#23
OCT: 2018

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

TURREM DATA Group

SMART4SEA TRAINING AND EDUCATION AWARD 2018
UNSUNG HERO OF INDUSTRY: HIGHLY COMMENDED, SAFETY AT SEA AWARDS 2017
BEST CYBER AWARENESS CAMPAIGN, INTERNATIONAL CYBER SECURITY AWARDS 2017

2018 Training Award SMART4SEA

Welcome to "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the shipping and offshore industry initiative, "Be Cyber Aware At Sea".

Issue 23 is once again generously sponsored by TDG Cyber Marine - part of the Turrem Data Group an expert player in the cybersecurity industry. The company offers leading edge and patented technologies to provide a more robust defence against the escalating threat from cybercriminal activity.

This month we look at a wide range of issues. We reflect on news regarding attacks on major ports, with San Diego and Barcelona both having reported recent cyber breaches. There is also criticism in some quarters, with cyber security experts claiming that shipping is just not doing enough. While others believe that slowly, but surely, the industry is beginning to make up for lost time.

Key maritime organisations are forcing the hand of operators, and there is simply no hiding from the need to do all possible to safeguard cyber security. From navies to oil companies, and even governments, pressure is building to ensure that systems are protected. Ships, ports, seafarers, companies, the entire supply chain - all needs to be secure. We are proud and pleased to be helping a little, but it is also about what you do...so please think about your role and how you can foster maritime cyber security.

The aim of Phish and Ships is to ensure that cyber awareness at sea is taking hold, and we are very proud to play our part. See https://www.becyberawareatsea.com/ for more details and please support our campaign. Don't forget to download our free resources, including our award winning (and free) posters...and there is even a superyacht flavour this time round.

MAKING UP FOR LOST TIME

The maritime industry has been slow to realise the dangers of cyber incidents but are 'making up for lost time', according to Patricia Keefe in her recent article for Marinelink.com.

Despite acknowledging the maritime sector's crucial role in propping up the economy, the industry has been slow to respond to cyber threats to its digitised systems and assets. While critics have telegraphed their concerns, physical vulnerabilities were prioritised, aided in America by the government's Port Security Grant programme.

Patricia Keefe pinpoints the first changes in dynamics to the publication of two reports: the Brookings Institute's 'The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities' published in 2013, and the US General Accounting Office's (GAO) 'Maritime Critical Infrastructure Protection' published in 2014. These directed criticism at the US Coast Guard for not conducting a risk assessment that 'fully addressed cyber threats, vulnerabilities and consequences'.

Following these reports, she notes an explosion in port cyber security concern in 2015 from 'a raft of industry organizations, government agencies here and abroad, academia, insurance companies, standards groups, think tanks and researchers'.

Receiving critical focus were maritime executives who failed to take a lead on cyber security, and their employees who were labelled 'the weakest link', giving rise to calls in 2016 for more cyber education. Raising awareness became the theme for 2016, coincidently the year in which Be Cyber Aware At Sea was conceived and created! Patricia highlights that there was movement in the campaigning to place 'cyber security on the same plane as safety management' as well as pushing for a 'cultural shift'.

Her verdict in 2018, 5 years after those first reports on cyber security at sea? Progress, good progress: From publishing of guidelines to stronger regulation and greater focus on cyber risk assessments, mitigation and strengthening cross-sector relationships. She highlights in particular that the normally 'highly complex and competitive' port community has come to work together through participation in security committees and cyber subcommittees. On one of these, the USCG's Area Maritime Security Committee the full range of participants in the sector, from shippers, government agencies, port authorities, terminal operators and even clients, are represented. It is an inspiring body that works to identify and resolve issues.

Looking ahead to 2019 and Patricia Keefe predicts 'greater emphasis on cyber risk management, resiliency and collaboration' with a particular note against complacency 'by getting maritime companies and ports to create contingency plans to enable them to recover as painlessly as possible from a successful attack'. Continued collaboration is also going to be imperative as the industry works to protect against cyber attacks.

Read more at http://bit.ly/2Dwimpj

US CYBER STRATEGY

The White House has issued a new cyber security strategy which it believes will give government agencies and law enforcement a stronger hand in responding to cybercrime and 'nation state' cyber attacks. President Donald Trump signed the document which features a prominent maritime focus.

The document states that maritime cybersecurity is of "particular concern" as "lost or delayed shipments can result in strategic economic disruptions and potential spillover effects on downstream industries."

It goes on to state, "Given the criticality of maritime transportation to the United States and global economy and the minimal risk-reduction investments to protect against cyber exploitation made thus far, the United States will move quickly to clarify maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure."

You can access the document here http://bit.ly/2zvDzMg

PORTS HIT BY ATTACKS

Two major international ports fell victim to cyber-attacks within the span of a week, recently putting the shipping industry on alert for a possible threat actor targeting the entire sector.

The first to fall was the Port of Barcelona, Spain, while the second attack was reported just a few days later by the Port of San Diego, in the United States. Neither of the two port authorities revealed any details about the nature of the cyber-attacks, leaving security experts to speculate about possible causes.

The cyber-attack on the Port of Barcelona did not affect ship movements in and out of the harbour, and a local newspaper reported that it impacted only land operations, such as loading or unloading of boats, although the Port denied there was a serious disruption to customers.

The Barcelona cyber-attack was followed by another one this week, this time against the Port of San Diego, a medium-sized cargo port on the US west coast.

"Port employees are currently at work but have limited functionality, which may have temporary impacts on service to the public, especially in the areas of park permits, public records requests, and business services," said Randa Coniglio, Chief Executive Officer for the Port of San Diego in a statement released a day after the attack.

San Diego officials have not revealed the nature of the attack. It is unclear if the two incidents are related or alike. The fact that the details have not emerged is a problem for the whole maritime industry, as sharing of information is increasingly important.

THEY SAY LIGHTNING NEVER STRIKES TWICE..!

Its not often that within one week you hear of two similar cyber attacks within the same industry but last month that is exactly what happened in maritime.

The online attacks on Barcelona and San Diego seem to have had minimal apparent fallout, however for a port to work at maximum capacity in a modern world it relies on its technology and uninterrupted data flow, so we should pay close attention to these incidents.

Frustratingly the finances of an attack are in the hackers' favour. They may purchase a simple $200 ransomware attack off the dark web and send it out to millions of email addresses, also bought from the same source. If successful, the hacker's $1000 investment can reap them big rewards while ultimately costing the victims millions.

To avoid this the industry needs to invest wisely. Unfortunately, while we all know this, the recent economic downturn in exports has led to lower investment and slower uptake.

Additionally each element of the industry also has to be as cyber hygienic as the rest; its all well and good to ask ship owners to spend money upping their game but ports have to invest in themselves too. There is no point in ships with the best digital defences sitting out on the water unable to off-load cargo!

The whole industry has a duty of care to their customers to work together. By the IMO's 2021 deadline vessels must implement a cyber platform but maybe the whole industry, ports and other various operators too, should take this deadline into account to make sure it all runs smoothly.

My advice is do the basics right – patching, updating and putting a 'what if' scenario plan in place for the critical moment - and educate. Education is as important as technology. The Be Cyber Aware at Sea campaign is both excellent and important, relevant to those on land as well as at sea.

TDG Cyber Security and TDG Cyber Marine work with a number of technology providers to help combat cyber attacks and, through our own custom-built security centre in the UK, can work alongside IT teams in organisations globally to keep attacks at bay.

The technological world is changing at a rapid rate and TDG can help by taking the noise out of this digital revolution so companies can get on with the day job...uninterrupted.

Steve Tytler – TDG Cyber Security Founder

TURREM DATA Group

DIGITAL SHIP BACK IN ATHENS

Over the past 12 months, 15 Digital Ship events have taken place around the world - in locations such as Oslo, Copenhagen, Bergen, Hamburg, Rotterdam, Limassol, Tokyo, Singapore, and London. We have covered the full spectrum of innovation and digital transformation in shipping – including what this means from a business perspective, for your operations and, of course, for Seafarers themselves.

We have looked at how autonomous shipping is directing the maritime future; we have discussed how the changing cyber threat landscape is driving planning and decision making; we have learnt what the impact of upcoming regulations and compliance issues may be and how to manage these; we have heard from exciting new entrants and start-ups looking to find a place in our industry world; we have reviewed shipping's position in the supply chain and how to better collaborate with our partners, and we have delved deeply into what digital disruption really means for our business bottom line.

Coming back to Greece for our 16th Annual Digital Ship Athens Conference & Exhibition, we aim to bring the year's conversations and discussions together, to look across the board at the "digital ship". Once again, we expect to host over 300 participants, including 140+ shipping companies.
The first day will cover 3 core sessions:

- The Maritime Satcom Summit - What's next in maritime connectivity and how will this power future developments?
- Blockchain in Practice -Digitising the global supply chain
- iShipping: Harnessing Maritime's Digital Future- Enabling collaboration, harmonisation and standardisation

The second day with consist of a special focus on Building Cyber Resilience – including a hackathon designed to address the real issues your companies are facing now and may face in the future. We will also host Roundtables on all the topics covered throughout the two days - to enable participants, speakers and sponsors to continue their discussions and ask the questions they really need answers to in an informal, interactive setting.

To Register visit:
https://www.athens.thedigitalship.com/register/
Or to find out more and other enquiries, please contact: lyndell@thedigitalship.com

CALL TO DROP ARCHAIC INSURANCE CLAUSE WHICH AFFECTS CYBER COVER

The boss of the cyber security outfit Naval Dome, has called on marine insurers to revoke a controversial insurance Clause (CL 380) and implement policies that insure against the risk of cyber-attacks on ship systems.

Speaking in Cape Town during the International Union of Marine Insurance's (IUMI) annual conference, Naval Dome CEO Itai Sela said that with the maritime industry increasingly moving towards connected, cloud-based technologies and autonomous operation, a 15-year-old Clause that excludes damage to computer systems, code or software is archaic.

The Clause in contention reads: Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to, by, or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system. 2.1: Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software program or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

Sela suggested the maritime industry should follow the automotive sector's lead. The sector has introduced software-based safety solutions to road vehicles that, despite not being initiated by the insurer, have proven to protect drivers (and insurers) against theft or damage, which helps towards mitigating risk and reduce premiums.

He said: "Why do insurers continue to implement CL 380 when there is a high probability that a computer will be hacked and, importantly, when there are many different ways and means of protecting shipboard computer systems?

"What we have is an industry on the cusp of a technological change. The rapid implementation of advanced autonomous technologies and machine learning capabilities will change the way in which ships are operated, but such developments will also leave the industry open to more system breaches and unauthorised intrusion unless there are systems and policies in place to mitigate against such risks.

"Why then, considering the current evolving maritime situation and the increase in cyber-attacks, which the insurance sector repeatedly warns of a need to protect against, is there no cyber insurance policy?"

INDUSTRY STILL EXPOSED

Cybersecurity firm Synopsys contends that the maritime industry is still highly exposed to cyber attack, has yet to take hypothecated attack research to heart and is years behind other industries.

Talking to Ship Technology, Adam Brown, manager of security solutions at Synopsys, stated that "Looking at some of the research that took place over the past 12 months or so, and the attacks done either by researchers or by real nefarious actors, we're making exploits based on things that we would've seen perhaps as vulnerable ten years ago in the normal internet world, in banking, or even in the automotive sector. And those things have mostly been re-mediated, however that is not the case in shipping."

With around 50,000 ships at sea or in port at any one time, the industry is peculiarly vulnerable to attack and, as the research institute, Future Directions International, reported 'the maritime industry appears still to be ill-equipped to deal with such future challenges as the cybersecurity of fully autonomous vessels.'

"There's a bunch of issues related to cellular devices on ships and how they're configured together on the network, and a lack of network segregation," Brown says. "So when you have a vulnerable device on an open network on a ship, or a vulnerable device is put on the internet on a ship, then that vulnerable device is wide open to any attacker in the world."

"If we just take a cruise ship for example, it will have on it at least one, if not two or four satellite communications terminals," Brown explained. "There is a lot of radio frequency power going through that satellite dish. Now, it turns out that those dishes can be controlled by third party actors, so an attacker can control where the dish is pointing. On a ship, there are some no-go zones where the dishes are not allowed to point, for example at a deck where there might be passengers. And that's done for safety reasons, because you don't really want to start roasting your passengers with your radio-frequency energy that's coming out of this dish.

"However if an attacker can control that and override the no-go zones, they could point it down at the passengers and expose them to excessive radio frequency energy, which wouldn't result in a burn per se, but there's been some medical research done that showed it can lead to microwave radiation. And if you point it at an electrical device, it can cause malfunction."

Although Brown admits that this is "off-the-wall vulnerability", he insists that such potential actions should not be taken lightly going forwards.

Looking ahead, there is a lot of ground to make up, with Ken Munro, security entrepreneur at PTP, stating that ship security is in its infancy and that the industry is exposed to risks which in other mainstream IT systems were eliminated years ago.

Brown issued a warning against treating the IMO's guide as a checklist: "Checklist security simply does not work. Attacks are constantly evolving; the attacker is constantly looking for a way in. What is much better is to have a deliberate security initiative. So that might be starting with having a policy and some processes, so things like keeping the software up to date, training the staff on security issues, just so that it's constantly something on the mind of the people.

"Shipping needs to do more," he adds. "We can see it starting, and it will be interesting to start to see some cybersecurity measurements appearing to see how they will compare against other industries."

https://www.ship-technology.com/features/shipping-still-unprepared-cyberattacks/

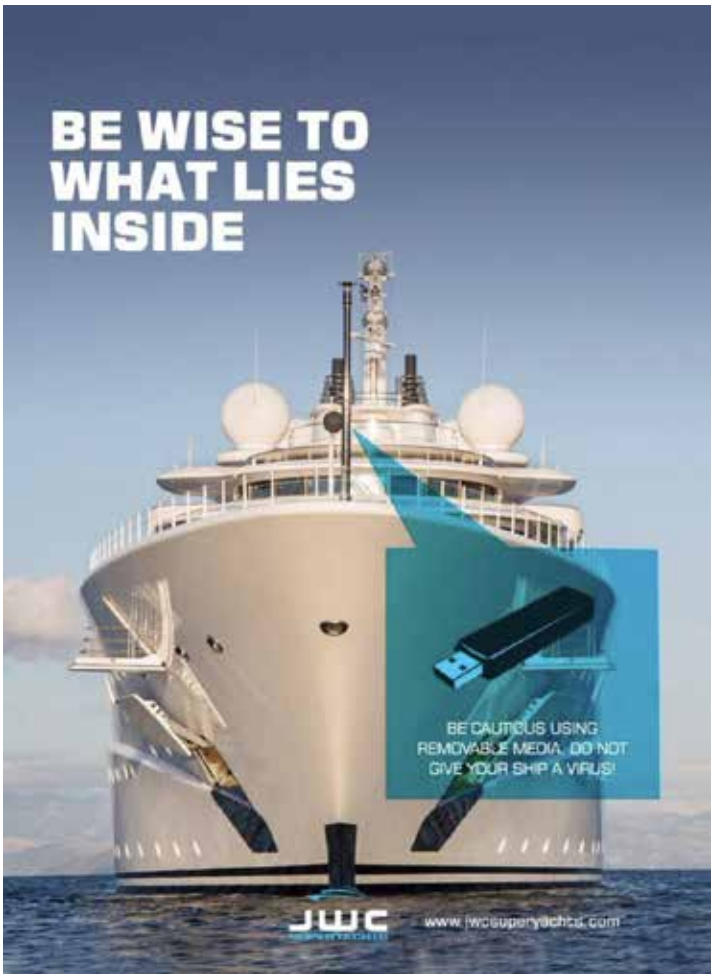
OIL COMPANIES TACKLING CYBER ISSUES

The Oil Companies International Marine Forum (OCIMF) is a key driving force in the development of safety rules and regulations in the tanker and offshore industry. Naturally, this role has seen them increasingly involved in maritime security issues.

An awareness of cyber security is one of the key revisions to OCIMF's latest Vessel Inspection Questionnaire (VIQ). OCIMF is now checking that cyber security awareness is actively promoted by the shipping company and crew on board.

Last year, back in April 2017, the OCIMF issued TMSA Version 3. In addition to the inclusion of ballast water management, fuel management and other items, Version 3 also contains a new Chapter 13 entitled "Maritime Security" with extensive on board and in the office cyber security vetting requirements. For the pre-fixture vetting review, Chapter 13 is dedicated to on board and office marine cyber security with OCIMF recommendations.

Speaking at a recent OCIMF event, speakers stressed that a maritime cyber event is not an 'if' but a 'when' event. They stressed that countermeasures have to be in place to isolate the damage. These new checks are an important part of that development.



MAKE SURE YOU ARE CYBER AWARE

One of the key pillars of the Be Cyber Aware at Sea campaign is our use of posters, and the fact that we provide them free to the industry.

The full series can be accessed and downloaded from our site for free, and we would urge all shipping companies to do so. All too often we hear of seafarers failing to get to grips with the firewalls, encryption, antivirus software and other means of heading off cyber attacks.

Seafarers need to not just be aware of what they are fighting, but of the things which can help them. So, we hope the poster acts as a timely and useful reminder.

It is not just shipping companies: if you are a seafarer welfare or training centre, why not grab yours and make sure you are doing your bit to raise cyber security awareness at sea. We also look at the issues facing superyachts too.

You can access high resolution versions of all our posters and resources at https://www.becyberawareatsea.com

A WAKE UP CALL

Major attacks have been a wake-up call for the shipping sector, creating a renewed urgency around tackling the threats posed to vessels and supply chains, as well as prompting an increasing interest in cyber insurance.

At the same time, new regulations will exacerbate the fall-out from any future failure. According to Volker Dierks, Head of Marine Hull Underwriting, AGCS Central & Eastern Europe, attacks have increased awareness of the potential for cyber business interruption losses and physical damage to vessels arising from a cyber-attack. As a result, shipping companies are now engaged in more detailed discussions with insurers about how to protect against cyber exposures.

"Three years ago operators saw ships as largely isolated from cyber risk but now they realize that their vessels and the logistics supply chain are all connected," says Dierks.

"There has been a significant increase in the awareness of the shipping industry as to the potential risks from cyber, be they malicious or accidental," agrees Chris Turberville, Head of Marine Hull & Liabilities, UK, AGCS. "As the technology on board increases, so do the potential risks. Safeguards need to be introduced at the same rate as new systems. We cannot wait for more significant problems to occur before we react."

Last year, the IMO issued guidelines on maritime cyber risk management and called for cyber risks to be addressed in existing safety management systems by 2021. According to Captain Rahul Khanna, Global Head of Marine Risk Consulting, AGCS this deadline is not soon enough: "The industry needs to take the initiative and address this much earlier than 2021."

While the vessel safety management system (SMS) is the best platform for the cyber security program to reside on, the fact that cyber is a non-traditional maritime risk should not be overlooked, Captain Andrew Kinsey, Senior Marine Risk Consultant, AGCS, believes.

Given the nature of this risk and the potential impact of the failure to adequately protect a vessel, a new approach is warranted. Robust training and auditing – including independent cyber-security audits to ensure procedures are adequate – and having dedicated personnel assigned to provide captains with effective guidance and procedures will be necessary, according to Kinsey.

PREPARING TO PENETRATE YOUR OWN SYSTEMS...

Gideon Lenkey, Technology Director at EPSCO-Ra shares his thoughts on the importance and implications of penetration testing...

A penetration test can mean a lot of things. It can range from a single module of a software application up to an entire enterprise and everything in between. The quality of work you get from any given vendor can also range wildly from scanner output with a cover letter up to and including sophisticated attack simulations with physical components and everything in between. Costs can also vary wildly between vendors for the apparent same services. It can be a bit overwhelming, especially if you're just starting to use penetration testing services as part of your security management program.

The first thing to consider is the scope of the testing and this is one area a lot of inexperienced practitioners get wrong, often by setting the scope too narrow. "Fortress mentality" is still around in some companies and it's often a factor in this mistake. The thought is that if the border defenses are really good 'no bad guys can get in'. While good border controls are an essential part of cybersecurity management, relying on them too heavily is a well documented formula for failure. When fortress mentality is present the tendency is to limit the scope to an 'external penetration test'. The thinking is that if the penetration test cannot breach the border controls then risk is low. This of course is folly as most contemporary attacks originate from inside the network using email phishing or otherwise attempting to get the user to open an attachment or visit a website. Additionally, when I hear someone ask for a test like this, the first thought that comes to mind is that they're not looking for opportunities for improvement, they're looking for documentation that nothing further needs to be done. Unless you're testing a specific application or security process the scope should include the elements of a contemporary attack. In other words, external and internal.

When possible, the scope and type of penetration test should be set with a specific goal in mind. In order to get to a specific goal requires a certain level of security management maturity; one in which you know and understand what is at risk, what the threats are and how much protection the asset warrants. This can best be understood by performing a risk assessment. This is a significantly different process than a penetration test as it seeks to identify potential risks and assign their likelihood and severity. A risk assessment can help you identify what is most important to protect and from what.

A penetration test can help you determine how effective the controls you put in place to manage that risk are. This is why if you haven't done a penetration test or a risk assessment you should perform the risk assessment first.

The most mature security management processes utilise risk assessment and penetration testing in conjunction with a documented framework such as NIST, ISO or CIS (to name a few). As a company's cybersecurity management process matures over time, a framework will most certainly be adopted. This will help document what is currently being done, why, how much it costs and what will follow for the next several years. In some cases a framework will be regulation specific like PCI DSS and in other cases the framework may be a hybrid of two or more frameworks that best fits the company's needs. To date, there aren't any maritime specific frameworks and it makes sense not to reinvent the wheel. The current frameworks are robust enough to satisfy the requirements of maritime if intelligently applied in conjunction with currently published maritime specific guidelines such as those available from the IMO.

No matter what the maturity level of your company's cyber security management practice is or whether or not you're using a formal framework, testing is important.

Penetration testing can help you better understand how real world attacks might play out against your people, processes and technology. By seeing your infrastructure and assets through the eyes of an attacker, you can easily make significant improvements to your security posture. To learn more about EPSCO-Ra see https://www.epsco-ra.com

CYBER INNOVATIONS LAUNCHED

Faced with a vibrant cyber-threat landscape to combat, this year we have seen companies truly step up to provide consumers across the maritime market with more options than ever to protect themselves and their businesses.

Last month Marlink launched Cyber Detection, the latest in their fully integrated ship and shore-based Cyber Guard portfolio. Cyber Detection monitors all outbound and inbound network traffic around the clock and enables customers to view threats affecting their vessels through an intuitive, web-based dashboard. Customers can set up to receive notifications on critical threats and compromised assets may be remedied using Cyber Guard solutions and additional optional assistance from a specialised team at Marlink's Security Operations Center (SOC).

The combination of machine and human intelligence is an integral part of Marlink's service. While using proven rule-based algorithms to detect malware or unauthorised network activity, Marlink's SOC experts investigate in parallel, any anomalies, and proactively hunt 'under the radar' threats.

While new products are an essential part of the arsenal against cyber criminals, so too are businesses coming together to share expertise, liaise products and strive to add value to their customer base. Cyber protection is a growth sector and maritime customers are being offered better deals than ever.

For example, recently HudsonAnalytix's cyber risk management subsidiary, HudsonCyber, has announced the inclusion of its award-winning HACyberLogix risk management decision-support software solution with DNV GL's Veracity industry platform. This means over 120,000 Veracity users will now have access to specific maritime risk management with cybersecurity expertise, capabilities and best practices, and receive meaningful cybersecurity guidance, insights, recommendations and trend analysis.

As Max Bobys, Vice President of HudsonCyber, stated: "This will provide shipping companies with an opportunity to continuously benefit from a customized roadmap of prioritized recommendations that will support them on their cyber risk management journey."

It is satisfying to know that while the hackers and cyber criminals are working hard to bring us down, there is an industry rallying to stay one step ahead, and we look forward to hearing more about the products and networking that will be part of the solution.

NEW TYPES OF SECURITY THREAT

The 2018 SMM event held in Hamburg featured the international conference on maritime security and defence (MS&D). Making the key note address, Rear Admiral Thorsten Kähler, Chief of Staff of the German Naval Command based in Rostock warned of the new challenges being faced by the military. These also featured worrying developments around maritime cyber security.

Kähler warned that new types of threats have arisen, such as cyber warfare. In pondering how to tackle these new problems, the Rear Admiral expressed his strong support for strategic cooperation, demanding more investment in personnel and equipment.

The Bundeswehr White Paper 2016 provides a solid basis for such efforts, he stressed. The White Paper on Security Policy and the Future of the Bundeswehr is the key German policy document on security policy. It is a strategic review of the current state and future course of German security policy.

It is thus the principal guideline for the security policy decisions and measures of the country. It establishes a framework in terms of concepts and content and provides starting points for strengthening the whole-of-government approach and developing further ministerial strategies.

You can access the 2016 White Paper here:

https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf

HACKER247

Our Knowledge Is Your Power

Whilst you're at sea ensure your family are safe online!

1 in 10 people are now victims of personal cybercrime, with some not even knowing their details have been compromised. Sophisticated hacking techniques are being developed daily and individuals, even ones educated in online fraud, often don't spot the signs until it's too late.

Fraudulent activity now incorporates a range of online misuse and it has become increasingly difficult to avoid becoming a victim of cybercrime, with age, race and social background of no interest to hackers, meaning anyone can be targeted.

Keep you and your family safe online whilst you're at sea with Hacker247, a new and secure platform from the founders of Turrem Data Group. Combining 30 years' experience, this innovative new service holds billions of stolen records from thousands of sources; this information expands to over 80 different types of data including emails, passwords, usernames, addresses and many more items of a personal nature.

Find out more when Hacker247 launches this month and protect your data from as little as £3.99, *our knowledge is your power.*

www.hacker247.co.uk

A Member of **Turrem Data Group**