Photos: www.pexels.com

Building up port cybersecurity capacity

A matter of great urgency

by **Tuomas Kiiski**

Recently, anything with a prefix "cyber-" has been over-popularized in media headlines and policymaking discussions. Nonetheless, the cyber domain – which initially sounded like science fiction – has become very, very real thanks to the escalating use of digital applications and networks in daily life, and the growing capacity to store and process data. However, a number of new threats emerged alongside these development-unlocking tech advances, catching some of the port industry players off guard.

This article is part of the HAZARD Project, co-funded by the EU within the Baltic Sea Region Interreg programme, which aims to mitigate the effects of major accidents and emergencies at key seaports in the Baltic Sea region through i.a. better preparedness, coordination, and communication, as well as by enhancing the handling of post-emergency situations. For more info please visit blogit.utu.fi/hazard.

Tuomas Kiiski, D.Sc. (2017, Econ. & Bus. Adm.) is a University Teacher in Turku School of Economics at the University of Turku. He also holds a M.Sc. and a B.Sc. in Economics and Business Administration, and a BBA in Business Logistics. His research interests are in maritime economics and Arctic shipping. Tuomas has also worked in freight forwarding and container shipping.

Like any emerging field, the cyber domain has its own terminology, which is still far from being systematized. Cyber threat, cyberattack, and cybersecurity are the three most commonly cited terms.

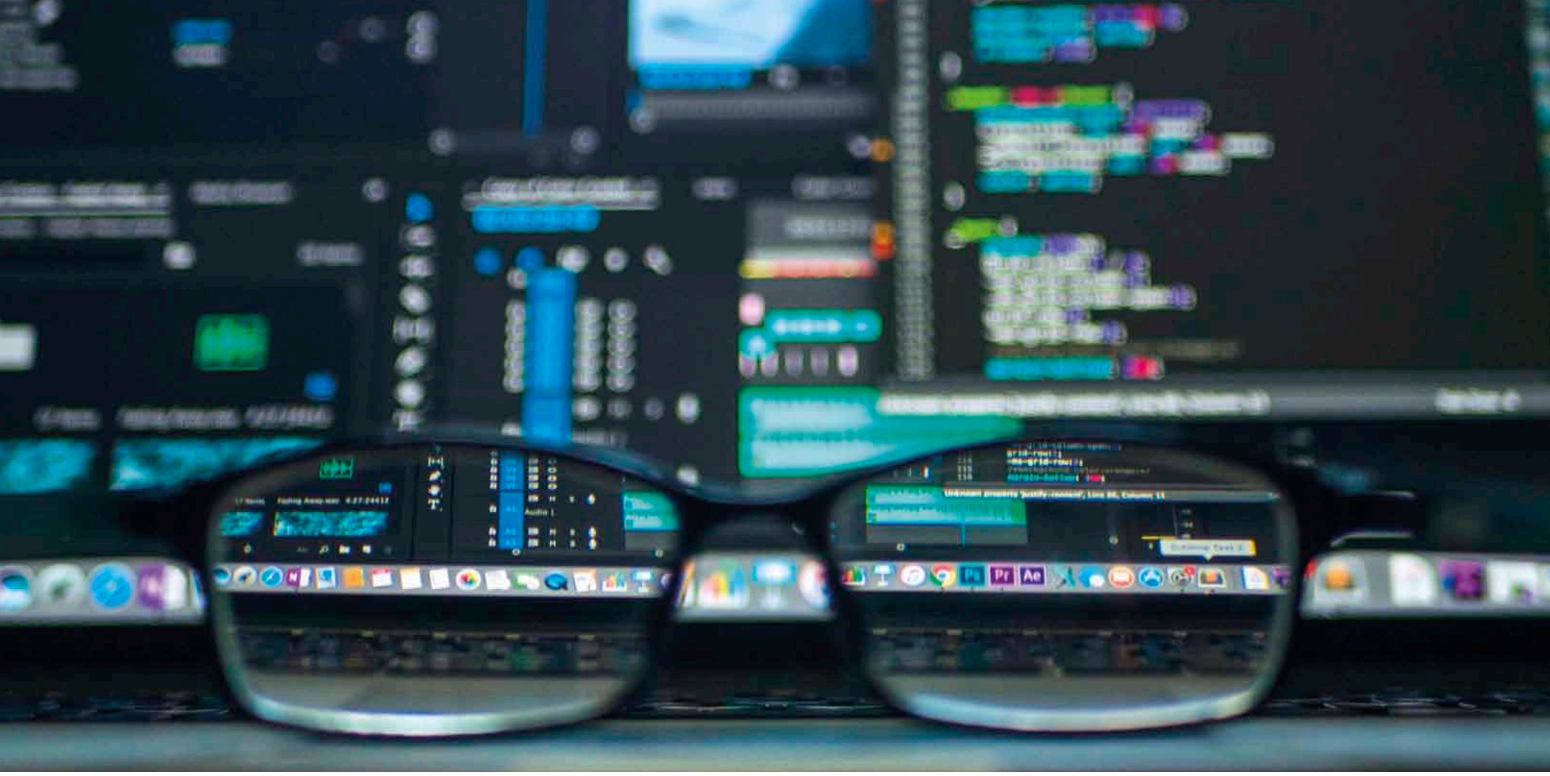
The first one is used to describe danger arising from cyberspace. Cyber threats are classified in growing order of severity as hactivism, cybercriminality, cyberespionage, cyberterrorism, and cyberwar. Each has individual elements relating to the actors, motives, and objectives involved. Depending on the parties concerned – hackers, cyber criminals, cyberterrorists, but also state agencies – their motives and objectives are diverse and often include excitement, fame, money, as well as influencing political agendas.

A cyberattack can be defined as a cyber threat that materialized. Methods of attack include phishing (an attempt to obtain sensitive information), malware (intrusive software, like computer viruses, worms, Trojan horses, etc.), and the so-called denial-of-service attack (where domains are shut off because their host servers cannot handle the sudden flood of access requests).

As a countermeasure, cybersecurity aims to maintain the desired state of access to and control of IT systems through diversified efforts. At a minimum, it calls for ensuring and maintaining password integrity and software updates. At a more sophisticated level, it requires adopting specific passive and/or reactive strategies for making the IT systems as resilient as possible to malicious acts.

Why ports?

Arguably, two of the most renowned cyberattacks against ports occurred in Antwerp in 2011, and against A.P. Møller-Mærsk's terminal operating arm, APM Terminals, in mid-2017. These cases illustrate opposite ends of the spectrum in terms of scale and consequences. What makes the Antwerp incident stand out was the fact that the multi-staged attack began already in 2011, when the port's container management system was breached in an attempt to smuggle narcotics, but it took until 2013



before the case was finally resolved. The damages from that attack were limited to missing containers.

While the Port of Antwerp was an isolated target, Maersk was a part of a wider cyberattack aimed at numerous industry players and governmental bodies in several countries. For APM, the attack temporarily halted some of its terminal operations, reportedly resulting in financial losses of up to USD 300 million. In addition to these two cases, a more detailed analysis shows that between 2010 and 2017, at least 10 other cyberattacks took place around the world that directly or indirectly involved the maritime sector.

Ports are particularly vulnerable to cyberattacks because of their multidimensional role and basic features. Globally, ports constitute key nodes of seaborne trade. From a national security perspective, they are part of the critical infrastructure that constitutes the backbone of society's functionality. Similarly, ports' operational features make them attractive targets in terms of the high level of automatization and reliance on data systems combined with massive throughput volumes, scope of operations, large number of operators, and high monetary values involved.

Login: admin, password: admin

Considering the recent growth of cybersecurity awareness in all spheres of public life, surprisingly little information is available on the current preparedness of ports against cyber threats. This is arguably attributable to three factors: the novelty of the topic, general secrecy policy related to security issues, and the discretionary nature of the subject. For example, the novelty of the topic is clear from the scant number of academic articles on it.

Yet there are signs that not only raise doubts over the capacity of ports to effectively counter cyberattacks, but also suggest that a complete overhaul of the regulatory framework is needed. In 2011, a study by the European Union Agency for Network and Information Security (ENISA) concluded that there is poor to non-existent awareness of cybersecurity-related issues within the maritime sector. Six years later, the matters have scarcely improved. A survey conducted for the HAZARD project in 2017 highlighted the insufficient level of preparedness, as well as a lack of proper regulations in Baltic Sea ports regarding cybersecurity.

Hindsight is 20/20

Consistent with the maritime industry's traditionally reactive approach to adopting new regulations, the development of cybersecurity regulations has been sluggish. The pace only picked up following the mounting reports of cyberattacks, and the subsequent increased awareness of cybersecurity.

Over the past five years, policymakers and other stakeholders at various levels have become engaged in cyber issues by adopting cybersecurity strategies or guidelines. For example, the European Union introduced its cybersecurity strategy in 2013, and respectively United States Coast Guard did the same in 2015 for critical maritime infrastructure. In 2016, the International Maritime Organization (IMO) introduced interim guidelines on maritime cyber risk management. BIMCO, along with several other shipping industry associations, published cybersecurity guidelines to tackle the issue, too.

Notwithstanding these efforts, the global regulatory status on mandatory port cybersecurity seems somewhat neglected. Cybersecurity is not included in any of the IMO Conventions related to port safety and security, such as the ones on International Ship and Port Facility Security (ISPS) or International Safety Management (ISM). However, some progress has been made: IMO's Resolution adopted in June 2017 will make cyber risk management on board ships mandatory as of January 1st, 2021.

Don't be the one to blame

When it comes to mitigating cyber threats in ports, there is definitely room for improvement. The current level of port preparedness seems inadequate, and the adoption of global mandatory regulations for port cybersecurity is still pending. The issue is both novel and of great urgency, as cyberattacks are becoming more common, with pervasive impacts on the society. The maritime sector in general, and ports in particular, is no exception, as demonstrated by the recent attack against APM Terminals (in this regard also read the articles *The threat hidden in the depths. Maritime cyber security* in BTJ 4/16, and *The threat is real. Preparing for and dealing with cyberattacks* in BTJ 3-4/17).

The scale of global shipping calls for a coordinated effort to ensure that adequate practices and regulations are adopted throughout the industry. ■