SUBSCRIBE: www.harboursreview.com

no. 4/2017 (16) september ISSN 2449-6022

Harbours review

Cyber security and risk management

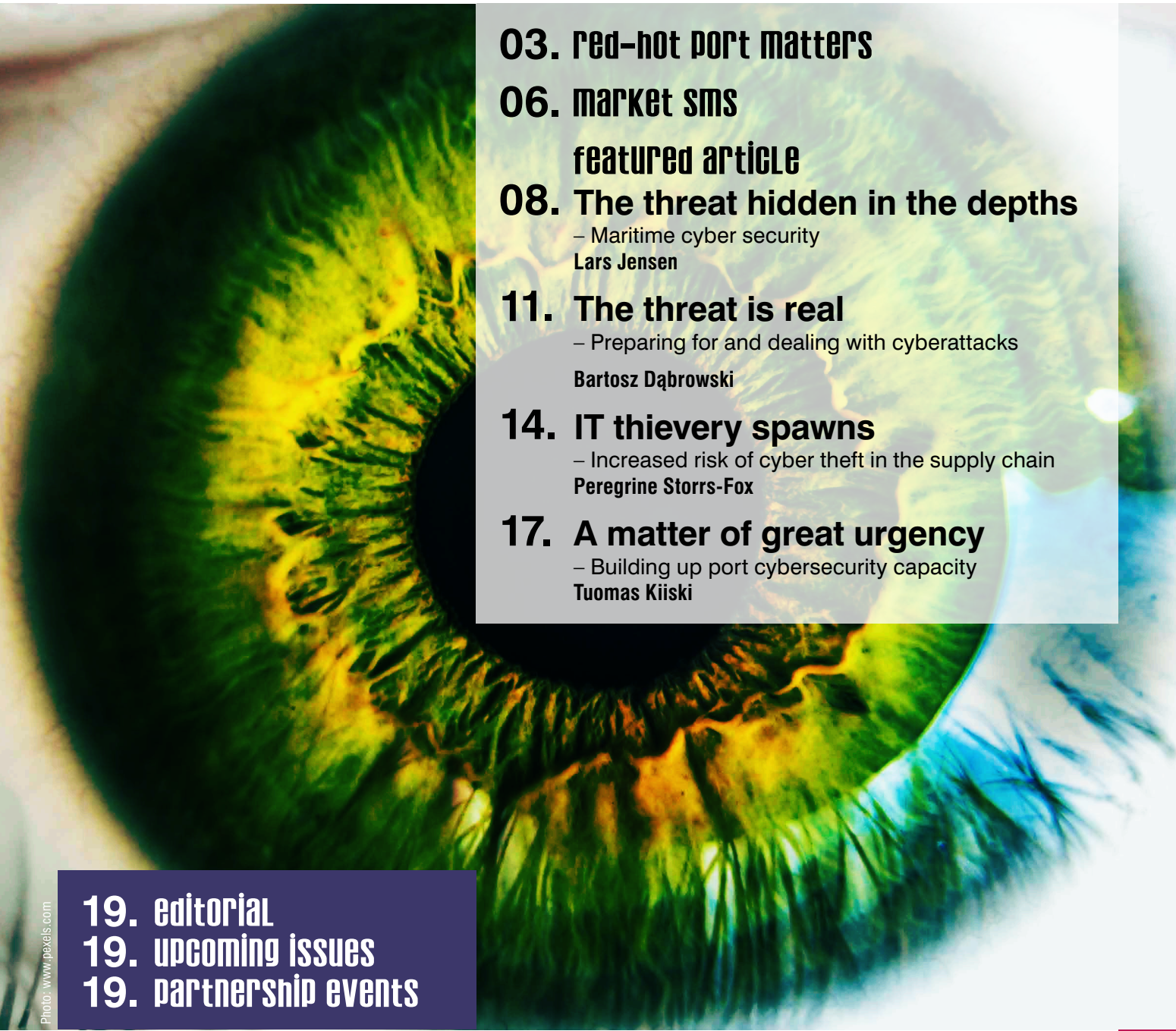


Photo: www.pexels.com

Experience the progress.

Mobile Harbour Crane

- Fast, efficient and versatile material handling equipment
- X-shaped undercarriage guarantees the best weight distribution
- 360-degree mobility - outstanding in the MHC market
- Stepless hydrostatic power transmission for smooth and sensitive operation
- Flexibility makes it effective for all areas of application in the harbour

mobile.harbour.crane@liebherr.com
facebook.com/LiebherrMaritime
www.liebherr.com

LIEBHERR

red-hot port matters

Photo: www.all-free-download.com

Photo: Liebherr

Kloosterboer deploys new machinery in Vlissingen

The Dutch company has opted for new port equipment manufactured by Liebherr – a mobile harbour crane as well as a reachstacker. The LHM 550 mobile harbour crane has a max lifting capacity of 144 tonnes and an outreach of up to 54 metres. It also features Liebherr's software tool Advanced Container Control installed in tandem with the Soft Touch Down system. The reachstacker is of the LRS 545 type, able to stack five containers high. Kloosterboer has put into operation its new equipment at the company's Vlissingen terminal located in Zeeland Seaports. Most recently, the fruit heavyweight Chiquita decided to land its shipments in the port, while at the same time CMA CGM added Vlissingen to its EURAF service which links the Benelux with West Africa. "Thanks to our new Liebherr mobile harbour crane in cooperation with the reachstacker LRS 545 we are very optimistic to meet or even exceed the needs of our customers. We now provide all what it take to efficiently unload, store, and distribute fruits and other temperature controlled cargo, conventional as well as containerised," Marc Rommers, Manager for Operations and Technical Department, Kloosterboer, said.

Photo: Associated British Ports

Investments in the Port of Cardiff

ABP South Wales is investing over GBP 4 million into warehouse improvements and handling equipment in order to support customers in the steel, forest products, and other general cargo sectors. All works are due to be completed by the end of 2017. Back in April last year, the British port operator took over the stevedoring of steel and general cargo operations at Cardiff from a third-party provider. "We have worked closely with steel sector customers over the past 18 months to best establish how the port can meet the needs of their individual businesses. This substantial investment has resulted in these businesses committing to remaining at the Port of Cardiff for many years to come," Matthew Kennerley, Director, ABP South Wales, said.

Lithuania's first LNG shipment from the US

The carrier *Clean Ocean* moored next to Lithuania's floating terminal *Independence* on August 21st, bringing approx. 140 thousand m^3 of Liquefied Natural Gas. As it was in the case of the first US LNG shipment to Poland, the load was bought from Cheniere Energy, with *Clean Ocean* being loaded at the company's terminal in the Port of Sabine Pass. The buyer, the state-owned Lithuanian Gas Supply, will feed the internal market with part of the shipment, while the remaining portion will be pumped to gas storage facilities in Latvia.

Photo: Dynagas

World's first LNG-retrofitted container ship

On August 23rd, Wessels Reederei re-launched the 2011-built 1,000 TEU of capacity *Wes Amelie*, whose engine was converted to run on Liquefied Natural Gas. The LNG conversion, completed by the German Dry Docks in Bremerhaven, was supported by the German Federal Ministry of Transport and Digital Infrastructure, and will likely be extended to other ships in the fleet (Wessels Reederei operates 15 *Wes Amelie*'s sister ships). The ship's initial bunkering was carried out by the Hamburg-based Nauticor at the Kühlhauskai Quay in the Port of Bremerhaven. In total, four trucks were brought to fill *Wes Amelie* with LNG. "Due to the smooth cooperation between the ship's crew, the Bremenports team, and our experienced specialists, the initial bunkering was a complete success," Sonja Neßhöver, Director of the LNG Portfolio, Nauticor, said. Christian P. Hoepfner, Authorized Representative of Wessels Reederei, added, "We are glad that the first transfer of LNG in Bremerhaven has been completed so smoothly. Our thanks go to the Harbor Security Office Bremerhaven, the Port Authorities of the Hanseatic City of Bremen, and the LNG supplier Nauticor, who have supported us actively in this project." "With the conversion of *Wes Amelie*, Wessels Reederei has become a pioneer in establishing LNG as fuel for container ships. We are happy to support that effort and are looking forward to future cooperation, taking into consideration that our second LNG bunker vessel will start operations in Northwest Europe next year with a focus on customers in the North and Baltic Seas," Mahinde Abeynaike, Managing Director, Nauticor, summed up.

Photo: Nauticor

North France and East Canada team up

HAROPA (gathering under one banner the ports of Le Havre, Rouen, and Paris) and the Port of Montreal have singed a co-op agreement. The main objective of the partnership is to strengthen and extend cooperation on various technical, sales, and research/innovation issues, as well as to develop synergies between the involved ports in the light of the Comprehensive Economic and Trade Agreement (CETA) between the EU and Canada, which will enter into force on September 21st. Specifically, HAROPA and the Montreal port will work on inter-port governance (e.g. pilotage and dredging, river resource management, social acceptability of port projects); sales and promotion (organising joint business meetings, setting up B2B social media platforms); as well as on innovation (the use of Artificial Intelligence and blockchain in the logistics supply chain). "As the leading French port system, HAROPA is very pleased about this agreement with Montreal which is, to-date, our major trade partner in Canada and our 2nd largest partner on the East-American coast. Through the experience acquired via about 30 twinning and cooperation agreements we have signed, we know all the synergy which will be set up with Montreal and the benefits for our two ports," Hervé Martel, President, HAROPA, said. Sylvie Vachon, Chairwoman and CEO, Montreal Port Authority, added, "Already about 40% of the goods going through the Port of Montreal come from or go to Northern Europe. The global economic and trade agreement between Canada and the European Union will strengthen these trade bonds and create a new favourable business environment to the growth of our trade and the structuring effects that will follow from that in our respective economies. This memorandum of understanding between HAROPA and the Montreal port authority is signed at a significant and historic time."

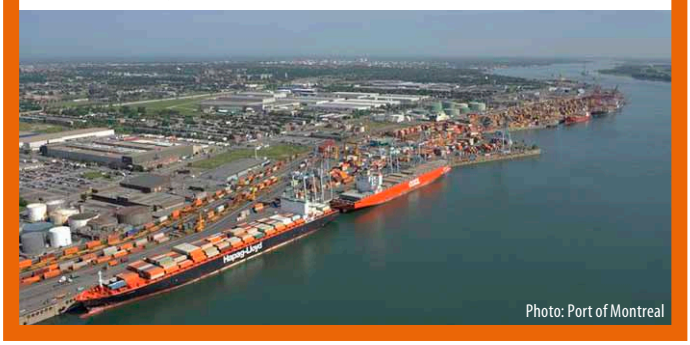


Photo: Port of Montreal

Brittany Ferries charters one of Stena Line's newbuilds

The companies have signed a five year-long charter agreement under which the third in a series of four new ro-paxes will sail under Brittany Ferries' colours. In the meanwhile, the first steel cutting ceremony has been held at the Chinese AVIC Weihai Shipyard, where Stena Line's new ferries are to be constructed. The first ship will be delivered in 2019, while the remaining three one year later the latest. Stena Line's contract with AVIC includes an option for four more ships. Each ro-pax will be 214.5 meters long and 27.8 meters wide, offering room for up to 1,000 passengers, as well as 3,100 lane metres of cargo space. The newbuilds, to burn conventional bunker for the time being, will be however gas-, scrubber-, and selective catalytic reduction-ready. According to Stena Line, the newbuildings are to emit 25% less CO_2 per cargo unit than comparable in size ferries. Stena Line plans to put the three new units on routes to and from its Belfast hub. Brittany Ferries, in turn, intends to link England and Spain with its chartered vessel.


Photo: Stena Line


Photo: DFDS

Tulipa Seways joins DFDS' fleet

The ro-ro ship started to serve the Rotterdam-Immingham route on August 22nd, joining the sister unit *Gardenia Seaways* which entered into service in July. The vessels are 210 meters long and each offer 4,076 lane metres cargo capacity.

APM Terminals Zeebrugge to change hands

COSCO Shipping Ports, a subsidiary of COSCO Shipping, has put on the table EUR 35 million for 74% of the container terminal's shares. The deal is expected to close by the end of November 2017. However, it is subjected to adjustments and fulfillment of conditions precedent. As part of the transaction, APM Terminals has proposed to buy back 25% of the Shanghai International Port Group shares, and will then sell them together with APM Terminals' own 51% stake in Zeebrugge to COSCO Shipping Ports. This transaction is subject to customary regulatory approvals, estimated to take three to four months for completion. APM Terminals Zeebrugge was launched in 2006 and offers now 1.0 million TEU/year of capacity. COSCO became its minority shareholder in 2014, buying a 24% stake.

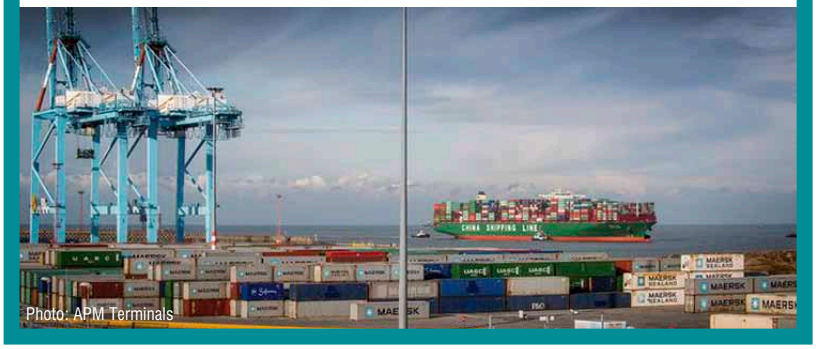


Photo: APM Terminals

OT Logistics takes over Rijeka's reins

The Polish company has come to an agreement with the Croatian pension funds Allianz ZB and ERSTE, taking over operational and financial control over the Rijeka port. OT Logistics, Allianz ZB, and ERSTE hold 32.56%, 15.15%, and 8.85% of the port's shares, respectively, giving them the majority stake of 56.56%. Earlier this year, OT Logistics increased its share level by acquiring 11.75% of the Port of Rijeka's stocks. The agreement, detailing how the parties will run the port authority, has been signed for a period of seven years. "Thanks to increasing our own stock commitment in the Port of Rijeka Authority as well as by partnering with other shareholders, we've gained tangible influence over the port's operations. Rijeka is a very important spot on the European transport map. We believe that it could become a gateway for the flow of goods between Europe, Africa, the Middle East, and the Arabian Peninsula," Zbigniew Nowik, President of the Board, OT Logistics, said. He then added, "Moreover, having 50% + 1 stock is still on our company's agenda."


Photo: OT Logistics

Konecranes' service agreement with MPET

The Finnish company will perform all of the maintenance and repair works on more than 150 of its Noell Straddle Carriers of different generations for MSC PSA European Terminal (MPET). "Last year, we exceeded the ten million TEU mark for the first time, which led to an increasing need for new machines. As a result, our fleet of Konecranes Noell Straddle Carriers has expanded by almost 100 machines in the past 12 months. To keep the availability of the straddle carriers as high as possible, we are now entrusting the service work on the machines to their manufacturer Konecranes. We are certain that we are well-equipped for the anticipated continued growth of the terminal over the long term," Randy Verresen, Manager Rolling Equipment, Antwerp Terminal Services NV, said. Tom Cerpentier, Regional Director Port Services, Konecranes, added, "Antwerp is one of the most important ports for us. In addition to straddle carriers, other types of Konecranes port equipment such as mobile harbor cranes, automated stacking cranes and lift trucks that are operated by various customers in the port need to be serviced and maintained. This is why our on-site service team comprises a total of 18 technicians and will now be strengthened by another 16 service experts specifically as part of the service agreement concluded with MPET for the straddle carriers."


Photo: Konecranes

FESCO rail-links China and Europe

The Moscow-based company has launched a weekly container train between Zhengzhou and Hamburg, the FESCO Silk Way Shuttle. The first westbound train with 42 containers was loaded with consumer goods, spare parts, equipment, and food products, on its way crossing Mongolia, Russia, Belarus, and Poland. The estimated transit time on the FESCO Silk Way Shuttle is 13-15 days.

Photo: FESCO

market sms

Photo: www.pexels.com

PORT OF YSTAD:

124,712 ro-ro cargo units handled in H1 2017 (+7.9% yoy)

The Swedish port saw five new all-time highs – the best first half year result ever, as well as in the turnover of total freight, trucks & trailers, pax cars, as well as the numbers of passengers served.

Port of Ystad's volumes

	H1 2017	Yoy
Total cargo traffic	1,718.7 thou. tn	+3.0%
Ro-ro cargo units, of which	124,712	+7.9%
Trucks & trailers	120,838	+9.0%
Railcars	3,874	-18.1%
Passengers	924,133	+7.1%
Pax cars	242,282	+7.8%
Busses	1,370	-1.7%

PORT OF ZEEBRUGGE:

18.3 mln tn handled in H1 2017 (-5.7% yoy)

Ro-ro traffic amounted 7.3 million tonnes in the reported period, up by 2.2% year-on-year. New cars advanced as well, by 3.3% yoy to 1.4 million units. In contrast, container volume fell by 5% yoy to 7.3 million tonnes, while dry bulk rose slightly to 733,965 tonnes (+1.2% yoy). Break-bulk noted a light drop by -0.4% yoy to 753,326 tonnes. Liquids decreased most, by 28.5% yoy to 2.2 million tonnes, however LNG shipments went up by 54.5% to 659,045 tonnes.

TRANS-SIBERIAN RAILWAY:

453.3 thou. TEU carried in H1 2017 (+38.8% yoy)

Transit traffic along the Transsib, serving i.a. the New Silk Road, amounted to 205.8 thousand TEU in the reported period, noting an increase by 64% year-on-year. The remaining 247.7 thousand TEU were carried domestically.

PORT OF ALGAVRE:

55,232 tn handled in H1 2017 (-63.8% yoy)

Commercial Quay of Faro made 54,333 tonnes (-64.3% year-on-year), while Commercial Quay of Portimão 899 tonnes (+100% yoy). The number of passengers in Portimão went up by 55.3% to 10,999 travellers.

CTSP:

319,000 TEU handled in H1 2017 (+10.7% yoy)

Container exports going via the Container Terminal Saint-Petersburg increased in the first half of 2017 by 11.7% year-on-year to a total of 176,300 TEU. At the same time, imports amounted to 142,700 TEU (+9.5% yoy), including 35,700 twenty-foot reefers. The share of rail-handlings totalled 30%.

LATVIAN SEAPORTS:

43.06 mln tn handled in I-VIII 2017 (+4.8% yoy)

With 23.05 million tonnes (+16.3% year-on-year), the turnover of dry bulk accounted for more than half of the volumes going through the country's ports over 2017's first eight months. Among many, handlings of dry bulk comprised coal (+30.3% yoy to 12.97 million tonnes), chemicals (-11.5% yoy to 1.92 million tonnes), and woodchips (+14.4% yoy to 0.97 million tonnes). Throughput of liquids saw a downtick of 13.3% yoy to 12.38 million tonnes, including 11.85 million tonnes of oil products (-13.7% yoy). General cargo traffic, on the other hand, rose by 8.9% yoy to 7.62 million tonnes. Containerised freight gained 14% yoy and totalled 2.97 million tonnes, timber contracted by 2% yoy to 2.25 million tonnes, while wheeled (ro-ro & ferry) cargo advanced by 13.3% yoy to 2.06 million tonnes. As for individual ports, Riga handled a total of 22.71 million tonnes (-4.9% yoy), followed by Ventspils – 15.06 million tonnes (+17.2% yoy), Liepāja – 4.17 million tonnes (+24.4% yoy), Skulte – 599.5 thousand tonnes (+27.8% yoy), Mērsrags – 295.6 thousand tonnes (-9.4% yoy), and finally Salacgrīva – 175.8 thousand tonnes (-12.3% yoy).

PORT OF TURKU:

62,154 trucks & trailers handled in I-VII 2017 (+2.2% yoy)

Out of the total, imports accounted for 15.4 million tonnes (+6.7% year-on-year), while exports added the remaining 10.6 million tonnes (+7.0% yoy). The Finnish Port of Turku made 1,323 twenty-foot containers (-0.5% yoy) over this year's first seven months. In total, the port handled 1,490.9 thousand tonnes (+5.4% yoy) in the reported period. Foreign traffic made 1,377.3 thousand tonnes (+1.4% yoy), of which exports went up by 0.2% yoy to 789.5 thousand tonnes, and imports by 3.1% yoy to 587.8 thousand tonnes. Domestic traffic totalled 113.6 thousand tonnes (+103% yoy). Exports rose by 801% yoy to 63.6 thousand tonnes, whereas imports by 2.2% yoy to 50.1 thousand tonnes. Turku's passenger traffic increased as well - by 0.4% yoy to a total of 1,967,206 travellers.

PORT OF SINES:
25.81 mln tn handled in H1 2017 (+7.3% yoy)

Containers observed the sharpest increase of 33.7% year-on-year to 926,212 TEU. In total, the port handled as much as 11.88 million tonnes of general cargo (+24.7% yoy), as well as 2.92 million tonnes of dry bulk (+6.5% yoy). Liquids, on the contrary, noted a downtick to 11.02 million tonnes (-6.6% yoy).

PORT OF KAVKAZ:
19.97 mln tn handled in I-VII 2017 (+32% yoy)

Grains throughput increased the most, by 420% year-on-year to 4.73 million tonnes. Sulphur and mineral fertilizers rose as well, to 2.22 million tonnes (+37% yoy). Handlings of oil and oil products went down by 13% yoy to 6.29 million tonnes, while of LPG to 75 thousand tonnes to -34% yoy. As many as 2,915,157 passengers visited the Port of Kavkaz, up by 3% yoy.

Source: portnews.ru

HAPAG-LLOYD:
4.22 mln TEU carried in H1 2017 (+14% yoy)

The figure includes almost 0.25 million TEU from the United Arab Shipping Company (UASC) with whom Hapag-Lloyd merged on May 24th, 2017. "The market in container shipping remains challenging, but we have managed to make very good progress in the first half year of 2017. We improved profitability significantly and the integration of UASC is largely completed in the third quarter. That will allow us to start capturing synergies very soon after the integration," Rolf Habben Jansen, CEO, Hapag-Lloyd, commented.

UKRAINIAN SEAPORTS:
76.2 mln tn handled in I-VII 2017 (+3.3% yoy)

Exports totalled 58.1 million tonnes (+3.6% year-on-year), followed by imports – 10.9 million tonnes (+18.8% yoy), transits – 6.5 million tonnes (+3.1% yoy), and coastal traffic – 700 thousand tonnes (-66.1% yoy). Increased grain handlings (+17% yoy to 22.3 million tonnes) were the main driver behind the rise in export traffic. The turnover of vegetable oils and construction materials rose as well – by 32% yoy and 50% yoy to 3.3 million tonnes and 2.6 million tonnes, respectively. However, exports of ores went down by 8.2% yoy to 13.3 million tonnes, while of metals and metal products – by 9% down to 7.9 million tonnes. The rise in transit traffic was chiefly driven by coal shipments – up by 112% yoy to 2.4 million tonnes. Turnover of metals increased here by 2.5% yoy to 200 thousand tonnes. With 54.9 million tonnes (+6.6% yoy), dry bulk accounted for the majority of Ukrainian seaports' freight throughput in the reported period. Liquids advanced by 7.6% yoy to 6.5 million tonnes. Container trade totalled 346,500 TEU (+4.7% yoy), out of which 173,200 TEU were imported (+4.8% yoy) 152,300 TEU exported (+2.5% yoy), 19,900 TEU made in transit (+26.9% yoy) and the remaining 1,000 TEU in coastal traffic (-24.2% yoy).

PORT OF ZEEBRUGGE:
18.3 mln tn handled in H1 2017 (-5.7% yoy)

Ro-ro traffic amounted 7.3 million tonnes in the reported period, up by 2.2% year-on-year. New cars advanced as well, by 3.3% yoy to 1.4 million units. In contrast, container volume fell by 5% yoy to 7.3 million tonnes, while dry bulk rose slightly to 733,965 tonnes (+1.2% yoy). Break-bulk noted a light drop by -0.4% yoy to 753,326 tonnes. Liquids decreased most, by 28.5% yoy to 2.2 million tonnes, however LNG shipments went up by 54.5% to 659,045 tonnes.

featured article

Photos: www.pexels.com

The threat hidden in the depths

by **Lars Jensen**, *CyberKeel's CEO*

CyberKeel is a 2014-founded Copenhagen-based company dealing with maritime cyber security. The company's employees combine unique expertise, deep insights, and experience from working earlier in the maritime industry, with hard-core cyber security skills – and its opposite, the world of hacking. CyberKeel's know-how allows to assist companies not only in enhancing their IT security, but also in raising staff awareness. For more information, please visit www.cyberkeel.com.

The rapid increase in satellite bandwidth combined with decreasing costs have resulted in the world's vessel fleet rapidly becoming an integral part of the Internet of Things. Ports and terminals are embracing automation with driverless vehicles, while others experiment with airborne supply deliveries using remote-controlled drones. At the same time, the world of shipping is finally catching up to the technology of the 21st century with processes and information exchanges being automated.

All of these developments are to be welcomed, as they drive efficiency and value. To put it another way, they are a necessity for any maritime company with the ambition to still be part of the industry ten years from now.

However, there is a hidden threat in this vast ocean of maritime opportunities. Unfortunately, it is a threat which many companies do not address, and of those that do, their approach is often flawed and ineffective. The threat is cyber-attacks, and despite its intangible nature, the damage it does is by all means concrete.

Let us then address this issue in three steps by answering the following questions: Is the threat real? What is the nature of it? And what can – and should – maritime companies do about it?

Is the threat real?

When CyberKeel was one of the first companies to address maritime cyber security some three years ago, most companies were of the opinion that the cyber-attack threat was mainly hypothetical, but not something that was actually happening. Much like a Hollywood movie script which might seem realistic at first glance, but eventually has no solid footing in reality. Additionally, cyber security companies are at times accused of scare-mongering for the sake of simply generating business for themselves. Hence, the question is a valid one: Is there actually a genuine threat, lurking in the depths?

Regrettably, there is no shortage of actual examples, many documented over the last couple of years. Shipping lines and agents have lost millions of dollars due to e-mail accounts being compromised and misused; maritime information systems have been hacked by criminals and used for smuggling purposes; electronic certificates have been stolen for fraudulent purposes; as well as both ports and merchant vessels experiencing cost-burdening downtimes due to cyber-attacks. Additionally, as the maritime industry is just now joining the Internet of Things in its earnest, it is only now becoming exposed to threats already befalling other industries. Industrial

"There is a hidden threat in this vast ocean of maritime opportunities. A threat which many companies do not address, and of those that do, their approach is often flawed and ineffective. The threat is cyber-attacks, and despite its intangible nature, the damage it does is by all means concrete.

systems have seen cyber-attacks shutting down power plants, physically destroying large-scale equipment, as well as erasing tens of thousands of computers in a single company (not to mention all the nation state hacking clashes). All in all, the threat is real and present.

What is the nature of the threat?

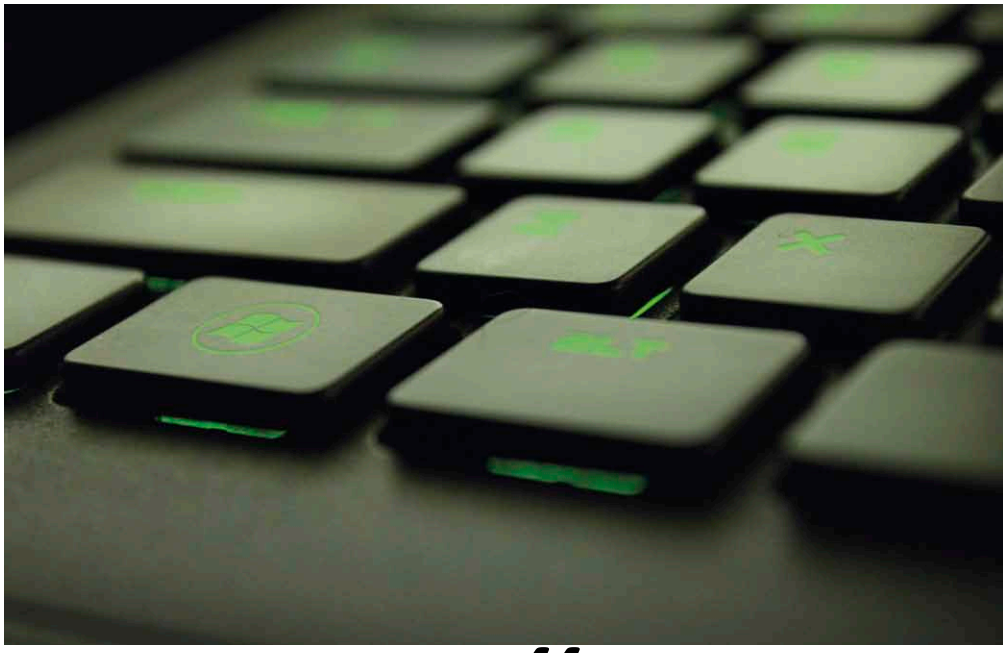
Let us start with dispelling another common myth. The main threat from cyber-attacks is not someone who hacks into an LNG carrier, and blows it up like some super-charged bomb while in port. Whilst this scenario might be conceivable in theory (for ideology-possessed terrorists), it is highly unlikely (for someone involved in money-focused organized crime). The actual threat is much more "boring."

It would be too lengthy in this article to go into depth about all the actors and vectors of threat involved, but in essence it boils down to three key aims, namely the theft of money; stealing information; and/or the denial of asset usage. Some attacks might target accomplishing several of these aims simultaneously.

The theft of money is already a large business, and also in the maritime industry. Either directly from maritime companies, or by manipulating their data to steal money from a third party. The theft of information – or the manipulation thereof – is also big business, as successful cyber-attacks towards maritime information databases can help to facilitate illicit shipments. For instance, a container shipment from origin to destination requires 20 to 50 handover points of critical information. All it requires is the successful penetration of one or two of these entities, and it is now possible to perform a "ghost shipment" where the container is moved across borders without anyone actually knowing this takes place.

More disconcerting is the denial of asset. It is a variation of the classical denial-of-service (DoS) attack, but instead of blocking access to computers, the intention is to render the use of an asset (such as a ship, terminal, or a port) impossible. Such attacks do not have to be sophisticated to work; all one needs is to overload critical systems with malware or deploy cheap GPS jammers in critical locations. None of these attacks would permanently render the assets useless – but that is not the purpose.

A denial-of-asset attack primarily has one of two aims. One is simply blackmail (not unlike ransomware attacks). The maritime company will eventually regain control over its vessel or automated terminal equipment – but how long will that take, and at what cost? When it strikes, it will likely appear more attractive to simply pay the ransom to get the asset up and running once again.



The other aim would stem from nation states. Any country engaged in armed conflict (or similar) with another state will, as an integral part of its warfare strategy, aim at disrupting the opponent's critical infrastructure, with the maritime sector certainly to be considered as such for states with any length of coastline. Consequently, each and every maritime company, irrespective of its ownership, could find itself targeted by nations desiring the operational shut-down of maritime activities in a certain area.

What should maritime companies do?

Whilst all the cyber threats can indeed sound daunting, heightening the cyber security levels can be done by employing relatively simple and inexpensive measures.

First – and most importantly – maritime companies need to understand that a cyber security strategy should be developed at the C-level. This means the CEOs along with their direct reports should all be part of this. Even though the IT manager will certainly have some tasks and responsibilities, the anchoring of the cyber security strategy cannot be with the IT manager alone, as simply he or she does not have the authority to deal with it singlehandedly (nor their departments as a whole). This is because cyber-attacks aim to exploit weaknesses in business processes as well as with ordinary staff, and unless these issues are not addressed extensively, any action taken by IT managers will be easy to undermine and compromise.

For land-based organizations, simple staff awareness sessions increase landside cyber security materially. Additionally, training for IT managers in simple tricks to heighten security using configuration tools they already have will further increase security. These steps are relative inexpensive, and do not require large investments in new software or in other tools. Secondly, a critical and practical review of back-up processes must be undertaken regularly. Any maritime company must be able to cope with the complete loss of all data.

"Whilst all the cyber threats can indeed sound daunting, heightening the cyber security levels can be done by employing relatively simple and inexpensive measures.

For seaborne assets, BIMCO released a set of voluntary guidelines for cyber security in early 2016, and CyberKeel was one of the contributors. These recommendations provide a very pragmatic approach to cyber security on-board vessels, where the reality of poor bandwidth, equipment malfunctions, and very low cyber awareness skills are prevalent.

Hence in short – maritime companies should neither panic nor should they ignore the threat. For starters, they need one or maybe a few days of workshops on understanding the threat within the context of their own business. Then by adjusting their procedures accordingly, and doing a bit of simple training, they will already have increased their cyber security levels significantly. Only when all these measures have been taken, implemented, and kept alive, should the next step of more sophisticated measures be considered. ■

140+ operators

840+ services

500+ ports

900+ terminals

EUROPEAN
TRANSPORT
MAPS

EUROPE:

all over the ro-ro & ferry,
container, and rail maps

www.**european**transportmaps.com

Photos: www.pexels.com

Preparing for and dealing with cyberattacks

The threat is real

by **Bartosz Dąbrowski**

On June 27th, the Danish shipping giant Maersk was among the companies and organizations that were hit by a major cyberattack. While the primary target of the Petya ransomware seemed to be Ukrainian authorities and enterprises, the incident resulted in cargo delays, order processing problems, and limited access to internal systems for bystanders, including Maersk, TNT Express, and DHL. The main lesson to be drawn from this latest cyberattack is that no one can feel 100% safe anymore. Yet, not all is doom and gloom, as each of us can exercise in cyber resilience.

> **"CyberKeel, a company specialising in cyber security, estimates that 44% of shipping lines has a low level of protection when it comes to the digital part of their businesses, with some among the Top 20 using low quality passwords, like "x" or "12345", to guard their assets.**

The recent hacking attempt affected Maersk mostly via its APM Terminals subsidiary, spelling serious problems for 76 sea container handlings facilities all around the world – from New York and New Jersey, via Barcelona and Rotterdam, to India's largest, the Jawaharlal Nehru Port. All terminals had to confront the crisis by finding alternative solutions, such as switching to external systems or even manual execution of orders. The restoration of business for APM was gradual, and only after reinstating IT systems was Maersk able to bring back container shipments to a normal state. While the whole disruption required a few weeks of intensive efforts to normalize the situation, the financial and operational impacts of the cyberattack are yet to be estimated.

In a statement, Maersk claimed that it was the first such incident in its history. That is exactly what most of the companies in the sector could have said in a similar situation. One can now wonder whether there haven't actually been other attacks like this, or if they've simply passed unnoticed. CyberKeel, a company specialising in cyber security, estimates that 44% of shipping lines has a low level of protection when it comes to the digital part of their businesses, with some among the Top 20 using low quality passwords, like "x" or "12345", to guard their assets (read more on pgs 11-12). Such doubts rise the question of how prepared companies and organizations are for another instance of a Petya attack, or an even more malicious one. And, more to the point, do they just lack the awareness of the threat in the first place?

Systems at risk

The maritime industry is generally believed to be a bit behind in the inevitable process of digitalisation. However, computers today deal not only with abstract data, such as registry of deliveries, but are being connected more and more to physical objects in what is dubbed the Internet

of Things (IoT). In the Maersk case, it was the terminals and delivery data that were affected, but we can easily imagine the dire consequences if autonomous vehicles and other heavy-duty machinery were the aim of a cyberattack.

While the IoT, with its aim to connect as many objects as possible, is still in its early stage of development throughout the logistics domain, the Electronic Chart Display and Information System (ECDIS) will become compulsory for all vessels by 2018. The ECDIS, freshly introduced in some organizations, may serve as an easy target for hackers aiming to load incorrect or outdated maps, to access the underlying operating system, or to spread malware. Some ECDIS systems are known to run with administrative rights and no password protection.

The Automatic Identification System (AIS) is another example of a weak spot in the maritime cyber security defense line. The AIS supplements the marine radar, which continues to be the primary method of collision avoidance for water transport, but they do not guarantee proper security. AIS communications lack authentication or integrity checks, which can lead to abuse by people using even a simple radio frequency receiver.

This all points to a seemingly unavoidable side effect of introducing next-gen technologies, namely to the creation of new vulnerabilities. As with pretty much any other risk, the probability of the worst case scenario becoming a reality can be either minimised, or otherwise – we can just as well be handing the login and password to hackers on a silver platter.

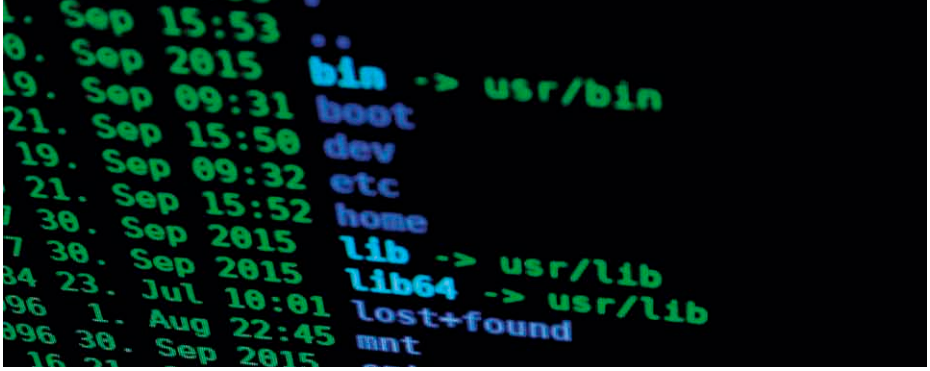
Time to think resilience

First of all, maritime companies must start taking the threat caused by hackers seriously, and doing this means introducing cyber resilience awareness and policies into their everyday routine. The aftereffects of cyberattacks are proving to be even more severe than vehicle and workplace accidents, extreme weather events, or fraud in general. Learning about legal liability and assuring proper insurance are among the basic parts of cyber security preparations. However, they will not bring about the continuance of operations during a crisis, retrieve data afterwards, or ensure a sound level of safety that saves the day in the future. Insurance, sadly to say, also has nothing to do with restoring customers' faith in us.

The responsibility for implementing and up-keeping a cyberresilient environment lies primarily within management boards and top level executive teams. Such an environment should be more or less managed using the same tools as with any other business-threatening risks, adding experience and expertise gained from technology-based businesses and communities. Even though dangerous, crises such as the Petya malware attack may bring a lot of critical knowledge and case study material for maritime organizations to further build their resilience on. Moreover, this doesn't have to be a single party effort; resilience can be, and essentially should be, strengthened through the entire value chain. Imagine company A being keen on cybersecurity, but its indispensable partner B is carrying little to none about it. This ultimately poses a threat to both of them (A can deem B not being so indispensable after all), as well as to their clients. In the end, if a cyberattack occurs, it is of great importance to those affected to share the information about attacker's tools and practices, because it leads to better understanding of industry incident trends.

Nevertheless, relying mainly on experience and "instinct" in addressing cyber threats is far from being the only, as well as the best, solution a maritime company executive should implement as a long-term strategy. This is because it's in fact really difficult to measure cybersecurity performance. Senior executives face a challenging task where traditional business performance metrics,

like revenue or cost, do not serve the new purpose. For cybersecurity, there's no one-size-fits-all. The obtained cybersecurity approach should match the overall business strategy, and the probability of various threat types should be included in the general business risk assessment, as the protection of company's assets is more efficient when it is prioritized and differentiated according to their value. Protection objectives should be defined for all employees to minimize the aftermath of an attack, too.



Train the tactics

However, many executives tend to concentrate mainly on the defensive part of cyber resilience. Although a highly qualified IT staff capable of detecting a threat and protecting their company's systems is by all means invaluable, there is no universal method for an unbeaten defence. Also, relying on IT people to sort out everything, so that other employees might as well forget about cyber resilience, is almost a certified way of getting into troubles. In fact, anyone may turn out to be responsible for a cyberattack, deliberately or out of sheer ignorance, as opening an infected attachment in an e-mail is enough to bring about serious problems. This means each and every employee should receive proper training to ensure that everyone is engaged in the company's cyber resilience day-to-day tactics. Everyone should be assigned a role in emergency plans, too, and be prepared to act when necessary. This particularly holds true for those on the front line, i.e. people managing strategic assets or responsible for company's communication, who should be meticulously trained.

Whereas IT staff's expertise will be crucial in the phase of recognizing the attack and reacting quickly, people representing the company may turn out to be as much useful after an incident – be it handling both the media and internal communications, calming down business partners and clients, as well as analysing what went wrong to adjust properly for any future event. However, much can be done before anything really happens. It is in the power of a company's or an organization's board to decide whether to take training and testing to a higher level. Great benefits can come from real-life stress tests as well as from collaborating with ethical hackers. By, for example, using fake phishing e-mails aimed at internal training, employees can fully understand the risk. Then, testing company's systems with commissioned cyberattacks may not only bring new ideas to IT staff on how to better mount their defense, but also help in clogging any leaking holes.

On guard

Once everybody involved directly or indirectly in a cybercrisis is updated about the recovery of the business as usual and action plans, the main task is to remain vigilant. It is never too late to draw conclusions from such crises, and share best practices with partners and peers. After all, the only ones benefitting from a non-cyberresilient industry are the offenders. ■

Photos: www.pexels.com

Increased risk of cyber theft in the supply chain

IT thievery spawns

by **Peregrine Storrs-Fox**, *TT Club's Risk Management Director*

Whilst technological advances undoubtedly provide greater operational efficiencies and opportunities for carriers and operators to mitigate their exposure to theft and fraud, unfortunately they equally benefit organised crime. As invasive cyber-technology becomes more widely available, the TT Club suggests that what has been observed in recent months could be a significant emerging risk to legitimate trade, exposing the operators in the supply chain to economic and commercial damage.

The TT Club has released a handbook entitled Supply Chain Security – Management, Initiatives & Technologies with useful contextual reference. For more info on how to obtain the paper visit the www.ttclub.com website.

The ingenuity of thieves and fraudsters has always surprised unsuspecting victims. The stakes are high and it is clear that the international supply chain, which by its nature facilitates movements across borders, is being targeted in order to fulfil trafficking of people and drugs, as well as other illegal trades such as dumping waste and intercepting valuable freight.

Recently, press reports identified another approach regarding IT-based theft; going beyond simply misleading other operators into thinking they are dealing with a legitimate company through the use of Internet-based clearance websites, it has been established that cyber criminals may access and take control of operators' IT systems.

Changing crowbars to keyboards

In the last weeks a small but significant number of incidents has been reported which at first appear to be a petty break-in at office facilities. The damage appears minimal – nothing was physically removed, however, more thorough post incident investigations revealed that "thieves" were actually installing spyware within the IT network of the operator. Interestingly, this involved physical installation. More typically the criminals identify targets (generally individuals) where the system's cyber security is inadequate, combined with sufficient access and authority rights. As such, operational executives who may travel extensively can be particularly exposed.

The type of information being sought and extracted may be release codes for containers from port and terminal facilities. However, spyware can record movements, key strokes, and even download and print documents and screen shots to an external source. In the instances discovered to date, the cyber criminals have apparently been focused on specific individual containers, taking steps to track the units through the supply chain to the destination discharge port. Once a container arrives, the perpetrators intervene, collecting the required release data from the unsuspecting operator's IT systems, ultimately facilitating the release of the container into their custody and control. The incidents to date are thought to have

> **"Criminal organisations are well resourced and focused on utilising emerging technologies, not only to perpetrate crime but also to mitigate the risk of detection. The cyber-criminals' ability to hack into email accounts and communication channels is well-established, and the risks to the logistics operator must not be ignored.**

been related to drug trafficking, by means of importing illegal substances through the supply chain unnoticed.

The use of such technologies, however, could very easily be replicated to infiltrate other areas of the supply chain, from freight forwarders through to warehouse operators. The potential scope of valuable information within the supply chain cannot be underestimated. In addition to the focused incidents experienced to date, there is room for highly selective and targeted cargo theft, human trafficking and general disruption of the global supply chain. Generally, security efforts focus on the potential for disruption and "business continuity"; these recent spyware infiltrations point more to criminal leveraging to achieve darkly profitable ends. Implementing effective computer logs and "dashboards"' (as part of detailed operational and performance management information) may arguably be more pressing than updating and testing appropriate response plans.

Simple security – R.I.P.

Criminal organisations are well resourced and focused on utilising emerging technologies, not only to perpetrate crime but also to mitigate the risk of detection. The cyber-criminals' ability to hack into email accounts and communication channels is well-established, and the risks to the logistics operator must not be ignored.

For instance, if a driver receives instructions to deviate from a planned delivery destination and to deliver to a nearby warehouse, from what appears to be a known and trusted source from within their own organisation, would they have concern to question it? Similarly, by accessing a warehouse operator's stock management system, a criminal organisation can achieve its ends by altering the logical versus actual stock levels held within a facility.

The ensuing losses can give rise to very large financial exposures, let alone commercial and reputational damage. The increased sophistication of such "cyber-attacks" of course makes it challenging for operators to build effective defences. Nonetheless, awareness is the first step, followed by thorough risk assessment. Boards and managements need to articulate a clear risk culture and deliberately follow through the process. In many cases, the human element is both the strongest and weakest spot in the armour – the potential for individual or contractor malfeasance may be thoroughly mitigated by others' alertness, thorough training and effective procedures (such as segregation of duties and "whistle-blowing").

Vigilance and due diligence in day-to-day operations – the more physical side – are clearly vital, together with general security of IT installations. However, it would also be wise for operators to investigate the means to a greater degree of protection from and detection of hacking and spyware activity. When reviewing IT systems, the 2013/2014 Global Fraud Report, issued by Kroll, identifies at least two key questions to consider: "If you discover that your systems have been compromised, does your system have the facility to trace and identify what was viewed, modified or taken?", as well as: "What would be the potential commercial impact on your business if it became known to your clients that such information had been accessed through your IT systems?"

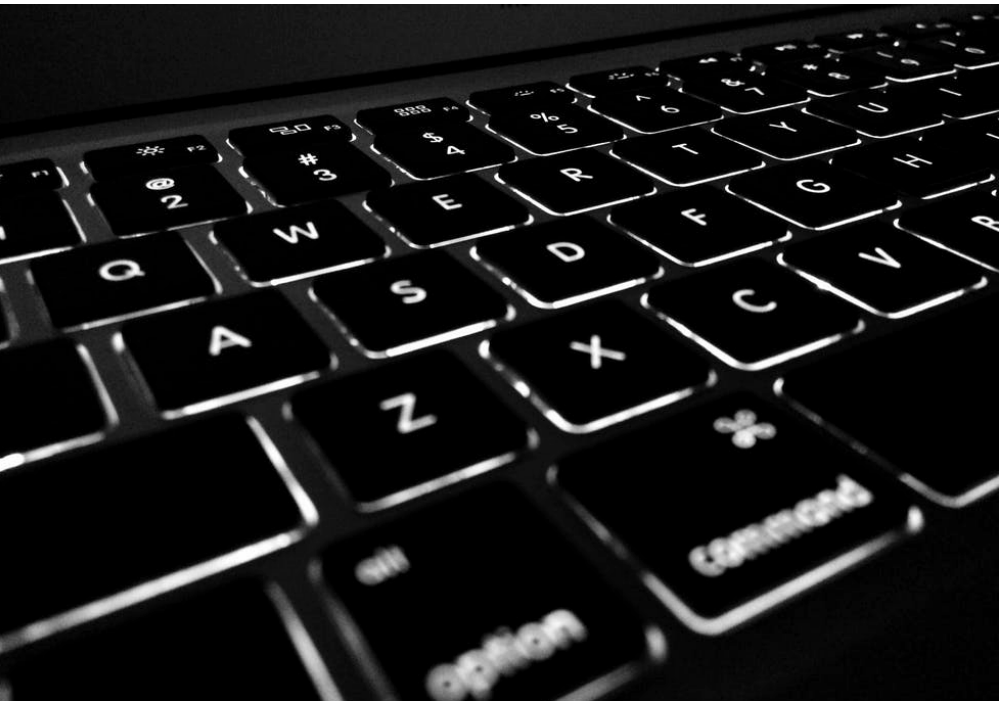
Security in the supply chain is no longer "simply" about the use of locks, alarms and tracking systems. Organised crime has spawned new risks. For those who need to consider this topic further, the Kroll report provides a thorough global overview, with many comments applicable to those involved in transport and logistics.

The wicked art of deceiving

The European Commission estimated that the value of cargo stolen in transit amounts to around EUR 8.2 bln per annum. The TT Club has seen an increase in the role fraud is playing in such losses. There is a marked trend in organised crime posing as legitimate operators or using Internet cargo clearing sites to facilitate the theft of high value cargo. Perhaps most worrying is that this is global.

Freight forwarders, and similar freight or truck broking operations, need to be aware that there has been an increase in commercial identity theft, whereby thieves pose as legitimate contractors and make off with millions of dollars of merchandise. Experts say the practice is growing so fast that it will soon become the most common way to steal freight. The Internet – on which we all rely heavily – facilitates such scams, enabling thieves to gain easy access to vast amounts of information. Online databases and cargo clearing sites help conmen to assume the identities of existing or plausible contractors and to search for specific commodities they want to steal.

In recent weeks there has been an amount of publicity about the frequency of incidents of bogus Chinese forwarders establishing online relationships with agents in the UK and sending container loads of cargo without the necessary bill of lading to secure the release of the container once landed at the UK port. Afterwards ransoms have reportedly been demanded by the Chinese agent in order to relay the necessary documentation. Without this, the UK



> **There is an increasing trend in the fraudulent use of Internet clearing sites too. Operators are particularly exposed on occasions when they need assistance in regions they are unfamiliar with, especially at short notice. In such circumstances operators may be tempted to use unfamiliar subcontractors sourced via such sites.**

forwarder can find himself with significant demurrage and storage bills, as well as large legal fees incurred in trying to extricate himself from the situation.

There is an increasing trend in the fraudulent use of Internet clearing sites too. Operators are particularly exposed on occasions when they need assistance in regions they are unfamiliar with, especially at short notice. In such circumstances operators may be tempted to use unfamiliar subcontractors sourced via such sites.

There are now documented instances where crime organisations have purchased legitimate but failing transport operators and continued to trade in their name, predominantly online and in a state of virtual insolvency, waiting for the opportunity to receive a valuable cargo before disappearing. More simply in other cases, fraudulent road hauliers advertise vehicles available for backloads, again hoping for an unsuspecting forwarder, in too much of a hurry to carry out proper checks, and with high-priced goods to move.

A recent case in the US highlights the problem. A truck broker posted a shipment on a clearing website, commonly used by freight forwarders to match up shipments with trucking companies. A trucking company called inquiring about the shipment and was advised to submit proof of insurance. Once the "proof of insurance" was received, the truck broker and trucking company agreed on a price and the trucker broker issued a dispatch confirmation listing the trucking company and the address where the cargo was to be picked up and delivered. The trucker picked up two truckloads, valued at USD 175,000, which never arrived at their intended destination. The criminals had gained access to the site and submitted fake insurance documents. The truck broker eventually called the actual trucking company and discovered that it only hauls freight in Florida, while the shipment was picked up in California.

Sealing the line of defence

TT Club advises that the abovementioned Internet risks can be successfully mitigated in a number of ways:

First – it is essential to have a robust approved subcontractor selection policy. The effective implementation of such a policy, even (and particularly) at times when time-sensitive moves are being arranged, is fundamental in reducing the risks associated with the use of clearing sites. TT Club's Stop Loss Information Sheet on "Theft Attractive Cargoes" includes a list of questions a freight forwarder or broker should be asking a prospective sub-contractor.

Second – clearing sites often include a disclaimer, denying liability in the event of fraudulent activity on the site. However, operators of such sites do have a duty of care to users. They will often make recommendations for safe usage, list best practices and give loss prevention advice in order to minimise a user's exposure to risk.

Third – subcontractors using free mail accounts such as Hotmail, Gmail and Yahoo should arouse suspicion. Similarly correspondence via Skype or other free videoconferencing should be avoided. Perpetrators will use different phone, fax and e-mails than the actual carrier. Use established means to perform an Internet search on the contractor's name; cross-check contact and other given details.

Fourth – when requesting insurance documents always ensure the original certificates are posted. Beware if documents are offered only in electronic format. Always seek to verify the legitimacy of the insurance policy with the insurer.

Last but not least – establish signage and license plate information on tractor/trailer and provide this information to the shipper for further confirmation at time of pick up. Require the shipper's warehouse or cargo releasing facility to photocopy the driver's license of the carrier and independently verify with the trucking company.

Ultimately, thieves will seek to identify the weakest link in any given supply chain and the Internet offers much opportunity. Due diligence procedures should be investigative, challenging, analysing, cross-checking and evaluating given information. Adopting a stringent approval procedure, before you entrust a new subcontractor with your customer's cargo and your own reputation, is demonstrably justifiable. ■

Photos: www.pexels.com

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.

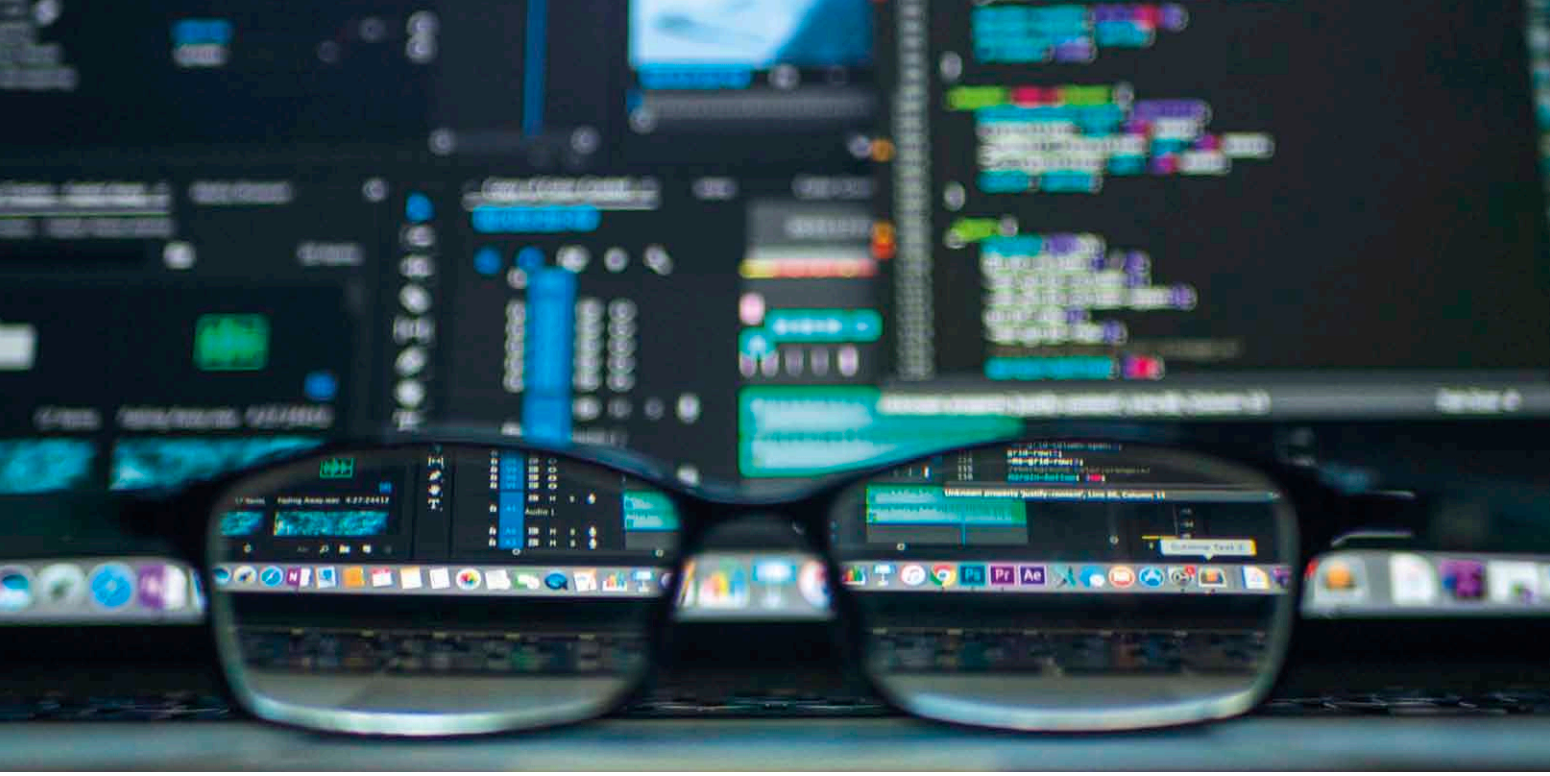
The first one is used to describe danger arising from cyberspace. Cyber threats are classified in growing order of severity as hactivism, cybercriminality, cyberespionage, cyberterrorism, and cyberwar. Each has individual elements relating to the actors, motives, and objectives involved. Depending on 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.

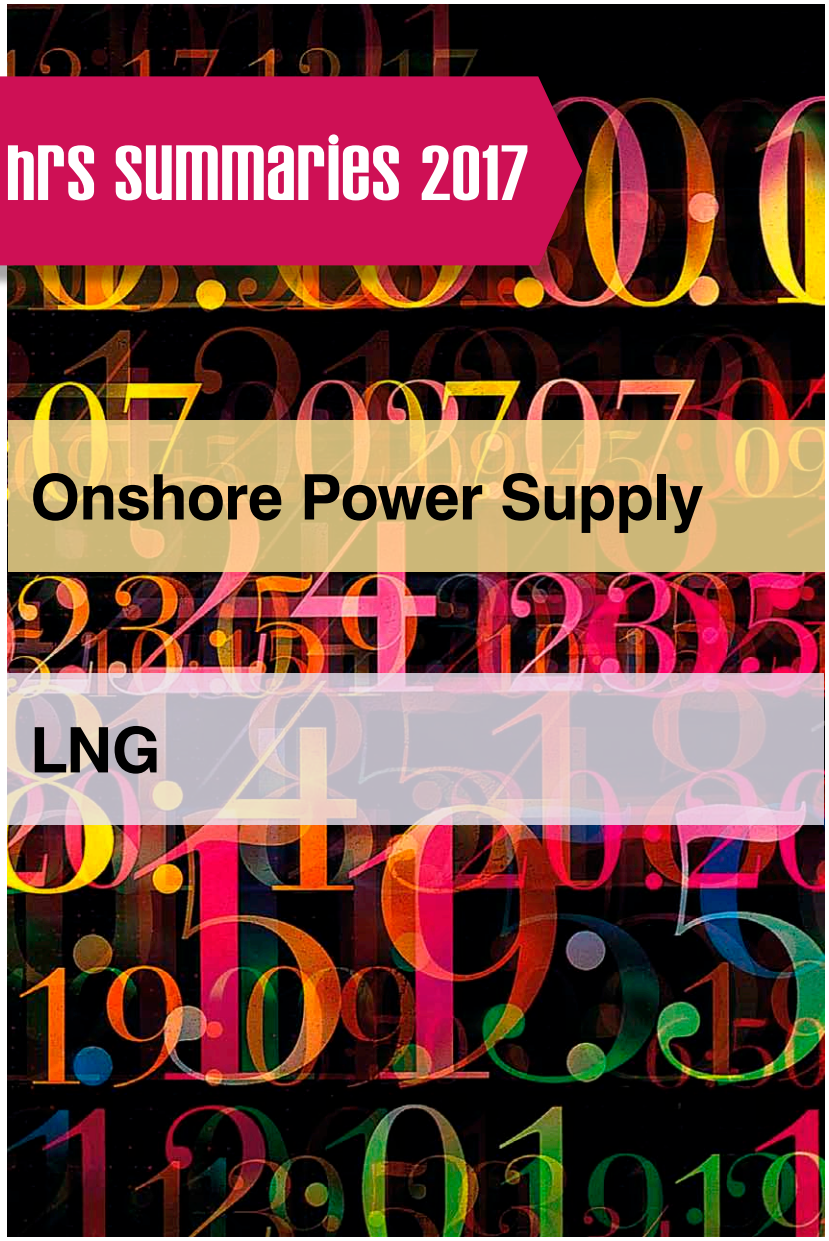
Notwithstanding these efforts, the global regulatory status on mandatory port cybersecurity seems somewhat neglected. Cybersecurity is not included in any of the IMO Conventions related to port safety and security, such as the ones on International Ship and Port Facility Security (ISPS) or International 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. ■

HRS summaries 2017



partnership events

2nd International Summit Green Shipping 2017
16-17 October 2017
NL/Rotterdam

3rd International LNG Congress
16-17 October 2017
ES/Barcelona

15th Annual 3PL Summit & Chief Supply Chain Officer Forum – Europe
16-18 October 2017
NL/Venlo

The Maritime Standard Awards
23 October 2017
AE/Dubai

Kormarine
25 October 2017
KR/Busan

LNG Bunkering Training Course, The Med
24-26 October 2017
ES/Barcelona

Port Investments & PPP Course
24-26 October 2017
UAE/Dubai

Harbours Review Spotlight
25-26 October 2017
SE/Gothenburg

Arctic Shipping Forum North America
30 October-1 November 2017
CA/Montreal

We invite you to cooperate with us!
If you wish to comment on any key port issue, share your feedback or have information for us, do not hesitate to contact us at:
editorial@baltic-press.com
+48 58 627 23 21

To join our 15,000+ maritime transport sector users society click HERE

previous editions

HR#13	BLUE INDUSTRY
HR#14	BALLAST WATER MANAGEMENT
HR#15	THE PAST, PRESENT, AND FUTURE OF THE CONTAINER. TOC EUROPE 2017 – SUMMARY

▪ **PUBLISHER** ▪ **Baltic Press Ltd** ▪
▪ ul. Pułaskiego 8 ▪ 81-368 Gdynia ▪ Poland ▪ tel.: +48 58 627 23 21/95 ▪
▪ editorial@baltic-press.com ▪ **www.harboursreview.com** ▪
▪ ***President of the board:*** Bogdan Ołdakowski

▪ **EDITORIAL TEAM** ▪
▪ ***Editor-in-Chief:*** Przemysław Myszka ▪ przemek@baltic-press.com
▪ ***Content Editor:*** Maciej Kniter ▪ maciej@baltic-press.com
▪ ***Proofreading Editors:*** Alison Nissen, Katarzyna Chmielewska
▪ ***Art Director/DTP:*** Danuta Sawicka

▪ **MARKETING & SALES (advertising, exhibitions & conferences)** ▪
▪ ***Head of Marketing & Sales:***
Przemysław Opłocki ▪ po@baltic-press.com ▪ tel.: +48 58 627 23 24
▪ ***Marketing & Communications Specialist:***
Aleksandra Plis ▪ aleksandra@baltic-press.com

▪ ***Subscriptions:*** www.harboursreview.com ▪

If you wish to share your feedback or have information for us, do not hesitate to contact us at: editorial@baltic-press.com