugs, arms and people trafficking, terrorism at sea, illegal immigration, marine environment degradations, as well as a range of foreign states' potentially disruptive activities at sea. Maritime security issues will play a key role in the 21st century's complex terrain – a terrain that confronts the complexity of geopolitical change (discussed in Global Strategic Trends – Out to 2045) and the complexity of technological change. The interplay between these two distinct areas will be the focus of this report. It is clear that cyber operations, in and against operators in the maritime environment, will be a distinct feature of the global future.

To inform this work Security Lancaster delivered a workshop in collaboration with DCDC with attendance from other UK Government departments and private businesses who operate in the maritime environment. This report identifies the key findings from that workshop. This includes; key areas of concern and vulnerability and recommended measures to protect operators in the maritime environment; a framework for considering future cybersecurity scenarios with a worked example; and how potential trends that are changing the future of the cyber maritime environment.

Framework

The core framework used to frame the discussion pertaining to cyber operations in the maritime domain can be discussed in terms of three elements - Information, Technology and People. Information relates to the data which sustains maritime operations, its uses and the ways which information can be undermined in the modern age. Technology encapsulates computer systems, both hardware and software, and larger platforms including ships and ports. Technology is fundamental in navigating the inhospitable maritime environment, it is the foundation on which the global economy is based but it is also both physically and digitally vulnerable. People are part of complex systems in the maritime environment; they interact with one another and computer systems in both creative and destructive ways. At every intersection of human and machine there is the possibility for error, manipulation, coercion or sedition. Importantly each element has a relationship to the other which may be a target for disruption, for example the level of trust a person has in technology will affect the relationship that the individual has with the information that technology generates or displays for consumption by the person. Therefore, this framework enables a critical reviewer undertaking scenario planning to consider the trends associated with each element and how these trends might affect the element relationships.

This framework was used during the workshop to provide the foundations for discussions exploring each of the key areas and their relationships. By discussing this framework with key stakeholders trends, vulnerabilities and recommendations relating to the maritime environment were considered enabling us to develop the framework in more detail and understand how key traits of the element underpin the emergent trends and propose recommendations to deal with potentially emergent issues. We argue that without the consideration of the elements and their interconnecting relationships scenario planning and trend analysis would be missing vital context.

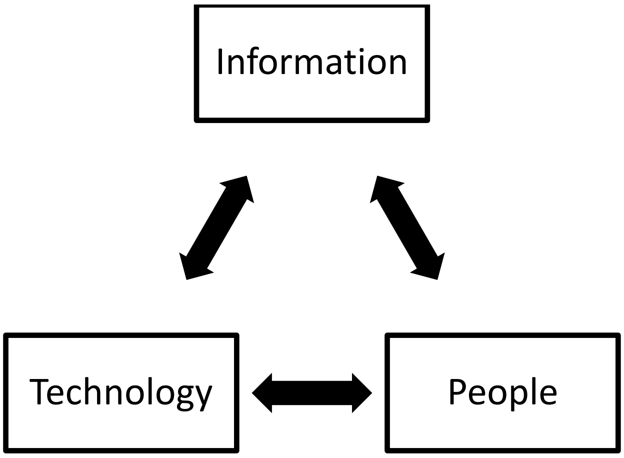


Figure 1: The Three Elements of Cyber Operations in the Maritime Environment

Extension of the Littoral

A key conclusion draw from the workshop discussions and our research is that the nature of the littoral is changing with the advent of complex digital systems supporting maritime operations. This is important when considering what needs to be secured and by whom in the maritime environment. Traditionally maritime operations, particularly in naval operations, only had to consider a maritime domain that only extended partly onto land around the costal area. One key aspect when considering the impact of the use of digital technologies is their ability to create dynamic connections between different locations in real time. Traditionally, maritime has be sea-locked, i.e. physically connected to the sea or other body of water. However, digital technology is connecting in-land facilities to maritime platforms. Consider the case of remote monitoring of engine platforms; those land based facilities act as if they are on-board the platform. In the case of the people, individuals can be connected to one or more social groups land based and be communicating in real-time, in much richer ways than they had previously been able to do.

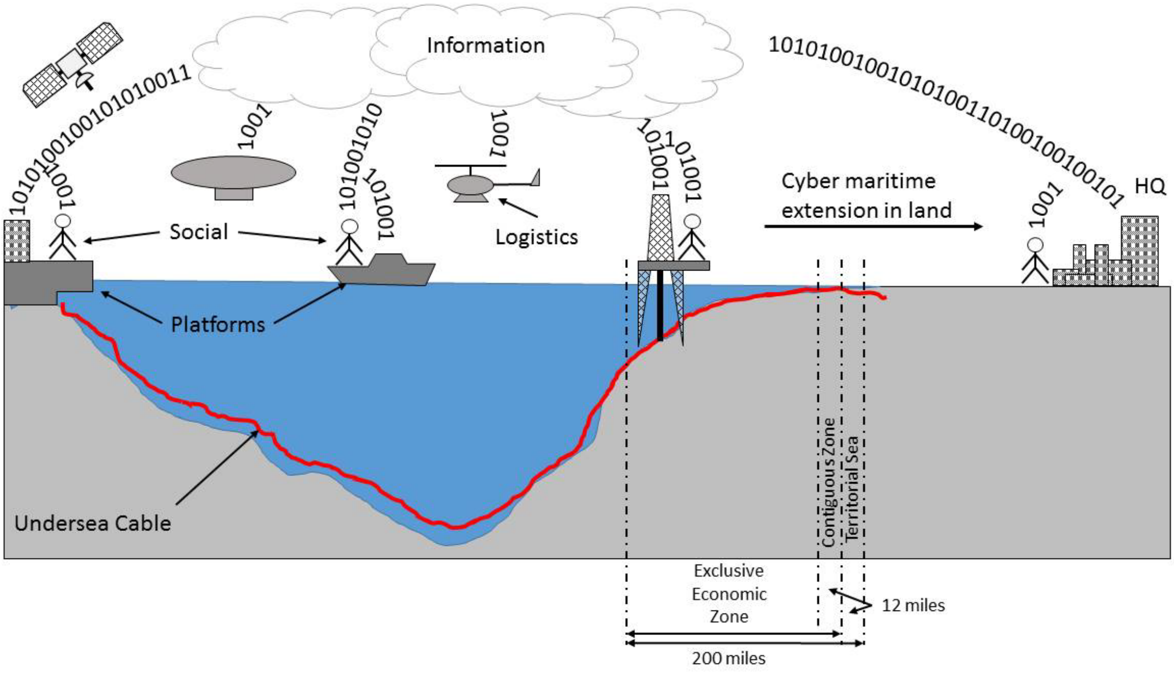


Figure 2: Extension of the Littoral under the influence of digital technology

This concept of extension is given in Figure 2 which also shows how People, Technology and Information interplay with each other in the physical world. The trend for increased interconnectedness does not seem to be dwindling. Therefore, when considering the concept of maritime security in the future it will be vital to consider how digital technology is extending the maritime operating environment beyond a standard littoral boundary.

Using the above framework this report is divided into three sections - Information, Technology and People. In each section the key traits and future trends of each element will be discussed. Based on these key traits and trends recommendations pertinent to governments and businesses will be presented at the end of each section. Once each element has been discussed this framework will be employed to inspect a key element of maritime operations for governments and for business – Logistics. The logistical efficiency of maritime operations is a matter of national and global security, it is also a key factor for the efficient running of global business. Maritime logistics relies heavily on information, technology and people making it a prime target for future adversaries. A conclusion will summarize the findings and recommendations of this report.

Information

Recent breakthroughs in communication and information technologies have impacted the way state and non-state actors interact within the maritime domain; it has generated opportunities as well as challenges for naval and commercial stakeholders as well as criminal actors. The sea is a vast space where platforms operate at a distance, whereas the complexity of the operations and of the on-board systems generates and calls for a constant flow of data.

Before the development of electromagnetic signals and cyber-communication, ships and other platforms were mainly operating in isolation (this was a platform-centric era). Ship commanders only knew their direct environment and had to make decisions based on observations, cognition, knowledge, doctrine and past experiences, resulting in potentially ill-informed decisions producing a limited operational impact. In the 21st century, network-centric operations tend to become the norm. Decisions, although still informed by doctrine and past experiences, are principally dependent on the flow of external data received. Platforms are networked to other platforms, sensors and commanders located at sea or on land via IP-based systems exchanging mainly digital information, allowing ship commanders and ISTAR operators to benefit from a common operating picture. This is supposed to result in better informed and thus efficient decisions, whereas increasing the risk of communication and information dependence.

Key Traits

Volume: By 2035, the volume of information received by a single ship will virtually be unlimited, leading to a potential overflow of information.

Quality: The quality or accuracy of the information matters more than the quantity.

Distribution: The tendency is towards a P2P rather than hierarchical distribution of information; every platform is a sensor within the global grid and every platform is networked.

Trustworthiness: Information must be trusted, which is getting more difficult in an environment where operations are mainly conducted jointly with partners, increasing the risk of a weaker link within the network.

Trends

Complexity of Information Management: Complex and non-hierarchical networks of information sharing, the increased speed of communication, the increasing number of information providers, sources and end-users involved in the process, all contribute to the complexity of information management. Processing the volume of information, making sense of the complex flow of data, transforming information into intelligence engenders a complex information management structure.

Information Breach: Communication being mainly dependent on IP-based systems, there is an increased risk of information breach. Information can be accessed, usurped or corrupted. The complexity of the networks and the multilateral and joint operating environment also contribute to increasing the risk of information breach.

Recommendations

Critical Enquiry: In addition to preventing unauthorised access to data and communication channels, ship commanders and system operators must further develop and consolidate their capacity to question the veracity of the data received, such as spotting errors on the radar screen (corruption), as well as questioning the veracity of the source indicated (usurpation).

Resiliency: It is crucial to remain in a position to make decisions even if the data received are seemingly corrupted, have been accessed or usurped, or if the cyber domain is under attack. For the C2 process to work under those conditions, other channels of communication should be privileged, which are not entirely dependent on IP-based systems. The existence of secondary systems and the presence of personnel able to fix and repair the vital systems are also crucial.

Education: Preventing, spotting and defending against cyber-attacks requires educating, training and drilling staff, so as they can efficiently respond to attacks, spot errors and continue to operate under cyber-attacks conditions.

Prioritization: Not every single system can be protected; it is thus imperative to decide which ones are crucial to operate platforms and weapon systems and make decisions informed enough and which ones can be shut off if necessary. Information should also be prioritised; ship commanders and system operators need only receive a certain type and amount of information, i.e. the one which is accurate and useful to make relevant decisions. The structure to process the information, to make sense of the data received, is thus crucial.

Conclusion

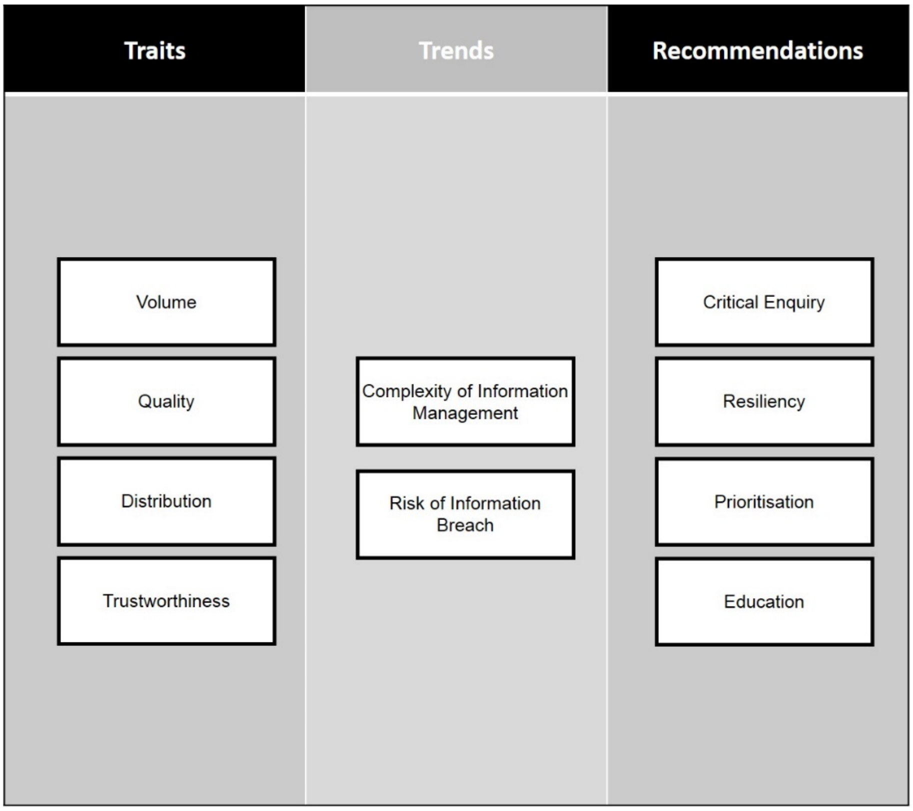


Figure 3: Summary of Traits, Trends and Recommendations in maritime information

The future of maritime operations from the perspective of Information will depend on the degree to which critical enquiry, resiliency, prioritisation and education will contribute to the adaptation to and the mitigation of the negative aspects of the key traits and future trends discussed above.

An idealist scenario for the future sees platforms from various friendly nations operating under information dominance, thanks to a fully integrated and networked C4ISTAR and a safe, secure and trusted communication system. Under those conditions, common operating pictures allow conducting effect-based operations; non-kinetic fires contribute to both the success of kinetic fires and to information dominance. The almost total reliance on external data and IP-based systems is not a problem as long as the security of the networks and systems is guaranteed.

However, an overreliance on the civilian sector (increasing the risk of ‘weaker links’), a lack of education and training, and a lack of resilience and prioritisation may cause the defence to fail in case the cyber domain is under attack. As a consequence, ships may have to operate without relying on the global grid of information, with a limited access to external data, and perhaps even without using all the on-board IT systems. Due to the current reliance on those systems to conduct any operation, this means that ships are likely not to be able to operate at all under those conditions.

This section has shown that the aim towards which we should tend is a more balanced situation, with a largely but not fully integrated C4ISTAR providing the conditions for information exploitation but not dominance. Based on a planned prioritisation of needs (in terms of systems to defend and information to obtain) and the development of non IP-based systems for communication, ships will develop a large degree of communication, information and cyber resilience, allowing C2 to be efficient even under cyber-attacks conditions.

Technology

Technology is fundamental to the modern maritime domain and may be considered to be computer driven systems which operate on a platform or work within maritime operations (such as ports) to produce outcomes.

Technology is both the hardware and the software in computer systems. This section will discuss the key traits of modern computer technology in the maritime environment, the trends which will affect technology in the future and recommendations concerning the impact of the cyber threat on technology in the maritime environment.

Key Traits

Utility: Technology is designed and implemented with a specific purpose in mind in the modern maritime environment; such purposes include guidance, sensing, controlling machinery or communicating. However the history of technology is not as linear as one technology for one specific job. Users often find secondary and tertiary functions for technology. While the designers may have only imagined a single use for their technology users can, out of necessity or further design, find new uses for existing technology. For example GPS systems were installed on ships to aid navigation, today ships rely on GPS systems for navigation. However system designers began to realise the GPS system could be used to provide accurate platform wide timing signals and interconnected systems which required accurate time keeping to their GPS system. The history of technology is complex and interconnected, it is the story of designers and users working in unison and at odds to create the next step. However secondary and tertiary uses of technology create potential security issues. Firstly, the technology may have been deigned to be secure in its intended function but the likelihood is that the designer did not considered security in the technology's tertiary functions. This leaves the secondary and tertiary functions of technology vulnerable. Secondly, the use of technology in a tertiary function may have a detrimental impact on the security of the technology as it is used in its primary function.

Interestingly the word Hacker, in its original sense, described someone who used or adapted a technology for a purpose it was not originally intended in a way it was not designed. Far removed from the Hollywood image of programmers breaking into clandestine computer systems, Hackers were hobbyists who found new uses for technology or used technology for new purposes. Hacking is not a new idea to sailors, indeed the use of lamp as a method of signalling (now used as signal lights) involved the innovative use of an existing technology to fulfil a new task.

Intrinsic Fragility: Writing computer code is complicated. In order to design a new piece of software it is necessary to learn entire languages which describe to the computer exactly what it is expected to do and how to go about doing it. This code can be many millions of lines long and is prone to designer error. As a result of complexity and human error digital technology is a fragile thing. Errors in coding lead to system vulnerabilities which can be exploited by adversaries for malevolent ends. These kinds of errors are considered by Symantec to be “highly critical” and victims of such fragility include PayPal. There are many reasons that such vulnerabilities come about, chief amongst them is human imperfection. Other factors include inefficient organisation. Large coding projects require large teams of people which are vulnerable to communication errors and personnel changes amongst other pressures. There is a further cause which is pointed to by David Rice in his book Geekenomics. Rice goes to great lengths exploring the disincentives for security at play in the software market. He hypothesises that the ability to patch software at a later date encourages developers to sell unfinished and even critically flawed software and that the dynamics of the software market make functionality much more important than good practice and security.

Hardware can be just as fragile as software. For example, the complexity of the manufacturing process of modern small scale integrated circuit (IC) manufacturing. Modern Integrated Circuit manufactures such as Intel and AMD regularly disable faulty parts of complex IC's, such as CPU and GPUs, in order to increase the potential product sales. These IC's are then sold as a lower specification hardware line, for example with fewer processing cores for CPUs. In fact entire subsystems can be disabled if found to be not up to specification. This shows that the manufacturing process does not produce hardware components that are 100% defect free and that what defines the operational level is the ability of an IC to pass a threshold test, so even within the product lines there is variation in capability and an economic imperative for IC manufacturers to sell higher specification products to cover the costs of manufacture. Therefore even within specific product lines there exists the possibility that bugs in the hardware exist that could cause problems in calculations. Beyond manufacture or design issues, it is worth note that the data stored and processed by these ICs are not hard binary ones and zeros, but messy physical concepts like voltages and currents that can be affected by noisy operations, temperatures, stray external physical effects, that may mean the data gets read or stored incorrectly. Therefore at both the hardware and software level there is intrinsic fragility in the systems that are used in the maritime environment on a day to day basis.

Aging Rates: Software ages much more quickly than hardware does. For example, many maritime operators have been adversely affected by Microsoft's decision to discontinue support for their Windows XP operating system, introduced in 2001. XP was a user friendly and robust system on which software could be mounted to control a wide range of applications at sea and on land. For Microsoft there was no business sense in maintaining the legacy product while pushing new and more sophisticated operating systems such as Windows 8.1 which included native touch screen support and integration with mobile devices which were non-existent in 2001. The lack of support for Windows XP means that continued use of the operating system would not be supported by Microsoft security updates. Windows XP lasted for just 13 years, many pieces of software which are more niche, less popular or less effective last much shorter periods of time. Yet the platforms and the industrial machinery which comprise them are designed to last much longer.

The Queen Elizabeth II Class aircraft carriers currently under construction in the UK are designed to last for 50 years. Parts for these platforms are required to last for 50 years or to be serviced continuously to produce a life span of 50 years. However the same policy would be inadvisable for the software used on HMS Queen Elizabeth II or HMS Prince of Wales. Considering the nonlinear growth of computer technology (discussed later) it is impossible to imagine that these ships will maintain their effectiveness in 50 years' time if they continue to use their inaugural computer systems.

Software will continue to have a dramatically shorter lifespan than hardware. In the maritime environment hardware will continue to be designed and built to last for decades. Whereas software will only last until a vulnerability is developed to attack it, until the vendor decides not to support it or until the vendor goes out of business.

This is a serious issue for maritime actors. Digital refits will become frequent occurrences but they will not stem the tide of exploits and attacks. Adversaries will always be able to produces attacks faster than it is possible to patch a system or to refit a platform. This will add a new consideration to the planning of platform design in the future and may require a fundamental rethinking of how technology is used in an environment which is characterised by large investments and long platform lifespans.

Replicability: The ability to share data has revolutionised the global economy in a very short time. Computers can copy data to new locations anywhere in the world. Once there the data can be dismantled, manipulated and exploited. This causes serious issues for software vendors who want to retain their intellectual property in order to make a profit. It also has dire consequences for consumers, including those in the maritime environment.

It is not only music, films and software that can be copied and reverse engineered. Malware can be captured and manipulated just as easily. Six months after the Stuxnet Worm attacked the Natanz facility in Iran, setting the Iranian nuclear programme back months if not years, the zero day exploits which allowed Stuxnet to interfere with the nuclear enrichment systems were available on the penetration testing resource Metaspolit. This meant that anyone who had access to this free resource could easily employ these exploits in their own attacks against users of the same technologies used in Natanz. As a result we are living in an age of open source cyber weapons where it is possible to download programmes which target industrial control systems, weapons, ships and more for free from the internet. This means that vulnerabilities in other people systems and attacks on those systems can have an adverse effect on the security of your own system.

Trends

Nonlinear Growth: Technology will continue to grow and develop in a nonlinear and difficult to predict fashion. Moore's Law is an observation that the number of transistors on an integrated circuit doubles every two years. This observation was first made in the 1970's and it has proved roughly correct ever since. Metcalfe's Law is an observation that the utility of a network grows proportionate to the square of the number of users of that network. This observation was made around 10 years after Moore's Law and continues to best describe the utility of the internet. These observations demonstrate that nonlinear growth is a key trait of technology. While these observations allow us to plan for what future technology might look like they do not allow us to see clearly how that technology might be utilised. For example in the 1970's Moore's Law predicted that computers would be about as complex as they are today but it did not imagine that such computing power would be used in the manner that it is or that it would have the effects on society, commerce and security that it has. As a result it is difficult to predict with an certainty what technology will look like in the maritime environment, even a matter of years from now.

Exponential Growth in Capability: Technological capability is being realized for increasingly low costs. This produces three important sub trends:

> *Bridging the digital divide:* The world can be divided into those capable of accessing technology, especially the internet, and those who are not. Exponential growth in capability means the digital divide is shrinking.

People can do more with less: More people are able to achieve goals, including exploiting vulnerabilities, with less equipment. The effect of this is that more people are included in the Information Rich Society, more people have technical skills and a wider knowledge base is created.

Price Reduction: Platforms once thought to be too expensive to recreate in order to attack are now widely available. For example 10 year old Industrial Control Systems are still prominent in many modern industries and yet they are easily sourced at low costs.

In the Maritime Environment this means that adversaries have an unknown and ever growing capability to attack platforms and their systems. Especially when we consider heavy machinery and ship building, these extremely expensive platforms are designed to last a very long time but the software installed therein is now cheaply or freely available to the increasing number of people with an internet connection.

Automation & Integration: The economic imperative to replace labour with systems has reduced the need for people on platforms. As a result systems now carry out a large number of complex and integral tasks on-board ships and other maritime platforms. The efficiency produced by this trend is a clear advantage, however automation and load borne by computer systems means that they are more integral than ever. As discussed these systems are highly fragile. As the trend for greater automation (even unmanned platforms) continues new vectors of attack will be created.

Further attempts to create efficiency in automatic systems leads to integration of systems which do multiple things. For the sake of argument it may be that a new ship has a communications system which governs both internal communications and external communications. In this scenario costs will have been cut by installing a single all-encompassing system and training will only be required to operate that one system. However should the external communications network be attacked the target will also have their internal communications breached. This means not only will the victim be unable to communicate safely with the outside world they will also be unable to communicate securely between decks. Had two separate systems have been installed there would have been some degree of resiliency on the platform. The trend to integrate technology makes sense when efficiency and economy are under consideration but not necessarily when security threats are taken into account.

Open Standards & Software Monopolies: Open standard technology will become central to the development of new platforms. That is to say that off the shelf technology which is widely available on the open market will be used throughout design and operations of platforms such as new ships, rigs and ports. Proprietary systems will continue to find their place, however open standard technology will continue to be appealing due to lower costs, service contracts and the capabilities that they will bring to the platform.

A reliance on open standard technology will cause security concerns. The maritime industry will become dominated by a small group of technology providers who produce and maintain industry standard technology and software. This will create a fleet wide if not worldwide reliance on systems which are easily obtainable by adversaries. Such systems will then come under increased attack. We have seen this before in personal computing. For a long time Apple marketed themselves are virus free on the basis that few adversaries made malware to target Apple computers. As the demand for Apple OS computers increased so did the production of malware targeting them.

However the complexity of the maritime environment will require that open standards technology be customised to the role of any given platform. This will require the use of subcontractors to configure and maintain off the shelf systems for unique purposes. Subcontracting will become more commonplace as will insider attack and system vulnerabilities based on the work of the subcontractor.

Information: Generated, Stored & Processed: Because of the volume of information generated by future technology new ways of storing and processing data will be employed. Data is likely to be stored "in the cloud" using off site servers which systems connect to. Such systems area already well-established throughout business and personal computing but the increased connectivity which will be enjoyed at sea will allow such storage systems to become available through-out the maritime environment. However the use of cloud storage systems is not without its pitfalls. Information security becomes a critical issue when data is trusted to a third party to protect – some critical maritime industries may require that their data is stored by in house cloud storage systems or they may buck this trend opting for a more secure but less efficient local storage solution.

It is possible although more unprecedented that processing will also happen "in the cloud". In this kind of a future the actual processing done by a system today could be performed in a controlled, maintained and safe environment remotely. This would allow consoles on the platform to become "dumb" terminals which act as a window through which the user sees data which is processed at a remote location. This would mean that system maintenance and refitting would only need to be done in that remote location rather than on platform but it would also mean that the platform becomes entirely reliant on the security of the connection they enjoy at sea.

It is therefore possible to produce a framework by which we can consider the use of Cloud computing in the future:

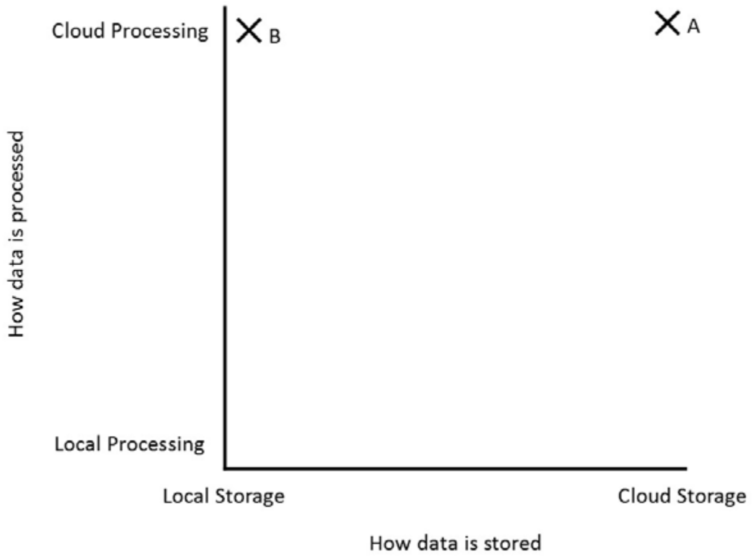


Figure 4:Possible futures for the storing and processing of information

This framework allows us to explore different possible futures. To illustrate this, in the future marked by point A all information is stored and processed remotely. In this future costs will be reduced by technical upgrades being performed in a secure environment while the platform is at some remote location, a subcontractor will hold a service contract for system maintenance and computing power and information will be easily shared between platforms. However the platform will be entirely reliant on its connection to the network and all data will be entrusted to a third party. In point B data is stored locally, i.e. on the platform but is processed remotely. In this scenario the cost savings of system upgrades is maintained but data is not entrusted to a third party unless it is utilised in processing.

Asymmetry of Attack: Attacks on technology will continue to be highly asymmetric. Low tech attacks will continue to have the ability to nullify high technology, technology will not design out vulnerability to low tech attacks. For example removing a fuse is extremely low tech and has the potential to disable a multimillion pound computer system. Likewise cost asymmetry will continue to characterise attacks against technology. Platform costs will continue to increase as new technology is implemented and platforms are required to perform more specialised or more diverse tasks. Inexpensive, even free attacks will continue to be effective against such platforms in the future. This will further alter the design concerns of future platforms.

Recommendations

Get Rid of What You Don't Need: Open standard technology often include modules and capabilities which are surplus to requirements. Whether this is a stock control system which also includes a customer relationship management system or a navigation system which also includes calendar for journey planning. If the module or system is not required it should be removed with security in mind. Systems which lay unused and ignored are considered low hanging fruit by adversaries who can use them to gain access to connected critical systems.

It should be remembered that technology has driven and will continue to drive dominance in the maritime environment (in both the military and civilian sectors). This report does not suggest that digital systems should be culled in order to secure the platform. Instead this report suggests that actors question the utility of a system versus the security risk it poses.

Redundancy is another key issue in this equation. Backup systems are vital and potentially lifesaving. When deciding whether redundancy systems are required serious thought must go into what might happen if the primary system were to fail.

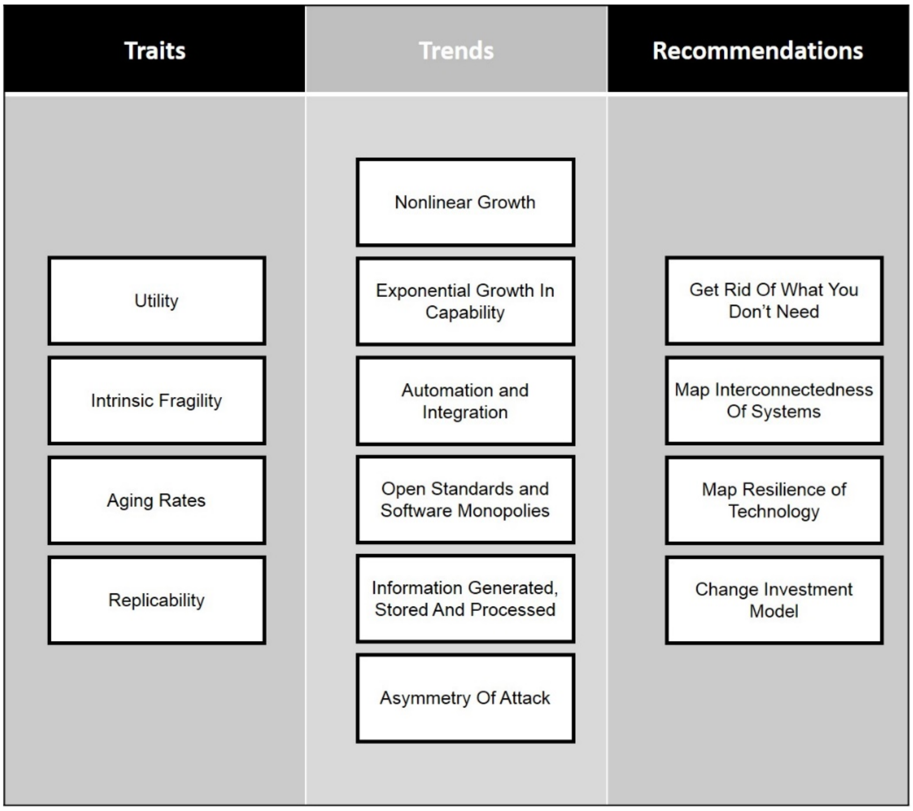
Map Interconnectedness of Systems: As discussed throughout this report interconnectedness characterises modern maritime operations and the wider globalised world. An apparently innocuous action in one system can cause strategic shock throughout other systems, even those which are not directly connected. This report recommends that resilience of technology is mapped in maritime infrastructure. This is an enormous task which will require understanding of highly complex (and sometimes sensitive) systems across the full spectrum of maritime operations. The objective of this study is to identify potential nexuses at which strategic shock could emerge.

Map Resilience of Technology: Mapping the resilience of technology in the maritime environment is highly important. The objective of this study is to understand weaknesses in maritime systems in order to bolster resilience in those areas and identify wastage in areas which are already highly resilient. This study should demonstrate systems which allow platforms or other infrastructure (such as ports) to operate even when they are disabled by error or attack.

Change Investment Model: The whole maritime industry must reassess its spending on long term platforms. Low cost, low skill and wide spread cyber attacks will end the era of long life platforms. Ship builders especially must consider whether it is right to spend billions of pounds on platforms and physical defensive systems when they have the potential to be nullified by a single well informed individual, thousands of miles away, with an internet connection and a few browser tabs open. Money may be better spent in cyber offence and defence. Another question that should be asked at the dawn of the age of cyber weaponry is – will you always need to be at sea to secure and exercise command in it?

Furthermore the timeline of platform development will need to be reconsidered. Projects which are developed over a long period will be designed with software which is far out of date by the time it is completed. A full assessment of the impact of this and what to do to mitigate the security risk which arise is recommended.

Conclusion



Traits	Trends	Recommendations
	Nonlinear Growth	
Utility	Exponential Growth In Capability	Get Rid Of What You Don't Need
Intrinsic Fragility	Automation and Integration	Map Interconnectedness Of Systems
Aging Rates	Open Standards and Software Monopolies	Map Resilience of Technology
Replicability	Information Generated, Stored And Processed	Change Investment Model
	Asymmetry Of Attack	

Figure 5: Summary of Traits, Trends and Recommendations in maritime technology

Technology will remain a central aspect of the maritime environment. Technology will grow and develop and become even more integral to our daily and professional lives. The benefits which technology will provide for future operators in the maritime environment are hard to predict but they will lead to new opportunities. They will also lead to new threats.

By actively investing in research into the interconnectedness and resilience of systems we will develop a clearer picture of the challenges we face in the maritime environment based on our need for technology. In addition good practices using technology, such as getting rid of what you don't need will reduce the chances of error or malicious attack. Most importantly but also must risky is the change in investment model for those at sea.

The maritime environment is expensive. In years gone by only those who had the capacity to build expensive ocean going vessels had the ability to secure sea lanes and exploit the maritime landscape for profit. Today ocean going vessels are extremely expensive creating a barrier to entry in the environment, this trend continues as technology breaks new ground in the capabilities of platforms. However for the first time in maritime history the positive correlation between capital spent and power is undermined, cyber attacks are low cost alternatives to physical attacks which have the ability to cripple maritime operations.

People

Even in the most secure computer systems there is a vulnerability which cannot be patched, corrected or rewritten. The human being is highly fallible and easily manipulated. They are also capable of free and critical thoughts which might lead them to breach security procedures or break the law in the name of their cause.

This section discusses the key traits which must be considered when exploring the role that people play in the malicious use of computer systems, future tends which will change how people perform cyber operations in the maritime environment and recommendations for mitigation and further research.

Despite the proliferation of highly advanced malware (such as Stuxnet, Flame and Shamoon) many cyber attacks do not target the platform itself. Targeting a platform requires intelligence including the intricate design of the hardware and software used in that environment. Once that intelligence is gathered malware must be tested in an identical environment to ensure that the attack will work. In the case of personal computing systems gathering intelligence and testing the attack is low cost and relatively straight forward, Microsoft's operating systems are very easy to come by. But such attacks are combatted by teams of developers and anti-virus specialists. It can be much easier to bypass technical elements in favour of targeting the people within the system.

The most famous and simple of such attacks is the Nigerian Lottery email which has become a piece of information era folklore. In this attack the victim receives an email informing them that they have won the Nigerian Lottery and that they should reply with their bank account details if they wish to claim their prize. Of course in this attack there is no prize. The attacker has obtained a long list of active email addresses and used a technique called phishing to capture financial information which can be used for criminal gain. While this is a primitive form of attack it is effective, more recent and sophisticated phishing attacks targeting websites of banks have demonstrated up to 45% effectiveness.

Social engineering, deception, identity theft, bribery and blackmail have been employed effectively online since the dawn of the World Wide Web. Today political and criminal actors such as hacktivist groups and cybercrime gangs regularly use such attacks against private enterprise and government departments around the world. In 2013 the defacement of the Associated Press twitter account, facilitated by a series of social engineering attacks carried out by the Syrian Electronic Army, led to a brief $140 billion drop in the value of the Dow Jones. Because of the interconnectedness of today's globalised world attacks which appear to be limited can have cascading and unpredictable effects.

However threats do not only come from outside agents. As Edward Snowden and Bradley (now Chelsea) Manning have proven the insider is as much of a threat as adversaries outside. Both of the individuals mentioned here used their trusted position within their organisations to capture sensitive information and distributed it openly online.

In the maritime environment people interact with computer systems extensively. Whether that is a ship's navigation system, a drilling rig, a ballistic missile system or something as mundane as employee records. At every intersection of man/woman and machine there is the possibility for error, manipulation, coercion or sedition.

Key Traits

Information Rich Society

Open Sources of Information: Information is freely available online about any subject. Previously finding data or instructions involved going to a library or finding an instructor. Today information about every topic (including how to launch social engineering and technical attacks) is now available online, nicely compiled by search engines. The World Wide Web was designed to make information easily accessible and the underlying structure of linked pages in a web structure continues to make information gathering easier than ever. Today private enterprise, individuals and communities endeavour to digitize knowledge for the good of mankind or in search of profit. A highly successful example of such endeavours is Wikipedia.

What is most astonishing is that such information is free to the user. While there is a cost associated with connectivity, this cost is restricted to the device used to access the web and the connection used to transfer data. Information which was once stored in private archives or the syllabus of expensive degree programmes is now accessible to anyone who has access to a data connection.

The maritime environment has its own open source information which could easily be used by malicious actors targeting the human element of computer systems, for example the AIS system which tracks ships locations in near real time. Or enthusiast forums such as Rum Ration - The Royal Navy Network which contain a wealth of intimate information about the maritime security environment. The Information Rich Society provides adversaries with unprecedented intelligence gathering capabilities simply by using Google.

Social Media: Social Media and the function of sharing personal information with other internet users have become common place. Individuals are offered the opportunity to communicate with their contacts online or to connect with new, unknown individuals through sites like Facebook, Twitter and LinkedIn. Social functionality is used for more specialist social activities by dating sites and enthusiasts networks.

Social media sites display the personal information users submit, forming an aspect of the individual’s online persona. This information can include name, address, phone number, email address, connections to other social media sites, media such as photographs and much more. The security of such information varies from site to site, some display all the information they have on a user for the world to see and some have very strict privacy rules which ensure only those the user allows can see their information.

Today it is possible to use search engines to quickly find the online presence of individuals using their social media accounts and piece together a picture of their lives, their preferences and their habits without having ever come into contact with them.

In the maritime environment social media can be used to track platforms and individuals through the data they produce. This data could come in the form of status updates informing concerned family and friends of a crewman’s location. Or details of an upcoming event which an individual is planning on attending. However the most important function of social media from the point of view of an attacker focusing on the human component of a system is how individuals are connected. Friend and contacts lists allow attacker to build up a picture of acquaintances, colleagues, friends and family members for use against the target maybe in the form of an identity theft attack or in the form of blackmail - especially effective when an individual is thousands of miles away from his or her loved ones. Each connection in a social network is a potential vector for social attack.

Ideology: As a result of the Information Rich Society ideologies and values have developed which shape the way the internet is used. The availability of free information and the flat rather than hierarchical nature of the internet's communications structure produces values of equality which hierarchical societal structure did not. Today for example it is possible for an individual to converse with politicians, celebrities, businesses and people from every corner of the globe in real time. Some online communities such as the hacktivist collective Anonymous are militant supporters of this equality of communication.

With information freely available, the ubiquitous sharing of valued personal information and the lack of hierarchy associated with the internet the concept of ownership has changed dramatically in the digital world. The most explicit example of this has been the music industry which has had to adapt its model of monetization away from physical sales and into digital downloads and music streaming applications such as Spotify. The internet has created egalitarian values which undermine long standing concepts of digital rights and intellectual property. Anonymous' first operation was a reaction to the suppression of a leaked video which depicted the Church of Scientology in an unflattering light. The Church attempted to remove all reference to the video from the web. To members of Anonymous information which had made it online through design or error was everyone's property whether the creator wanted it to be or not. Concepts of equality and new understandings of information sharing and ownership form the political motivations for many insider attacks.

The maritime environment is characterised by economic competition, managed environmental impact and naval powers. Activist organisations such as Greenpeace have invested highly in disrupting activates in the maritime environment which are contrary to their world view. The ideology of the Information Rich Society normalizes the idea that sensitive information of a business or military nature is in the public's interest and therefore public property. This forms a motivation for attacking maritime assets.

Anonymity: The internet allows users unprecedented anonymity. This phenomenon is perhaps best illustrated by the famous New Yorker cartoon "On the internet nobody knows you're a dog."

Anonymity allows internet users to make conscious decisions about the persona which they present online. It also allows users to present fictional personas or to impersonate others with ease. The use of identity theft and impersonation

Figure 6: "On the internet, nobody knows you are a dog" - The New Yorker

facilitates the kinds of social engineering attacks discussed above. As a result trust is central to internet communication.

Anonymity combines with the Information Rich Society in interesting ways. Firstly criminal and morally suspect behaviour become more appealing online. From hate filled debates in the comments section of online videos to fraud, piracy and data theft – the ability to hide behind an alternative persona or to use a proxy to hide your location reduces the likelihood of reprisal. Furthermore the inability of the attacker to see the direct impact of the attack on the victim takes a significantly lesser psychological toll.

Secondly the values and ideologies supported by the Information Rich Society make anonymity a trait which is highly prized. Initiatives which have been seen to counteract individual anonymity online have been met by severe resistance in many online communities. In 2012 the SOPA bill was highly criticised by anonymity activists and motivated hacktivist organisations to launch cyber attacks against the US government.

Anonymity makes the internet a forum for free thought and expression, the ultimate realisation of a liberal society. It also facilitates criminal activity from petty fraud to attacks on a national security scale. In the maritime environment anonymity makes attacking the human element of computer systems easy (facilitating deception), morally justifiable (the impact of the attack is hidden) and low risk (you might not get caught).

Connectivity: Connectivity is a prerequisite for cyber attack including those which target people rather than platforms. The internet is comprised of networked machines which store and transport data through cabling which transfers information at the speed of light. This infrastructure is both global and resilient.

The global nature of the internet means that attacks can come from any location. Today the proliferation of mobile data networks (GSM, 3G and 4G) and mobile devices which are comparable in capability to desktop computers means that individuals can be targeted by social engineering attack emanating from isolated locations, locations beyond jurisdiction or indeed from the middle of the ocean. Whereas previous forms of electronic warfare required some degree of geographical connection social engineering attacks can occur wherever the attacker and the target can both send and receive data.

Such networks are highly resilient. Once again the initial concept of the internet facilitates this. The network is highly distributed allowing information to pass through any number of variable routes from the host to the client machine. What is more the reliance of modern operations on the internet means that it is not necessarily in the best interests of an organisation being attacked to simply unplug from the internet. As a result using disconnection as a form of mitigation is fraught with difficulties.

In the maritime environment connectivity is a perennial issue. Modern navies and maritime businesses require up to date connectivity in order to receive and send command and other data such as weather patterns or course changes. For many years crews were isolated from the rest of the world while at sea but technology is changing that. Already US naval ships have their own Wi Fi networks and private firms are attracting the best crew they can by offering compressive connectivity to employees. This means that new individuals who were once unreachable are now targets for remote attackers.

Cost Asymmetry: It is now possible to for an actor situated in the UK (or anywhere else) to influence the commanding officer of a multimillion pound platform situated in the Indian Ocean and render that platform inoperable. This attack can be carried out at near zero cost – using the benefits of the Information Rich Society. With very little technical knowhow – using the instructions found in open sources of information or experienced contacts found through social media.

An example of a way in which individuals can be manipulated online at low cost has been researched by Monica Whitty. Whitty looked at a type of online fraud which employed the promise of a meaningful real world relationship in order to extort money from the target. Whitty believes that nearly 230,000 people fell victim to romance fraudsters in the UK alone. This is a prevalent and effective kind of online social engineering. Of the 592 online romance scam victims registered in the UK in 2011 203 of them lost more than £5,000. This example is not specific to the maritime environment but it does illustrate a vector of attack which would be highly effective at sea – a romance confidence scam targeting isolated individuals in powerful positions.

A motivated individual anywhere in the world now has the potential to cause damage to operations in the maritime environment. For the first time maritime operators, in particular navies are at an asymmetric disadvantage. No amount of money spent on technical fixes will cure the human propensity to be tricked, blackmailed or to further their own political ends.

Trends

Information Availability: Every year more information is becoming available online and the thirst for this information will continue to grow as business and personal lives become reliant on the Information Rich Society. How this information is searched or used may change but the ubiquity of open sources of information is highly likely to remain. More interesting will be what happens to the sharing of information in the coming years. Whether social media sites such as Facebook have longevity is hard to say but the desire for human beings to connect with one another and to share information will certainly remain. The question is what will the sharing of personal information look like?

There are two extreme possibilities in this space. Firstly, people will share every element of their lives through new technologies and new online portals. For example wearable medical trackers are currently in development to track a person’s health remotely. When combined with already available wearable GPS systems and social media it is possible to imagine a future in which users share their real time medical and locational data. In this extreme example it would be possible to search for an individual and see their location, heart rate, blood oxygen, how many steps they’ve taken that day and many other variables. Of course the second extreme may be a response to current fears over online safety. Future generations may see that current social media users share too much of their lives and respond by shunning social media finding more secure, less intrusive forms of communication. In this case groups of users who know each other in their daily lives might communicate through encrypted devices and over trusted networks.

The basis on which personal information is shared will also have two extreme possibilities. Current social media users are becoming awake to the fact that social media monetise their user’s personal information by selling targeted advertising space. This is a market which is growing enormously and which is underpinning new models of business. In the first extreme possibility users will accept this as the price they pay for the use of free online social media, they will give up all of their information for free in order to get targeted advertisements and use the service for free. The second extreme may involve users putting a premium on their personal information. Personal information is vital to the survival of social media and these enterprises or the next generation of these enterprises will pay a premium for user's information in order to make advertising profits.

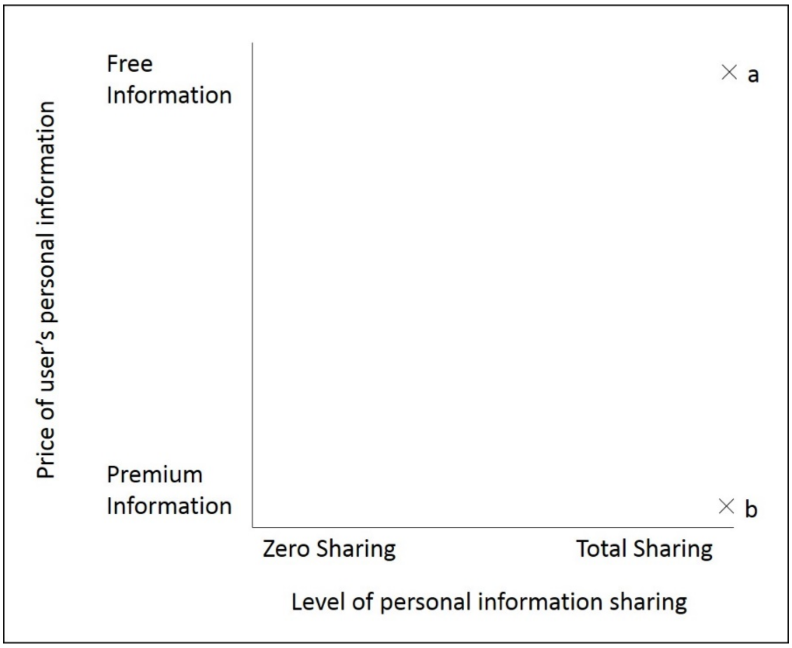

Price of user's personal information
Free Information
Premium Information
a
b
Zero Sharing
Total Sharing
Level of personal information sharing

Figure 7: Possible futures of information sharing

When thinking about personal information in the future we can produces a two axis framework which will allow us to consider different possible futures. Somewhere within this two dimension space is the way in which sharing personal information will take place in the future. In this figure position "a" represents a future in which users are happy to give away all of their personal information freely. In position "b" users are happy to share all of their information at a premium.

Connectivity: Connectivity will be the next key trait which will impact the human element of cyber operations. Connectivity is essential for the globalized world it will become ubiquitous throughout the world allowing new markets and new innovators to grow and to share. Ronald Deibert suggests that the most significant change in the internet's history will come in the coming decades as the next billions people, mainly from Asia are connected to the internet.

What is more the cost of this connectivity will decrease dramatically. Some efforts are already being made to reduce the cost of connectivity to zero in some regions. Both in terms of networking and in terms of affordable devices. These factors combined will mean that every individual on the planet can have access to the internet and therefore to every other individual on the planet, making the availability and easy of social attack a pandemic problem.

In the maritime environment even the most isolated crew will be connected to the rest of the world through global wireless networks or unforeseen technical fixes. This will provide more up to the minute information for decision makers and perhaps revolutionize industries such as shipping, fishing and mineral extraction. However it will also open the door to social attacks on previously isolated individuals from a much greater number of potential attackers.

Recommendations

Further Study: There must be more studies into how adversaries can use the traits and trends above to cause damage in the maritime environment. This study should detail how and why an attack might take place, identify those to be most likely and most easily attacked and when operators in the maritime environment might be most at risk (during demonstrations, conflicts etc.)

Education: In order to mitigate social engineering attacks education is extremely important, this education should be based on the studies suggested above.

The national curriculum should take online manipulation serious. School are being directed to deal with cyber bullying after a number of high profile case, this direction should extend to information about general online safety in work and in the personal lives of the future generation of maritime actors.

Maritime operators take health and safety extremely seriously. Working in one of the most inhospitable environments on earth requires a serous approach and a keenness for detail in promotion of health and safety. Such an approach should be applied to online safety training. Every individual should be educated on how their online presence may cause a vulnerability for their employer and in how to identify and react to a cyber threat in the same way they would to adverse weather or a fire at sea.

Procedures: Cyber attacks to platforms and maritime infrastructure are currently an inevitability. The effect of these attacks are uncertain and difficult to predict. The same could be said of kinetic attacks and physical accidents. In these cases there are detailed and well-rehearsed procedures in place to protect human life and critical systems. Such procedures must be created for or adapted to cyber attacks. Drills should be run where multiple systems are shut down to simulate attack or where operators are fed spoofed information.

Maritime operators such as navies and private enterprise must have policies in place to protect their employees and their employee's social networks should they become a target for an attack. There must be a well-known and effective procedure should an employee come under attack either direct or through their social network. For example, a commanding officer should know exactly what to do, who to talk to and how their safety will be guaranteed should an adversary capture private or embarrassing information about that individual and blackmail them with it.

Create Resilience: It must be understand that social engineering attacks will happen. In order to mitigate this operators must create resilience with backup systems.

One way of doing this to restrict access for employees. Only allowing user's access to the system they must have to be effective.

Operators must create a working environment which is on the lookout for insider threat. And have a media response and legal policy for insider attacks when they happen.

Conclusion

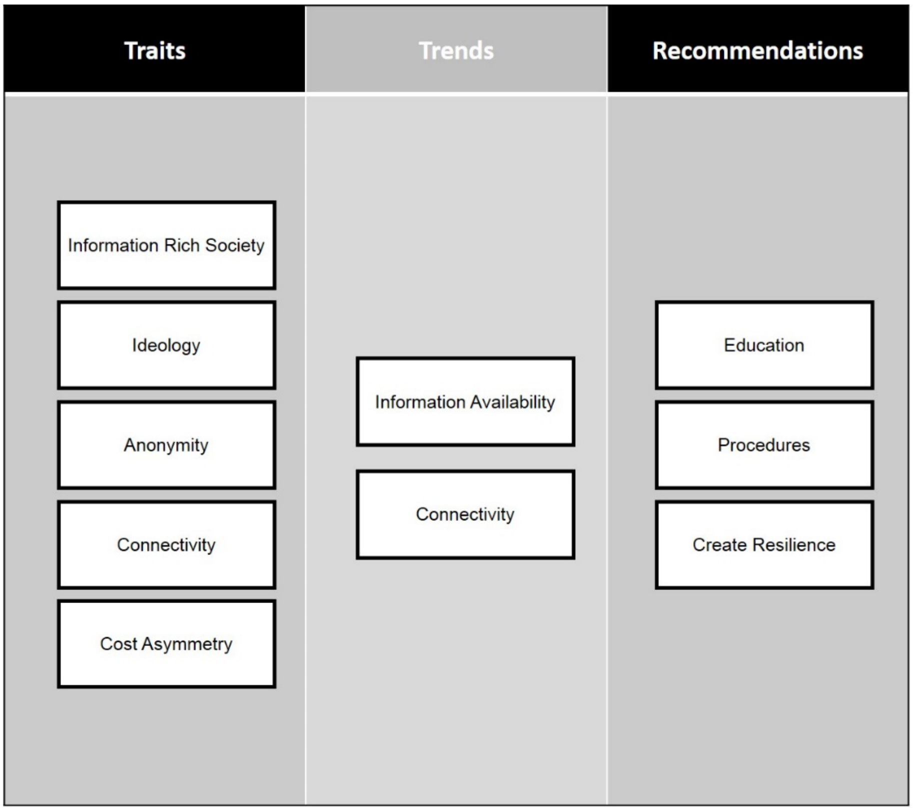


Figure 8: Summary of Traits, Trends and Recommendations pertaining to people's role in maritime cyber security.

People form a critical vulnerability within computer systems which endangers information, the platform itself and those who use the system.

The insider threat will be present for the foreseeable future and is likely to become more intense as our Information Rich Society normalises egalitarian attitudes towards intellectual property and information sharing. Government and industry will both be affected by data leaks as official and industrial secrets are highly prized either for financial, political or ideological gain. Both sectors will also be affected by insider attacks on systems which, in the maritime environment, could have an extremely damaging effect on national and international stability. The disgruntled systems administrator or engineer will continue to be a security threat as platforms become more capable and therefore more integral.

Likewise, the outsider threat of social engineering will persist. Adversaries will find new and innovative ways to disrupt operations using the personnel within the target organisations. Online anonymity will persist either by way of ideological pressure stemming from the Information Rich Society (such as The Right to be Forgotten) or by way of technical solutions such as dark networks. This persistent anonymity will continue to allow adversaries to use social engineering techniques.

In the maritime environment ubiquitous connectivity will make once isolated individuals targets for outsider attacks. Where limited connectivity or completed disconnectedness was once enjoyed at sea, drivers of change such as Google (Project Loon) and the Facebook backed Internet.org are pushing for global connectivity. It is likely that they will achieve this goal as the potential for profit is so vast. Individuals will accept ubiquitous connectivity as a fundamental principle of the Information Rich Society and maritime organisations will encourage such connectivity as a means of attracting the best personnel to their operations. Indeed high quality employees will expect access to their digital persona wherever they are. Global connectivity will mean that individuals on platforms will generate data on a daily basis which could be used against them by an outsider employing social engineering tactics. This data will also offer adversaries a continuous window of opportunity to carry out social engineering attacks.

Ubiquitous global connectivity will have another impact on maritime operations which is more difficult to predict. There is likely to be a polar shift in the demography of the internet as connectivity becomes available in new areas, especially throughout Asia. As the next billion users come online the Information Rich Society will be added to as new content, customs and ways of using data are generated by new users. Today the internet is dominated by its innovators in the West but in the future this will not be the case. The digital centre of gravity will shift eastwards. In the maritime environment this means that outsider threats will come from new sources, in particular once isolated communities who are adversely affected by globalised maritime activity and mineral extraction will be cyber capable.

With ubiquitous connectivity in new regions, including at sea, information will be generated at an unprecedented rate and due to technological innovation unprecedented quality. This information will be utilized by outsiders to create a more complete profile of targets which will proliferate well targeted and highly effective social engineering attacks. This information could take the form of personal information as generated through social media or in the form of open source information such as AIS data today.

The cost of social engineering attacks such as phishing, identity theft, and online blackmail and bribery will remain extremely low. The cost of connecting will be lowered by the desire for technology firms to connect with the next billion internet adopters. These adopters will have access to the Information Rich Society and will become potentially dangerous actors with an ability to disrupt multimillion pound operations with little outlay.

The potential damage caused by outsider social engineering in future should necessitate a fundamental reimagining of private security and national defence spending. Navies such as the Royal Navy will continue to find a role for large and costly ocean going platforms in order to secure sea lanes vital for global commerce and national prosperity. However the potential for a near zero cost, highly informed and sophisticated social engineering attack, targeted at crew who are connected at all times, by an adversary who is anonymous and remote; forms a threat which is asymmetric and unprecedented in naval history.

Maritime cyber security logistics: 2035

Logistics is fundamental to modern economy and security. The ability to move people, food and machines across territory increased the scale and intensity of the global economy and modern warfare. The etymology of logistics refers to the skill in arithmetical calculation. For any maritime organisation logistics is vital.

Indeed many maritime organisations are in the business of logistics whether that is shipping, transportation or resupply. In this way maritime logistics is essential for the vitality of national economies and predicates naval organisations whose primary purpose it is to keep maritime logistics secure in the name of national security.

Specifically in the military sense logistics facilitate the transformation of war from an event that is prone to various vulnerabilities - lack of food, disease, shortage of troops - into a process that is shaped by calculation and planning. Militaries can plan for long term operations, sustaining operations that are world-wide. Militaries can include into their planning the possibility of accidents and strategic surprises. Logistics makes the military resilient: fast, efficient and flexible. For navies, especially blue water navies, resilience far from friendly waters is a primary concern.

States in a global economy depend on a logistics that makes possible the import and export of food, energy, goods and technology. Without the ability to calculate what a state needs for the short, medium to long term - and the infrastructure to enable the import and export of goods - states become potentially vulnerable to a number of social, economic and security hazards. States need to be able to plan for the long term – and put in place the logistics to ensure the movement of everything that sustains life in the modern world.

From a private business prospective logistics is central to keeping platforms in operation whether that is a containership, a mineral extraction rig or an LNG carrier. The cultivation of new and existing markets relies on the ability to sustain life and machinery at distance for a prolonged period of time. In today’s ultra-competitive economy the desires for logistic efficiency is more vociferous than ever.

Military logistics have been fundamental to the development of the logistics that has shaped modern economies and industries. But in the 21st century the spaces of innovation in logistics is in the commercial realm. For example, corporations like Amazon operate in a highly competitive market where the strategic objective is not simply to use new technologies to cut costs – but to create a logistical infrastructure that is so fast and efficient that it can compete with physical retailors both in terms of cost and choice. Such ferocious competition has caused business and industry to lead innovation in logistics, innovation which was once the terrain of the military.

Maritime logistics in 2035 will, as it is today, be dominated by computer systems. Skill in arithmetic calculations is and will continue to be derived from complex machines and software. As with all computer systems maritime logistics in 2035 will be comprised of Information, Technology and People. In order to discuss what this might look like trends in the three elements of maritime logistics computer systems will be explored, using these trends as a basis three instances of short future fiction will be presented as a system to consider future vulnerabilities in maritime logistics.

Key Trends

Information

Smart Consumption: Advances in smart data enhances the capacity of states to become as efficient as possible: the drive to efficiency is enhanced by the desire to build smart homes and smart cities that are able to shape consumer behaviour. Following this trend ports and platforms will become smart. New technology will produce more data than ever before and this data will be utilized in new ways. This will lead to efficient logistics but it will also form a new avenue for cyber attack.

Technology

Automation: Platforms, in a drive for efficiency, will integrate autonomous systems to track, dispense and provide logistical support. Ports will become more autonomous based on advanced and ever more resilient software and new technologies.

Unmanned Systems: Unmanned systems will become important in both the production and distribution/delivery of products. The impact of this will be twofold: 1) unmanned systems will provide logistical support faster, more efficiently and over greater distances. This maybe in the form of drone resupply. 2) Unmanned platforms will require far less logistical support. If trends in the development of unmanned platform design (such as submarine and surface drones to fulfil military and industrial roles) continue the burden of supporting life at distance using logistics may be overcome.

3D Printing: In both the military and commercial realm 3D printing will become increasingly central to logistics. Certain products will not require movement from factory to port to distribution by sea or air because the will be printed when a product is needed. In 2014 we already have the ability to print complex and high quality items with moving parts (for example NASA are testing 3D printed parts which to replace traditionally manufactured components which can withstand 6,000 degrees Fahrenheit).

People

New Organisational Structures: New technology and new uses for technology and information will necessitate new organisations. The lines between states, companies and networked organisations (terrorists, criminal organisations etc) will blur. The resulting toll on human beings within logistical systems at sea is difficult to determine but it will have a severe impact on their personal and political ideologies. It may be that future maritime employees have more allegiance to the information rich society at large than a nation state or employer. This means that the insider threat will be more apparent than ever.

Jobs: Despite advances in unmanned technology and automation people will still form a cornerstone of maritime logistics operations. People will be required to develop, oversee, maintain and command computer systems. People will therefore continue to be a vulnerability within computer systems, indeed it is possible that a single individual be given such wide ranging command of autonomous systems that their error, manipulability or malfeasance could be more devastating than ever before.

Future Fiction –Scenarios for Maritime Logistics in 2035

Ideal Outcome

Renewable energy, robotics and 3D printing has enhanced the energy security and independence of European states. The anxiety about new technology resulting in high unemployment has not materialised: the technology has generated a new generation of high skilled jobs in the maintenance and supervision of the infrastructure that are transforming life around the globe.

Global events have less impact domestically. The anxiety about rising food costs leading to unrest has been lessened by the production of bioengineered food around the world, aided by the rich states. The political and social unease in Europe about migration has faded as citizens have embraced the argument that Europe depends on migration to sustain economic vitality in a world economy where growth has made Europe just one of many prosperous and dynamic regions.

Commercial and military logistics are shaped by efficient unmanned systems. It is common for armed forces on humanitarian missions to print replacements for vital technology: the ability to use a 3D printer is as an essential part of training for all armed service personnel. The future soldier depends on a growing number of technologies that enhance the capability of the smart soldier: the sophisticated technologies that 3D printers cannot deliver are delivered by more traditional means, although certain craft are unmanned and in some terrains drones are used to distribute resources.

In the 2020s criminal networks became skilled at hi-tech logistical crime. But by 2035 criminal activity in the distribution and transportation of foods in increasingly unmanned processes is easily detected. A great deal of effort had been placed in detecting insider threat in the management of the technology essential to logistical support.

Mixed Outcome

The benefits of 3D printing and bioengineered food are mixed. Some people are uncomfortable about eating lab grown good and will pay slightly more for imported ‘real’ food. There are still technical issues with the printing of 3D goods: the consumption of goods made overseas is still fundamental to the global economy.

In military operations overseas there is growing concern about the use of 3D printing. There have been some highly publicised cases of subtle sabotage in designs used for products that have endangered armed personnel. During one humanitarian intervention an unspecified actor managed to disrupt the supply chain of vital logistics by attacking a small but vital link in the complex chains that produce armed vehicles that were being retrofitted with new defences against innovative tactics employed by local insurgents.

In commercial logistics the rerouting and ‘skimming’ of certain goods by criminal organisations is widespread. But the small scale nature of these problems is not serious enough to result in a radical rethink of logistics. The most serious disruptions occur because of human error, some small events cascade through the global logistics chains causing wider issues. The consensus is that while there is still the potential for crime and accident in both the military and commercial realm the benefits of new technologies outweigh the costs.

Worst Case Scenario

Growing social and economic unrest in states that manufacture consumer goods like clothes is able to shut down ports through a mixture of both old and new techniques. A combination of factory blockades, attacks on platforms and the digital disruption of ports is constant problem for multinational corporations. Some of the unrest is organised by political parties in rival territories who use the information rich society to follow new vectors of attack. But the impact can be costly for multinationals who deal with a commercial threat horizon that constantly produces new logistical problems at every stage of the journey from factory to consumer.

The risk posed by attacks on the new logistics is no longer negligible. The delay and disruption caused both by sabotage and crime is major cause of concern to both the military and the commercial world. The maritime environment is under constant threat as private information is necessarily released into the public domain. 3D printing has only worked for the most basic objects. Criminals constantly devise new ways to undermine the logistics that is essential to security and economy. In an economy that is intensely competitive finding innovative and non-attributable ways to slow down your competitor is sometimes an attractive option.

Conclusion

Logistics is at the intersection of Information, Technology and People. It is a strong example of the kinds of problems that will be faced as technology developed in the maritime environment. New technology is necessitated by human endeavour. This leads to new information produced and used and new relationships between people and machines. Logistics at sea is a matter of profit or loss, of success or failure and of life or death. Attacking computer systems via information, technology or people will be an extremely appealing mode of operation for adversaries in 2035.

The future of logistics is reliant on developments in computer technology. A less widespread but equally valid conclusion is that logistics is reliant on the developments of computer security. In order to create such security and therefore resilient logistics, measures must be taken to mitigate the threats outlined throughout this report.

Conclusion

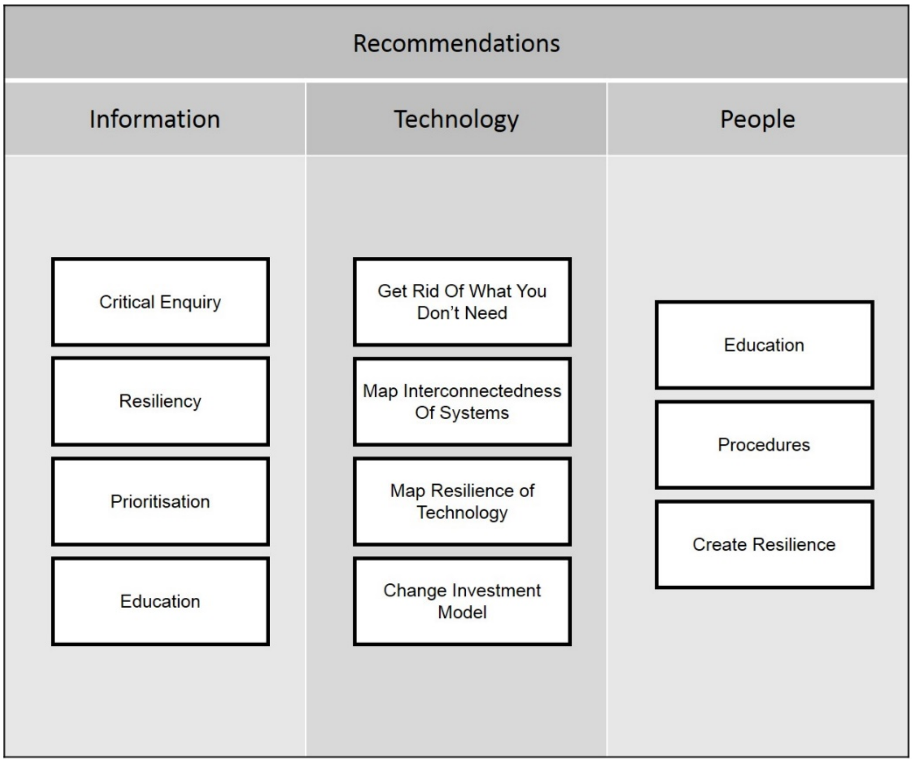
This report has developed a framework for thinking about cyber security in the maritime domain. That framework consists of three elements: Information, Technology and People. Each element is as important as the other and must be considered together in order to understand the challenges within the maritime environment.

The maritime environment is radically changing as it adopts new technology and ways of working in order to provide efficiency gains and reduce costs of operations. The framework set out in this document has developed through discussions with key stakeholders and represents the core areas identified during exploratory discussion sessions. While perhaps not complete it does provide a repeatable methodology to explore future scenarios where cyber security and the maritime environment intersect. It also provides a useful mechanism to explore how the maritime environment is being affected and changed by the introduction of digital technology.

All computer systems include information, technology and people and at all stages of their interactions and operations there is the potential for danger. The acknowledgement that danger exists within computer systems should not be misinterpreted as a suggestion that the use of computer systems should be restricted. Indeed the benefits which computing has delivered to the maritime environment so far have increase profits, lead to a more integrated awareness of maritime operations, opened new markets and most importantly saved lives. Computer systems in the future hold potential to change human existence for the better, they should be embraced but designed and operated with security as a primary consideration.

It is also clear that the study of cyber security must be holistic. In order to discuss cyber attacks in the maritime environment one must look for evidence, precedence and developments outside of the maritime domain. The internet transcends geographical boundaries. In order to address the specific issues of a maritime operator or the potential vulnerabilities within the maritime environment in any meaningful detail (in order to produce step by step recommendations in order to mitigate tangible and urgent threats), testing and analysis must target individual systems. Without mapping the interconnectedness of a system and mapping its resilience, without a picture of the people and the information which make up the system it is not possible to mitigate threats effectively.

Nevertheless this report has been able to contribute key recommendations which should be addressed immediately in order to reduce the cyber threat in the maritime environment.



Recommendations

Information	Technology	People
Critical Enquiry	Get Rid Of What You Don't Need	Education
Resiliency	Map Interconnectedness Of Systems	Procedures
Prioritisation	Map Resilience of Technology	Create Resilience
Education	Change Investment Model	

Figure 9: Recommendations Summary

Writing Team

About the Authors

Oliver Fitton: PhD Student in Politics Philosophy and Religion

Oliver Fitton is researching for a PhD in International Relations in the department of Politics, Philosophy and Religion at Lancaster University. His research focus is cyber attacks using social engineering techniques in conflict, how and why individuals turn to digital technology for political and other ends.

Daniel Prince: Associate Director for Business Partnerships and Enterprise at Security Lancaster

Daniel Prince is an associate director for Security Lancaster, managing business partnerships and enterprise. Prior to this he was the course director for the multi-disciplinary MSc in Cyber Security teaching penetration testing, digital forensics and information security risk management. Daniel holds a PhD in Computer Science and has worked on projects with numerous large technology companies such as Cisco and Microsoft.

Mark Lacy: Associate Director for Security Futures at Security Lancaster

Mark holds a PHD in International Relations and prior to his work in Security Lancaster he was part of a team that set up an inter-disciplinary theme year on New Sciences of Protection: Designing Safe Living' which brought together designers, technologists and social scientists to collaborate in various ways on emerging security problems and their social, economic and political impacts.

Basil Germond: Lecture in Politics Philosophy and Religion

Basil is a Lecturer in Diplomacy, Foreign Policy and International Relations Theories, and Programme Director for our MAs in Diplomacy. He specialises in naval affairs, maritime security and maritime geopolitics, as well as in European security and the geopolitical actorness of the EU. His research interests cover the maritime dimension of the European Union, maritime security, current naval developments, maritime strategy and maritime geopolitics, the European Union's geopolitics, energy security and the Arctic region, and borders and frontiers in IR.

Bibliography

Olson, Parmy. We Are Anonymous, (Back Bay Books: New York, 2012)

Rice, David. Geekonomics, (Addison-Wesley Professional: Boston, 2007)

Whitty, Monica T. “Anatomy Of The Online Dating Romance Scam”, Security Journal, (2013)

Buchanan, Matt. “AMD Phenom X3 Triple Core Processors Are Crippled Quad Cores in Disguise”, Gizmodo, 27th Match 2008, Available at: http://gizmodo.com/373185/amd-phenom-x3-triple-core-processors-are-crippled-quad-cores-in-disguise, [Accessed: 6th August 2014]

CBS News. “Who is the Dow Jones-wrecking Syrian Electronic Army? A hacker explains”, CBS News, 1st May 2013, Available at: http://www.cbc.ca/news/technology/who-is-the-dow-jones-wrecking-syrian-electronic-army-a-hacker-explains-1.1330203 [Accessed: 8th August 2014]

Danchev, Dancho. “How many people fall victim to phishing attacks?”, Zero Day, 4th December 2009, Available at: http://www.zdnet.com/blog/security/how-many-people-fall-victim-to-phishing-attacks/5084 [Accessed: 6th August 2014]

Nguyen, Tuan An. “Unlocking AMD CPU Cores Safe Say Mobo Makers”, Tom's Hardware US, 5th June 2009, Available at: http://www.tomshardware.com/news/amd-phenom-athlon-cpu,8012.html [Accessed: 6th August 2014]

RT. “Internet Strikes Back: Anonymous’ Operation Megaupload Explained”, RT, 20th January 2012

Shimpi, Anand Lal. “The Phenom II X4 810 & X3 720: AMD Gets DDR3 But Doesn't Need It”, AnandTech, 9th February 2009, Available at: http://www.anandtech.com/show/2721 [Accessed: 6th August 2014]

Shrout, Ryan. “Intel Core i5-3350P Ivy Bridge Processor Review - No Integrated Graphics”, PC Perspective, 26th November 2012, Available at: http://www.pcper.com/reviews/Processors/Intel-Core-i5-3350P-Ivy-Bridge-Processor-Review-No-Integrated-Graphics [Accessed: 6th August 2014]

Siddharth, Sumit & Doshi, Pratiksha. Five Common Web Application Vulnerabilities, Symantec, 27th April 2006, Available at: http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities [Accessed: 5th August 2014]

Security Futures' mission is to is create a space where we could develop innovative techniques to think about the future, techniques that draw together the insight and expertise of researchers working across different disciplines. In this collaborative space, researchers and other partner organisations have the freedom to explore questions about security and technology. But also to formulate the questions that we might need to start asking about the emerging trends in technology, society and security. A space where we can bring together people working on the cutting edges of technology, social, legal and political disciplines to ask questions about the world we live in. A space where we might begin to imagine new horizons and start to see the problems that

Security Lancaster delivers research and education that innovates and creatively challenges the way that individuals, organisations and societies secure and protect themselves. This is achieved via engagement and collaboration with governments and companies from a range of sectors. Our approach delivers the very best use-inspired and pure research alongside cutting edge education that delivers real impact. Current activities deliver ground-breaking research and postgraduate training through programmes as diverse as an MA in conflict, development and security and an MSc in cyber security. Security Lancaster works with Doctoral Training Centres actively researching security related areas and has recently been awarded Centre of Excellence in Cyber Security Research by GCHQ and the EPSRC.

This work was funded by Security Lancaster via the auspices of Lancaster University's Faculty of Science and Technology.

Science and Technology Business Partnerships and Enterprise

As well as working with a range of external partners, ICT and Security form part of a wider theme based team across Science and Technology at Lancaster who offer expertise in:

- Advanced Manufacturing
- Energy
- Environment
- Health & Human Development
- Quantum Technologies
- Mathematics and Statistics

Working in Partnership

Across the themes we form collaborative partnerships around these 5 key areas:

- Collaborative Research and Consultancy
- Training and Education
- Co-location and Secondment
- Student Placements
- Product Development and IPR

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Lancaster University, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

For more information on the research work that Security Lancaster undertakes and information on how you can collaborate with us please visit our website

http://www.security-centre.lancaster.ac.uk