News

STRONG TANKER MARKET EXTENDS PEAK SEASON EARNINGS

The Baltic and International Maritime Council (BIMCO) reported that tanker earnings for crude oil tankers have risen to new strong levels in the first quarter of 2015, with averages unparalleled since 2008. The demand for crude oil tankers remains high even though the winter months are far behind us. Following the winter peak season of 2013/14, crude oil tanker earnings collapsed and remained low during spring, before rebounding over the summer. This was not the case in the winter peak of 2014/15. The market appears to have kept momentum, keeping the crude oil tanker earnings at a high level. The average VLCC earnings were around $51,000 per day in the first quarter of 2015, i. e. 76 % higher than in the first quarter of 2014, when they averaged to approximately $29,000 per day. This also applies to Suezmaxes earnings, which amounted to around $50,000 per day in 2015 and around $31,000 in 2014. Although the difference was not as large in the Aframaxes, it was still noticeable with around $40,000 per day in Q1 2015 and around $29,000 last year.

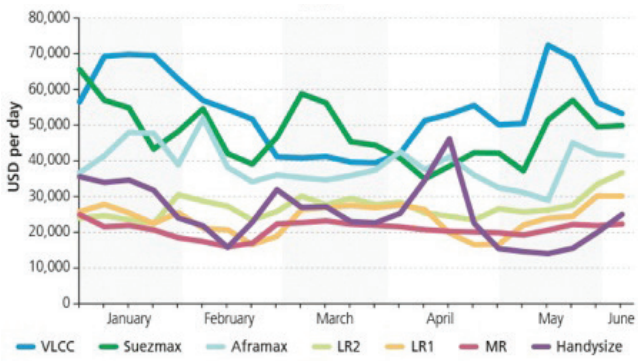

Figure 1.
Tanker Earnings 2015.
Source: BIMCO, Clarksons.

As published in the https://www.bimco.org.

STOWAWAYS: THE HIDDEN TRUTH?

The IMO has recently released its annual statistics for stowaways in 2014. The headline figures could provide a good news headline, 'A 40 % decrease in reported stowaway incidents in 2014', but is this really the case?

It is difficult to believe that, considering mass, irregular migration around the world, in particular from North Africa across the Mediterranean, only 120 cases were reported worldwide in 2014, which is a 40 % decrease from the 203 reported in 2013. I suppose this could be seen as a good news story and an argument that security has improved in all ports, thus deterring people from attempting to embark on ships in an unconventional manner. However, the report only takes into consideration caught or identified stowaways, not their total number. How many stowaways actually managed to evade capture? We are unlikely to ever know the real numbers but with the record levels of illegal migration from Africa witnessed in 2014[1], and a reported reduction in stowaway numbers, this rather than being good news suggests that incidents were almost certainly not reported or security at the ports failed to stop them.

It is difficult to estimate the exact number of incidents that have gone unreported, or the number of stowaways who successfully completed their journey undetected. The IMO's stowaway report for 2008 set a high point of 494 incidents and 2052 actual stowaways, i.e. seven times of what was reported in 2007 and twice as many as reported in 2009. However, none of the reports attempts to explain the spike. Is it just an anomaly? Has security at ports really improved so much since 2008 that these irregular migrants dare not risk being caught on board a merchant ship while accepting the possibility of death in the Mediterranean? Has the security situation in Africa or the Middle East improved so much that there is no need for these methods of illegal migration, or do the 2008 figures represent a closer approximation to the actual numbers of stowaways? Unfortunately, we are unlikely to ever know the actual numbers involved.

Maritime security is at the heart of this issue. Instead of being political or economic migrants, these stowaways could be

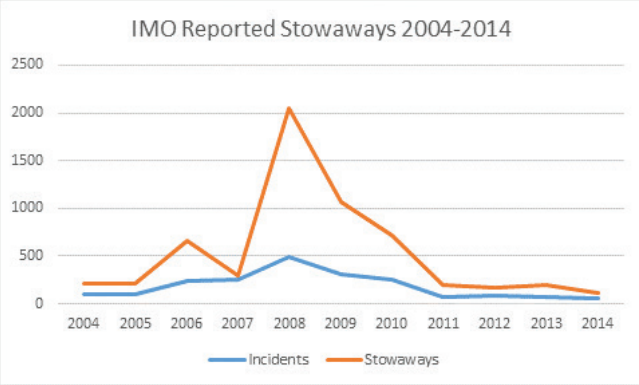

Figure 2.
Irregular migration numbers source.
Source: http://www.dryadmaritime.com.

terrorists attempting to gain access to western countries by less protected routes. The Islamic State has already made its intention to use the irregular migrant routes in the Mediterranean to enter southern Europe clear. What is to stop them from attempting to do so as stowaways? Until we have clear reporting and a better understanding of the problem, it is likely that ports, and some shipping companies, will ignore it. There should be no stigma attached to being recorded in the IMO's stowaway statistics since this represents a demonstrable success on the part of the shipping companies and ports which cought them, rather than let them slip away. The question is, 'are we seeing the full scale of the problem or is the truth, like the stowaways, hidden from our view?'

As published in the http://www.dryadmaritime.com

MARITIME CRIME FIGURES FOR Q2 2015

The following narrative accompanies Dryad's maritime crime figures for Quarter 2 (April to June) of 2015, assessing the situation across our main areas of maritime interest. The report is not limited to traditional piracy and maritime crime, but includes commentary on other threats and issues; from civil war and terrorism in Yemen and Libya to criminal gang-enabled mass migration – areas and issues upon which we report regularly to our clients. The narrative, compiled by Dryad's regional analysts, is set against a highly visible, complex and dynamic international backdrop.

Southeast Asia

There has been a 22 % increase in reported incidents across Southeast Asia in comparison with the first six months of 2014; 120 instances of piracy and maritime crime have been reported to Dryad. 12 vessels were hijacked in the first half of the year; which is a three vessel increase in comparison with the same period last year. The purpose of ten of these hijacks was cargo theft, eight of which were successful; MT Sun Birdie and MT Orkim Harmony were both recovered with their cargo intact. The boarding and subsequent robbing of vessels transiting the Singapore Strait continued apace with 48 vessels reporting incidents in the first six months of the year, which is a 118 % increase from the 2014 figures. The most significant decline in incidents was in the anchorages to the east of the Singapore Strait. While 18 vessels were boarded in the area in the first six months of 2014, only five were boarded in the same period of this year. The robbing of vessels at anchor around Southeast Asia continues, with most cases occurring in Bangladesh and Vietnam.

The arrest of two groupus of hijackers in the first six months of the year will likely result in the declining number of hijackings of small, local product tankers in the area. However, this will almost certainly be just a temporary setback for the crime syndicates which appear to be able to evade arrest and recruit new members to carry out the actual attacks. Dryad expects to see a resumption of attempted hijacks in July.

With little apparent evidence of coordinated security patrols of the Singapore Strait by the three surrounding nations, the criminal gangs who board passing vessels are operating almost with impunity, sometimes boarding three vessels a night. The vast majority of these boardings take place in the eastbound Traffic Separation Scheme (TSS) between Pulau Karimun Kecil and Pulau Besar. Until effective patrols are put in place these crimes will almost certainly continue.

Indian Ocean

There have been no incidents of piracy across the HRA in Q2. The last confirmed vessel to have been fired upon by suspected Somali pirates in the Indian Ocean HRA was in February 2014. Interestingly, there have been only six advisory notices promulgated by the UKMTO in Q2, and only one of these has been in the BaM/Southern Red Sea. This sudden reduction in suspicious incident reports coincides with the intervention of the Saudi led coalition in Yemen. The only confirmed reports of maritime crime were four cases of robbery; three from vessels at Kandla, India and one in Mombasa, Kenya. These incidents were carried out by opportunistic local criminals and have no links to Somali piracy.

The civil war in Yemen is still raging with daily airstrikes by coalition aircraft on Houthi positions. In the Gulf of Aden, the port city of Aden is one of the most violent areas, with rival factions fighting intensely over large areas of the city. Vessels attempting to dock at Aden have been fired upon with rockets and shells and the refinery at Aden was hit and reported to be burning out of control. Despite being in Houthi hands, the Red Sea ports of Hodeidah and Saleef continue to operate. All vessels heading

for these ports are required to have the appropriate permissions to arrive there; on approach, they are stopped and searched by Saudi and Egyptian warships with any non-conformity resulting in the vessels being denied entry to the ports.

During Q2, three vessels were harassed, with two being fired upon by Iranian military vessels in the Strait of Hormuz. One vessel, MV Maersk Tigris, was arrested and forced to sail to Bandar Abbas where she was anchored under Iranian control for nine days before being released. The Iranian authority's rationale for this arrest was an unpaid bill from over 10 years ago. However, in the week prior to this incident, a convoy of Iranian vessels heading towards Yemen, and suspected of delivering supplies to the Houthis, was intercepted by US naval forces and forced to turn back to Iran.

The Southwest Monsoon has now taken hold of the Somali Basin/ Arabian Sea and will continue through to mid-September. During this period, sea conditions will be outside of limits of operation of small crafts. There is very little opportunity for Somali pirates to operate in open ocean areas during the Monsoon. Conditions within the Gulf of Aden and the Southern Red Sea will, for the greatest part of this period, be within limits of pirate operations, but there are no current indicators suggesting the resumption of pirate activity.

Gulf of Guinea

In April and May, at least 20 mariners were taken from five vessels off the shores of Rivers and Akwa Ibom States in Nigeria. Kidnapping of crew for ransom still remains the most significant threat to seafarers in the region. Given the historical frequency of attacks off Bayelsa State, Nigeria, it is somewhat surprising that there has been only one attack offshore this year, with none occurring during this last quarter. Dryad believes it is only a matter of time before attacks on a range of commercial shipping resume in this area, with the prime motive of crew kidnapping for ransom.

There have been no incidents of cargo theft in West Africa since MT Mariam was hijacked off the coast of Warri on 11 January. This form of piracy in the region has reduced in frequency since two tankers were hijacked in June and July 2014 off the coasts of Ghana and Togo. That said, as the risk of attack remains a very real one, there should be no room for complacency amongst product tanker operators.

Overall, there have been 16 confirmed incidents reported in the second quarter of 2015 compared to 18 in the first quarter, and 15 in the same period last year – records of Dryad's reportable incidents in the Gulf of Guinea are generally consistent with the number of recorded incidents in previous years.

Mediterranean

The extremely unstable political and military situation in Libya continues, affecting adjacent countries as well as normal shipping and trading operations, as is the continuing humanitarian crisis of Mediterranean migration emanating from Libya and other countries.

Oil export remains of critical importance to Libya's economy and continued fighting seriously affects the country's ability to maintain its finances. It was anticipated that Q2 would see this improve, but the hopes that Ras Lanuf and As Sidr would reopen have not yet been realised and these oil export terminals remain closed to tanker traffic. UN sponsored talks in Morocco are at a critical juncture with both sides meeting for face to face talks at the end of the period. The acceptance of the negotiated plan will hopefully reduce the level of violence but, as with any similar agreement, it is only the continued acceptance by the lowest level of fighters on all sides that will prevent the re-ignition of violence.

Further attacks on merchant ships in the vicinity of the Libyan coast have occurred following the attack on MT Araevo on 4 January. MV Tuna 1 and MT Anwar Afriqya were both attacked in May, in waters off Derna and Sirte, respectively. More recently, an unconfirmed report suggests that a probable fishing vessel was attacked off Benghazi in June.

In Q2, the Islamic State has had mixed success in establishing itself in Libya. While it had some success in Sirte, it appears to have been ejected from Derna. Its reach has expanded to adjacent countries with the attacks in Tunisia on both the Bardo Museum in March and on the beach in Sousse being claimed by IS affiliated groups. Despite the indirect maritime nature (cruise ship passengers and beach hotel victims), there is insufficient evidence for Dryad to change its previous opinion that the terrorist threat to transiting merchant traffic is low.

The risk to foreigners ashore in Libya, however, remains high throughout the country, with visiting workers in danger of inadvertently being caught up in the heavy fighting ashore, as well as facing the threat of kidnap. These conditions mean that vessel crews are strongly recommended not to leave the confines of the terminals and ports they work in.

On migration, the recent UN report stating that over 137,000 migrants crossed the Mediterranean in the first 6 months of the year compared to only 75,000 in the same period last year further highlighted the scale of the humanitarian crisis. The European Unions' efforts to deal with the problem have not yet been fully approved by the United Nations. However, additional Coastguard and Naval vessels are operating in the area alongside charities, such as Migrant Offshore Aid Station (MOAS), in an attempt to

prevent the loss of life seen earlier this year. Despite these efforts, commercial vessels are still being engaged in rescue operations involving large numbers of migrants. There are also threats to navigation in the transit areas as traffickers act covertly with unlit boats at night.

Latin America and the Caribbean

Reports of robbery from sailing vessels and anchored merchant vessels have reduced from 10 in Q1 to four in Q2. Two of these were robberies from sailing vessels at anchor and two from MVs at anchor. There is a threat to sailing vessels throughout the Caribbean. Yachts anchored in exposed bays are targeted due to the perception that the owners are wealthy and carrying large amounts of cash. These attacks commonly see the use of extreme violence with knives and guns often used. Despite the continued uncertainty in Venezuela, there have been no instances of crime reported against MVs in the country's ports. Ports in Brazil, Peru and Colombia have seen robbery from vessels at anchor and alongside in the recent past. Sensible security measures should be put in place when operating in these areas.
As published in the http://www.dryadmaritime.com

RISING FROM THE ASHES

The federal government is now taking steps to reverse its 2010 decision to terminate the nation's LORAN program. The LORAN program was initiated during World War II, when US and Allied forces fighting in the Pacific Theater needed a good means of navigation in that vast ocean. The US Coast Guard was charged with establishing and operating chains of Loran-A stations throughout the Pacific. With the war's end, the program was extended to coastal areas of the United States and elsewhere. Over time, Loran-A was replaced by Loran- C, which provided both greater coverage and improved accuracy. As part of the digital revolution, the Coast Guard began exploring the possibility of developing an enhanced version of Loran in 2000, soon referred to as eLoran. In an effort to reduce the hemorrhaging federal deficit, the Administration's Budget for 2010 proposed the termination of the Loran program, using these terse words: "The Budget also supports the termination of outdated systems such as the terrestrial-based long-range radionavigation (LORAN-C) operated by the U.S. Coast Guard resulting in an offset of $36 million in 2010 and $190 million over five years." Although only the bean counters thought this was a good idea, the Department of Homeland Security and the U.S. Coast Guard bit their respective tongues and went along, as did the Congress. Thus, Loran-C was terminated as was the work on the development of eLoran.

Figure 3.
E loran.

Similar to Loran-A and Loran-C, eLoran is a low-frequency terrestrial navigation system utilizing a number of transmission stations emitting a precisely timed and shaped radio pulses. In eLoran, the pulses are centered at 100 kHz. Each station emits a sequence of eight pulses spaced 1000 microseconds apart. The stations are grouped into chains, each consisting of one master station and two or more secondary stations. The master station transmits first, followed by successive transmissions from each of the secondary stations in the chain. The master/secondary transmission sequence is repeated periodically, with the period between repetitions referred to as the Group Repetition Interval (GRI). Unlike the hyperbolic Loran-C system, modern eLoran receivers can simultaneously measure the "time of arrival" of signals from many stations in multiple chains. Using solid-state transmitters and atomic clocks, eLoran provides extremely accurate timing. The transmitters also provide a data channel carrying correction and integrity messages. Using built-in microprocessors, eLoran receivers output latitude and longitude directly, eliminating the need for Loran-line charts. The eLoran system operates in much the same way as GPS or other global navigation satellite systems (GNSS), but as a complementary and independent system. There are no failure modes in common with GNSS systems. Operating at significantly higher power than satellite-based systems, eLoran is much more difficult to jam or spoof. Since at least 2004, studies have pointed out the nation's (and indeed the world's) increasing reliance on GPS and other GNSS for positioning, navigation, and timing (PNT). Surveyors, farmers, and others rely on GPS to accomplish many of their tasks. Modern transportation networks rely on GPS for their operation and safety. Modern communication, financial, and power networks could not operate without the precise timing provided by GPS. Of the 16 commercial sectors identified as vital to the nation's economy, security, and health – referred to as critical infrastructural sectors – at least eleven rely extensively on GPS. GPS technology and GPS-supported applications are deeply embedded into the fabric of our modern lives. Computers, cellular telephones, automatic teller machines (ATMs), and electronic chart display and information systems (ECDIS) would all cease to operate properly without the PNT output available from GPS. While GPS is taken for granted, it is a relatively recent

development and is highly vulnerable. Solar flares and other high-energy electromagnetic fields (natural or man-made) can temporarily or permanently disrupt transmissions.

Terrestrial or airborne transmitters can jam or block reception of satellite signals over wide areas. Due to the lower power of the satellite signals, receivers can be spoofed or fooled into accepting and utilizing bogus signals.

The Government Accountability Office (GAO) reported that there are significant concerns about the sufficiency of efforts of the critical infrastructure sectors to mitigate the anticipated adverse effects of GPS signal loss. Other studies have shown that the only reasonably available mitigation technology to address GPS signal loss is Loran.

The federal government seems to be finally awaking from its self-induced slumber on this vital issue. On 23 March 2015, the Department of Transportation (DOT) published a notice seeking public comments regarding potential plans by the government to implement eLoran as a complementary PNT capability to GPS. On 27 March, representative John Garamendi (D-CA) presented the bipartisan National Positioning, Navigation, and Timing (PNT) Resilience and Security Act of 2015 (H.R. 1678). If enacted into law, the bill would require the Secretary of Defense, in coordination with the Commandant of the Coast Guard and the Secretary of Transportation, to provide for the establishment, sustainment, and operation of a reliable, land-based positioning, navigation, and timing system to provide a complement to and backup for GPS, to ensure the availability of uncorrupted or non-degraded PNT signals for military and civilian users if GPS signals are corrupted, degraded, unreliable or otherwise unavailable. The General Lighthouse Authorities of the United Kingdom and Ireland (GLA) have never given up on eLoran. Rather, since 2007 they have constructed transmitter sites and conducted tests at sea to determine the accuracy and robustness of the system. In partnership with other European nations, there are now nine operational transmitters providing coverage for northwest Europe. The Russians have converted their Chayka radionavigation system to broadcast a signal that is compatible with eLoran. Only time will tell if the legislative and executive branches of the federal government have the political will to move forward on this vital and long overdue initiative. The technology is readily available, but it will take determination to make these first tentative steps a reality. Scarce funds will have to be appropriated. Priorities will have to be rearranged. While the government has imposed a number of resilience requirements on the private sector, it has omitted to take an important step of its own. Measures are being taken to rectify that oversight. In mythology, the phoenix is a long-lived bird that is cyclically regenerated or reborn. A phoenix obtains new life by arising from the ashes of its predecessor. The allusion fits the situation with Loran. Loran-A gave birth to Loran-C. After its death, Loran-C may be about to give birth to eLoran.

THREATS TO GLOBAL NAVIGATION SATELLITE SYSTEMS

Originally developed to guide Allied convoys safely across the Atlantic, the use of synchronized low frequency radio signals as a navigational aid revolutionized modern maritime navigation in the 1940s. Faced with operating ships and aircraft over vast areas, researchers pioneered the use of radio signals to aid navigation in regions where poor weather conditions made traditional methods—such as dead reckoning and celestial navigation—exceptionally difficult. This system was eventually named LORAN. When in range of three or more shore-based transmitters, LORAN receivers placed onboard ships and aircraft allowed operators to fix their location within minutes regardless of the weather. The original system, known as LORAN-A, and its eventual replacement, LORAN-C, were operated by the U.S. Coast Guard and other nations until 2010. The U.S. portions of the system were phased out in favor of the satellite-based Global Positioning System (GPS) which became operational in July 1995. The latest LORAN Position Navigation and Timing (PNT) system known as "eLoran" is currently in use or under consideration in several countries. Eventually, Loran C systems throughout the world are expected to be replaced by eLoran. The impact of GPS on the commercial transportation industry has been enormous. Everything that moves—ships, cars, trains, aircraft, and even farm equipment—is now navigated by GPS, or a similar GNSS system. Companies worldwide use GPS to time- stamp business transactions, maintain records, and ensure traceability. Major financial institutions use GPS to synchronize their computer networks around the world. Large and small businesses now use automated systems which can track, update, and manage multiple transactions made by a global network of customers. These systems require accurate timing information available through GNSS Systems such as the GPS (National Coordination Office for Space-Based Positioning, Navigation, and Timing, 2014).

The commercial maritime industry has become especially reliant on GNSS technology. eCharts provide a continuous, real time plot of the true and relative movements of both the vessel and nearby objects, often using radar images and Automatic Information System (AIS) transponder signatures superimposed on the electronic chart (see Figure 1). Most merchant marine academies continue to teach their cadets skills such as how to fix a vessel's position using terrestrial and celestial bearings. However, these techniques are less frequently used in the modern shipping industry, which continues to move irreversibly towards the use of fully integrated electronic bridges.

Yet, in the event of a GNSS compromise, these basic seaman skills may be necessary to counter a cyber attack. Several other satellite-based PNT systems are also in operation. In 1995, the same year that GPS became operational, the Russian Federation announced

the deployment of the GLONASS. This system has been hampered by uneven funding and suffered a well-publicized 11-hour service outage in April 2014, among other failures. In Asia, China plans to deploy its BeiDou-2 (formerly known as COMPASS) satellite navigation system. The BeiDou-1(BDS) system currently provides only regional coverage, however China has announced plans to provide global coverage by 2020. In Europe, the European Space Agency (ESA) continues with the development of the Galileo satellite navigation system. When complete, Galileo will provide low precision PNT services to the general public, while high precision services will be available for a fee to commercial and military subscribers.

Figure 4.
Sample eChart. (Ship Technology Global, 2014).

GNSS Signals produced by PNT satellite systems range between 1162 and 1610 MHz (see Figure 2). U.S. GPS emits two types of signals: one which is broadcast on a single frequency and available free to all users; and second which is broadcast on a separate encrypted frequency available only to the military. These two signals, are equally accurate. However the availability of the second signal on a different frequency allows the military to compensate for naturally occurring interference within the ionosphere, resulting in a more accurate fix and greater system resiliency. It is important to note that GNSS pulses are extremely weak. GPS signals have been compared to the light emitted by a "40 Watt light bulb as seen from 11,000 miles away (17,700 km)" (Daniels, 2014). As such GNSS signals are vulnerable to: (1) jamming and interference - the broadcast of a stronger signal that intentionally or unintentionally blocks or impacts a GNSS satellite signal; (2) spoofing - the broadcast of a false GNSS signal, but of a slightly greater power which deceives the GNSS receiver into locking onto the spoofed signal. A spoofing attack can be

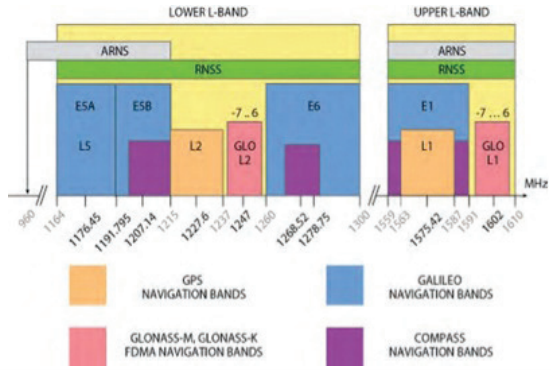

Figure 5.
GNSS frequencies, including Radio Navigation Satellite Service (RNSS); and Aeronautical Navigation Satellite Service (ARNS) frequencies. (MicrowaveJournal.com May 2012).

very difficult to detect.

(3) meaconing - the intentional delay and re-broadcast of a GNSS signal intended to introduce error into receivers;

(4) Extreme Space Weather (ESW) - solar activity such as solar flares, coronal mass ejections, high-speed solar wind, and the impact of energy particles on the earth's ionosphere.

(5) other vulnerabilities - kinetic or laser attacks on satellite constellations or collisions with space debris are only a couple of the other known susceptibilities of the GNSS. Shipboard Systems Affected by the Loss of GNSS Signals – a significant portion of navigation equipment on the bridge of a modern ocean- going commercial vessel (see Figure 3) and various offshore energy platforms will likely be affected by the loss of GNSS signals. For the components listed above, the loss of GNSS may not prevent the component from functioning through an alternate sensor input. However, tests conducted by the General Lighthouse Authorities (GLA) of the United Kingdom and Ireland in 2008 showed how easily error messages and auditory warnings prompted by the loss of the GPS can distract (and overwhelm) a vessel's bridge team (Grant, Williams, Ward, & Basker, 2008). This can be especially dangerous for vessels operating in confined waterways, near shallow areas, or maneuvering in higher traffic densities.

These vulnerabilities are not unique to the maritime industry. A number of other industries are also at risk. For instance, the aviation and financial industries are heavily dependent on properly functioning PNT systems and would be affected in varying degrees by a cyberattack on the GNSS. Largely unique to the maritime industry however, is that much of marine environment information transfer is via radio frequency (RF) and not a dedicated hard-line network or directional microwave dish. A good example of this type of transfer are positioning

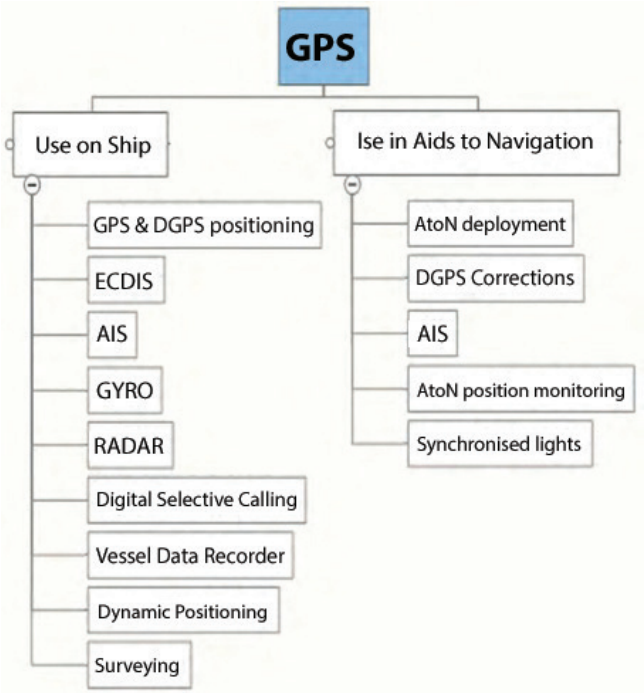

Figure 5.
Maritime navigation equipment that use GPS as a data input. (Grant, Williams, Ward, & Basker, 2008).

Figure 6.
Small jammers that can be purchased via the Internet.
Source: U.S. Government

signals emitted by satellite systems. Data being sent to and from shipboard computers along with other shipboard technology are cyber; therefore interference with the data flow constitutes a cyber threat. Ergo, a Maritime Cyber Security (MCS) issue.

Figure 7.
Coverage area of the GPS jamming unit at 25m above ground level on maximum power of 1.58W ERP. (Grant, Williams, Ward, & Basker, 2008 - Image courtesy of DSTL).

GNSS Jamming Equipment

With some exceptions, the use of GNSS jammers is generally illegal in the U.S., Canada and Europe. Despite this, jammers of various sizes and power ratings (see Figure 5) are available via the internet. These small handheld jammers are extremely difficult to locate and suppress for law enforcement officials because they can be used intermittently, disguised or hidden easily, are highly mobile, and if necessary disposed of quickly by perpetrators. Advanced GPS receivers are more resistant to jamming than conventional designs. For example, receivers equipped with nulling antennas are more resistant to jamming than receivers without them (Jones, 2011). Figure 5 shows the area affected by a GPS jammer during tests conducted at Bridlington, U.K. along the coast of the North Sea in 2008. During the test, a jamming unit was positioned 25m above ground, with the maximum power of 1.58 watts. These tests demonstrated that relatively small jamming units can effect GNSS reception over great distances (Grant, Williams, Ward, & Basker, 2008).

Threat Scenarios

At this time, the three most likely GPS maritime cyber threat scenarios to consider are:

• Jamming of a port or other congested waterway by an individual or a small group of non-state actors using small, portable jammers.

Rapid movement of these individuals, coupled with intermittent use of the jammer(s) would make it very difficult for local law enforcement officials to track and arrest the perpetrators quickly. Attacks of this type can result in significant economic losses, as well as loss of confidence by system users.

• State-sponsored GNSS Jamming.

The best documented examples of state-sponsored jamming attacks occurred in the Republic of Korea (see Table 1). On three different occasions, the Republic of Korea was subjected to intentional, high-power jamming by North Korea over a wide area. The source of these attacks appear to have been large truck-mounted jamming units placed at strategic geographical locations (Figure 6). Amongst many attacks, the 2012 attack affected over 1000 aircraft and 250 ships (Seo & Kim, 2013).

• State-sponsored Spoofing.

Eventually, spoofing may pose a significant maritime threat to GNSS as it has the potential to lead vessels astray into dangerous waters, resulting in significant loss of life (cruise liners and ferries) or environmental damage. Presently, spoofing requires a level of technical sophistication that is normally presented through nation states. However, small groups have conducted successful spoofing tests, most notably students of the University of Texas under Professor Todd Humphreys.

Primary Defenses Against Jamming

• Improved Maritime Training and Education.

Ship crews should be taught how GNSS systems interact with shipsystems and how to recognize when GNSS signals may have been compromised. The maritime industry should also be encouraged to maintain basic seamanship skills, such as dead reckoning and the ability to use piloting instruments. Routine ship drills should include signal loss and spoofing of the signal.

• Improved Equipment. The development of new GPS receivers capable of identifying non-GPS signals by their relative location (jamming and spoofing signals come from terrestrial locations not satellites) and strength (jamming and spoofing signals must by necessity be stronger than GPS satellite-generated signals). In addition to receiver signal strength alarms and specialized antennas, the effects of intentional jamming could be mitigated through the use of inertial navigation systems (INS) and Inmarsat offers radio frequency (RF) jamming detectors. However, at the moment, it is unclear when such equipment will be available to and employed by the commercial industry, or how much it will cost.

• Installation of Powerful Alternate Ground Based PNT Systems. Coastal nations most at risk should consider the installation of alternate (back-up) or complementary, land-based PNT systems, such as enhanced LORAN (known as eLoran).

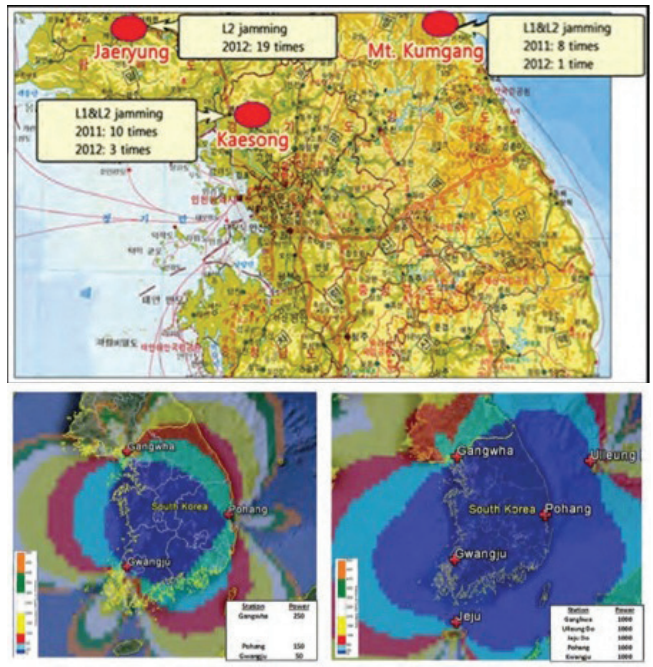

Figure 8.
Location of North Korean Jammers.

Rather than purely "back-up", it is "complimentary" in that the low frequency of the powerful eLoran signals permits PNT reception in GNSS denied environments. However, the main benefit of such systems is to provide PNT users with a second and more resilient PNT signal – one that is too powerful to be effectively jammed or spoofed.

Recommendations

Worldwide dependence on Global Navigation Satellite Systems (GNSS) continues to grow. Ongoing advancements in jamming technology and the availability of small, portable jammers constitute a significant threat to maritime commerce and safety. In the face of a GNSS jamming attack, most commercial ports could be forced to suspend operations until the source of the interference is located and suppressed. It is very possible that a group of individuals operating small, portable jammers could force the closure of a major seaport or international maritime chokepoint. The economic consequences of such an attack could amount to billions of dollars. In the long-term we also anticipate that more powerful jamming technology and delivery systems (such as broadband jammers and drones) will become

widely available and constitute two of the greatest threats to GNSS. The maritime community needs to become more vigilant, actively train to recognize and respond to cyber attacks including jamming and spoofing, and encourage the immediate installation of complementary PNT systems such as eLoran in strategic maritime locations.

Table 1.
Intentional High-Power Jamming of Korea.
Source: Maritime Reporter & Engineering News, May 2015.

Intentional High-Power Jamming of Korea			
dates	August 23-26, 2010	March 4-14, 2011	August 28-May 13, 2012
Jammer Locations	Kaesong	Kaesong and Mt. Kumgang	Kaesong
Affected Areas	Gimpo, Paju, Gangwon	Gimpo, Paju, Gangwon	Gimpo, Paju, Gangwon
GPS Disruptions	181 cell towers 15 aircraft, 1 military vessel	145 cell towers, 106 aircraft, 10 vessels	1.016 aircraft, 251 vessels

As published in the May 2015 edition of Maritime Reporter & Engineering News - http://magazines.marinelink.com/Magazines/MaritimeReporter

CATERPILLAR CONTINUES TO BE SUCCESSFUL IN DUAL FUEL ENGINE RETROFITS, SUPPLIES COMPLETE GAS SYSTEM FOR FUER WEST TANKER

Hamburg, Germany – Building on the success of recent MaK diesel engine dual fuel retrofit conversions, Caterpillar Marine is currently underway on another dual fuel engine retrofit conversion onboard the 472 foot Fure West tanker, owned by Furetank Rederi A/B. The MaK™ M 43 C diesel engine onboard the tanker will be retrofitted in hull, in the 7 cylinder M 46 dual fuel platform, with each cylinder offering 900 kW of rated power. Additionally, Caterpillar is also supplying the complete gas system for the tanker, including bunker stations, 2x LNG tanks measuring 4.15 meters by 24 meters and the vaporizer.

This project, backed by the European Union and developed with the Zero Vision Tool, will mark the second MaK engine dual fuel retrofit. In 2014, Caterpillar successfully completed the dual fuel engine retrofit conversion on the Anthony Veder Coral Anthelia LNG carrier. "We're pleased to continue to build upon our successful track record of dual fual conversions in the commercial marine industry and offer an increased scope of supply to our customers," Finn Vogler, Caterpillar Marine senior engineer noted. "We have a market-ready technology available that our commercial marine customers can be completely confident in and after our success onboard the Coral Anthelia, we have seen the demand for MaK dual fuel solutions increase substantially."

With a bore of 460 millimeters and stroke of 610 millimeter, the M 46 dual fuel engine was designed for electric drive propulsion systems as well as mechanical propulsion systems. Although designed for unlimited operation on LNG, marine diesel oil and heavy fuel oil, the M 46 DF will reach industry-leading efficiency in gas mode. The M 46 DF was strategically engineered to allow for the retrofitting of current M 43 C engines. Additionally, existing M 32 E engines can be retrofitted into the MaK M 34 DF dual fuel platform. As a result of the synergies between the two platforms, Caterpillar can perform in hull retrofit conversions without having to move the engine block or perform extensive machining. Cat dealer Pon Power had a significant role in the Fure West conversion. "We're able to differentiate our solutions in the market by offering a collaborative partnership with our dealers to ensure the retrofit conversions are completed in an expedited manner and with a reduced number of parties involved as a result of our ability to provide the complete gas system for a vessel as well," Vogler noted.

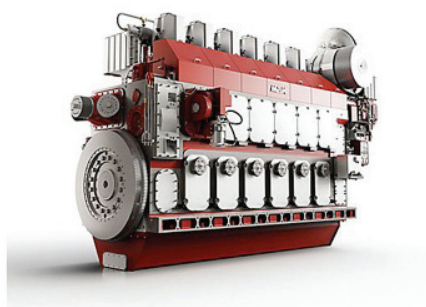

Figure 9.
Caterpillar.

About Caterpillar Marine

Caterpillar Marine, with headquarters in Hamburg, Germany, brings together all the marketing and service activities for Cat and MaK™ marine diesel, dual fuel and gas power and propulsion systems within Caterpillar Inc. The organisation provides premier power solutions in the medium- and high-speed segments with outputs from 93 to 16,800 kW in the main propulsion and 10 to 16,100 kWe in marine generator sets, as well as a comprehensive portfolio of propulsion solutions. The sales and service network includes more than 2,100 dealer locations worldwide dedicated to providing support to customers in ocean-going, commercial marine and pleasure craft wherever they are.

About Caterpillar

For nearly 90 years, Caterpillar Inc. has been making sustainable progress possible and driving positive change on every continent. Customers turn to Caterpillar to help them develop infrastructure, energy and natural resource assets. With 2014 sales and revenues of $55.184 billion, Caterpillar is the world's leading manufacturer of construction and mining equipment, diesel and natural gas engines, industrial gas turbines and diesel-electric locomotives. The company principally operates through its three product segments - Resource Industries, Construction Industries and Energy & Transportation - and also provides financing and related services through its Financial Products segment. For more information, visit caterpillar.com. To connect with us on social media, visit caterpillar.com/social-media.

Power Range	5400-8100 kW
Engine Specifications	
Speed Range	500-514 rpm
Emissions	IMO II
Aspiration	Turbocharged
Bore	460.0 mm
Stroke	610.0 mm
Rotation (from flywheel end)	Counterclockwise / Option for Clockwise
Configuration	Inline 6,7,8,9
Dimensions & Weights	
Minimum Dry Weight	94000.0 kg
Minimum Length	8271.0 mm
Maximum Length	10528.0 mm
Minimum Height	5130.0 mm
Maximum Height	5501.0 mm
Minimum Width	2878.0 mm
Maximum Width	2878.0 mm
Benefits & Features	
Related Products	

DNV GL'S UNMANNED FLNG CONCEPT BOOSTS SAFETY AND REDUCES COSTS

DNV GL has developed a new unmanned floating LNG concept that overcomes many of the challenges currently faced by those looking to unlock the potential of remote offshore gas fields.

Called Solitude, the concept demonstrates how technological advances – most of the technology already within reach — can be combined into a solution offering a 20 percent reduction in annual OPEX, adding only a few percent increase in CAPEX and at the same time increasing the overall safety.

FLNG technology is developing rapidly as part of the industry's quest for resources in more remote waters. A number of concepts have been discussed, but only a few are currently under construction, as many oil and gas companies have experienced double-digit growth in both capital and operational expenditure over the last decade.

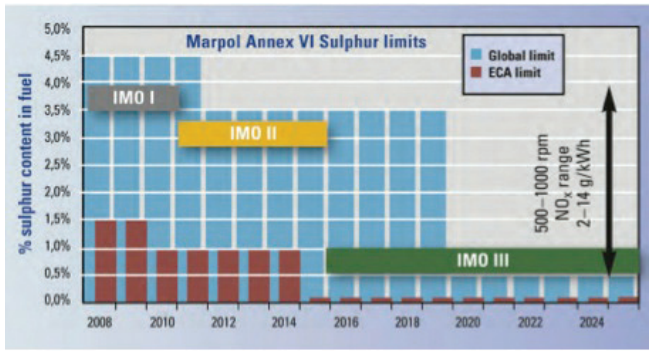

Figure 10.
Upcoming IMO III emission regulations,selected operation profi les and diesel fuel costs make the M 46 DF a preferred engine regarding lowest cost of operation..
Source: www.wartsila.com.

Foreseeing the need for more remote projects to be able to overcome even more challenging cost barriers, whilst still meeting increasingly stringent safety and environmental standards, DNV GL embarked on an Extraordinary Innovation Project to explore the future of LNG technology.

"Solitude has been developed with maintainability foremost in mind," says Elisabeth Tørstad, DNV GL CEO Oil & Gas. "By changing the focus from maximum efficiency to maximum reliability, and selecting robust processing options with built-in redundancy, we were able to develop a solution that ensures production levels and boosts the economic viability of FLNG projects."

Solitude makes use of advanced but widely available technology to provide its power. Power that would otherwise be generated by high-maintenance gas turbines can, for example be generated by fuel cells. This improves power generation reliability and reduces the unit's environmental footprint.

Equipment throughout the FLNG is modularised and monitored from shore with much of the routine maintenance and fault elimination being carried out by self-programming autonomous inspection and maintenance units (robots). The topside has a system of rails that run along each process train, providing these robots with access to all equipment.

Wireless sensor networks act as eyes, ears and noses, feeding information to a condition monitoring system that overseas fault detection, proactive maintenance and repair planning.

As there will be no one living on board or working on the topside during normal operation, the associated personal safety risks are eliminated. When people enter for extensive maintenance works,

the topside would be prepared as a safe working environment. A new support and accommodation vessel concept and its associated docking system on FLNG further boost the safety of interventions.

"Existing frontier oil and gas projects have resulted in tremendous technological developments, particularly in the subsea realm, and Solitude draws on this," says Tørstad. "Operators are already controlling subsea installations and simple, fixed offshore installations from shore. Given the on-going advances in autonomous systems and remote operations, unmanned offshore installations are a natural development over the next few decades."

"While Solitude is a holistic concept, many of its solutions can be implemented independently – and some are already available today. These projects are our way of thinking out loud. Our aim is to present high-level concepts that can form a basis for discussion and be further developed in collaboration with the industry. We see Solitude as a new opportunity for the future," ends Elisabeth Tørstad.

DNV GL's Extraordinary Innovation Projects are part of the organization's commitment to provide foresight into the future. Five percent of the company's revenue is invested in research and development.

About extraordinary innovation

Innovation starts with understanding the current situation, being open-minded, learning from others and playing with ideas. In DNV GL's Extraordinary Innovation Projects, we use this approach to take a fresh look at the industries we work with and the challenges they face. Our aim is to inspire our stakeholders to think differently and support the development of safer, smarter and greener solutions to their problems.

About DNV GL

Driven by its purpose of safeguarding life, property and the environment, DNV GL enables organisations to impove the safety and sustainability of their business. We provide classification and technical assurance services, along with software and independent expert advisory services to the maritime, oil & gas and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers make the world safer, smarter and greener.

As published at https://www.dnvgl.com/news/dnv-gl-s-unmanned-flng-concept-boosts-safety-and-reduces-costs-24193

IS MARITIME SIMULATION THE SOLUTION TO MARITIME CYBER SECURITY THREATS

The U.S. Executive Branch has declared the cyber threat one of the most serious economic and national security challenges we face as a nation, and that America's economic prosperity in the 21st century will depend on effective cyber security. Before the maritime industry sounds the danger signal, it needs to monitor other industries and branches of the government and take proactive preventative measures. There is no better place to prepare future and current mariners for these challenges than maritime simulators.

Cyber Security

Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks via the Internet by cyber criminals. The advent of computers, network devices and telecommunications capable of transporting data via radio frequency, opened up a whole new world of vulnerabilities to hackers wishing to tap, steal, destroy or alter data. It ushered in a new era of potential maritime threats that go well beyond physical piracy such as the Maersk Alabama. With the recent GPS spoofing of a yacht by students of the University of Texas, the maritime sector has entered into a new arena which must be addressed as Maritime Cyber Security. In early 2013, the U.S. Executive Branch, as a world leader and major target for terrorism, signed an Executive Order (EO) 13636 to Improve Critical Infrastructure (CI) Cyber Security and Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21). It established an All Hazards approach to critical infrastructure security and resilience. The cyber security EO establishes a requirement for federal agencies to collaborate with their respective industry sectors to identify Critical Infrastructure that can be impacted by cyber activity.

This initial foray by the federal government has led other departments and agencies to take initial steps to address the growing issue of cyber threats. The U.S. Department of Transportation, Maritime Administration (MARAD), being one of those proactive organizations, has recently teamed up with the Ship Operations Cooperative Program (SOCP) to cooperatively develop Information Systems Security Awareness Computer- Based Training (CBT) on cyber threats in the maritime environment. This is a first for the U.S. maritime community to recognize and take action to assist vessel owners and operators with training U.S. mariners on best practices to reduce the risks and vulnerability associated with information systems

and devices. The newly developed cyber training will give mariners a comprehensive overview of the range of threats that information systems and devices are subject to, and the practices recommended to minimize those vulnerabilities. Best practices addressed in the training include a wide range of topics, from maintaining network security, to the use of workplace computers for private purposes, good password practices, and issues concerning the use of social media like Facebook and Twitter. The training also addresses issues faced by mariners working aboard vessels, such as specifi c log-in policies and rules surrounding working with sensitive information. The Department of Homeland Security (DHS), through the United States Coast Guard (USCG), has also taken to task these growing threats and established that American ports, terminals, refineries, vessels and supporting industries are vital for the safekeeping of the nation's infrastructure, security and economy. In short, there are as many potential avenues for cyber damage in the maritime sector as there are cyber systems. While only some cyber-attack scenarios in the maritime sector could credibly lead to a transportation security incident, we must identify and prioritize security and survival at sea.

Security and Survival at Sea

Will the next hacker chess match take place on the high seas, involving oil tankers, container ships and other specialized vessels transporting approximately 90 percent of the goods moved around the world? Many devices are connected online which makes them more vulnerable to attack. As the maritime and offshore energy industries connect ships and oil rigs to computer networks, they expose considerable weaknesses that hackers can exploit. For example, it was discovered that pirates off the coast of Somalia and other key piracy areas hand pick their targets by tracking vessels by AIS, ECDIS and radar. In the oil industry, hackers have caused much turmoil, including the tilting of an oil rig, causing it to be shut down, as well as accessing networked computing systems on another rig and entering malware that took trained personnel almost three weeks to clear. Other events have included smugglers hacking into networked systems to locate containers with drug contraband and cleanly confiscate the drugs without being detected. They even went so far as attempting to delete shipment data. While data on the extent of the maritime industry's exposure to cyber-crime is hard to come by, a study of a related energy sector conducted by insurance companies recently indicated that much of it may be insurable. As the energy and oil industry has been targeted for some time, statistics indicate that the attacks already have a billion dollar impact on the world economy. In the maritime ndustry, the number of known incidents appears to be low due to either the companies being unaware of the cyber-attacks or because of the desire to keep such news from reaching the press with potential detrimental business impact on the company. There are several documented reports about hackers compromising maritime cyber security. But scientists indicate they have identified security issues in three key navigation systems used by mariners: GPS, Automatic Identification System (AIS), and the system for viewing digital nautical charts Electronic Chart Display and Information System (ECDIS). The maritime domain and the energy sector have been increasingly turning to technology to improve production, while reducing costs and shortening delivery schedules. These technologies have now become a liability because the equipment became accessible to outsiders. As vessels continue to increase in size and the crews diminish in numbers, with the paramount shift in vessel operations, ship owners and yards have been adding increasing quanitties of automated and remote monitoring systems to vessels. This has led to a dilemma, since systems and devices on vessels can raise productivity and improve safety on the one hand, while simultaneously giving hackers more systems to compromise and control. It is fairly well known that a significant portion of computing and network devices are connected to the internet using serial ports with poor security. Devices range from simple traffic apparatuses such as stoplights, which have been proven to have been controlled remotely by hackers, to complex items for the oil and gas industry which monitor and control oil rigs. It has been reported that some ships switch off their AIS systems when passing through waters where pirates are known to operate, or fake the data to make it seem they're somewhere else. Some shipping companies are now taking cyber risks as true and credible threats and taking necessary measures to beef up network and telecommunications security. Recent studies of U.S. ports have established that only a handful conducted cyber assessments and even fewer developed a response plan. Very little federal money has been allocated to the maritime industry for cyber security projects or training. This lack of cyber security preparation by U.S. ports actually carries over to the shipping companies most of which have been discovered to have substantial security issues. However, on the bright side, maritime computing and network systems have only been compromised to a limited extent. This may have something to do with the fact that they have not been a high priority and have slipped under the hackers' radar screens unnoticed. What should concern many in the maritime industry is that the main ship navigation systems including GPS, AIS and ECDIS receive data via radio frequency transmission at sea and as such are extremely vulnerable to hacking. The recent IMO 2010 Manila Amendments made AIS and ECDIS mandatory on larger commercial and passenger vessels. This new requirement has increased the need of shipping companies for security measures and protocols capable of

protecting these devices from intrusion by outside sources. It has also been known for some time that ECDIS systems and the required software update downloads can be compromised by hackers with severe repercussions. This came to light last year with the grounding of a U.S. naval vessel in the Pacific Ocean where it was reported that the ECDIS charts were incorrect and may have had an impact on the accident. A related discovery has been the widespread abuse of AIS by the maritime sector. Many ships deliberately transmit incorrect AIS position data for security reasons in certain parts of the world, including off the coast of Somalia; in the Caribbean, smugglers do it to avoid tracking and arrest by law enforcement and fishermen for financial gain by fishing in forbidden areas. The need for the maritime community to understand the principles of information systems and cyber security and how they apply to on-board equipment before they can implement changes and conduct training so the personnel are aware and can act accordingly, is of paramount importance. Several areas the maritime industry will need to come abreast with are the following:

GPS SPOOFING

There are many recent stories portending to GPS spoofing, including the June 2013 project at the University of Texas where they employed GPS spoofing as they hacked and manipulated the software to disorient the navigation system on a luxury yacht. Upon cloaking the device and transmitting the false signal, the yacht changed course abruptly when it received the false signal. Although this occurred because a system linked to the ECDIS handled the steering instead of a helmsman, it still happened. This opened up a new issue of the manner of establishment of the accuracy and correctness of GPS signals.

eLORAN

GPS has vulnerabilities that pose potential risks. In 2008, in response to presidential direction, the U.S. government announced that they would establish a nationwide resilient terrestrial-based system to augment GPS, going by the name of eLoran. This new system would build upon and modernize the old Loran-C system, while being less expensive to operate and much more accurate. The U.S. is not alone in recognizing GPS vulnerabilities; numerous other countries including most of Europe, India, Russia and China have installed or will install eLoran systems. Unfortunately, the US Department of Homeland Security planned to dismantle the remains of the old LORAN-C infrastructure even though it can be feasibly used for the new eLoran. The good news is that there are currently plans in place to resurrect and enhance the old system and turn it into a state of the art electronic terrestrial-based system which will complement and backup GPS. It was recently reported that prominent aids to navigation on the approach to and within San Francisco harbor have now been added into the electronic aid to navigation (eATON) system. San Francisco has become the Beta port in the U.S. as it is the first to begin using this unique system. The process is not expensive to implement, as it does not require the U.S. Coast Guard to install electronic transmitters on the aids to navigation. Due to the fact that the aids to navigation are located at fixed positions in the ocean or on land or fixtures such as the Golden Gate Bridge, they have their own electronic identification assigned to them which is added into the Automatic Identification System (AIS). The center span of the Golden Gate Bridge is marked by RACON, and bridge towers by eATON digital markers. In the San Francisco area, the system is also being used in conjunction with reporting points in the Traffic Separation Scheme (TSS), including the San Francisco "SF" buoy that serves as the embarkation point for the Bar Pilots. It has been reported by the USCG that ATONs will not replace the actual physical navigation aids but supplement the existing technology, as well as add a virtual layer of aids to navigation in areas in which that was previously physically impossible or impractical. This now allows the USCG to place an eATON in the TSS at places which were previously too deep, as well as mark a bridge tower that was practically needed the most during reduced visibility. This technology will eventually allow the USCG to install transmitters on buoys to allow prudent mariners to track the actual position of the buoys as opposed to where they should be if nautical charts were consulted. In a conflicting statement, it was also recently reported that certain aids to navigation will be removed off the coast of California. This decision was based on the presumption that all vessels are equipped with Electronic Chart Display and Identification System (ECDIS) in accordance with the IMO 2010 Manila Amendments which required the system to be installed on most vessels (tied to class and size) over a six-year period starting as of 2012. This could have disastrous consequences because a significant part of the maritime industry, including towing, fishing and recreational are not required to have ECDIS. Additionally, even for blue water international commercial fleets, reliance on ECDIS and GPS alone can be dangerous, especially in light of the recent GPS spoofing phenomenon. Prudence and situational awareness demand that professional mariners rely on visual aids. Otherwise, just try to imagine what would happen in case of an electronics failure and loss of ECDIS or both of them on a commercial vessel?

ECDIS

ECDIS is believed to have some underlying software security vulnerabilities that could have disastrous consequences for ships at sea. The basis of ECDIS is a navigation based charting system

which uses a computing system to digitally display nautical charts along with the exact location and tracking of the ship. This is a dramatic alternative and improvement to paper maps and the current system of hand plotting positions. ECDIS's are installed on the bridge of a vessel and larger vessels are required to have two of them, one as backup. When properly used with an ENC chart, they can replace paper nautical maps, which is an increasing trend in the maritime industry. The problems do not arise when the ECDIS is in standalone mode, but when several ECDIS's are networked together and when data is downloaded via an external source, whether through a USB port via a memory stick or via the net. Based on the recently released IMO 2010 Manila Amendments, regulations were implemented which now require the EDCIS to be installed on all commercial vessels of a certain size. This will slowly eliminate reliance on paper maps and take the maritime industry on a journey into the electronic world where the next evolution will be the use of portable smart devices by navigators. Safeguards need to be put in place for ECDIS data updates, as well as for external security breaches when used in a networked setting.

AIS

When AIS is operated as intended, it is a useful navigational aid that can be instrumental in collision avoidance. As previously published, due to the configuration of the system, much of the transmitted data can be manipulated or distorted. This was recently confirmed by several sources including the Israelis. They noticed that vessels transmitting AIS spurious signals were nowhere near their actual location and on other occasions they also had phantom ships appear that could not be found. This system, along with the GPS and the recent spoofing episode, needs to be enhanced to include some type of signal authentication process so that erroneous signals will not be displayed.

Smart Ships

Smart ships are on the horizon and are anticipated to make an appearance sometime between 2020 and 2030, going about their normal business at sea without a crew and totally monitored from shore. Shipyards are already constructing fully sensored vessels which can be monitored after delivery and at sea for maintenance and servicing purposes. These vessels can take two forms and be either autonomous or unmanned. Autonomous is defined as a vessel primarily guided by automated on-board decision systems but controlled by a remote operator in a shore-based control facility. Unmanned is one step beyond autonomous and is fully controlled from a shore-based control station. Key features would be the standard maritime policy of having redundant systems and emergency backups on board. Where does this new technology take us in the maritime simulation world? Possibly as is done with USAF, we will have ship drone training and certification. This could tie into the scenario with a fully integrated navigation suite of GPS, eLORAN, EATON and a digital visual sensor system capable of being fully controlled and monitored 24/7/365.

Marine Simulation

Maritime simulation is important as it imitates the operation of a real life vessel in a safe environment. The simulation of cyber threats and scenarios will allow us to focus on the new cases of spoofing and jamming through the mariner's heavy reliance on Radio Frequency (RF) transmissions that can potentially be comprised. Simulation can be used to show the possible real effects of alternative conditions and courses of action on the vessel. Simulation is of utmost importance especially when we need to interact in congested waterways, narrow channels, dense traffic and with many other restrictions including dangerous cargoes. What simulation will allow us to do is introduce many of these potential cyber threats from real life environment and let the mariner exercise and respond in real time. In developing the next wave of maritime education, going beyond Vessel Security Officer (VSO) is a logical step, as is the creation of a new position of a Vessel Cyber Security Officer (VCSO) in a Maritime Cyber Security (MCS) program. This position could be an extension of the VSO or a new certification. In either case, having crew members with these skill sets who can act as responsible officer(s) on each ship is essential. They would be responsible for all levels and details of cyber security and defense. In the recently released STCW 2010 Amendments, the IMO has already proactively moved forward by introducing an Electro Technical Officer (ETO) and an Electro Technical Rating (ETR). How does the industry move forward and get to that logical level of training and preparedness? It first needs to review existing maritime simulations to determine the equipment and systems we are using. The next step is determining the manner of their integration, as well as the built-in securities. From this we can embark on a journey of determining how cyber threats could attack, destroy or disable the equipment … or in the worst-case scenario … take command of it. In the end, it is through the awareness training and education that mariners will be able to thwart these infiltrations. Another source of mariner awareness and training must be the use of the Internet and the download of data potentially corrupted by viruses, worms, phishing, spoofing and hacking. Regardless of whether corruption is due to improper training or lack thereof or circumstances or oversight due to fatigue, it must be avoided. A similar path applies to the use of vessel email and the threat of receiving spear phishing emails purported from reliable

sources with clickable links to websites that are fraudulent and will take control of your computer back door or install a virus. To summarize, as we move forward, we need to incorporate into the syllabi of all maritime simulation courses the basics of Maritime Cyber Security (MCS) as it is an ever present threat that will not go away. It is only by diligence and proper training and awareness that seagoing mariners will be prepared and ready to take appropriate action when warranted.

The Author

Emil Muccin currently holds the position of Assistant Department Head, Maritime Business Division of Marine Transportation Department and is also an Associate Professor of Nautical Science at the United States Merchant Marine Academy. He was previously a Marine Transportation Department STCW Coordinator. He is also the Faculty Advisor to the Cyber Defense and Propeller Clubs. Emil graduated from the USMMA with a BS in Nautical Science and from Pace University with an MBA in Information Systems. He sailed for many years as the Master of paddle wheelers on the Hudson River.

As published in the June 2015 edition of Maritime Reporter & Engineering News

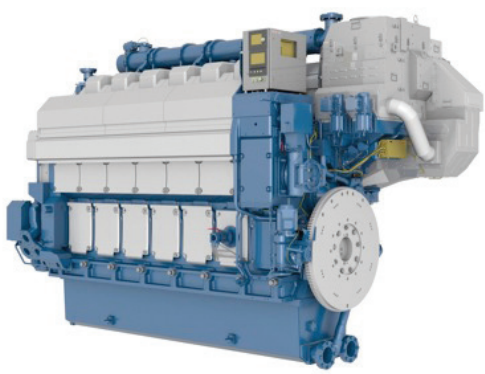

Figure 11.
6-cylinder in-line Wärtsilä 34DF engine.
Source: www.wartsila.com.

WÄRTSILÄ 34DF DUAL-FUEL AUXILIARY ENGINE BECOMING THE GLOBAL STANDARD FOR LNG CARRIER APPLICATIONS

Wärtsilä Corporation Press release
27 August 2015 at 10:00 AM E. Europe Standard Time

The upgraded version of the Wärtsilä 34DF engine is rapidly becoming established as an industry standard. The three major South Korean shipyards are supporting the use of this engine for auxiliary applications in the LNG Carrier segment where dual-fuel engines are favoured. South Korea currently has more than 80 % of the total order book for LNG tankers, while the Wärtsilä 34DF engine has achieved an auxiliary application market share of approximately 70 % in this sector.
In the first half of this year Wärtsilä was awarded contracts for 56 Wärtsilä 34DF dual-fuel auxiliary engines for 14 new LNG Carriers being built for four different owners. This means that Wärtsilä has already received orders for nearly 100 such engines from these three yards since its re-launching with a higher MCR (maximum continuous rating) in 2013. All these orders were placed by South Korea's three leading shipyards and the ships are being built for European, American and Asian owners.
"The Wärtsilä 34DF dual-fuel engine is a powerful, versatile, and efficient engine that is helping shipping move into the gas age. The impressive track record of 100 engines sold in a two year period speaks for itself. While the success has been universal, with contracts from yards and owners globally, the fact that the world's largest shipbuilding nation, South Korea, is increasingly opting for the Wärtsilä 34DF is especially gratifying," says Lars Anderson, Vice President, Engine Sales, Wärtsilä Marine Solutions.

The Wärtsilä 34DF engine

The Wärtsilä 34DF was originally introduced in 2008 and was based on the successful Wärtsilä 32 engine platform. In 2013 it was upgraded to provide 11 percent more power and increased efficiency without changing the physical dimensions. The upgraded version has a power output range from 3,000 to 10,000 kW at 500 kW per cylinder.

Wärtsilä in brief

Wärtsilä is a global leader in complete lifecycle power solutions for the marine and energy markets. By emphasising technological innovation and total efficiency, Wärtsilä maximizes the environmental and economic performance of the vessels and power plants of its customers. In 2014, Wärtsilä's net sales totalled EUR 4.8 billion with approximately 17,700 employees. The company has operations in more than 200 locations in nearly 70 countries around the world. Wärtsilä is listed on Nasdaq Helsinki, Finland.

As published at www.wartsila.com

Figure 12.
Mr. Ki-tack Lim (Republic of Korea).
Source: www.imo.org

Mr. Ki-tack Lim (Republic of Korea) elected as IMO Secretary General

Mr. Ki-tack Lim (Republic of Korea) was elected the Secretary General of the International Maritime Organization (IMO), with effect from 1 January 2016, for an initial term of four years.

The vote took place during the 114th session of the 40-member strong IMO Council, held 29 June-3 July 2015. The decision of the Council will be submitted to the IMO Assembly, which is scheduled to hold its 29th session 23 November-2 December 2015, for approval.

Mr. Lim is currently the President of Busan Port Authority. He served as the Republic of Korea's Deputy Permanent Representative to IMO from 2006 to 2009 and was Chairman of the Sub-Committee on Flag State Implementation (FSI) from 2002 to 2004.

As published at www.imo.org