# Notices to Master Mariners

PERIODIEKE UITGAVE VAN DE NEDERLANDSE VERENIGING VAN KAPITEINS TER KOOPVAARDIJ

## THEMANUMMER


NR 3 - OKTOBER 2019


jaar loodsen we zo'n tienduizenden schepen Nederlandse havens en Vlaamse havens aan Schelde in en uit. Aan boord is dan altijd één onze 450 registerloodsen, omdat na het mij- werk op zee, het centimeterwerk in de haven gt. Ja, de laatste 200 meter van een reis zijn k hachelijker dan 5000 mijl op zee. Want hoe ds je een schip met een lengte van meer n 300 meter veilig door een complex en druk bevaren havengebied? Hoe manoeuvreer je dichte mist of bij windkracht 7? Alleen een re terloods heeft hier de juiste kennis en ervarin voor. De registerloods adviseert de kapitein over de te voeren navigatie. Meer weten ov het Loodswezen?

**Kijk op www.loodsworden.nl**

## COLOFON

Notices to Master Mariners verschijnt 4 maal per jaar en is het officiële en onafhankelijke orgaan van de Nederlandse Vereniging van Kapiteins ter Koopvaardij (NVKK). De NVKK is opgericht in 1943 en aangesloten bij:
IFSMA, International Federation of Shipmaster's Associations
CESMA, Confederation of European Shipmaster's Associations.

**ALGEMENE ADRESGEGEVENS:**
**Postadres:**
Nederlandse Vereniging van Kapiteins ter Koopvaardij,
Wassenaarseweg 2,
2596 CH 's-Gravenhage
**E-mail:** nvkk@introweb.nl
**Website:** www.nvkk.nl

---

**Dagelijks Bestuur:**

| | | |
|---|---|---|
| Voorzitter: | L. van den Ende, | ☎: 06-83944694 |
| Vice-voorzitter: | J.P. Bosma, | ☎: 06-13827308 |
| Secretaris: | D. Roest, | ☎: 06-23850923 |
| Penningmeester: | J. Boonstra | ☎: 06-13639145 |

**Betalingen:**
T.n.v. Penningmeester NVKK, Den Haag
Bankrekening: IBAN: NL14 INGB 0002 4653 14

**Redactie:**
H.A. L'Honoré Naber,
J.P.Bosma
C.J.W.Herfst
J.C.Ulrich

**Bijdragen van:**
J. Boonstra
P.P. van der Jagt

**Redactieadres:**
via postadres NVKK of
e-Mail: nvkk.notices@gmail.com

**Informatie over contributie, betalingen, lidmaatschap, SWZ/MARITIME, CESMA, IFSMA:**
Zie website: www.nvkk.nl

**Advertentieaquisitie:**
Via Secretaris NVKK

**Productie:** Blad.NL



## VOOR UW AGENDA

**10 oktober** Amsterdam, Koninklijk College Zeemanshoop: NVKK-Symposium **'Veilig Varen (Z)Onder Cyberdreiging'**
Aanvang 13:00 uur

**9 januari 2020** (onder voorbehoud)
Amsterdam, bij Loetje aan 't IJ:
**Nieuwjaarsreceptie**, Aanvang 16.00 uur

## INHOUDSOPGAVE



## OP DE VOORPAGINA:

'Cyber Security'
door Darwin Laganzon, Pixabay

## QUOTE

'Technological progress is like an axe in the hands of a pathological criminal'

*Albert Einstein*

Geachte collegae,

We hebben weer een zomer met prachtig weer achter de rug en ik hoop dat u er van genoten heeft.
Na een kort zomerreces heeft de vereniging haar activiteiten weer opgepikt. Zoals u in de laatste Notices heeft kunnen zien en lezen, was de vereniging weer present bij de 4 Mei herdenkingsplechtigheden in Rotterdam, Amsterdam en Den Helder waar kransen en bloemen gelegd werden. Ook legde NVKK leden een krans bij de herdenking einde tweede wereldoorlog in Den Helder op 15 Augustus jl.
Op 24 Juni werd de vereniging door IFSMA en CESMA leden vertegenwoordigd in Parijs bij het seminar ter herschrijving van IMO-resolutie A.8257(20) voor Vessel Traffic Services.
Gedurende de afgelopen maanden zijn verschillende NVKK-"container" collega's betrokken geweest bij het OVV-onderzoek naar het incident met het containerschip MSC Zoë.
In dit nummer speciale aandacht voor ons symposium van 10 Oktober te Amsterdam met als onderwerp;

**"Veilig Varen (Z)Onder Cyber Dreiging"**

Het belooft weer een interessant symposium te worden met vooraanstaande sprekers uit de sector over een zeer belangrijk en actueel onderwerp waar de koopvaardij zeker nog een inhaalslag te maken heeft. Ik hoop dan ook dat u aanwezig kan zijn, maar het aantal plaatsen is beperkt. Dus, als u zich nog niet heeft ingeschreven, doet u dat dan nog snel.
Ik wens u allen een prettige nazomer en de collegae op zee een veilige vaart.

Leen van den Ende
Voorzitter.

*(afbeelding: National Security Archive)*

## SYMPOSIUM 10 OKTOBER 2019

# “Veilig Varen (Z)Onder Cyberdreiging”

Programma en sprekers:

**13:00 – 13:30**
Inloop

**13:30 – 13:40**
Inleiding en huishoudelijke mededeling College Zeemanshoop

**13:40-13:50**
Welkomstwoord Voorzitter NVKK.

Moderator: Jeroen de Jonge (Business Director Naval Programs TNO)

**13:50-14:20**
Keynote spreker Koninklijke Marine Jeroen de Jonge - Cyber threats and Geo-Politics

**14:20 – 14:50**
Sarah Olierook - Senior advisor staff Port of Rotterdam Harbour Master Divison
Cyber security in the Port.

**14:50 – 15:20**
Pauze

**15:20-15:50**
Glenn Rittereiser - Cyber Security Officer at Maersk.
Shipowner’s answer on cyber security threats.

**15:50-16:20**
Jeroen Kortsmit – General Manager JRC Europe at Alphatron Marine
Cyber security protection of vessel’s nautical equipment

**16:20 – 16:50**
Q&A

Maritiem Instituut
Willem Barentsz

# Maritieme hbo-opleidingen, cursussen en trainingen

www.miwb.nl

NHL

Postbus 26 8880 AA West-Terschelling T 0562 44 66 00

*(Afbeelding: Tumisu, Pixabay)*

**Fourteen Maritime Organizations Protest Jamming and Spoofing**

At the IMO's annual "Day of the Seafarer" on June 25, fourteen maritime organizations have sent a letter to U.S. Coast Guard Commandant Karl Schultz, which urged the USCG to raise the issue of jamming and spoofing of GPS and other Global Navigation Satellite System (GNSS) signals at the next IMO Council meeting. The letter states that "GNSS signals have become an important part of marine operations and interferience with them places the efficiency and safety of maritime operations at risk, and can impact seafarer lives." A recent report on Russian interference *[ zie artikel elders in dit nummer]* on navigation signals in the Black Sea and Syria as well as another study that spanned from Europe to the Far East were cited as evidence of the problem. The U.S. Maritime Administration has issued several advisories for GPS signal interference in the Eastern Mediterranean during the last two years.
GPS signal interference is seen by many to be a violation of International Telecommunications Regulations, which concludes that "All transmissions with false or misleading identification are prohibited."
The letter also recognizes that some nations feel it necessary to block GPS and GNSS signal for security reasons, but the reality of blocking signals impact vessels operating in international waters or for those in innocent passage through territorial waters. The group concludes that mariners should be notified in order to preserve navigational safety. The letter requests the Coast Guard to propose a resolution at the upcoming IMO meeting next month and should include:

- GNSS signals are important to safety navigation;
- Member states should enact measures to prevent unauthorized transmissions on GNSS frequencies;
- Member states should refrain from interfering with GNSS signals except when required for security reasons;
- Member states interfering with GNSS signals for security reasons should issue Notices to Mariners, which specify time periods and areas impacted to help minimize negative effects on maritime operations.

The letter was coordinated by the Resilient Navigation and Timing Foundation, a scientific and educational charity.

**Source:** The Maritime Executice, 25 June 2019

**Full letter:** https://rntfnd.org/wp-content/uploads/Multi-sig-Ltr-to-USCG-IMO-GNSS-Jamming.pdf

**Malware attack exposes cyber vulnerabilities at sea**

Less than two months after warning of cybersecurity problems on ships, the US Coast Guard has revealed that a large international vessel has suffered a cyberattack. On Monday 8 July 2019 the Coast Guard issued a Marine Safety Alert (*) reporting a successful malware attack on a vessel back in February. The alert describes the affected craft as a 'deep draft' vessel on an international voyage. It experienced a "significant cyberincident" on its way to the Port of New York and New Jersey.
The crew avoided losing complete control of the ship, but this should be a wake-up call. The report explained the findings of the cybersecurity team that investigated the incident:

*The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities.*

The Coast Guard hasn't revealed the exact nature of the attack, but the crew knew about the security risk to the ship's network before the attack happened, the report said. "Most" crew members didn't use the network for personal business like checking email or making online purchases, it said (it only takes one, though). The crew did use the network for official business like updating electronic charts and managing cargo data, and members would routinely plug USB drives into the ship's systems without scanning them for malware, the report added.

**Source:** Sophos Naked Security

**The USCG report:**

The U.S. Coast Guard has recently issued marine safety alert 0619 (*) to warn the maritime community of a potentially serious cyber incident aboard a merchant ship early this year. In February, during an international voyage to the Port of New York and New Jersey, an unnamed deep draft vessel reported that it had been affected by a malware attack. A Coast Guard-led team analyzed the vessel's network and found that while the malware had "significantly degraded" its functionality, essential control systems had not been affected. However, the team determined that the vessel was operating without effective cybersecurity measures in place, exposing safety-critical control systems to "significant vulnerabilities." What is more, these risks were "well known among the crew" prior to the incident.
To address the deficiencies that came to light in this incident, the Coast Guard provided a short list of simple starting points for cyber hygiene. These include:

- Use individual credentials for each employee on the network, not just one generic username and login for everyone. Avoid the use of administrator accounts for non-administrator purposes.
- Do not use USB sticks without scanning them for malware first on a standalone, isolated computer system.
- Segment your computer networks into subnetworks to make it harder for an adversary to gain access to essential systems.

- Use basic antivirus software and update it regularly.
- Install patches and updates for computer software and operating systems regularly. Patches are often issued to fix known security vulnerabilities.
- Conduct cybersecurity assessments to understand the extent of cyber vulnerabilities.

"It is unknown whether this vessel is representative of the current state of cybersecurity aboard deep draft vessels," the USCG said. "It is imperative that the maritime community adapt to changing technologies and the changing threat landscape by recognizing the need for and implementing basic cyber hygiene measures." The advisory drew an incredulous response from several cybersecurity experts. "What comes as a shock to me, if I am honest, is that the measures which the Coast Guard 'strongly recommends' . . . are hardly advanced in nature," wrote cybersecurity reporter Davey Winder for Forbes (**). "That [this list] was the outcome of the investigation speaks volumes for the lack of security awareness at sea."
The incident is far from the first account of an onboard malware attack. The 2018 edition (***) of the ICS *Guidelines on Cyber Security Onboard Ships* describes two incidents in which outside vendors accidentally introduced malicious software into a ship's systems, including one incident affecting a ship's electronic power management system and another affecting the ship's business network.

**Source:** The Maritime Executive, 9 July 2019

**Referenties:**

**(*) USCG safety alert 0619:**
https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

**(**) Forbes article of Davey Winder:**
https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?ss=logistics-transport#1041393641aa

**(***) Publication, Guidelines on cyber security onboard ships:** https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

**Warning of Iranian GPS Jamming in Strait of Hormuz**


*A U.S. official told CNN that Iran has deployed GPS jammers on the island of Abu Musa, lower left (file image MarEx)*

An escalating tension in the Persian Gulf over the last months continues to pose serious threats to commercial vessels. Associated with these threats is a potential for miscalculation or misidentification that could lead to aggressive actions, the US MARAD warned. Vessels operating in the Persian Gulf, Strait of Hormuz, and Gulf of Oman may also encounter GPS interference, bridge-to-bridge communications spoofing or other communications jamming with little to no warning.

Six attacks against commercial vessels, the shoot-downs of a US Navy drone (*) and an Iranian drone (**) and the seizure of the UK-flagged 'Stena Impero' (***) by Iranian authorities have caused disruption over the last months in the Strait of Hormuz, a major shipping route for world oil supply.
Reports by CNN this week say ships sailing in the region have reported unusual GPS interference, among other problems, and the US believes Iran is to blame.
With this respect, the US Department of Transportation's Maritime Administration issued a warning on Wednesday highlighting threats and advised vessels operating in this area to review security measures, ensure AIS is transmitting at all times, and monitor VHF Channel 16. Specifically:

**1.** To afford best protection in the region, US-flagged commercial vessels are encouraged to:

- Simultaneously register with both the UK Maritime Trade Office (UKMTO) and US Fifth Fleet Naval Cooperation and Guidance for Shipping (NCAGS) Watch when entering the Indian Ocean Voluntary Reporting Area (VRA) by e-mailing them the Initial Report from Annex D of Best Management Practices to Deter Piracy and Enhance Maritime Safety in the Red Sea, Gulf of Aden, Indian Ocean and the Arabian Sea (BMP5).

- Provide transit plans for the Strait of Hormuz (SoH) and Persian Gulf (PG) to UKMTO and US Fifth Fleet NCAGS via a single e-mail, including the time of entering/exiting the SoH Traffic Separation Scheme, an outline of the navigation plan for operating in the SoH and PG, and speed restrictions or other constraints.
- In the event of any incident or suspicious activity, call UKMTO or the US Fifth Fleet Battle Watch and activate the Ship Security Alert System immediately.
- Answer all VHF calls from coalition navies.
- Utilize other reports included in Annex D of BMP5 as necessary, including both UKMTO and Fifth Fleet NCAGS on each of these reports.

**2.** All vessels should be aware that US and other coalition naval forces may conduct maritime awareness calls, queries, and approaches to ensure the safety of vessels transiting the Persian Gulf, Strait of Hormuz, Gulf of Oman, and Arabian Sea.
*If a US flag commercial vessel suspects it is being hailed from a source falsely claiming to be a US or coalition naval vessel, the U.S. Fifth Fleet Battle Watch should be immediately informed.*
**3.** If hailed by Iranian forces, US flag commercial vessels should provide vessel name, flag state, and affirm that they are proceeding in accordance with international law as reflected in the Law of the Sea Convention. The master should immediately inform the US Fifth Fleet Battle Watch.
**4.** If Iranian forces seek to board a US flag commercial vessel navigating these waters, the ship's Master should, if the safety of the ship and crew would not be compromised, decline permission to board, noting that the vessel is proceeding in accordance with international law, and immediately inform the US Fifth Fleet Battle Watch.
**5.** If Iranian forces board a US flagged commercial vessel, the vessel should immediately contact the US Fifth Fleet Battle Watch. The crew should not forcibly resist the boarding party. Refraining from forcible resistance does not imply consent or agreement to that boarding.
**6.** The Maritime Global Security website at https://www.maritimeglobalsecurity.org/offers industry issued best practices, including BMP5, and guidance to mariners by geographic region and provides contact and subscription information for regional maritime security reporting centers.
**7.** Vessels operating in this area are advised to establish contact with both UKMTO and the US Fifth Fleet NCAGS Watch, and to include both on all update or incident report emails, as detailed above. By including both as addressees on each email, awareness will be enhanced without creating an additional reporting burden.

**Source:** Safety4Sea, August 8, 2019
https://safety4sea.com/us-marad-updated-guidance-for-ships-in-strait-of-hormuz/

**Referenties:**
(*) Shooting of USN drone: https://safety4sea.com/iran-shuts-down-us-surveillance-drone-in-strait-of-hormuz/

(**) Shooting of Iranian drone: https://safety4sea.com/us-takes-down-iranian-drone-in-strait-of-hormuz/

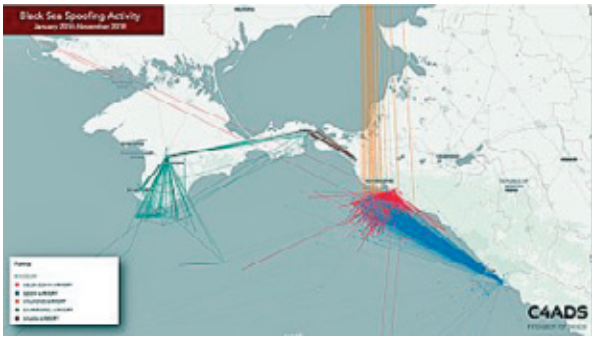
(***) Seizing of Stena Impero: https://safety4sea.com/iran-seizes-british-flagged-oil-tanker-in-strait-of-hormuz/

**CNN Politics bulletin:** https://www.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/index.html

**Russian GPS Spoofing Threatens Safety of Navigation**

*Dana A. Goward*

A new report by the non-profit analytic group C4ADS shows that Russian jamming and spoofing of GPS signals is far more extensive and frequent that previously thought (*).
The report - "Above Us Only Stars – Exposing GPS Spoofing in Russian and Syria" - outlines the discovery of almost 10,000 instances of spoofing detected over the course of two years impacting over 1,300 unique vessels. Ship locations ranged from the Mediterranean, Black Sea, and Gulf of Finland, to the waters off Vladivostok. While a majority of the vessels were in Russian territorial seas, a substantial number were in international waters.


The report also drew a strong correlation between the movements of Russian President Vladimir Putin and the spoofing events. This reinforces speculation among many that the impact on ships is merely a by-product of the Russian government trying to protect its VIPs from drones.

Much of the spoofing has the effect of causing receivers to report their locations as at airports. Most drones are programmed at the factory to fly away from airports.
A form of spoofing sometimes called "smart jamming" was also detected and is discussed. This involves transmission of seemingly valid GPS signals that do not allow a receiver to calculate a location. This can cause many receivers to not function properly while also not reporting a fault.
Some of the incidents and phenomena discussed in the report were discovered by Professor Todd Humphreys of the University of Texas, Austin. Working with sensors on the International Space Station, he developed a methodology that allows disruption of GPS signals to be detected and reported in near-real time.
The Resilient Navigation and Timing Foundation also cooperated in preparation of the report. In 2017 the foundation revealed extensive spoofing activity in the Black Sea with ships reporting their locations via AIS at airports. As a result of this recent report, the foundation intends to raise safety of navigation concerns with US delegations to the International Maritime Organization and the International Telecommunications Union. The foundation has also approached the US government about establishing a more complete system for detecting and warning mariners about GPS disruptions world-wide.

*Mr. Dana A. Goward is the President of the Resilient Navigation and Timing Foundation, a 501(c)3 scientific and educational charity supporting policies and systems to protect GPS/GNSS users.*

**Source:** The Maritime Executive, April 2, 2019

**Full report can be downloaded from:**
https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf

*Russian jamming and spoofing drone - Foto: Resilient navigation and Timing Foundation - Rostec/Kalashnikov*


MARITIME SECURITY ALLIANCE
Experts in layered defense protection against piracy
www.maritimesecurityalliance.com
Early Detection
Avoidance
Discouragement of Approach
Anti Boarding
Obstruction of Movement
Safe Room

**Petya Attack Shows the Need for Cybersecurity Rules**

*Ian W. Gray*

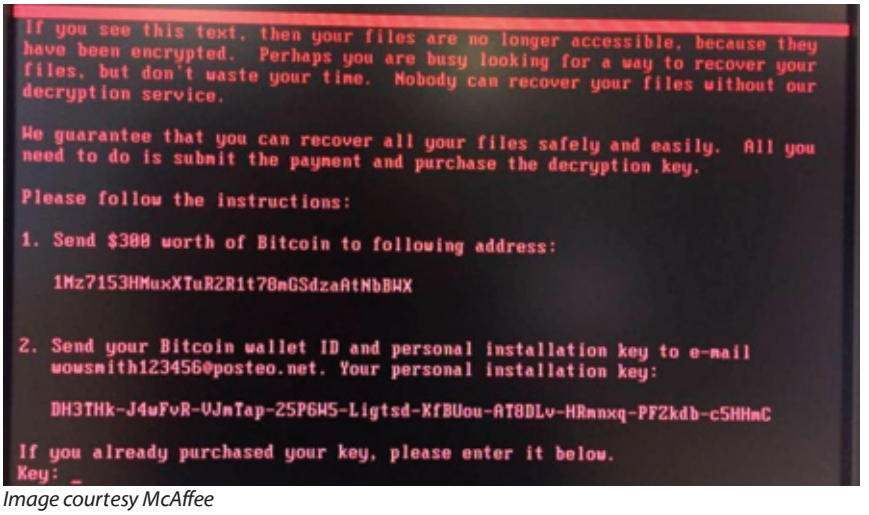


*Image courtesy McAffee*

For the last several years, the International Maritime Organization has been discussing the possible implications of cyber-attacks to the global commerce. In June 2017, the IMO published its Interim Guidelines on Maritime Cyber Risk Management with the intent to provide a risk management framework and prevent large-scale cyber-attacks. These threats manifested themselves when A.P. Moller-Maersk was hit by the global "Petya" cyberattack.

The Petya ransomware exploited the same Microsoft Windows vulnerability (dubbed EternalBlue) from the WannaCry ransomware program, which infected thousands of computers. That ransomware spread through a patched vulnerability that was unavailable for unsupported versions of Windows. Petya had a similar effect on the Danish shipping company, forcing them to shut down systems to contain the attack. Though Maersk's ships were able to safely maneuver, Maersk's APM Terminals unit was unable to handle cargo (*) at select sites around the globe. Multiple ports were affected, including the Port of Los Angeles, Port of Rotterdam and Jawaharlal Nehru Port Trust.

The attack came just days after the IMO Maritime Safety Committee (MSC) 98 meeting, where a new paper (**) proposed making cyber risk management onboard ships mandatory. Previous International Union of Marine Insurance guidelines made these requirements voluntary. These risk assessments were developed by shipowners associations and classification societies, like BIMCO, the International Chamber of Shipping (ICS), Intertanko, Intercargo and Cruise Lines International Association (CLIA).

MSC 98's cyber risk management proposal arrives as the shipping industry is leaning heavily towards digitization and automation. In May 2017, Maersk published a statement announcing that they were partnering with IBM to digitize their administrative processes and transactions with blockchain technology. Other partnerships with companies like Microsoft promise to streamline supply-chain

management and lower operational costs through data science. Additionally, several shipping companies are beginning to test autonomous operations onboard ships. While the industry is developing in a direction that will likely increase efficiency and decrease costs, the necessary safeguards to protect these automated systems are not fully realized. The Petya ransomware illustrated the potential effects of a cyberattack on a major shipping company and port terminals. The attack could have been far more severe, affecting navigation or engineering systems on merchant ships, with possible threat to human life or to the environment.

If shipowners begin to take accountability for cyber security, the industry is likely to progress towards a less vulnerable state. Initiatives to harden their digital infrastructure will take considerable time and resources. These actions will require significant threat modeling, including penetration testing, table-top exercises and periodic audits. The progressive move towards an automated and digitized shipping infrastructure increases the urgency of these corrective actions, as existing vulnerabilities could be exploited by attackers for financial gain or strategic objectives.

The proposal from MSC 98 called for ships to identify cyber risks and implement safeguards. The meeting also recommended that these safeguards take effect under the International Safety Management (ISM) Code, with a deadline of January 1, 2021. Owners could risk having their ships detained if they fail to meet the ISM standards for cyber risk.

While there have been previous incidents of cyber-attacks on merchant shipping, the Petya ransomware illustrates the potential effects of well-executed hacking. 2021 is a practical deadline for ship owners to implement cyber risk management frameworks, but it is unclear if existing cyber practices can meet the rapid pace of new technology onboard ships. The shipping industry will have an upstream battle to implement safeguards and identify methods to assess vulnerabilities. The consequences of failure to meet these standards could affect not only the ship owner, but global commerce as a whole.

*Ian Gray is a cyber intelligence analyst for cybersecurity firm Flashpoint. He is a Navy veteran and a former naval science instructor at Kings Point United States Merchant Marine Academy. Any views expressed within this report are solely the author's and are not necessarily reflective of any organization with which he is associated.*

**Source:** The Maritime Executive, 30 June 2017

**(*) The Maersk case:** https://maritime-executive.com/article/maersks-cargo-operations-hit-hard-by-cyberattack

**(**) IMO Measures to enhance maritime security:**
http://www.nepia.com/media/689025/MSC-98-5-2-The-incorporation-of-Cyber-Risk-Management-in-Safety-Management-Systems-United-States-.PDF

**Interactive CyberWar map**

*Een uiterst informatieve interactief overzicht van alle huidige spelers op cyber gebied, die is samengesteld door het National Security Archive*, een non-profit organisatie van de George Washington University in Washington, U.S.A.*


The CyberWar Map is a visual guide to some of the most prominent players and events in state-to-state cyberconflict created as a part of the National Security Archive's Cyber Vault Project. This resource focuses on state-sponsored hacking and cyber-attacks.
Clicking on map elements will produce links and descriptions for documents relevant to each subject. Elements, connections, and documents will be added on a regular basis to this ever-evolving research aid.
All links lead to unclassified or declassified sources.

**Note:** Since each edition will have a new URL, bookmarking the CyberWar Map will not incorporate running updates. Please access this resource through the link on the Cyber Vault Project home page.

**De CyberWar map is te vinden op:**
https://embed.kumu.io/0b023bf1a971ba32510e86e8f1a38c38#apt-index

** As a registered 501(c)(3) non-profit organization, the National Security Archive is committed to pursue generally recognized "best practices" with respect to legality, ethics, accountability, and transparency.*

**GPS Wars**

*Michael Martelle*

First fielded in the 1970s, Global navigation satellite systems (GNSS) like the U.S.'s Global Positioning System (GPS), Europe's Galileo, and Russia's GLONASS have become critical to modern societies. These systems provide the position, navigation, and timing (PNT) information an impressive array of both military and civilian functions now rely on. Since the 1990s, civilian uses for PNT have also become integral to the functioning of U.S. critical infrastructure and the U.S. economy. These uses include time-stamping financial transactions from ATMs to high-speed trading; synchronizing and regulating the electric grid; enabling real-time communications; weather monitoring and earthquake detection; precision farming; and coordinating and routing first responders.

Military operations are particularly reliant on GNSS for navigation systems on aircraft, vessels, vehicles, and unmanned vehicles including drones and missiles; synchronizing operations; and pinpointing targets. The Persian Gulf War has become the exemplification of how readily-available PNT information boosts military effectiveness. Beyond the use of GPS for navigation, network-centric warfare relies on precise timing information to enable secure real-time communications.

The near-universal reliance on PNT information has led militaries to explore "deliberate defensive and offensive action to assure friendly use and prevent adversary use of PNT information through coordinated space, cyberspace, and electronic warfare (EW) capabilities" (**JP 3-14 Space Operations, II-3**) (*), an approach known as navigation warfare (NAVWAR). To ensure PNT functions, the U.S. has examined alternative solutions including interoperability with other GNSS systems like Europe's Galileo and Japan's QZSS and nontraditional PNT solutions such as using quantum clocks for timing information. The U.S. is also engaged in upgrading the GPS system, transitioning from Block II to Block III satellites, which

have improved capabilities to help increase GPS resilience and counter jamming and other interference.
The need for resiliency measures has become more sharply apparent in recent years. During the massive Russian exercise Zapad 2017, and again during NATO's 2018 Trident Juncture exercise, **GPS signals were disrupted** (**) causing civilian air traffic to rely on manual navigation. Russian activity is the likely cause of the 2017 outage, and the Norwegian Ministry of Defense has **definitively stated** that Russian jamming from the Kola Peninsula was responsible for disruptions during Trident Juncture. These actions, and questions surrounding the current disruption to the Galileo system currently attributed to ground infrastructure difficulties, indicate that NAVWAR represents an increasingly relevant facet of conflict involving information and information-enabled systems.
The following documents from the Cyber Vault Library serve as an introduction to this important sub-field.

**Source:** National Security Archive, 17 July 2019

**References:**
(*) Joint Space Operations, 10 April 2018:
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf
(**) Article FP-The GPS Wars Are Here, 17 Dec. 2018:
https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/
(***)CNN Politics and video-Russia jammed GPS during major NATO military exercise with US troops, 14 Nov. 2018: https://edition.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html

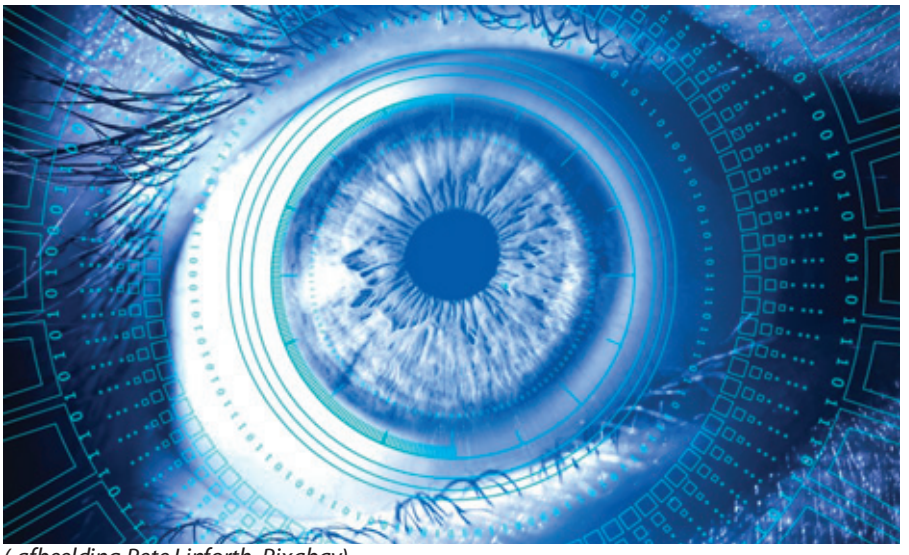
**LORAN Overboard**
*Michael W. Carr*

I had heard enough. This constant debate on the need for electronics. Someone would say, "Well, celestial is great, but you really need electronics, I mean what if it's raining, or too rough, or there is no horizon….?"
At first, I would respond to these queries with politeness and a feeling of duty to clear the air. "Yes, of course, there will be times when it is difficult" I would slowly respond, "But there are so many options with celestial. You have 57 different stars to shoot, you have the sun and moon and four planets."
Here we were sailing to Norfolk from Bermuda, shooting stars every day at morning and evening twilight, and the sun throughout the day, including my favorite, Local Apparent Noon (LAN), when you can obtain both latitude and longitude with a single line of position (LOP). This is done by timing your LAN shot and computing longitude using the shots Greenwich Mean Time (GMT). Computing a noon fix with a LAN shot is a thing of beauty, and always a sight to behold when plotted on your

plotting sheet. An act deserving of a fresh cup of coffee and a brief respite from daily activity.
So, here we were, once again debating the need for electronics. Then came the words which threw me into action.
Someone said, "Look we have this LORAN onboard, it's so simple and accurate, why would you go to all the effort to plot celestial fixes when you can just pull latitude and longitude off the LORAN?"
"Well," I said, "A lightning strike, a loss of electricity, a short circuit inside that magic box, there are a multitude of potential things which can cause us to lose the LORAN"
I was on a roll now, "But my Cassens and Plath sextant always works, it measures precisely to a 0.1 of a nautical mile, and it never fails me."
"That is why I shoot morning stars, evening stars, the sun, moon, and planets."
"I can walk onto any vessel, anywhere in the world, and if I have my sextant I can navigate the oceans."
There was more bantering about the pros and cons of celestial and then my brain blew a circuit breaker. I still don't know what exactly triggered me into action.
I stood up from my seat in the cockpit, walked down the companionway steps, over to the LORAN mounted above the chart table, and disconnected it's power and antennae cables. I then unscrewed the unit from its mounts and carried it back up the companionway to the cockpit.
A gaggle of the crew was still there, idly engaged in scuttlebutt and debating the difficulty in taking moon shots.
"Listen Up" I interrupted.
"See this LORAN I am holding in my hand?"
"I wonder if it floats or sinks?"
There were quizzical looks, I could see they were confused by my question.
I then leaned back with the LORAN in my right hand and threw it astern as far and as high as I could. That silly electronic box made a large arc in the sky and then fell into our wake and floated away.
"I guess it floats," I said, and then sat down and resumed drinking my coffee.
There was silence. Then more silence. Then some outcry. Really? Why did you do that? Some mild panic. What if thick fog settles in? What if it rains for the next 5 days?
"Well," I finally said, "I am not in the least concerned or worried." We can safely and effectively navigate our way to Norfolk, and we did.
Sun lines, running fixes, morning stars, evening stars, moon shots, amplitudes, azimuths, planets, LAN, more running fixes. Computation of set and drift, estimated positions, and continuous DRs. Patience, consistently, thoughtful plotting, studious navigation.
And then, on the day and at the time we calculated Chesapeake Light appeared on our horizon, broad off our starboard bow. Right there where it should be. "Imagine that," I said aloud. Pure magic.
I stood in the cockpit, steering us along, all sails set, making 10 knots on a broad reach, steaming cup of coffee in my hand. And in my head I am thinking, "I wonder how that LORAN is doing now, floating across the ocean". I smiled to myself.
"Let's trim the foresail" I yelled to the crew, "She's luffing at the peak".
Drive on, keep her to it.

**Source:** GCaptain, Michael W. Carr, 19 aug. 2019

## 10 steps to maritime cyber security



*( afbeelding Pete Linforth, Pixabay)*

**A guide to manage cyber risk**

*Ships are increasingly using systems that rely on digitization, integration, and automation. As a result security of data and other sensitive information has become a major concern of the maritime sector. Training and awareness of appropriate company policies and procedures may provide an effective response to cyber incidents. Here are some guidelines to help maintain maritime cyber security.*

**Maritime Cyber Security Step 1: Network security**

Nowadays, networks are critical to the operation of a ship. It is imperative that these systems do not expose systems to cyber-attack. However, shipboard computer networks usually lack boundary protection measures and segmentation of networks. Such networks are among the most common cyber vulnerabilities on board existing ships, according to a paper published by the International Chamber of Shipping. Simple policies implementation and appropriate architectural and technical response can help manage and/or prevent these attacks from causing harm to your organisation. Onboard networks should be partitioned by firewalls to create safe zones. The fewer communications links and devices in a zone, the more secure the systems and data will be.

**Maritime Cyber Security Step 2: Malware prevention**

Malware is any malicious content which is designed to access, gain control and damage systems. In other words, a malware could seriously impact your ship's systems or services. Organisations should implement an appropriate anti-malware policy to defend in depth their networks both onboard and ashore, filter out unauthorized access and malicious content.

**Maritime Cyber Security Step 3: Risk Management Regime**

Why to embed an appropriate risk management regime across a shipping organisation? Organisations should clearly communicate their approach to risk management with the development of applicable policies and practices. These aim to maintain marine cyber security, ensuring that personnel onboard and ashore is aware of the approach, how decisions are made, and any applicable risk boundaries.

**Maritime Cyber Security Step 4: Secure configuration**
Configuration management improves the security of systems and eliminates the risk of compromise of both them and any information. Therefore, organisations should develop a strategy to remove unnecessary functionality from systems, and quickly fix known vulnerabilities!
**Maritime Cyber Security Step 5: Managing user privileges**
All users should be provided with a reasonable level of system privileges and rights needed for each role. The granting of highly elevated system privileges should be carefully controlled and managed; this principle is sometimes referred to as 'least privilege'.
**Maritime Cyber Security Step 6: Employees education and awareness**
Personnel both onboard and ashore play a critical role in a shipping organisation's security and so it's important that security rules and the technology provided enable them to do their job. A systematic delivery of awareness programmers and training always deliver security expertise as well as help establish a security-conscious culture within the organisation.
**Maritime Cyber Security Step 7: Incident management**
It is of high importance that an organisation identifies any internal or external source of specialist incident management expertise. Effective incident management policies and processes may help to improve resilience and reduce any impact with respect to maritime cyber security.
**Maritime Cyber Security Step 8: Monitoring**
Good monitoring is the answer to the question "How do I detect actual or attempted attacks on systems and services?". Monitoring allows organisations to ensure that systems are being used appropriately, complying with any regulatory requirement.
**Maritime Cyber Security Step 9: Removable media controls**
Wondering why to produce removable media policies? These can control the use of removable media for the import and export of information, limit the types of media that can be used together with the users, systems, and types of information that can be transferred.
**Maritime Cyber Security Step 10: Remote system access**
Remote system access not only offers great benefits, but it also exposes new risks. Risk based policies and procedures should be established in order to support remote access to systems, applicable to service providers.
Either way, cyber incidents can put both organisation's operations and human lives at risk. One thing is sure, operators will not be able to defend themselves alone! Like in many other digital developments, experts suggest cooperation and collaboration and resilience to find the right answers when it comes to maritime cyber security.

**Meer lezen? Klik op:**

**Checklist Maritime Cyber Security**


**Maritime cybersecurity**
Requirements for 2019-2020

**Cybercrime represents an acute and rapidly growing threat across all maritime sectors.** The impact of a cyber incident is no longer limited to malfunctioning computers or employees not being able to use email. There is a direct, negative impact on the business and the bottom line.
Download our **checklist** and receive "all you need to know" information about:

1. The IMO Guidelines on Maritime Cyber Risk Management
2. BIMCO's Guidelines on Cyber Security Onboard Ships
3. Prove IMO compliance through class notation

**Downloaden op:** https://www.dualog.com/checklist

**IMO:**
**The Guidelines on Cyber security onboard ships**


**Downloaden op:**
http://www.imo.org/en/OurWork/Facilitation/Electronic%20Business/Documents/guidelines-on-cyber-security-onboard-ships.pdf


**TNO:**
**Whitepaper: Ketenweerbaarheid tegen cyberdreigingen**

**Downloaden op:**
http://publications.tno.nl/publication/34623640/YdXqcd/TNO-2017-ketenweerbaarheid.pdf


**Pocket Guide to Cybersecurity for Seafarers**

As the industry continues to become an easy target for cybercriminals, it is not only the duty of shipping companies and authorities but also of maritime professionals to ensure cybersecurity on ships by becoming aware of the possible threats and consequences.
Marine Insight is introducing a free pocket guide for maritime professionals to create awareness about cyber crimes and cyber safety

This guide will provide details on:

- Importance of cybersecurity
- Common ways for cyber attacks on ships
- How to identify a cyber attack
- Security against cybercrime
- Responding to cyber attacks
- Security measures and contingency plans.

**Downloaden op:** https://www.marineinsight.com/marine-safety/download-new-free-guide-cybersecurity-for-seafarers/

**Alianz:**
**Safety and shipping review 2018**


**Downloaden op:**
https://maritimecyprus.files.wordpress.com/2018/07/allianz_safety_shipping_review_2018-s.pdf

**DNV:**
**Maritime cyber security services and solutions**

Benefit from tailored DNV GL solutions for maritime cyber security addressing systems, software, procedures and human factors.
Cyber security has become a concern and should be considered as an integral part of the overall safety management in shipping and offshore operations. Our recommended practice (RP) explains the 'how to do' and not just the 'what to do'.
We use a structured approach to effectively assess and manage your cyber security by combining IT best practices with an in-depth understanding of maritime operations and industrial automated control systems. In addition, our RP gives guidance supporting preparations for ISO/IEC 27001 certification.
Get your copy of our DNVGL-RP-0496 on cyber security resilience management for ships and mobile offshore units in operation by submitting the form.
**Downloaden op:**
https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html

**EUROPEAN UNION AGENCY FOR CYBER SECURITY**

https://www.enisa.europa.eu/topics/national-cyber-security-strategies

**NCSS Interactive Map:**

Visit our **interactive map** to see all the national cyber security strategies in Europe. The ENISA NCSS Map lists all the documents of National Cyber Security Strategies in the EU together with their strategic objectives and good examples of implementation.

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

**Maritime Cyber Security Guidance:**
Here you will find a library of useful resources including maritime and offshore industry cyber security best practice guidelines, cyber risk assessment advice and a suite of the latest information, that can be used to help you through your studies or for continued professional development. Please feel free to read them online or click and download them for offline use:
https://www.maritimecybertraining.online/page/library

**Cyber Security in the Maritime Industry - is it safe?:**
Download your copy of our latest FREE whitepaper to find out more about the scale of the problem, hacking, the rise of digitalisation - is it to blame, who is the right person to deal with cyber security and what impact does social media have on cyber security... are you prepared to defend your business against 'invisible pirates'?
http://ubm.seatrademaritimeevents.com/cyber-security-6/

**GPS spoofing: What's the risk for ship navigation pdf-document (15 april 2019):**
https://img1.wsimg.com/blobby/go/8cf68d66-f7e3-4ca6-b9b1-63a1a2b11109/downloads/GPS%20Spoofinng%20-%20whats%20the%20risk%20for%20ship%20naviga.pdf?ver=1555342103914


*Pride of Rotterdam refit 2018, foto: P&O- Remontowa Shiprepair Yard, Gdansk, Polen*

## Radio Medische Dienst artsen op werkbezoek Pride of Rotterdam 9 maart 2019

Na een voorbereiding van een paar maanden en het afstemmen van agenda's was daar eindelijk de dag dat de Radio Medische Dienst (RMD) artsen, op één na, de Pride of Rotterdam konden bezoeken. Ons bestuurslid, Kapitein Ben Kollen was de gastheer.
Na een ongehinderde rit verzamelden allen zich bij de vrachtpoort van het P&O ferry terminal in Europoort. Voor de beveiliger die hier voor het eerst "duty" had, was de aankomst van dit team even nieuw. De namen van allen lagen echter keurig klaar en na registratie werden rap alle passen uitgedeeld. Via een aparte inrit/slagboom konden we het vrachtterrein op rijden en na 300 meter kwam de ramp van de Pride in zicht. Hier stond onze collega Ben Kollen ons op te wachten om oprij aanwijzingen te geven. Rap werden we tussen op en afrijdende tractoren door naar een veilige parkeer plaats geloodst op dek 5. Het lossen van de trailers was nog volop aan de gang met het nodige lawaai, maar al snel verwisselden we het autodek voor de rust van de accommodatie. Wij gingen met de lift naar het dek onder de brug. Na een voor de bezoekers lange wandeling door gangen met hutten kwamen we bij de trap naar de brug. In de conference room achter de brug werden we gastvrij ontvangen met koffie/thee en gebak.
Tijdens de koffie bleek al gauw dat RMD artsen 24/7 beschikbaar moeten zijn! De arts van de wacht haalde zijn tablet tevoorschijn na een alert en kreeg ter plekke een verzoek voor medisch advies. Hij verliet de koffie tafel en vond op de ruime brug zijn plekje om zich op zijn advies te concentreren. Zo staat een RMD arts in Europoort op de brug van de Pride of Rotterdam advies te geven voor een schip ter hoogte van de Eastern Seaboard van Florida. Een blijk van de efficiency van deze dienst, terwijl het ook meteen aangeeft hoe relevant de RMD is.
Relevantie was ook de reden van dit bezoek. Velen van ons kennen de RMD nog uit de tijd dat er via de marconist in codes met het Rode Kruis ziekenhuis in Den Haag werd gecommuniceerd. Door de jaren heen en met de voortschrijdende technologie is de RMD aanzienlijk veranderd. De RMD valt nu officieel onder de KNRM en is na 2 jaar overleg met betrokken instanties waaronder de NVKK een ISO gecertificeerde maritieme huisartsen post geworden. Als onderdeel van het advies van de RMD commissie , waarin onze voorzitter zitting heeft, en de eisen van de ISO certificering,

was een bezoek aan een schip vereist. Onze voorzitter vond mede bestuurslid en kapitein Ben Kollen van de Pride of Rotterdam dus bereidt dit bezoek te ontvangen en de artsen de nodige informatie en een rondleiding te geven.
Het eerste wat op viel bij de rondleiding over het schip was het onderhoud dat gedaan werd door de officieren op de brug. De tweede stuurman en zijn vrouwelijke collega waren bezig met het controleren en testen van het brandalarmering systeem. Het belang daarvan is natuurlijk overduidelijk met al die autodekken en passagiers accommodatie en de korte tijd in de haven dient dan ook goed gebruikt te worden.
Tijdens de rondleiding zagen we o.a. hutten, lounges, restaurants , winkels , duty free en het casino. Deze ruimten werden schoon en weer gereed gemaakt voor de nieuwe gasten voor de reis naar Hull aan het einde van de dag. Uiteraard werd het hospitaal aan boord bezocht en een blik in de medicijn kast geworpen.

Hier zagen we onder andere beademing apparatuur , AED's en de bekende genummerde doosjes en flesjes die het gebruik voor de stuurman of kapitein na een Radio Medisch advies vergemakkelijken. Ook de reddingmiddelen werden niet overgeslagen waarbij een bezoek aan de vlotten met chutes vanaf het passagiers dek niet werd overgeslagen. Deze vlotten werden overigens een paar maanden later getest tijdens een grote oefening met het zusterschip de Pride of Hull in de tweede Maasvlakte, welke alle media aandacht kreeg.
Hoewel niet opgenomen in ons programma werd, na toestemming van de HWTK, op verzoek, nog een kort bezoek aan machine kamer gebracht. Vanaf een van de dekken konden de artsen een blik werpen op de grote motoren en machinerieën die er dagelijks voor zorgen dat er een veilige verbinding is tussen Europoort en Hull in Engeland. Volgens collega Kollen trouwens een kalmer en comfortabeler traject dan de noordelijker routes in de Noordzee.
Na 3 uur aan boord werden we weer veilig uitgeleide gedaan door de kapitein tussen de nu weer oprijdende lading. Luisterend naar de opmerkingen van de bezoekers bij het afscheid was het bezoek geslaagd en heeft het de bezoekende artsen een aardig inzicht gegeven. Door omstandigheden kon onze voorzitter ,die lid is van de "RMD commissie" niet aanwezig zijn, waardoor ik als penningmeester de honneurs mocht waarnemen. Het was een waar genoegen dit te mogen doen en ook voor mij was het een leerzaam bezoek aan een type schip waarvan ik alleen de buitenkant kende.

***JB 28-8-19***

**15 augustus 2019-Herdenking Den Helder**

Op 15 augustus heeft weer de herdenking einde tweede wereldoorlog in Den Helder plaats gevonden. Het was een sobere en plechtige gebeurtenis en het weer werkte gelukkig mee. Geen regen en af en toe zon. Ds. Moens leidde de plechtigheid. Er waren toespraken namens de gemeente Den Helder, de Koninklijke Marine en een dominee. Na de toespraken werden de kransen gelegd. Voor het monument "Voor Hen Die Vielen" stonden drie rekken voor een krans, de overige kransen moesten op de treden van het monument worden gelegd. Als eerste werd door de loco burgemeester een krans gelegd namens de gemeente Den Helder, daarna een krans namens de Koninklijke Marine. Als derde kwamen wij namens de NVKK om een krans te leggen. Er waren twee fotograven aanwezig die van alles een foto maakten, ook wij zullen zeker op de foto staan. Misschien kunt u dit navragen bij het 15 Augustus comité of die opdrachtgever zijn en of zij foto's beschikbaar kunnen stellen aan de NVKK? In het gehele gebeuren zijn wij als vertegenwoordiger voor de koopvaardij belangrijk want het zijn allemaal marine of marine gelieerde instellingen die een krans leggen. Als een van de laatsten werd een krans gelegd namens de Raad van Kerken in Den Helder. Bij de aanvang wordt de koopvaardij wel genoemd als deelnemer aan de oorlogsinspanningen, maar het is toch Marine wat hier de klok slaat. Dus als het kan moet de NVKK zolang mogelijk hier blijven komen om de koopvaardij te vertegenwoordigen. Wat mij zelf betreft, ik ben ook niet meer een van de jongsten en merk dat mijn fysieke toestand achteruit gaat. Dus of ik dit volgend jaar nog kan doen??? Overigens zag de krans er prima uit, het bestond uit witte bloemen en was voorzien van linten, neem aan met de tekst "Namens de NVKK", maar dat heb ik niet kunnen zien.

***P.P. van der Jagt***

**Video:** https://youtu.be/yqox8fMpaBI

## Van het secretariaat

**Overleden:**
A.N. Ribbens Nedlloyd
H.J. Poelenjee Nedlloyd

**De NVKK nam deel aan de volgende activiteiten:**

| | | |
|---|---|---|
| 9 juli 2019 | Rotterdam | Bespreking uitgave Juridisch Handboek Kapitein |
| 15 juli 2019 | Rotterdam | Overleg Alphatron |
| 6 augustus 2019 | | Telefonisch overleg Onderzoeksraad voor Veiligheid |
| 15 augustus 2019 | Den Helder | Kranslegging |
| 6 september 2019 | Driehuis | Crematie kapitein H. J. Poelenjee |

**Vergader- en activiteitenkalender 2019 en 2020:**

| | | |
|---|---|---|
| 10 oktober 2019 | Amsterdam | NVKK Symposium |
| 9 januari 2020 *(datum onder voorbehoud)* | Amsterdam | Nieuwjaarsreceptie Bij Loetje aan 't IJ. Aanvang 16.00 uur |

**IFSMA promotional video, kijk op:** https://youtu.be/9wDIxa4y7-w

## Van de redactie

1. **Kopij voor Notices:**

De redactie ontvangt graag kopij voor de Notices. Heeft u iets meegemaakt of wilt u uw mening over een onderwerp geven, neem dan contact op met de redactie.

2. **De redactie is op zoek naar iemand die 4x per jaar het overzicht van 'Kort Maritiem Nieuws' wil schrijven.**

De redactie is te bereiken via nvkk.notices@gmail.com of nvkk@introweb.nl.

**LINKS NAAR WEBSITES**

***N.B.*** *In de Notices to Master Mariners worden veel links gegeven naar websites, waar men meer informatie kan vinden en/of downloaden. Met de hardcopy van dit blad zult u de link moeten overtypen. Gemakkelijker is, om de NVKK website te bezoeken en daar de digitale versie van het blad te bekijken. Daarop kunt u alle links wél gebruiken.*

People
on demand

# KAPITEINS - HWTK'S VOOR SHIP DELIVERIES

**TOS vaart wereldwijd voor diverse klanten schepen over. Wij zoeken voor deze gevarieerde en mooie reizen gemotiveerde zeevarenden. Iets voor jou?**

TOS is een belangrijke speler op deze exclusieve markt. Onder TOS regie varen wij jaarlijks tientallen schepen, variërend van sleepboten tot vracht- en passagiersschepen, naar de gewenste bestemming. Wij hebben werk voor functies variërend van (ASD) kapitein of werktuigkundige tot kok of matroos.

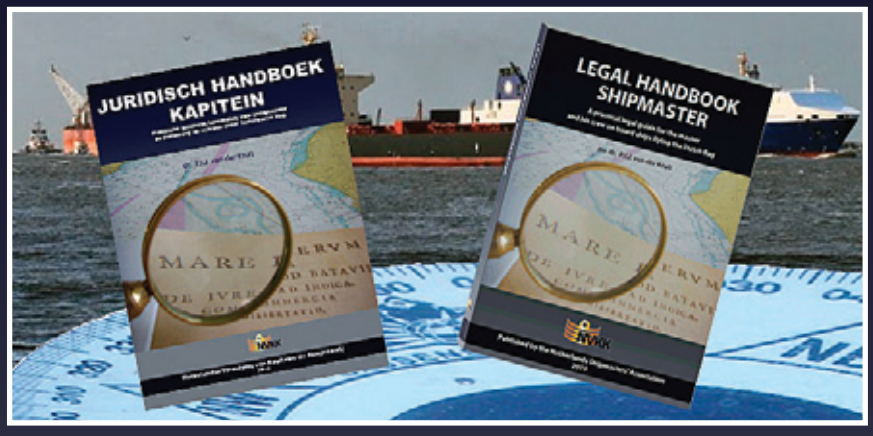
## Meld je aan!

TOS (Transport & Offshore Services)
Waalhaven O.Z. 77
3087 BM Rotterdam
**T** +31 10 436 62 93
**E** info@tos.nl

Maritime
Offshore
Onshore

**NVKK SYMPOSIUM**
**10 oktober 2019**
**'VEILIG VAREN (Z)ONDER CYBERDREIGING'**

# STAY ON COURSE




with your copy of the
**LEGAL HANDBOOK SHIPMASTER**
a practical legal guide for the shipmaster
and his crew on board ships flying the Dutch flag

a publication of the Netherlands Shipmasters' Association,
in English or in Nederlands

NVKK

**FIRMITAS ADVERSARIA SUPERAT**