70th International Astronautical Congress (IAC), Washington D.C., United States, 21-25 October 2019.

IAC-19-D5.4.3

New Internet Satellite Constellations to Increase Cyber Risk in Ill-Prepared Industries

Joel D. Scanlan[a]*, Jarrod M. Styles[b], David Lyneham[b], Margareta Holtensdotter Lützhöft[c]

[a] *University College, University of Tasmania, Churchill Ave, Sandy Bay, Tasmania, Australia 7005*, joel.scanlan@utas.edu.au
[b] *Cromarty Pty Ltd, 86 Charles St, Moonah, Tasmania, Australia, 7009*, jarrod.styles@cromarty.com.au & david.lyneham@cromarty.com.au
[c] *Department of Maritime Studies, Western Norway University of Applied Sciences, Postbox 7030, 5020 Bergen, Norway*, Margareta.Holtensdotter.Lutzhoft@hvl.no
* Corresponding Author

Abstract

The deployment of the Starlink, OneWeb, LeoSat and Project Kuiper satellite constellations will have a transformative impact on the availability of the internet globally. The existing satellite-delivered Internet access from providers is operated from geostationary orbit resulting in high latency connections, with limited bandwidth. The recently completed Iridium Next constellation is comprised of 66 satellites in low-earth orbit (LEO) and provides a maximum speed of 1.4Mbit/s bandwidth. This bandwidth is a fraction of the 100s Mbit/s and Gbit/s speeds within the proposed constellations of OneWeb and Starlink, each containing hundreds, and up to thousands, of satellites. These offerings promise global access, with low latency and high bandwidth. These platforms will be transformative in their impact on global access to the Internet, with many unforeseeable positive and negative outcomes. This paper will discuss what it suggests is a likely increase in cyber-attacks on ill-prepared industries due to the rapid adoption of highspeed Internet delivered through these proposed constellations. The industries we suggest are most at risk are those which are geographically dispersed; unable to currently attain reliable and fast Internet access and have existing legacy software systems with poor security. This will be explored within the context of the maritime and offshore industries as a case study, since they currently make use of the existing limited satellite connections for non-mission critical tasks but are looking to transition to shore-based control and increased automation of shipboard systems. The industry has not formerly been at great risk from cyber-attack due to geographic isolation and limited connectivity to the systems. However, the satellite constellations will enable them to have fast, high-bandwidth connections nearly anywhere on the globe. There are a range of industries, or at least sections within industries, that are ideally suited to utilise these new platforms that formerly did not need to be concerned about cyber-attacks, and as such do not have a strong security design culture. These will be contrasted to the much better-prepared networks, such as stock exchanges, that have been spoken of by providers as being an ideal use case. This risk is not the responsibility of the Internet providers, who in this case are the companies building these expansive constellations. However, it may be in their best interest to raise awareness among prospective clients in non-traditionally connected industries.

Keywords: Cyber Security, Satellite Internet, Maritime

1. Introduction

Network connectivity is a utility. The ability to communicate across vast distances has repeatedly transformed human activities across the last two centuries. Many new businesses and industries have grown from a simple change of communication technology coupled with a spark of creativity. However, with each leap forward in the ability to communicate, there has also been new opportunities for malicious users to leverage the technological advancement to their own ends, causing harm to other users.

The global cost of cyber-attacks is close to $600 billion annually, nearly one percent of global GDP, up from $445 billion in 2014 [1]. Large scale, government driven initiatives to counter this threat, such as the GDPR, have played a sizeable role in business awareness of these threats. It is projected that the benefit of IT systems to the global economy between 2010 and 2030 will be $130 trillion USD [2] and as they need to be protected in all sectors from cyber-attacks.

Satellites have been a crucial part of global network communication for 50 years. However, these systems are about to undergo a dramatic change, which could cause a paradigm shift for connected devices across the whole Internet. Current communication satellite networks provide connectivity that is both expensive and limited in speed and throughput. As a result, the vast bulk of all traffic is sent via terrestrial networks. The proposed satellite constellations, from multiple companies, each present a scenario where a packet of data could be most quickly and efficiently delivered via a satellite than by traversing the existing terrestrial fibre

networks. Such changes, accelerating the speed of communication globally, present an exciting opportunity to leverage the power of computation and networks in new ways. It can be argued that it will be a dramatic change, and one of the most important advancements in the underlying infrastructure of the Internet in decades [3-7]. However, as with previous advancements in computer networks, the risks associated with hacking activities could also be increased through bad actors targeting new systems using these advanced networks.

This paper will explore a history of networking paradigm shifts, highlighting security problems which have occurred with each generation. Following this, an overview will be presented of what is currently known of the technological change which will occur over the next decade, and then explore how this may then impact users of this new network in positive and negative ways. This will be explored within the context of industrial control systems, with a specific focus on the global maritime sector. Finally, the paper will discuss these possible impacts and what actions can be taken to mitigate some of the risks that could arise with this network advancement.

2. Cyber threats: a history

The proliferation of computer systems and networks since the middle of last century has had a dramatic impact on many industries globally. A large portion of the initial adoption of computers and networks was driven by military interests [8] which then led to their use within secure contexts and the development of computer security models to maintain the confidentiality and integrity of these systems [9]. However, since the mid-80s the primary focus of these systems has been outside of military contexts. Consequently, security of these systems has been relegated to a secondary or tertiary consideration with the primary concerns being in line with business needs and usability. This has resulted in breaches of security as new systems have been deployed without due concern given to user security. This paper is aiming to highlight that near-term developments in satellite delivered Internet will not only result in new, exciting developments but will simultaneously create opportunities for malicious users to negatively affect users and systems. This section will explore a few examples where paradigm shifts have been followed by security problems.

1.1 Historical overview of attacks

Classically within Computer Security threats can be categorised as violations of one or more of three basic principles: confidentiality, integrity and availability. This section will examine each in turn, briefly highlighting examples where attacks have become well known, or commonplace, and it can be argued that they should have been preventable if the target of the attack had been more alert to the presence of the danger.

Confidentiality is the most simply understood of the security goals. Fundamentally, this means that private data is only accessible to those who are authorised. Many of the early examples of computer crime from the 1980s [10, 11] are examples of this kind of attack, where attackers made use of relatively open networks to search out data, enabled by guessable, or easily attained, usernames and passwords. Such early attacks were largely upon systems run by naïve owners, not appreciating the risk that was present. However, if we consider the biggest news relating to cyber security in the last decade it largely concerns breaches of private data: Sony (2011) 77 million accounts [12], Target (2013) 110 million accounts [13], Yahoo (2013) 3 billion accounts [14], Equifax (2017) 143 million accounts [15]; and Marriott (2018) 500 million accounts [16]. The frequency and size of the breaches are evidence of companies' willingness to capitalise on this dramatic reduction in the cost of storage of large amounts of data without the concomitant investment in security measures.

The second security goal is that of Integrity. This is commonly defined as data being left as the last authorised person left it. At a foundational level it is all about trust. Can a system or resource be trusted to contain true and accurate data? Has the software been modified? Botnets containing hundreds of thousands to millions of comprised computers have been common across the last decade, their owners unaware that their systems integrity has been compromised [17]. Is the data being reported correct? If it is not, then perhaps markets will be dramatically affected [18]. Is the content on a website real or fake? If it is fake, we end up with Trump as President of the USA [19]. The recent popularity of Blockchain technologies, separate to the 'get rich' aspect of the cryptocurrencies, has largely been driven by the need to have verifiable data integrity. This in itself does not demonstrate an attack, but reflects concern about the trustworthiness of financial systems, IoT data [20], cloud computing [21], social media [22] among others all adopting blockchain technology.

The final of the three goals is Availability: that resources are present when they are required. A common attack of this type has been referred to as a 'worm': a computer virus that self-replicates and spreads through a network, using resources at the expense of normal users. The first worm was created in the late 1980s [23], but at times since then, when paradigms have adjusted, a worm has often followed. A series of worms attacked Windows machines across a sequence of years following the dotcom boom, as home internet usage was exploding: first in 2000 with ILOVEYOU [24], then Code Red and its variants in 2001 [25] and the Slammer [26] and Blaster [27] worms

in 2003. A lot of users were unaware of the importance of patching their systems, and further, Microsoft was not as vigilant around finding flaws as it is today. Recent ransomware attacks such as CryptoLocker (2013) [28], WannaCry (2017) [29] and NotPetya (2017) [30] have all had devastating effects on access to data within systems after ransomware was packaged within a worm. The increased reliance upon data was not paired with an appropriate security posture, and with the absence of effective backup procedures, breaches have left some hospitals, governments and businesses crippled. However, the most obvious example of a loss of availability is a Denial of Service (DoS) attack. These come in various forms, from creating the inability to visit a webpage as first occurred in 2000 [31], disrupting games [32] and music platforms [33], to even stalling the Australian Census in 2016 [34]. As soon as a new platform appears, it seems only a matter of time before a user attempts to disable access to it, ever adaptive, seeing it as a new challenge.

1.2 Current opportunities faced with emerging threats

The fundamentals of what is occurring within cyber-attacks have remained consistent through the history of the Internet as seen in the previous section. As new systems are deployed, attack vectors that could arise within the new system are not fully considered, and breaches of one of the three types mentioned occur. Awareness of users or businesses to the possible kinds of threats plays a significant role in protection from such attacks. Botnets are a classic example of the computational power that can be illegally harnessed when hundreds of millions of users of Internet users unknowingly install malware on their systems [35]. Ideally, users need to be informed about the risks the risks systems are facing. Often this is not realistic, however this leaves the burden on the system designers to foresee and prevent user error.

In recent years there has a large interest in the Internet of Things (IoT) devices, and their ability to gather data. It is projected that the number of devices will clear 20 billion shortly after 2020 [36]. This large investment in hardware and network-connected devices has also produced a new attack surface for malicious users to target. A range of attacks [37] have already occurred in this space, and discussion around the need to better understand the risks in this area [38]. IoT devices have been broadly seen as disposable, or simple data gathering tools, and some of the attacks that have occurred demonstrate that lessons learnt in other areas were not applied in their design, or at least were skipped in aiming to create cheap products [39].

Learning from the past is vital in designing secure solutions for the future. Users have, to various degrees, gained an understanding of not installing random software on their computers and avoiding suspicious websites. However, in recent years there has been an explosion in smart phone-based malware affecting millions of users [40-42]. The lessons learned within personal computing need to be applied to smart phones and other mobile devices. While the worms of the early 2000s infected millions of users, they weren't particularly clever in the damage they inflicted. Due to the increased importance of the data, and indeed often the extremely personal nature of the data that is commonly on our devices, attackers have adapted to not be as disruptive, but instead have opted to chase profit. Encrypting private files and holding the owner for ransom is now a common and an effective attack. Attackers have adapted, chasing the rewards, and can rely on ill-prepared victims, who have not backed up their data and are willing to pay a ransom to regain access.

Smart phones and IoT devices as targets, data repositories being made inaccessible until a ransom is paid, and extensive swarms of compromised machines in a botnet are all threats which did not exist, or at least to the same scale as today, at the height of the dot com boom, or in the networks and systems that existed pre the world wide web. As advancements occur, whether driven by technological advancements (cost of data storage and transmission) or commercial interests (new market segments), the same risks to user security exist. The attacks which are implemented will evolve, but the underlying premises of the security goals being violated remain the same. The remainder of this paper will discuss a technological change which is about to occur and will highlight some ways in which this will alter the landscape of data transmission on the Internet. The paper will describe some scenarios where business interests (and others) will be quick to utilise this improved technology and highlight how this could occur without the required diligence to enable effective mitigation of new risks to the security of their systems.

3. Satellite Internet Constellations

The first communications satellite, SCORE, was launched in the year following Sputnik. Five years later the first commercial satellite Telstar [43] entered orbit. Since that time communications satellites have filled a vital role within global communication networks. According to the Index of Objects Launched into Outer Space, maintained by the United Nations Office for Outer Space Affairs (UNOOSA), there are 5,278 satellites orbiting the earth, of which just over 700 are communications satellites [44]. Communications satellites carry signals for telephone, radio, television and internet services.

Historically communications satellites have primarily been in geostationary orbits (GEO), so that the satellite appears to be stationary to ground stations not requiring them to track the path of the satellite. A

geostationary orbit places the satellite at 35,786km from earth. At such a distance a large area of the earth is covered, requiring only three such satellites to provide coverage to the whole planet (excluding the poles). Currently, of the over 700 communication satellites orbiting earth 468 are in a geostationary orbit [45].

During the 1990s several commercial communications satellite constellations were proposed and then implemented including SPACEWAY [46], ViaSat [47], Globalstar [48] and Iridium [49]. SPACEWAY and ViaSat both delivered Internet access, while the Iridium and Globalstar focused primarily on telephony. Both SPACEWAY and ViaSat operated geostationary satellites to provide their services, which, while providing Internet service to those who did not have terrestrial based options, operated with a fundamental limitation: high latency. At an altitude of 35,786km, satellites in geostationary orbit have a roundtrip time (RTT) exceeding 500ms in the best case. Often service would be slower. This is the same constraint faced by the privatised INMARSAT constellation [50], whose 13 GEO satellites provide data and telephony services to governments, aid agencies and a range of businesses including shipping, airline and mining industries. To counter the latency problem faced by satellites in GEO the O3b constellation operates at an altitude of 8,063km [51]. The O3b constellation of 20 satellites provides services to ships, offshore platforms, and regions with poor terrestrial connectivity. The result is a vastly improved RTT of 150ms, a quarter of their GEO counterparts, but slower than terrestrial options. The O3b network, like the Globalstar network, also does not provide global coverage, and does not provide broadband speeds. Recently, Iridium has completed its NEXT constellation which is an upgrade to their existing constellation that had been in service for 17 years. The NEXT constellation was completed in January this year and is now operational; providing users with voice and data at user terminal speeds of up to 1.4Mbps [52]. The constellation contains 66 satellites at an altitude of 781km.While it offers a low latency solution, it has low bandwidth.

Currently there is no operational constellation which addresses global broadband Internet connectivity at low latency.

3.1 The Proposed LEO Constellations

Over the last five years there has been a series of new satellite constellations proposed: Starlink [53], OneWeb [54], Project Kuiper [55], Telesat [56] and LeoSat [57]. Several of these have been from companies who have not previously operated communications satellites. These constellations are aiming to transform the way data is transmitted over long distances. The fundamental premise that these companies are aiming to leverage is that the speed of light is faster in a vacuum than in fibre optic cable. The refractive index of optic fibre is approximately 1.5, meaning that light travelling down the fibre is only reaching 67% the speed of light [58]. If, instead of travelling long distances through optic fibre, a route through space could be taken, where the data can travel at the full speed of light, a faster path between two points exists. Several of the proposed constellations are planning to use optical inter-satellite links to transmit data across large distances, hopping from one satellite to the next. Fig 1 below illustrates a

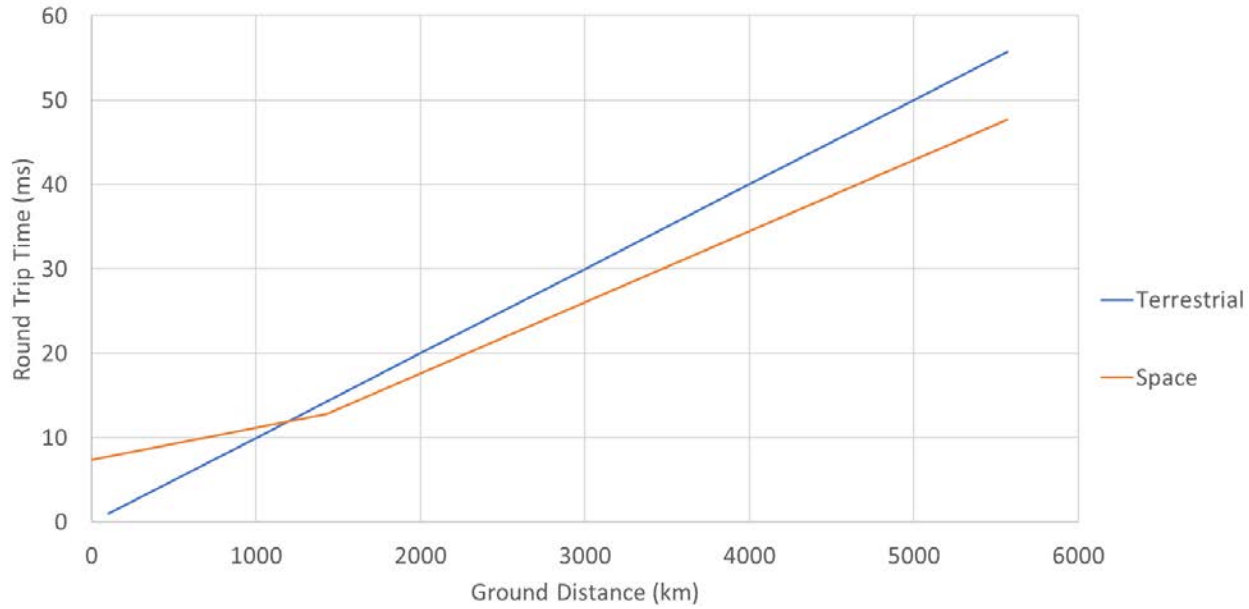

Fig. 1 A projected round trip time between two locations via a LEO satellite constellation at 550km altitude.

Table 1. Summary of proposed satellite constellations, with breakdown of lowest orbit shell and full constellation listing all the shells.

	Lower Orbital Shell				Full Constellation	
	Satellites	Orbit (km)	Planes	# per plane	Satellites	Orbits (km)
Starlink - Phase 1	1,584	550	72	22	4,409	550, 1110, 1130, 1275, 1325
Starlink - Phase 2	2,493	335.9	---	---	7,518	335.9, 340.8, 345.6,
OneWeb	1,980	1,200	36	55	4,540	1200, 8500
Telesat	72	1,000	6	12	117	1000, 1248
Kuiper Project	784	590	28	28	3,236	590, 610, 630
LeoSat	78	1,400	6	13	108	1400
Iridium NEXT	66	781	6	11	66	781

calculated estimate by the authors of the difference between a purely terrestrial delivery via optic fibre, and delivery via a series satellites (which is also in line with other authors [5, 6] similar calculations of Starlink prior to recent changes to their proposal). This shows that after approximately 1100km, a path via a satellite at an altitude of 550km is faster than travelling through optic fibre (the change shortly after this point in the line on the graph will be discussed below). Previous generations of communications satellites typically delivered Internet access via GEO satellites at 35,786km altitude, with a minimum RTT of 500ms (up and down to the same spot). With an optimum path of terrestrial fibre, a packet of data could circumnavigate the earth in this period with time to spare. The point at which the slope of the line changes in Fig 1 demonstrates the end of the maximum area covered by a single satellite; the change indicates the ground distance after which multiple satellites are always required for transmission. The low latency connection that LEO satellites offer clearly demonstrates what the new constellations are aiming to leverage. However, by being in LEO, a far greater number of satellites are required for global coverage; from a handful in GEO to proposals of thousands of satellites. The dramatic drop in cost of launching hardware into space has allowed such an approach to have a much-improved change of being realised. Since 2010 there has been a 20 fold decrease in the cost of launching into LEO with no signs of this trend slowing [59].

In Table 1 there is a summary of five satellite constellation proposals, and the currently operational Iridium NEXT constellation [60]. Starlink [53] by SpaceX is the largest, which will be deployed in two phases, with nearly 12,000 satellites proposed across eight shells of varying altitude, with the lowest at 335.9km; OneWeb is the next largest at 4,540 satellites [54], but with a lower shell twice the height of Starlink and a upper shell in medium earth orbit (MEO); the Kuiper Project by Amazon [55] is the most recently announced and the third largest at 3,236, and also has the second lowest lower shell at 590km. The remaining two LeoSat [57] and Telesat [56] are proposing substantially smaller constellations, operating at a higher altitude. The total, if all implemented, is 19,928 satellites, nearly four times the 5,278 operational satellites currently orbiting earth, and completely dwarfing the current 700 operational communications satellites.

There are a range of differences between the different proposals beyond size, they are not the focus of this paper, but will be briefly mentioned here. There are three different ranges of radio frequency being used across the constellations to communicate with terrestrial receivers: L, Ka and V band. L, used by Iridium, while currently operational, has the lowest bandwidth capacity; Ka, to be used in OneWeb, Kuiper Project and LeoSat has more throughput, with the most bandwidth capacity in V band being proposed for use by Telesat; finally, Starlink will use a combination of Ka (Phase 1) and V (Phase 2). Actual, real-world bandwidth speeds are conjecture at this point. However, SpaceX has said the system will be able to provide broadband service at speeds of up to 1 Gbps per end user in phase 1 [61], while OneWeb has said it will achieve speeds of 2.5 Gbps [62]. This is a substantial improvement over existing offerings and at a much lower latency.

A final difference between the proposals is the use of inter-satellite links. Starlink, Telsat, LeoSat and Iridium all propose, or currently are equipped with, optical links between satellites in orbit. This enables them to route traffic through the network in space, at the speed of light, with low latency and high-bandwidth. Both the OneWeb and Kuiper Project proposals make use of what is referred to as a “bent-pipe” architecture [54, 55, 63]. This design requires data to be sent to space, and then back down to earth, before then returning to space if it is not close enough to its destination yet. This results in worse latency than being transferred directly between satellites in space. The bent pipe approach would still provide fast access, but noticeably higher latency than the other proposals.

In May of 2019 SpaceX launched 60 test satellites at an altitude of 440km, and most then proceeded to their

operational altitude of 550km [64]. This joins prior launches of test satellites by SpaceX and OneWeb. Four months later, SpaceX President Gwynne Shotwell stated that SpaceX would attempt to undertake 24 launches (presumably each of 60 satellites) in 2020, following several more in 2019 [65]. Such a launch frequency is unprecedented and could result in the constellation being able to enter service late in 2020. Even if this is not achieved, but an aggressive timetable similar to this is implemented, the 550km shell of 1,500 satellites could be completed and operational sometime in 2021, with additional shells to follow, increasing the capacity and capability of the network in a continuous manner.

The proposed constellations, as shown above, represent an ambitious and dramatic increase in on-orbit communications hardware. The next section will briefly comment on the possible impacts of this change.

3.2 The Impact of the New LEO Constellations

The Internet is one of the most transformative technologies ever invented due to its unique ability to connect people across vast distances for the purpose of sharing information. The benefits of Internet access are most accessible when four conditions are met: ease of access, high-bandwidth, low-latency and low cost. Currently, broadband access is not available at all locations on the planet, and the LEO constellations explained in the previous section aim to provide global coverage. According to the World Bank, only 35% of the population in developing countries have access to the Internet [66]. Internet access is seen as a key tool in providing education and job creation. Lifting the Internet penetration rate to 75% has a projected benefit of adding $2 trillion USD to the global annual GDP.

Even in the developed world there are areas without fast, reliable broadband Internet. The proposed constellations create a more level playing field in terms of access and speed. Geography is no longer a limiting factor in access to Internet infrastructure. SpaceX has said that they expect the cost of a terminal to Starlink to be about $200 USD [67], which is certainly expensive in many parts of the world. However, it is cheaper than the current options, and it is a reasonable assumption that it will become cheaper with time. This global infrastructure initiative bypasses geographic complications, financial limitations, and sociocultural factors, providing unprecedented Internet connectivity.

These new satellite networks will provide the fastest Internet access available on the planet. Historically, low latency was key in several scenarios and has resulted in construction of expensive links in financial systems [68], and is seen as a tool for making money moving forward [69] where the adage of “time is money” is true. The lower the latency of the connection, the faster you can get your trade into the stock market, beating your competitors. The LEO networks will enable faster links between global stock markets, but also enable a remote sheep herder in a poorer nation to have the same connection.

The bandwidth available to users in the projections SpaceX (up to 1 Gbps) [61] and OneWeb (2.5 Gbps) [62] vastly outstrip any estimates of the global average Internet access speed. The global average bandwidth is very hard to estimate, but values in the area of 7.2Mbps are suggested [70], although it is worth noting that value does not include half of the world that still have no access at all [71].

These proposals are aiming to provide a service that is globally accessible, consisting of high bandwidth and low latency, while aiming at a low cost. If the companies can successfully deploy the satellites and the network functions as expected, it will be disruptive in multiple ways. Existing telecommunications providers will face direct competition to their current terrestrial fibre networks It will accelerate the rate of the adoption of the Internet in the least-developed nations, increasing access to education, and combat poverty through job growth [71].

In addition to these opportunities, it will also create new opportunities in developed countries to increase the connectivity of existing systems or connect previously offline systems to the Internet. Petry and Salam [72] argue that LEO networks will be required for 5G networks to fulfil their promise in connecting safety-critical systems, such as future autonomous vehicles, for which existing networks do not provide the required speed and access. The ability of satellite networks to enable geographically dispersed systems to easily connect to the Internet will better enable a range of industries which function in remote areas to undertake their work. This includes environmental monitoring, mining, forestry, energy generation and maritime, all of which currently either have some connectivity, or have complex networks at locations with limited or no links to the rest of the world. Industrial control systems often require specialist knowledge and are commonly operated from a great distance away. The ability for real-time control in these contexts enables increased numbers of such systems or more efficient use of existing systems. Many of these industries are exploring increased automation and in some cases autonomy, often to reduce the numbers of humans being in risky or unfulfilling expensive jobs. Greater connectivity, and at low latency, enables such systems to be fully integrated into global networks to ensure that they can operate in a safe manner, and can be constantly monitored. LEO satellite constellations will facilitate dramatic change in many industries where connectivity or latency is currently a barrier to future advancement. It is clear that the long-distance monitoring and increased production capacity will have significant benefits both financially and pragmatically.

However, such a paradigm shift is not without risk. As was seen with rapid adoption of networks historically, the benefits of connectivity also brings new vulnerabilities. With increased adoption of computer systems in cars, for instance, and a near future that includes autonomy, there are many researchers highlighting the cyber risks of a connected vehicle [73-76]. Risks within supervisory control and data acquisition (SCADA) and distributed control systems (DCSs) have been discussed for many years [77-79]. The risks to IoT systems have risen to prominence following the dramatic impact of the Mirai botnet [37]. However, many of the threats discussed in these examples are within traditionally connected contexts, where systems have been built and integrated with the Internet over many years. In more geographically dispersed contexts, access to the Internet will very rapidly change over the next few years, and the business case to connect existing systems (which have not been online before) to networks will be very appealing. This paper argues that this dramatic shift in attack surface for those systems and networks will be highly risky if not undertaken with due care. To illustrate this a case study is presented here of the maritime industry. This will aim to briefly explore an industry where there is a clear value in adopting the new connections, but there, in the authors opinions, is a very real risk to existing systems as can be demonstrated by their level of awareness and preparedness of existing systems.

4. Case Study: Maritime

Shipping transportation systems and offshore platforms are becoming increasingly connected. The IT systems are a vital part of operations relating to navigation, control systems, engineering and the logistics operations. Currently there is an increased focus on shipboard IT systems as the industry plans for increased levels of autonomy, with more shore-based oversight and control [80, 81]. For these innovations to occur, ships may need to be constantly connected to shore-based networks, and the advent of constellations described in this paper will accelerate this rate of adoption and change [82]. However, such adoption will increase their level of risk from cyberattack. The effect of an attack in this context is substantially different from other working contexts [83]. The worst outcome is not the loss of data, but the possible loss of maritime infrastructure, harm the environment or even the loss of life. If seafarers and offshore workers are not aware of these risks, they may be ill-equipped to respond in the event of an attack.

Building and maintaining a mobile, technologically complex and connected vessel that is cyber-resilient requires a significant investment in skills and resources to be made throughout the entire life-cycle of the vessel. There is a range of motivations for cyber-attacks against maritime vessels including facilitating piracy, political activism, nation state conflict and being targeted unintentionally by a random attack [84]. Several of these will be summarised here to highlight increased risk facing the sector, and the overall need for thorough preparedness of the industry to such incidents.

In 2017 Maersk, the world's largest container shipping company, was the victim of a highly publicised cyberattack [85]. This attack affected their shore-based networks, costing in excess of 300 million USD as operations globally were brought to a standstill. The attack was not targeted at Maersk but was the global cyberattack dubbed 'NoPetya'. This attack was not the first-time attacks of this nature have occurred within the onshore operations of the shipping and offshore energy sectors. The 2012 cyberattack on the Saudi Aramco company resulted in the theft of files and the disabling of 30,000 computers, taking months for a full recovery [86]. A 2014 Norwegian Government report described how fifty Norwegian oil and energy sector companies has been attacked in the previous year [87], and a 2017 industry survey found that 39% of ship owners globally had been attacked in the previous 12 months [88]. These high-profile incidents highlight the vulnerability of the shore-based networks across the maritime and energy sectors to cyberattack.

In addition to these shore-based attacks, where the networks have been connected to the Internet for decades (and preparation should be highest), there have also been attacks on offshore systems. These systems have for a long time been effectively air-gapped from the internet. With the increased connectivity globally, however, they are now connected periodically or even continuously (with a low-bandwidth, high-latency connection). In addition to this network connectivity risk, ship board systems are increasingly built using off-the-shelf hardware and software [89]. This means that existing vulnerabilities discovered in other contexts can be exploited in attacks on maritime systems. Furthermore, due to periodic nature of their current network connections, they often do not get patched as readily as in shore-based use cases would.

In 2013 a newly-constructed oil rig was found to be infected with malware through many systems, including key safety systems [90]. More recently in 2017 hackers reportedly took control of the navigation systems of a German-owned container vessel en route from Cyprus to Djibouti for 10 hours [91]. Merchant vessels are not the only ships compromised; a Naval vessel in 2017 was found to have malware in the platform management and integrated bridge systems [92]. Further, in a 2017 penetration test by an Israeli security company Navel Dome was able to successfully alter the position, heading, depth and speed of a vessel, moving through the ships systems after an email opened by the Captain installed malware on their machine [93].

In a 2017, survey 47% of seafarers said that they had sailed on a vessel that had been the target of a cyber-attack [94]. However, in many cases the attacks that have occurred, could have been the result of those same seafarers unknowingly giving the attackers a foothold. Crew who plug in a phone to a USB port to charge can unwittingly provide a mechanism for installing malware onto shipboard systems [95]. Similarly, USB sticks are a very common way for malicious software to spread between devices [95, 96], and are commonly used within normal operations. Both examples are seen by users as being innocuous activities, which could not do any harm. However, this shows a lack of awareness of the common attack vectors used by malware writers to get into systems in order to gain control. In systems that are not connected to the internet such infections may cause serious problems; for example, a malfunction during complicated manoeuvrers such as docking. However, if these systems were connected to the Internet, such an infection could be even more serious and result in control of the vessel being handed to the malware author.

A number of independent researchers and industry organisations have identified maritime cyber maturity as low, with limited awareness of the issue by key stakeholders [84, 97]. The industry has been responding to this growing threat, as can be seen by steps being taken such as the strategic development by bodies such as the International Maritime Organisation (IMO) [98] and the Baltic and International Maritime Council (BIMCO) [99] among others [100, 101] who have produced standards and advice for ship operators. Such moves will hopefully have a positive impact on ship builders and the vendors of software used within ship systems. However, many of the changes that are recommended are of a technical nature and will only have a lasting effect on the cyber security of a system if the crew and shore-based personnel maintaining vessels are also aware of the risks, and their role in the security of shipboard systems. Such changes will take substantial time and could be easily outpaced by the adoption rate of high speed, low latency connections, via LEO based satellite Internet. Crew are underprepared for dealing with cyber incidents onboard, and an increase in likelihood of such events puts crew, ships and other infrastructure at risk.

5. Mitigation and Discussion

The new satellite constellation proposals, with their global connectivity improvements, and possible rapid rollout, present a scenario where industries may increase their systems connectivity with minimal expense. The possibilities of highly-connected systems with greater automation, autonomy and data collection is very appealing. However, as described in the previous sections, it may be that this change brings with it increased cyber risk for these systems. Industries which are geographically isolated, such as maritime, have historically had a very minimal attack surface for malicious cyber actors to target. However, through the new constellations they will have access to what is arguably the best connection available. This will dramatically alter their attack surface, and their security posture needs to be adjusted at the same time as any change in their use of network connections. These private networks already suffer attack as illustrated by the Maersk [85] and Aramco attacks [86]. If those networks had been connected through to boats or oil wells the impact would have been very different. Previous paradigm shifts have resulted in cyber-attacks on unprepared users in the home PC market [25-27], mobile computing [41, 42], cloud computing [102, 103] and IoT areas [37]. It is likely that similar events could occur if adequate planning does not occur by businesses which adopt satellite connections to bring formerly disconnected systems online. Many systems which could fall into this category are industrial in nature (mining, agriculture, transport) or are utilities (power and water). Outages in these sectors have roll-on effects to other industries and present a scenario where ransomware users could be in the situation of ransoming infrastructure [104, 105] and not just users' personal files. Within industrial contexts there is commonly extensive legacy code which was never written with the expectation of being connected to other systems or networks. These systems may still use old operating systems such as Windows XP and Windows 7 [106], to keep the legacy code operational.

Countering this risk is the challenge that industries face, whether they are connected via optical fibre or satellite; however, those with conventional connections have already been weathering cyber-attacks for a while. The first step is to learn from what has come before, and follow the same advice as many other sectors (such as finance, business, education and health) as recommended by national bodies like the American NIST Cybersecurity Framework [107] or the Australian Government Information Security Manual [108]. Following such fundamentals will include simple strategies around network separation, perimeter defences, system virtualisation, use of virtual private networks, intrusion detection systems, system hardening and software updates. Vital in this space are careful regimes of backups of operational systems to enable fast recovery from any incidents.

Users are vital to the security of any system, and their training in cyber awareness in a manner that is appropriate to their context is essential. Within a maritime context training has been suggested as being key but needs to be paired with appropriate cross-disciplinary skills within teams communicating in a global context to facilitate appropriate responses when

an attack occurs [109]. If users are not educated about cyber risk, unsafe actions will be carried out by users on systems putting the systems at risk.

In any of these systems there is no one solution to enable that they are safe and secure. Cyber-security is a complex area, with hardware, software and personnel-related measures needing to be in place.

6. Conclusion

We are on the verge of a dramatic change in the underlying architecture of the Internet. Over the next decade satellite constellations delivering the Internet will vastly improve access to the Internet globally. This is an exciting opportunity for those in poorer nations to gain access to information and communication services, but will also enable existing industries with limited access to now connect. This paper has suggested that in this latter case there is a risk that the change could result in negative consequences if precautions are not taken to protect these systems as they come online. Historically it can be seen that mistakes have been repeated in relation to cyber security on multiple occasions as paradigms have shifted. This new paradigm will affect systems running legacy code that were not designed with security as a high priority now being connected to networks. This places them at risk, and in some cases could place substantial industrial infrastructure in harm's way. The Maritime industry is an interesting and relevant sector for concern, and it was explored as a case study in this paper. It is an industry with clear historical difficulties in getting reliable Internet access and has a clear benefit from greater access. However, the industry also has a history of its shore-based networks being vulnerable and connecting them to vessels will bring added risk. To mitigate this risk (and similar in other industries), it is important that systems becoming more network connected are examined in depth. The more assessible the system the broader the range of possible mechanisms of attack or misuse. A strong security posture is vital to enable these systems to continue operating smoothly after they are connected to corporate networks or the Internet.

References

1. Lewis, J., *Economic Impact of Cybercrime-No Slowing Down.* Santa Clara: McAfee & CSI (Center for Strategic and International Studies), 2018.
2. Hughes, B.B., D. Bohl, M. Irfan, E. Margolese-Malin, and J.R. Solórzano, *ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance.* Technological Forecasting and Social Change, 2017. **115**: p. 117-130.
3. Graydon, M. and L. Parks, '*Connecting the unconnected': a critical assessment of US satellite Internet services.* Media, Culture & Society. **0**(0): p. 0163443719861835.
4. Klenze, T., G. Giuliari, C. Pappas, A. Perrig, and D.A. Basin. *Networking in Heaven as on Earth*. in *HotNets*. 2018.
5. Bhattacherjee, D., W. Aqeel, I.N. Bozkurt, et al. *Gearing up for the 21st century space race*. in *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*. 2018. ACM.
6. Handley, M., *Delay is Not an Option: Low Latency Routing in Space*, in *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*. 2018, ACM: Redmond, WA, USA. p. 85-91.
7. Keppel, D., *An Empirical Exploration of the Potential Benefits of Applying Big Data Analytics for Improved Space to Space Operations Management in the Satellite Industry*. 2018, Toulouse Business School.
8. Isaacson, W., *The innovators: How a group of inventors, hackers, geniuses and geeks created the digital revolution*. 2014: Simon and Schuster.
9. Landwehr, C.E., *Formal models for computer security.* ACM Computing Surveys (CSUR), 1981. **13**(3): p. 247-278.
10. Stoll, C., *The cuckoo's egg: tracking a spy through the maze of computer espionage*. 2005: Simon and Schuster.
11. Mitnick, K., *Ghost in the wires: My adventures as the world's most wanted hacker*. 2011: Little, Brown.
12. Baker, L.B. and J. Finkle, *Sony PlayStation suffers massive data breach.* Reuters, April, 2011. **26**.
13. Stanwick, P.A. and S.D. Stanwick, *A security breach at target: A different type of bulls eye.* International Journal of Business and Social Science, 2014. **5**(12).
14. McMillan, R. and R. Knutson, *Yahoo triples estimate of breached accounts to 3 billion.* Wall Street Journal, 2017.
15. Gressin, S., *The equifax data breach: What to do.* US Federal Trade Commission, as viewed Oct, 2017. **1**.
16. Chapman, J., *How safe is your data? Cyber-security in higher education.* Higher Education Policy Institute Policy, 2019.
17. Tyagi, A.K. and G. Aghila, *A wide scale survey on botnet.* International Journal of Computer Applications, 2011. **34**(9): p. 9-22.
18. Xie, L., Y. Mo, and B. Sinopoli, *Integrity Data Attacks in Power Market Operations.* IEEE Transactions on Smart Grid, 2011. **2**(4): p. 659-666.
19. Allcott, H. and M. Gentzkow, *Social media and fake news in the 2016 election.* Journal of economic perspectives, 2017. **31**(2): p. 211-36.
20. Conoscenti, M., A. Vetro, and J.C. De Martin. *Blockchain for the Internet of Things: A systematic literature review*. in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. 2016. IEEE.

21. Gaetani, E., L. Aniello, R. Baldoni, et al., *Blockchain-based database to ensure data integrity in cloud computing environments.* 2017.
22. Shah, S.N., *Device-driven non-intermediated blockchain system over a social integrity network*. 2017, Google Patents.
23. Eisenberg, T., D. Gries, J. Hartmanis, et al., *The Cornell commission: on Morris and the worm.* Communications of the ACM, 1989. **32**(6): p. 706-709.
24. Knight, P., *ILOVEYOU: Viruses, paranoia, and the environment of risk.* The Sociological Review, 2000. **48**(2_suppl): p. 17-30.
25. Moore, D. and C. Shannon. *Code-Red: a case study on the spread and victims of an Internet worm*. in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. 2002. ACM.
26. Moore, D., V. Paxson, S. Savage, et al., *Inside the slammer worm.* IEEE Security & Privacy, 2003(4): p. 33-39.
27. Bailey, M., E. Cooke, F. Jahanian, and D. Watson, *The blaster worm: Then and now.* IEEE Security & privacy, 2005. **3**(4): p. 26-31.
28. Liao, K., Z. Zhao, A. Doupé, and G.-J. Ahn. *Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin*. in *2016 APWG Symposium on Electronic Crime Research (eCrime)*. 2016. IEEE.
29. Mohurle, S. and M. Patil, *A brief study of wannacry threat: Ransomware attack 2017.* International Journal of Advanced Research in Computer Science, 2017. **8**(5).
30. McQuade, M., *The untold story of NotPetya, the most devastating cyberattack in history*. 2018, Wired.
31. Calce, M. and C. Silverman, *Mafiaboy: How I Cracked the Internet and why It's Still Broken*. 2008: Penguin Group Canada.
32. Jeff Yan, J. and H.-J. Choi, *Security issues in online games.* The Electronic Library, 2002. **20**(2): p. 125-133.
33. Etherington, D. and K. Conger. *Large DDoS attacks cause outages at Twitter, Spotify, and other sites*. 2016; Available from: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/.
34. Chowdhury, A. *Recent cyber security attacks and their mitigation approaches–an overview*. in *International conference on applications and techniques in information security*. 2016. Springer.
35. Barroso, D., *Botnets-the silent threat.* European Network and Information Security Agency (ENISA), 2007. **15**(2007): p. 171.
36. Golio, M. *Strategic Planning for RF Technologies-Implications for 5G and IoT Emerging Radio Products*. in *2018 IEEE MTT-S Latin America Microwave Conference (LAMC 2018)*. 2018. IEEE.
37. Kolias, C., G. Kambourakis, A. Stavrou, and J. Voas, *DDoS in the IoT: Mirai and other botnets.* Computer, 2017. **50**(7): p. 80-84.
38. Nurse, J.R.C., S. Creese, and D.D. Roure, *Security Risk Assessment in Internet of Things Systems.* IT Professional, 2017. **19**(5): p. 20-26.
39. Zhang, Z., M.C.Y. Cho, C. Wang, et al. *IoT Security: Ongoing Challenges and Research Opportunities*. in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. 2014.
40. Brewster, T. *25 Million Android Phones Infected With Malware That 'Hides In WhatsApp'*. 2019; Available from: https://www.forbes.com/sites/thomasbrewster/2019/07/10/25-million-android-phones-infected-with-malware-that-hides-in-whatsapp/#78edd54e4470.
41. Landman, M. *Managing smart phone security risks*. in *2010 Information Security Curriculum Development Conference*. 2010. ACM.
42. Mylonas, A., A. Kastania, and D. Gritzalis, *Delegate the smartphone user? Security awareness in smartphone platforms.* Computers & Security, 2013. **34**: p. 47-66.
43. Dickieson, A., *The Telstar Experiment.* Bell System Technical Journal, 1963. **42**(4): p. 739-746.
44. *Index of Objects Launched into Outer Space, United Nations Office for Outer Space Affairs (UNOOSA)*. 2019; Available from: http://www.unoosa.org/oosa/index.html.
45. *UCS Satellite Database*. 2019 3/31/19; Available from: https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.
46. Fitzpatrick, E.J. *SPACEWAY: Providing affordable and versatile communication solutions*. in *19th NASA Propagation Experimenters Meeting (NAPEX 19)*. 1995.
47. *ViaSat Inc*. Available from: http://libraries.ucsd.edu/sdta/companies/viasat.html.
48. Dietrich, F.J., P. Metzen, and P. Monte, *The Globalstar cellular satellite system.* IEEE Transactions on Antennas and Propagation, 1998. **46**(6): p. 935-942.
49. Fossa, C.E., R.A. Raines, G.H. Gunsch, and M.A. Temple. *An overview of the IRIDIUM (R) low Earth orbit (LEO) satellite system*. in *Proceedings of the IEEE 1998 National Aerospace and Electronics Conference. NAECON 1998. Celebrating 50 Years (Cat. No. 98CH36185)*. 1998. IEEE.
50. *Inmarsat plc* Available from: https://www.inmarsat.com/.
51. *Arianespace launch VS05 > Soyuz ST-B – O3b: Mission accomplished*. 2013; Available from: http://www.arianespace.com/press-release/arianespace-launch-vs05-soyuz-st-b-o3b-mission-accomplished/.

52. *Iridium Certus*. 2019 21/09/2019]; Available from: https://www.iridium.com/services/iridium-certus/.
53. *SpaceX Non-Geostationary Satellite System*. 2018; Available from: https://fcc.report/IBFS/SAT-MOD-20190830-00087/1877671.
54. *Application for Fixed Satellite Service by WorldVu Satellites Limited*. 2018; Available from: https://fcc.report/IBFS/SAT-MOD-20180319-00022.
55. *Application for Fixed Satellite Service by Kuiper Systems LLC*. 2019; Available from: https://fcc.report/IBFS/SAT-LOA-20190704-00057.
56. *Application for Fixed Satellite Service by Telesat Canada*. 2018; Available from: https://fcc.report/IBFS/SAT-PDR-20170301-00023.
57. *Application for Fixed Satellite Service by LeoSat MA, Inc*. 2018; Available from: https://fcc.report/IBFS/SAT-PDR-20161115-00112.
58. Coffey, J., *Latency in optical fiber systems (white paper)*. 2017.
59. Jones, H. *The Recent Large Reduction in Space Launch Cost*. 2018. 48th International Conference on Environmental Systems.
60. *Application for Mobile Satellite Service by Iridium Constellation LLC*. 2016; Available from: https://fcc.report/IBFS/SAT-MOD-20131227-00148.
61. *Application for Fixed Satellite Service by Space Exploration Holdings, LLC, SAT-LOA-20161115-00118 / SATLOA2016111500118*. 2016; Available from: https://fcc.report/IBFS/SAT-LOA-20161115-00118.
62. *Application for Fixed Satellite Service by WorldVu Satellites Limited - SAT-AMD-20180104-00004 / SATAMD2018010400004*. 2018; Available from: https://fcc.report/IBFS/SAT-AMD-20180104-00004.
63. del Portillo, I., B.G. Cameron, and E.F. Crawley, *A technical comparison of three low earth orbit satellite constellation systems to provide global broadband*. Acta Astronautica, 2019. **159**: p. 123-135.
64. SpaceX, *Starlink Press Kit*. 2019.
65. Henry, C. *SpaceX plans 24 Starlink launches next year*. 2019; Available from: https://spacenews.com/spacex-plans-24-starlink-launches-next-year/.
66. *Connecting for Inclusion: Broadband Access for All*. 2018; Available from: https://www.worldbank.org/en/topic/digitaldevelopment/brief/connecting-for-inclusion-broadband-access-for-all.
67. Mosher, D. *Elon Musk just revealed new details about Starlink, a plan to surround Earth with 12,000 high-speed internet satellites. Here's how it might work*. 2019 22/09/2019]; Available from: https://www.businessinsider.com.au/spacex-starlink-satellite-internet-how-it-works-2019-5?r=US&IR=T.
68. Anthony, S. *The secret world of microwave networks*. 2016; Available from: https://arstechnica.com/information-technology/2016/11/private-microwave-networks-financial-hft/.
69. Lee, T., *Latency in fragmented markets*. Review of Economic Dynamics, 2019. **33**: p. 128-153.
70. *Internet Speeds by Country (Mbps)*. 2017; Available from: https://www.fastmetrics.com/internet-connection-speed-by-country.php.
71. *ICT Facts and Figures 2017*. 2018; Available from: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.
72. Petry, H.-P. and S. Salem, *5G and Satellites: A Viable Ecosystem?*, in *Future Telco: Successful Positioning of Network Operators in the Digital Age*, P. Krüssel, Editor. 2019, Springer International Publishing: Cham. p. 53-62.
73. Onishi, H. *Paradigm change of vehicle cyber security*. in *2012 4th International Conference on Cyber Conflict (CYCON 2012)*. 2012.
74. Axelrod, C.W. *Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks*. in *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. 2017. IEEE.
75. Thuen, C., *Commonalities in vehicle vulnerabilities*. 4th escar USA, 2016: p. 113.
76. Eiza, M.H. and Q. Ni, *Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity*. IEEE Vehicular Technology Magazine, 2017. **12**(2): p. 45-51.
77. Ralston, P.A., J.H. Graham, and J.L. Hieb, *Cyber security risk assessment for SCADA and DCS networks*. ISA transactions, 2007. **46**(4): p. 583-594.
78. Cárdenas, A.A., S. Amin, Z.-S. Lin, et al. *Attacks against process control systems: risk assessment, detection, and response*. in *Proceedings of the 6th ACM symposium on information, computer and communications security*. 2011. ACM.
79. Cheminod, M., L. Durante, and A. Valenzano, *Review of security issues in industrial networks*. IEEE Transactions on Industrial Informatics, 2012. **9**(1): p. 277-293.
80. Levander, O., *Autonomous ships on the high seas*. IEEE Spectrum, 2017. **54**(2): p. 26-31.
81. Rødseth, Ø.J., *From concept to reality: Unmanned merchant ship research in Norway*. I: Proceedings of Underwater Technology (UT), 2017.
82. Höyhtyä, M., J. Huusko, M. Kiviranta, K. Solberg, and J. Rokka. *Connectivity for autonomous ships: Architecture, use cases, and research challenges*. in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. 2017.

83. Tam, K. and K. Jones. *Cyber-Risk Assessment for Autonomous Ships*. in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. 2018.
84. Jensen, L., *Challenges in maritime cyber-resilience.* Technology Innovation Management Review, 2015. **5**(4): p. 35.
85. Saul, J., *Global shipping feels fallout from Maersk cyber attack*, {Saul, Editor. 2017, Reuters.
86. Axelrod, R. and R. Iliev, *Timing of cyber conflict.* Proceedings of the National Academy of Sciences, 2014. **111**(4): p. 1298-1303.
87. *Notifications of Data Interruption, National Security Authority (Norway)*. 2014 23/11/2018]; Available from: https://nsm.stat.no/aktuelt/varsler-om-datainnbrudd/.
88. FutureNautics, *Ship Operators Cyber Security Survey*. 2017.
89. Johnson, C.W., *Why We Cannot (Yet) Ensure the Cybersecurity of Safety-Critical Systems.* 2016.
90. Shauk, Z. *Malware offshore: Danger lurks where the chips fail*. 2013 [cited 2018 23/11/2018]; Available from: https://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/?is_eu=1.
91. Magee, T. *Can you hack a ship? Global maritime industry ripe for hacking*. 2017; Available from: https://www.techworld.com/security/can-you-hack-ship-global-maritime-industry-ripe-for-hacking-3674517/.
92. Zwan, W.R.v.d. and R. Mastenbroek, *Myth of the air gap, you are under attack*, in *MECSS 2017 Conference Proceedings* 2017.
93. *Cyber penetration tests underscore maritime industry's nightmare security scenario*. 2017; Available from: https://www.ajot.com/news/cyber-penetration-tests-underscore-maritime-industrys-nightmare-security-sc.
94. FutureNautics, *Crew Connectivity 2018 Survey Report*. 2018.
95. Tam, K. and K.D. Jones, *Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping.* Journal of Cyber Policy, 2018. **3**(2): p. 147-164.
96. Santamarta, R., *Maritime security: Hacking into a voyage data recorder (VDR)*. 2015, IOActive.
97. Cimpean, D., J. Meire, V. Bouckaert, et al., *Analysis of Cyber Security Aspects in the Maritime Sector*. 2011.
98. IMO, *Guidelines on Maritime Cyber Risk Management* 2017, MSC-FAL.1/Circ.3.
99. BIMCO, CLIA, ICS, and INTERCARGO, *The guidelines on cyber security onboard ships version.* 2016.
100. DNV-GL, *Recommended practice dnvgl-rp-0496: Cyber security resilience management for ships and mobile offshore units in operation*. 2016.
101. *Cyber-enabled ships: ShipRight procedure assignment for cyber descriptive notes for autonomous & remote access ships*. 2017, Lloyds Register.
102. Ramgovind, S., M.M. Eloff, and E. Smith. *The management of security in cloud computing*. in *2010 Information Security for South Africa*. 2010. IEEE.
103. Popović, K. and Ž. Hocenski. *Cloud computing security issues and challenges.* in *The 33rd International Convention MIPRO*. 2010. IEEE.
104. Zimba, A., Z. Wang, and H. Chen, *Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems.* Ict Express, 2018. **4**(1): p. 14-18.
105. Ghafir, I., J. Saleem, M. Hammoudeh, et al., *Security threats to critical infrastructure: the human factor*. The Journal of Supercomputing, 2018. **74**(10): p. 4986-5002.
106. *Manufacturers on Windows XP are risking their systems.* 2019; Available from: https://drivesncontrols.com/news/fullstory.php/aid/5999/Manufacturers_on_Windows_XP_are_risking_their_systems.html.
107. *NIST Cybersecurity Framework*. 2019; Available from: https://www.nist.gov/cyberframework.
108. *Australian Government Information Security Manual (October 2019).* 2019.
109. Berner, G., R. Hopcraft, J. Scanlan, M. Lutzhoft, and J. Earthy. *A Virtual Teams model for supporting maritime technology management*. in *Human Factors 2018 Conference*. 2018.