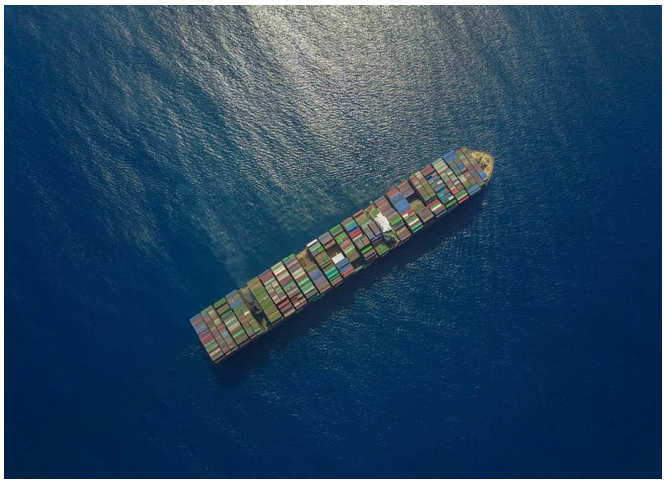
Why 50,000 ships are so vulnerable to cyberattacks

14 June 2018, by Keith Martin And Rory Hopcraft



The shipping industry has been slow to prepare adequate cybersecurity. Credit: Alexandersonscc/pixabay, CC BY-SA

The 50,000 ships sailing the sea at any one time have joined an ever-expanding list of objects that can be hacked. Cybersecurity experts recently displayed how easy it was to break into a ship's navigational equipment. This comes only a few years after researchers showed that they could fool the GPS of a super-yacht into altering course. Once upon a time objects such as cars, toasters and tugboats only did what they were originally designed to do. Today the problem is that they all also talk to the internet.

The story so far

Stories about maritime cybersecurity are only going to proliferate. The maritime industry has been slow to realise that ships, just like everything else, are now part of cyberspace. The International Maritime Organisation (IMO), the UN body charged with regulating maritime space, has been late and somewhat slow in considering appropriate regulation when it comes to cybersecurity.

In 2014, the IMO consulted their membership on what maritime cybersecurity guidelines should look like. Two years later they issued their interim cybersecurity risk management guidelines, which are broad and not particularly maritime specific. And now, unsurprisingly, ships are being hacked.

Complexity of the maritime industry

There are several core issues that make cybersecurity for the maritime industry particularly challenging to address.

First, there are many different classes of vessel, all of which operate in very different environments. These vessels tend to have different computer systems built into them. Significantly, many of these systems are built to last over 30 years. In other words, many ships run outdated and unsupported operating systems, which are often the ones most prone to cyber-attacks.

Second, the users of these maritime computer systems are constantly in flux. Ship crews are highly dynamic, often changing at short notice. As a result, crew members are often using systems they are unfamiliar with, increasing the potential for cybersecurity incidents relating to human error. Further, the maintenance of onboard systems, including navigational ones, is often contracted to a variety of third parties. It is perfectly possible that a ship's crew have little understanding of how onboard systems interact with each other.

A.P. Moller-Maersk's entire fleet was delayed due to a cyber-attack in 2017. Credit: Wikimedia/Nils Jepsen, CC BY

A third complexity is the linkage between onboard and terrestrial systems. Many maritime companies stay in constant communication with their vessels. The cybersecurity of the ship is also dependent, then, on the cybersecurity of the land-based infrastructure that makes this possible. The implications of such dependencies was made clear in 2017 when a cyber-attack on the systems of A.P. Moller-Maersk resulted in cargo delays across their entire fleet. This is particularly challenging for the IMO who can govern the likes of port regulations, but have very little control over the wider systems and processes of maritime operators.

Steps in the right direction

In 2017, the IMO amended two of their general security management codes to explicitly include cybersecurity. The International Ship and Port Facility Security Code (ISPS) and International Security Management Code (ISM) detail how port and ship operators should conduct risk management processes. Making cybersecurity an integral part of these processes should ensure that operators are at least conscious of cyber-risks.

Hopefully, this is the start of a more holistic approach to maritime cybersecurity regulation. The knowledge gained from these new cyber-risk assessments may enable the IMO to develop a broader set of cybersecurity regulations. There is a lot of low-hanging fruit to be picked, for example by harmonising some equipment requirements with existing cybersecurity standards adopted by other sectors.

Turning the ship around

The maritime industry is undoubtedly behind other transportation sectors, such as aerospace, in cybersecurity terms. There also seems to be a lack of urgency to get the house in order. After all, the cyber-specific amendments to the ISM and ISPS don't come into force until January 1 2021, and they only represent the beginning of a journey. So the maritime industry seems particularly ill-equipped to deal with future challenges, such as the cybersecurity of fully autonomous vessels.

On the positive side, the slow and steady approach to development of cybersecurity regulations at least provides the opportunity to learn from other sectors and fully understand maritime cybersecurity risks, rather than make hasty ill-informed decisions.

Development of robust maritime cybersecurity regulations is going to be a very slow, and possibly painful, process. But, the ship has started turning.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

APA citation: Why 50,000 ships are so vulnerable to cyberattacks (2018, June 14) retrieved 3 March 2021 from https://phys.org/news/2018-06-ships-vulnerable-cyberattacks.html