FutureDirections international

INDEPENDENT STRATEGIC ANALYSIS OF AUSTRALIA'S GLOBAL INTERESTS

Associate Paper

21 August 2018

The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges

Professor Vivian Louis Forbes
FDI Associate

Key Points

- The volume, impact and sophistication of cyberattacks have grown at an alarming rate. Worldwide, nearly 17 million attacks reportedly occur each week.
- With around 50,000 ships at sea or in port at any one time, the maritime transport industry is highly exposed to cyberattacks.
- Vessels do not need to be attacked directly. An attack can arrive via a company's shore-based Information Technology systems and very easily penetrate a ship's critical onboard Operational Technology systems.
- The International Maritime Organisation (IMO) reacted quickly in introducing guidelines in response to terrorist attacks on shipping, but has arguably been slower in formulating appropriate cybersecurity regulations.
- The maritime industry appears still to be ill-equipped to deal with such future challenges as the cybersecurity of fully autonomous vessels.

Summary

The maritime industry is heavily reliant on electronic commerce ("e-business") in many of its daily business transactions, including recordkeeping, human resources data, the loading and discharging of cargo and the location of containers on the docks, on land transportation and on ships. About 50,000 ships are at sea or in ports at any one time. The industry is therefore exposed to cyberattack threats that can have severe repercussions. Companies are

increasingly using cutting-edge techniques to stop cyber criminals from breaching their networks, but many are still not effectively protected. While governments have enacted legislation to counter such attacks, the implementation of legislation and international conventions does not, at present, appear to be entirely effective.

Analysis

A "cyberattack" is any attempt by a hacker(s) to damage or destroy a computer network system or an Internet-enabled application or device. The victims of cyberattacks may be random or targeted, depending on the criminal's intent. Cyber-thieves employ constantly evolving web programming languages to create a cheap ransomware service. On infected machines, ransomware encrypts data and frees it only when victims pay for it to be unscrambled.

Cyberattacks have grown at an alarming rate – in volume, impact and sophistication. While a ransomware attack is just one form of cyberattack, other assaults take place when hackers create malicious code known as malware and distribute it through spam e-mail, or "phishing", campaigns. Reportedly, nearly 17 million attacks occur each week. Despite actual and potential daily threats, nearly 90 per cent of enterprises are still not effectively protected against cyberattacks.[1]

About 50,000 ships are at sea or in port at any one time (see Figure 1, below). The maritime industry is thus heavily exposed to cyberattack threats which can have severe repercussions.

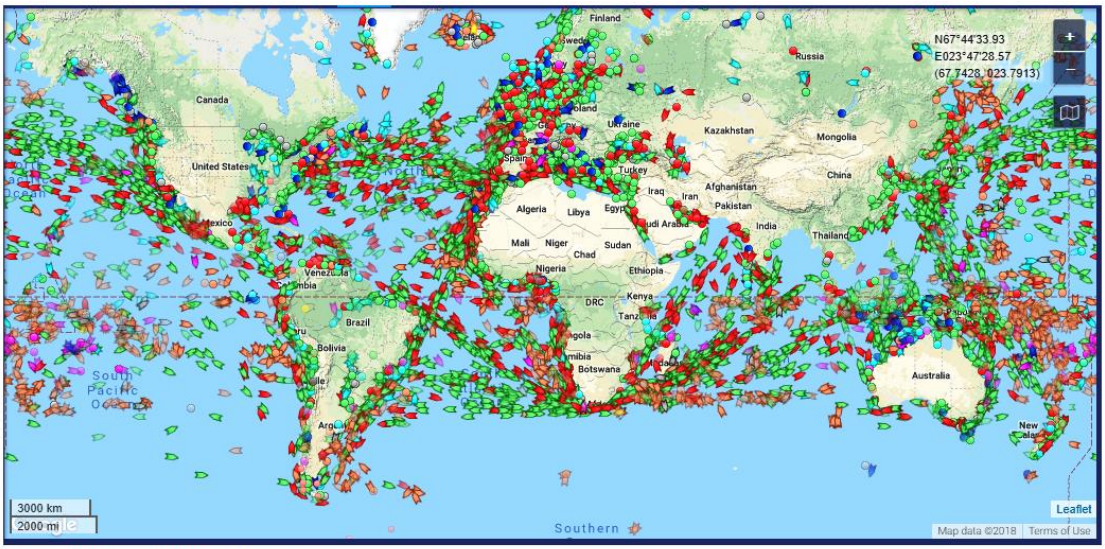

Figure 1: Ships at Sea: GMT Noon, 6 August 2018.
Source: An extract of map from *Marine Traffic*: www.marinetraffic.com/en/ais/home

[1] Check Point Software Technologies Ltd (https://checkpoint.com); Cheung, S., Lindquist, U. and Fong, M.W., 'Modelling Multistep Cyber Attacks for Scenario Recognition', *Proceedings of the Third DARPA Information Survivability Conference and Exposition* (DISCEX III), Washington DC, 22-24 April 2003, pp. 284-92.

Trends to July 2018: The Non-Maritime Context

Despite all the many advances in modern technology, it is still a dangerous world. Technology brings many benefits but it also brings many problems, not least in the contexts of security, speedier communications and higher standards of living enjoyed by some sectors of the community while, in contrast, large numbers of the populations of developing countries experience very basic, or even lower, levels of income for their survival. Cryptocurrencies and digital cash systems are vital vehicles for the laundering of stolen funds by cyber-thieves. Indeed, virtual cash is instrumental in the digital transfer of money that may or may not be able to be tracked down. It has been estimated that between US$80 billion and US$120 billion ($110 billion and $165 billion) of the cash generated by cybercrime is laundered annually. A significant proportion of that cash is channelled through various cryptocurrencies and digital payment systems to hide its origins.

In November 2016, Europe's largest manufacturer of wires and electrical cables lost £34 million ($59.5 million) in a "whale attack", when cyber-criminals deceived the staff at the finance department into transferring money to the wrong bank account. Similar tricks take place on a weekly basis around the world. On 11 April 2018 it was revealed that Russian cyber-criminals had targeted the United Kingdom in 40 separate incidents over the previous six months in what was described as a significant increase in the scale and severity of malicious cyber activity globally.

A daily glance through the Technology section of BBC *World News* presents the reader with an array of reports of "online scammers" fleecing their victims of thousands of pounds. Indeed, the Kent Police stated on 19 July 2018, that internet scammers had defrauded 45 people in that county alone of the collective sum of £128,000 ($224,000) by pretending to be broadband internet suppliers. The victims were all phoned and requested to give remote access to their computers on the pretence of their accounts being hacked or maintenance being carried out. The fraudsters were then able to get into the individuals' internet bank accounts.

Another report, from a cybersecurity company, on 20 July 2018, stated that hackers – allegedly the "Money Taker" gang – had targeted Russian banks to steal £700,000 ($1.22 million) in an attack that began in late-May. The gang initially concentrated on a piece of networking hardware known as a router, which they were able to compromise and use to gain access to the bank's internal networking systems. Once on the network, the fraudsters took the time to find the specific computer that authorised money transfers. The transfer of funds began on 3 July 2018, according to cybersecurity company *Group-IB*, which was called in to assist in the investigation. The Money Taker gang had already targeted other financial firms: during 2017, it was suspected of stealing nearly £7.5 million ($13 million) from US, British and Russian companies.

In another major incident, reported on 27 July 2018, fifty prison inmates in the US state of Idaho hacked the prison's IT system to artificially boost their personal bank accounts by stealing nearly US$225,000 ($308,000). The improper conduct did not involve taxpayers' dollars, although the culprits had hacked the prison's *JPay* system. *Jpay* is a private company that allows prisoners in the US access to portable devices which can transfer money,

download music, games and video entertainment, and exchange communications with family members. The conduct was intentional and not accidental.

BBC World News reported on 6 August that a Taiwanese company tasked with producing computer chips for Apple's *iPhone* had been infected with malware on 4-5 August 2018. The company had to shut down parts of its factories. The attack featured a "mutation" of the notorious *WannaCry* ransomware and is a warning that any organisation, even those working at the forefront of technological developments, can fall victim to malware.

Reports of maritime cybersecurity threats and incidents will increase greatly as technology becomes more sophisticated, the electronic and print media becomes more attentive and cyber-hackers launch ever more devious attacks. The maritime industry has been relatively slow to realise that ships, just like everything else, are now intricately linked to cyberspace.

The International Response (or the Lack Thereof)

The International Maritime Organisation (IMO), through the adoption of the International Ship and Port Facility Security Code (ISPS Code), introduced a prompt response to actual and potential terrorist attacks on ships during the late-1990s, especially in the wake of the 11 September 2001 attacks on US soil, the bombing of the French tanker MV *Limburg* and the USS *Cole* in the Gulf of Aden. The ISPS Code entered into force in 2004 and is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security standards for ports, ships and government agencies. The ISPS Code prescribes the responsibilities of governments, shipping companies, shipboard personnel and port/facility personnel to detect security threats and adopt preventive measures against security incidents affecting ships or port facilities used in international trade.[2]

The Container Security Initiative was launched in 2002 by the US Bureau of Customs and Border Protection. Its purpose was to increase security for container cargo shipped to the ports of the United States. The US-initiated Proliferation Security Initiative, launched in 2003, is a global effort that aims to stop the trafficking of weapons of mass destruction, their delivery systems and related materials to and from state and non-state actors of proliferation concern.

When it comes to cybersecurity, however, the IMO has been accused of being somewhat slow in formulating appropriate regulations. In 2014, the IMO consulted its membership on what a maritime cybersecurity code should contain. In 2016, interim cybersecurity risk management guidelines were issued. They were broad in content and, in hindsight, it may be argued, were not particularly maritime-specific.

In 2017, the IMO amended two of its general security management codes to explicitly include cybersecurity. The ISPS and International Safety Management Code (ISM) infer how port and ship operators should undertake risk management processes. Operators are to be at least conscious of cyber risks and make cybersecurity an integral part of their processes.

[2] *International Ship and Port Facility (ISPS) Code*, Part A, 1.2.1, International Maritime Organisation: London, 2004.

The cyber-specific amendments to the ISPS and ISM do not enter into force until 1 January 2021. Thus, the maritime industry, in mid-2018, still appears to be ill-equipped to deal with such future challenges as the cybersecurity of fully autonomous vessels. The development of forceful maritime cybersecurity regulations is necessary even though it may be a sluggish, costly and possibly painful process.

Electronic transactions – digitalisation – have become the new normal and a means of survival for companies in the maritime industry. Although often thought of as being quite a conservative industry – understandable, given the vast investments made in ships and port infrastructure – companies are now investigating the opportunities presented by the "Internet of Things" and Artificial Intelligence to boost their performance and cut costs. It is to be hoped that the results will not come at the expense of customer relations and the quality of services offered, as has been the case in many other industries.

Attacks on the Maritime Industry

The maritime industry has experienced several attacks within the space of the last 18 months. A recent victim, on 25 July, was, according to media reports, the Chinese shipping company China Ocean Shipping (COSCO). The company's network applications in the United States and elsewhere, including Argentina, Brazil, Canada, Chile, Panama, Peru and Uruguay, were affected and suffered failure. The company's ships were not affected, however, and continued operating normally; by 30 July, operations were back to normal mode.

Ship- and shore-based operations are cyber-connected. If shore-based and ship-based Information Technology (IT) systems are linked, it could open the floodgates to shipping companies, leaving them highly susceptible to an attack. Vessels do not need to be attacked directly because an attack can arrive via the company's shore-based IT systems and very easily penetrate the ship's critical Operational Technology (OT) systems.

In 2017, I.H.S. *Fairplay* conducted a maritime cybersecurity survey which found that many companies had experienced a cyberattack during the previous twelve months. Of those attacks, the majority were ransomware and phishing incidents of the kind that affect companies around the world, and were not at all specific to the maritime sector.

Indeed, shipping companies continue to be largely unprotected from potential cyberattacks, even after the high-profile June 2017 "Petya" ransomware attack on the Maersk Shipping Company. In that attack, the company's container shipping, oil tanker and tug boat operations were crippled by computer outages that allegedly slashed the company's profits by up to US$300 million. A financial disaster of that magnitude sends shockwaves through the maritime industry and shipping companies are increasingly concerned about the lack of effective security on their vessels.

Current IT defences, however, are usually not sufficient to repel cyberattacks. Shipping companies have become increasingly reliant on the interconnectivity between IT and OT systems to automate operations on ships. The higher number of systems connected to the Internet has heightened the risk of cyberattacks, the effects of which can be devastating, as witnessed by Maersk.

The US military was warned by the Pentagon, on 30 July 2018, not to install software believed to have been compromised by Chinese or Russian state-backed hackers. Official warnings about software supply-chain attacks are frequent.

The Maritime Industry: Complex and Confusing

There are several key issues that make cybersecurity for the maritime industry particularly complex, challenging and confusing. There are many different classes of ships, tugs and boats, all of which operate in very different environments. These vessels tend to have different computer systems built into them. Many of those systems are designed to last no more than three decades. Placed in another context, many ships operate outdated and unsupported operating systems, which are the ones most prone to cyberattacks.

The users of these maritime computer systems are in constant change. Ship crews are highly dynamic, often changing at short notice or more regularly over periods of three to six weeks. As a result, crews are often using systems that they are unfamiliar with, increasing the potential for cybersecurity incidents relating to human error.

The maintenance of shipboard systems, including navigational systems, is often contracted out to a variety of third parties. Much the same situation exists in land-based small enterprises. It is perfectly possible that a ship's crew may have little understanding of how different onboard systems interact with each other.

The linkage between onboard and terrestrial systems adds to the complexity. Many maritime companies stay in constant communication with the Masters of their ships. The cybersecurity of the ship is also dependent, in turn, on the cybersecurity of the land-based infrastructure that makes it possible.

Responses to Cyber Threats by Governments: Select Analysis

The first significant official Australian acknowledgment of cyberattack as a national security issue was raised in the 2000 *Defence White Paper*, which inferred that cyberattacks against critical Australian national information infrastructure were a possibility. The Defence Department was tasked with playing a key role in developing effective responses to such attacks. An *E-Security Initiative* was launched in May 2001 and an *E-Security Review* was made public on 19 December 2008.

The potential impacts of the emerging threat of cyberwarfare against Australia's defence infrastructure was emphasised in the 2009 *Defence White Paper*. In response, the Government established the Cyber Security Operations Centre and, in November 2009, the *Cyber Security Strategy* was released. In October 2017, the Australian Cyber Security Centre (ACSC) issued its annual *Threat Report*. Throughout 2017, the ACSC and its international partners continually observed the targeting of routers, including Australian routers, by malicious, sophisticated threat adversaries. Apparently, Australia, fortunately, has not yet been subjected to malicious cyber activity that would constitute an official cyberattack.

Each country is starting to adopt a cybersecurity stance. The General Data Protection Regulation (GDPR) for Europe came into effect on 25 May 2018, and the US, too, is putting

policies in place. In Asia, a number of countries, in late-2017, were more actively talking about their own cybersecurity requirements. In the future, it is likely that all ships will have to abide by certain cyber regulations as they sail the sea lines of communication from port to port worldwide.

The European Union Council, on 19-20 October 2017, asked for the adoption of a common approach to EU cybersecurity following the reform package proposed by the European Commission in September 2017. On 20 November 2017, the Council called for the strengthening of European cybersecurity and the enhancement of cyber-resilience across the EU.

The UK *National Security Strategy* of 2015 reaffirmed cyber threats as a Tier One risk to UK interests. The UK Government noted on 13 September 2017, in its *Cyber Security Code of Practice for Ships*, that cybersecurity is of increasing concern for many industries across the global economy, including the maritime sector. The maritime sector transports 95 per cent of British trade and must be protected. Indeed, all maritime trade should be protected.

Conclusion

The disruption caused by a cyberattack – or a compromised system – could be significant. A compromised ship system could initiate physical harm to the IT and OT systems on the ship, to its personnel and/or cargo, potentially endangering lives or causing the loss of the ship; the loss of sensitive information including commercially-sensitive or personal data; and, criminal activity, including fraud, kidnap, piracy, theft of cargo, or the imposition of ransomware. Cybersecurity is not just about preventing hackers from gaining access to systems and information. It is also about protecting digital assets and information, ensuring business continuity and making sure that the maritime industry is resilient to outside threats. It is essential to keep ship systems safe from physical attack and to ensure that supporting systems are robust.

While downtime can be a frustrating inconvenience when a cyberattack targets a manufacturing process or a logistics system and international shipping, the results can be exceptionally expensive. One year after the cyberattack on Maersk Shipping that shocked the maritime world by proving that it can happen to the very best, the importance of cybersecurity has come to the fore, especially in the wake of the attack on the COSCO shipping company.

Historically, the sea has been one of the most important conduits of economic prosperity. Due to the inherent dangers of the maritime environment – maritime terrorism, trigger-happy hijackers and sea pirates, negligent mariners and, now, cyber-criminals – the shipping industry must be more vigilant than ever if the global economy is to be sustained.

*****

*****

About the Author: Dr Forbes is a Distinguished Research Fellow and Guest Professor at Wuhan University, China; an Adjunct Research Professor with the National Institute for South China Sea Studies and an Adjunct Professor at the University of Western Australia. He is affiliated at the professorial level with other institutions in Australia, China and Malaysia and has a mercantile marine background.

*****

Published by Future Directions International Pty Ltd.
80 Birdwood Parade, Dalkeith WA 6009, Australia.
Tel: +61 8 9389 9831
Web: www.futuredirections.org.au