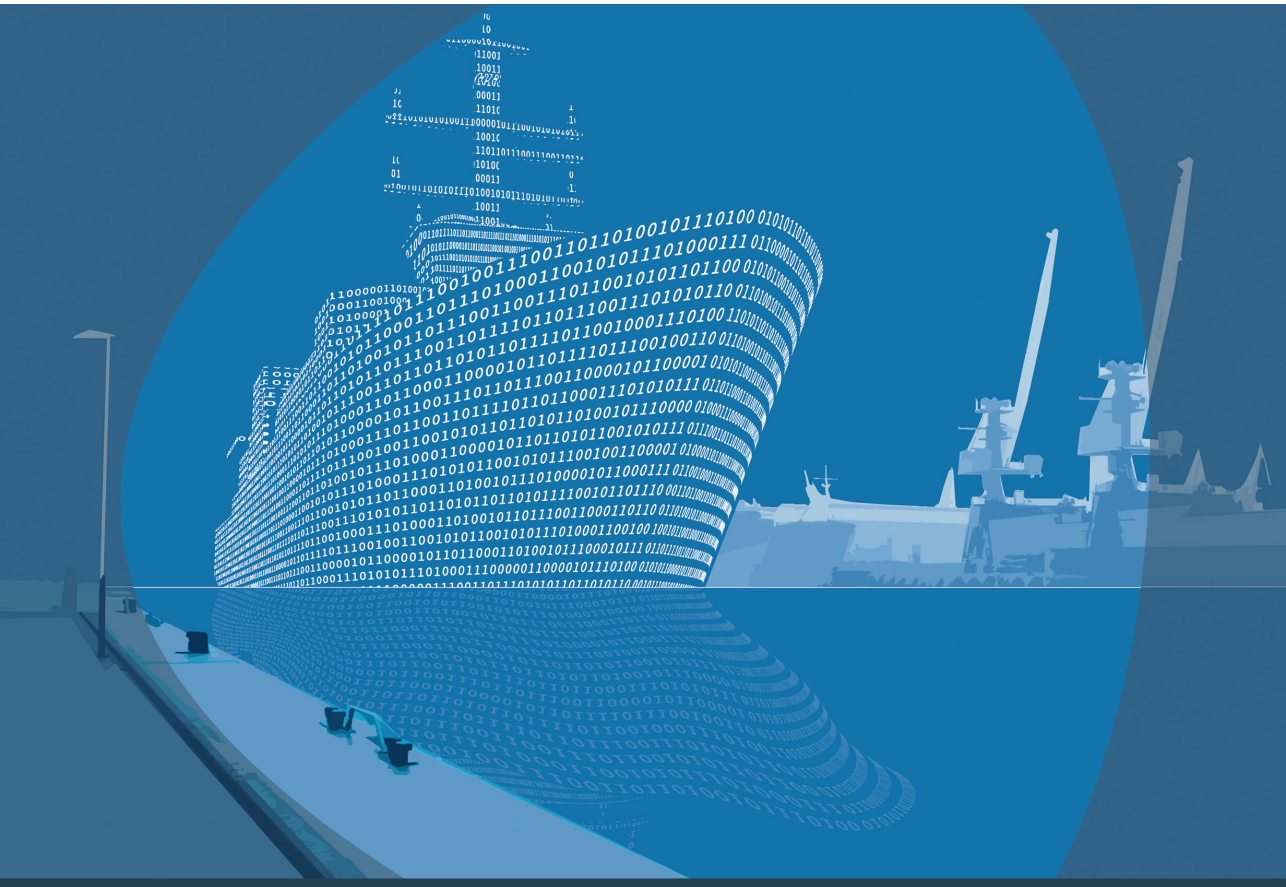
Lampe Schwartze Group



Look-Out 2016

Maritime Domain Cyber: Risks, Threats & Future Perspectives

Published by Hans-Christoph Enge and Dennis Göge

Look-Out 2016

Maritime Domain Cyber:
Risks, Threats & Future Perspectives

Published by Hans-Christoph Enge and Dennis Göge

The Publishers

Enge, Hans-Christoph

Hans-Christoph Enge is a lawyer by education. After finishing his legal studies in Hamburg where he specialized in maritime and marine insurance law, he worked for various shipping and insurance companies in New York, London, and Paris. Since 1990, he has been one of the managing partners of Lampe & Schierenbeck, later Lampe & Schwartze Group, responsible for marine and transport activities. Founded in 1858, it has more than 200 employees and is a special insurance provider for commercial and industrial risks, as well as one of the largest marine underwriting agencies in Europe. Further activities include risk-management and -analysis in respect of logistical, nautical and political hazards. Moreover, Enge is active in various committees of maritime industry and trade, as well as marine insurance associations. Currently, he is also the Chairman of the German equivalent to the Joint Hull Committee. He is a lecturer at various universities and a co-author of marine insurance law text books.

Göge, Dennis

Dr.-Ing. Dennis Göge holds a Diploma in Civil Engineering, a Diploma in Structural Mechanics and a Doctoral Degree in Aerospace Engineering. He started his career at the German Aerospace Center (DLR) in 2000 as Research Scientist. In 2005 he became Deputy Department Head and Head of a Research Group at DLR in Göttingen, Germany. After having worked from 2005 to 2007 in this position he then joined the Science and Technology Organisation (STO) of NATO in Neuilly-sur-Seine, France, as Executive Officer. In 2010, Dr. Göge has been appointed Executive Board Representative and Program Coordinator Defence and Security Research at DLR in Cologne, Germany. Actually, Dr. Göge is representing DLR in various national and international supervisory bodies, advisory councils aand committees. He is Member of the Science and Technology Board (STB) and Chairman of the AVT Panel of NATO's Science and Technology Organization (STO). In addition, he is an advisor to the Federal Ministry of Defence and to the Federal Ministry for Economic Affairs and Energy, Germany. He has published more than 30 scientific articles, holds two patents in the field of aerospace engineering and received several national, e.g. the Reinhard-Furrer-Award 2005 from the Wernher-von-Braun Foundation, and international, e.g. NATO Excellence Award 2015 of Applied Vehicle Technology (AVT).

Imprint

Published by:

Lampe & Schwartze KG
Herrlichkeit 5-6 | 28199 Bremen | Germany
www.lampe-schwartze.de/en

Date:

October 2015

Table of Content

List of Abbreviations

AIS	Automated Identification System
AIS-SART	Search and Rescue Transmitter
ANavS	Advanced Navigation Solutions
ARPA	Automatic Radar Plotting Aid
AtoN	Aids to Navigation
BMP	Best Management Practice
CIA	Central Intelligence Agency
COLREG	Conventions on the International Regulations for Preventing Colli sions at Sea
COSPAS-SARSAT	Cosmicheskaya Sistema Poiska Avariynyh Sudov — Search And Rescue Satellite-Aided Tracking
CV	Computer Vision
DLR	Deutsches Zentrum für Luft- und Raumfahrt e.V. / German Aerospace Center
DoS	Denial-of-service (attacks)
DSC	Digital Selective Calling
ECDIS	Electronic Chart Display and Information System
ETO	Electro-technical Officer
EU NAVFOR	European Union Naval Forces
GEO	Geostationary Earth Orbit
GMSK	Gaussian Minimum Shift Keying
GNSS	Global Navigation Satellite System
GoA	Golf of Aden
GPS	Global Positioning System
GPS C/A	Coarse/Acquisition
ICT	Information and Communication Technology
IMB	International Maritime Bureau
IMO	International Maritime Organization
IR	Infrared

ISPS	International Ship and Port Facility Security
LEO	Low Earth Orbit
LNG	Liquid Natural Gas
LORAN	Long Range Navigation
LOT	Polskie Linie Lotnicze LOT S.A.
MEO	Medium Earth Orbit
MF	Medium Frequency
MRQ	Marine Risk & Quality
MSCHOA	Maritime Security Center — Horn of Africa
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks
NATO	North Atlantic Treaty Organization
OCR	Optical Character Recognition
PCASP	Privately Contracted Armed Security Personnel
PMSC	Private Maritime Security Company
PNT	Position Navigation and Time
PPD	Personal Privacy Devices
RFID	Radio Frequency Identification
SLOC	Secure Sea Lines of Communication
STCW	(International Convention on) Standards of Training, Certification and Watchkeeping for Seafarers
TEU	Twenty-foot Equivalent Unit
UK	United Kingdom
US	United States of America
VDE	VHF Data Exchange
VHF	Very High Frequency
VTS	Vessel Traffic Service
WRC	World Radiocommunication Conference

Preface

Uwe Beckmeyer

The German maritime sector is traditionally important to the German economy. In order to maintain our lead what is a highly competitive market, we now need to focus on research and development activities. As a major exporter, Germany needs maritime safety and security that it can rely on. Given the increasing role that information technology is playing in the maritime sector, we are now facing the threat of cyber-attacks on maritime infrastructure.

According to feedback from both government and industry, awareness about cyber security in the maritime sector has been comparatively low since this first became an issue over two decades ago. The strengths of the shipping and maritime industries are based on many years of experience and on their capacity to reliably perform central tasks: ensuring that seafaring is safe and secure, serving offshore platforms, and transporting persons and goods in order to support passenger traffic and global supply chains. For a number of different reasons, the development cycles for upgrading critical communication, navigation and operational components on, for example, bridges and infrastructure are slower than in certain other industrial sectors. However, now that the maritime sector has begun to make use of information technology and automation processes, this situation has begun to change.

As a result of these developments, government and private industry have started to focus on a range of issues relating to awareness of cyber vulnerabilities in the maritime sector. Given the importance of the maritime economy for both Germany and Europe, it is absolutely essential that a systematic and deep-reaching analysis of current and future dangers and threats be undertaken. By basing this analysis on information provided by maritime customers, we will ensure that the maritime sector will be prepared for actual future challenges. The development of new technologies to protect maritime systems and infrastructure against cyber threats will not only safeguard the economic system, including global trade routes, but will also strengthen the position of German technology providers in what is a highly competitive international market. Furthermore, this initiative will serve to supplement a number of government measures in the maritime sector, such as the National Maritime Technologies Masterplan and the new High-Tech Strategy – Innovation for Germany.

Cyber Risks an Threats: A Demanding Challenge for the Maritime Industry

Georg Klöcker

On June 21 2015, 1,400 passengers of the polish airline LOT stranded at Warsaw Chopin Airport. What happened was that hacker had attacked the computer systems of the national airline, hence 10 national and international flights were cancelled, a dozen delayed. According to the airline, the offender paralyzed the computer systems which manage the flight plans.

On May 12 2015, the domestic intelligence service of the Federal Republic of Germany (German: Bundesamt für Verfassungsschutz) informed the administration of the German Bundestag that its computer system "Parlakom" had been hacked and attacked to an extensive degree because the offenders illegally used administrator rights to steal a big volume of data and thereby also obtained access e.g. to confidential e-mails of members of parliament.

In 2011, a criminal syndicate took advantage of the general security vulnerability in the computer systems of cargo owners, container services and the port of Antwerp. Undiscovered they smuggled cocaine and heroin for years from South America to Europe and stored the drugs between cargo and goods in containers which they tracked until the drugs had reached their target location.

These three examples out of numerous cyber incidents during the last few years show very clearly in which way criminal and terrorist actions could, or most likely will strike us in future and how vulnerable our infrastructures are - especially when it comes to sensitive structures such as information, communication and supply relevant systems. All three examples highlight the potential of damage and loss cyber attacks can cause to the European economic system and its societies.

The same risks also apply when it comes to cyber warfare between states. NATO Deputy Assistant Secretary General for Emerging Security Challenges, Jamie Shea, assessed in 2014 that:

> "for the first time we state explicitly that the cyber realm is covered by Article 5 of the Washington Treaty, the collective defense clause. We don't say in exactly which circumstances or what the threshold of the attack has to be to trigger a collective NATO response and we don't say what that collective NATO response should be… This will be decided by allies on a case-by-case basis, but we established a principle that at a certain level of intensity of damage, malicious intention, a cyber-attack could be treated as the equivalent of an armed attack."[1]

Maritime industry and logistics, today, are based on its solutions with global interfaces to improve efficiency and international networking. Technical dimensions of shipping and of ships themselves are not only depending on its technology in cases of communication. Various data like machinery performances are submitted automatically to basement institutions or shipping companies, comparable to the airfreight industry. The process of information technologies will definitely proceed and, as a logical consequence, turn into complex risk-scenarios which currently seem to be difficult to be solved. Substantial and challenging questions therefore are:

How are we going to handle digital attacks in general, especially regarding on how to detect and to deter them as well as to defend our systems and structures?

Are we nowadays capable to understand and to determine the dimension cyber risks and threats imply, which at the end seems to be an important precondition concerning the implementation of adequate measures?

---

[1] Jamie Shea, quoted in: Ranger, Steve (2014): NATO updates cyber defence policy as digital attacks become a standard part of conflict. NATO has updated its cyber defence policy in the light of a number of international crises that have involved cyber security threats, online in: http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/, 30.06.2014 (State:30.07. 2015).

Let us take a step back: According to the CIA World Factbook the German coastline measures 2,389 kilometers; not more than 3.6 percent of the coastline of the European Union in total. However, Germany is quite a maritime country when it comes to the capacities of the maritime industry as well as certainly to Germanys strong export economy.
This, on the other hand, is predominantly depending on external primary energies, products and materials. The economic strength of Germany is knotted very strongly to external impacts and therefore depends on operational trade routes, efficient logistical networks as well as on secure sea lines of communication (SLOCs) and safe infrastructures. There are approximately 2,750 so-called hidden champions existing worldwide, 1.300 (48 percent) are German owned midsized enterprises which are global market leader within their industries. The German economy is with an increasing tendency strongly engaged in foreign markets, or even enrooted. According to a poll conducted by the German Chamber of Commerce and Industry in 2015, the German industry increasingly invests in foreign countries to approach promising markets with higher growth potentials than traditional regions of interest. Furthermore, companies these days go for cost efficiency and therefore seek direct access especially to raw materials and products and of course to specialized local personnel.
The last decade clearly showed the interdependency and importance of safe and secure SLOCs. Because of the increase in piracy especially along the coast of Somalia, maritime security moved into the focus of interest of all engaged and effected stakeholders. The instability of Somalia, the lack of a capable government and true international aid led into fragility, chaos and at the end into a failed state. Land-based economic and social problems developed into top priority maritime threats. During 2007 and 2013, the international maritime industry faced a quick raise of piracy incidents within, initially, the Golf of Aden (GoA). A problem no one really had on the agenda now popped-up and within months became a mayor topic for the shipping industry worldwide. Since 2013, the International Maritime Bureau (IMB) releases strongly decreasing numbers of approaches and attacks. Up to date numbers have dropped down tremendously. What are the reasons for these developments and how can they be preserved? The director of the IMB, Pottengal Mukundan, stated late 2014 that:

> “the single biggest reason for the drop in worldwide piracy is the decrease in Somali piracy off the coast of East Africa. […] IMB says Somali pirates have been deterred by a combination of factors, including the key role of internatio-

nal navies, the hardening of vessels, the use of private armed security teams, and the stabilizing influence of Somalia's central government. […] It is imperative to continue combined international efforts to tackle Somali piracy. Any complacency at this stage could re-kindle pirate activity." [2]

All stakeholders involved developed, coordinated and implemented relevant structures, processes and operational measures. The international alliance installed appropriate missions along the Horn of Africa and a greater operational area in the Indian Ocean which were authorized by the national parliaments of the participating member states. Within their mandates, the international allied forces still today protect merchant vessels against attacks. The answer to piracy therefore was to pool the perception of challenges and to share solution building processes and operational actions.

German politics and the shipping industry discussed right from the beginning of this new generation of piracy the need, the benefit and the legal possibilities of the deployment of Privately Contracted Armed Security Personnel (PCASP) on merchant vessels. The German Parliament adopted the relevant law (German: Seeschiffbewachungsverordnung), which not only legalized and organized the employment of Private Maritime Security Companies (PMSC) but constitutes a clear legal framework and represents the first high quality standard for private security services on board of German flagged vessels. The maritime industry itself e.g. developed guidelines (Best Management Practice, BMP) to harden vessels against attacks and established a Piracy-Reporting Center as well as cooperations e.g. Maritime Security Center – Horn of Africa (MSCHOA) which was established by EU NAVFOR. All risk relevant reports and counter piracy measures clearly affect insurance-relevant risk rating e.g. when it comes to kidnap and ransom or war cover insurances. Speaking about piracy there are established structures between politics, the maritime industry, insurance, security, and relevant national authorities in charge.

As pictured at the beginning, today we are facing a new asymmetrical threat and challenge. The up-to-date-reported cyber attacks on maritime infrastructures such as ports and logistic hubs as well as on ocean going vessels are just the tip of the iceberg we are heading to. Today, we are just able to adumbrate its depth and complexity. We do not seem to be ca-

[1] Mukundan, Pottengal (2014): Somali pirate clampdown caused drop in global piracy, IMB reveals, online in:https://icc-ccs.org/news/904-somali-pirate-clampdown-caused-drop-in-global-piracy-imb-reveals, 15.01.2014 (State: 30.07.2015).

pable to clearly foresee the impact on the security of our trade routes, infrastructures and logistical networks. The perception of cyber attacks is much younger than the existing threat itself and it implies much more asymmetrical components and complex threat potential than piracy does. This is the major problem and challenge we are facing: the controllability of risks begins with the holistic comprehension of the threat.

Digital threats both stem from governmental institutions and criminal groups. Most badly affected aims of cyber attacks are risk dimensions of maritime business and logistics and especially include interest of the ship, its cargo and also liability-relevant items. The market of transport insurances yet does not offer at least one general standardized solution in reference to these special threats. While some policies include cyber risks, others exceptionally don't. It is still very unsure if and how cyber risks are going to be dealt with in the future. That is why defending, analyzing and managing cyber risks are highly relevant processes so far.

This publication shall initiate a process to find an efficient solution in reference to the special conditions of maritime shipping industry by seizing active processes of other business dimensions and related industries. This introduction and the following articles sketch the basis for the political and security policy aspects related to maritime cyber security. It is an attempt to set the political framework for the issues at stake. In the digital information age following the wake of an ever globalized world cyber security as well as its complexity, however, requires a much broader treatment, by both, academia and practitioners. E-applications penetrate all facets of society and thus an inter- and transdisciplinary approach on an academic level should be accompanied by detailed theoretical and practical analyses of technical, economic, legal, governance, insurance-related, ethical and anthropologic factors. The publishers and authors are convinced that only such holistic approach, consisting of various theoretical, empirical and policy-related concepts and addressing multifaceted aspects of cyber security, has the capability to contribute to a sustainable reduction and mitigation of cyber risks in the maritime domain.

Future publications of this series will accompany the general security policy framework by providing an overview on the state of research in security studies, discuss the ethical dimension of the contrast between liberty and security and highlight the psychological and technical factors of human-machine interactions in maritime cyber security. Furthermore, technical aspects, addressing vessel, port and terminal automation and security, general IT-security (and safety) and the implementations of business solutions will be put forward. Legal experts, insurance providers and public as well as international actors will provide

insights in the policy frameworks and daily practices of current trends and developments in protecting valuable maritime assets and critical infrastructure at sea. Lastly, the final issue of the series will deal with concrete policy recommendations that will help to proactively increase cyber security and mitigate risks evolving in case of successful attacks.

On the basis of the introductory article on security policy aspects of the maritime cyber security (Masala/Tsetsos 2015), the following article by Christoph Günther (2015) will cover the technical aspects of e-navigation, vessel automation and maritime traffic surveillance and discuss their strengths and weaknesses as well as address potential technical solutions that can minimize the risks. It thus represents the first detailed analysis of this series.

A Demanding Challenge for the Maritime Industry

Carlo Masala and Konstantinos Tsetsos

1. The Emerging Relationship between Maritime Security and Cyber Security

In the digital information age e-enabled vehicles, vessels, infrastructure, communication and management systems are the norm. As the vanguard of globalization worldwide air, maritime and land-based transportation, communication and mobility are increasingly dependent on information and communication technology (ICT), network-centric operations and wireless communication systems. The impact of digitization in commerce and services has, in part, enabled the pace with which globalization is taking place. Cyber-physical control systems, traffic control, logistics, network operations and safety management systems represent the tools to keep the increasingly interconnected global economy effective, profitable and on track. Although the maritime domain represents the most important benchmark for the global economic development, maritime cyber security has received only little attention. In fact, most of the world's largest ports have only limited cyber security strategies or cyber incident response plans in place, while the involved organizations have yet to establish company-wide cyber risk awareness programs. Future cyber threats will originate from hackers and crackers, often thousands of kilometers away from their targets, and their ability to crack vital vessel and port systems may very well have severer consequences for the maritime domain than more visible threats posed by maritime terrorism or piracy ever had. This is even more surprising considering the fact that modern maritime trade and the flawless functionality of ports represents a necessary prerequisite for contemporary industrial and service-based economies. Maritime trade is so crucial that even small disruptions would seriously hamper the flow of global commodities, raw materials and resources and lead to economic implications of unmeasurable proportions.

Current maritime security primarily deals with physical safety and security. Originating from accident investigation safety aspects concentrate on the prevention of environmental pollution and accident mitigation, such as ship collisions and vessel survivability, whereas maritime security aspects are characterized by anti-piracy and anti-terror measures, port

security, prevention of vessel misuse and maritime surveillance. Both maritime safety and security rely heavily on network-operated systems, information and communication technology, while ports more and more employ digital logistic systems (such as automated entry and cargo management systems or autonomous cranes). Ports and cargo terminals are the most important critical infrastructures and play a key role in facilitating a country's access to international trade. They represent the gateway and entry point to the global market, are intangible economic assets and valuable hubs in any supply chain. They connect the producers, suppliers and distributors with the customers and play a crucial role for the national and regional economic development. In light of increasing tonnage of goods, cargo and containers international ports have to process, automation and digitization have gradually acquired a major role in keeping logistic supply chains running.

#	Port	Country	Volume 2013 (in million TEUs)	Cyber Security awareness program
1	Shanghai	China	32.53	Yes
2	Singapore	Singapore	31.65	Yes
3	Hong Kong	China	23.10	Yes
4	Shenzhen	China	22.94	No
5	Busan	South Korea	17.04	No
6	Ningbo-Zhoushan	China	16.83	No
7	Guangzhou Harbor	China	14.74	No
8	Qingdao	China	14.50	No
9	Jebel Ali, Dubai	United Arab Emirates	13.30	Yes
10	Tianjin	China	12.30	No
11	Rotterdam	Netherlands	11.87	No
12	Port Kelang	Malaysia	10.00	No
13	Kaohsiung	Taiwan	9.78	No
14	Hamburg	Germany	8.86	Yes
15	Antwerp	Belgium	8.64	Yes

Fugure 1: Top 15 world container ports and cyber security awareness

[1] Own creation by the authors. Cyber security awareness was assessed by (1) the existence of a cyber security section on the port's homepage, (2) cyber-related security reports by port authorities, (3) an analysis of security measures information provided by port authorities, (4) the existence of a cyber security office, and (5) telephonic inquiries made by the authors over the existence of cyber-related action and awareness plans with public relations offices of the respective ports.

The need for further automation and digitization stems from the fact, that more and more producers, suppliers and ports have adopted a zero-inventory "just-in-time" delivery system to increase, both, their processing speed and their economic competitiveness. In contrast to land-based critical infrastructure and air-based navigation or traffic control systems, cyber security in the maritime domain is still in its nascence phase. As figure 1 shows nine of the

top 15 world container ports do not publically address IT security issues on their main homepages, an indication that highlights a limited cyber risk awareness culture. This article will discuss current trends in maritime digitization, highlight the risks and vulnerabilities for ports and vessels stemming from increased automation and reflect on the necessity of political cyber security measures in the maritime domain. Technical aspects maritime systems, even if briefly explained in the course of this article, will be elaborated with increased detail by the subsequent article of Günther (2015).

2. The Future Relevance of Maritime, Infrastructures and Port Cyber Security

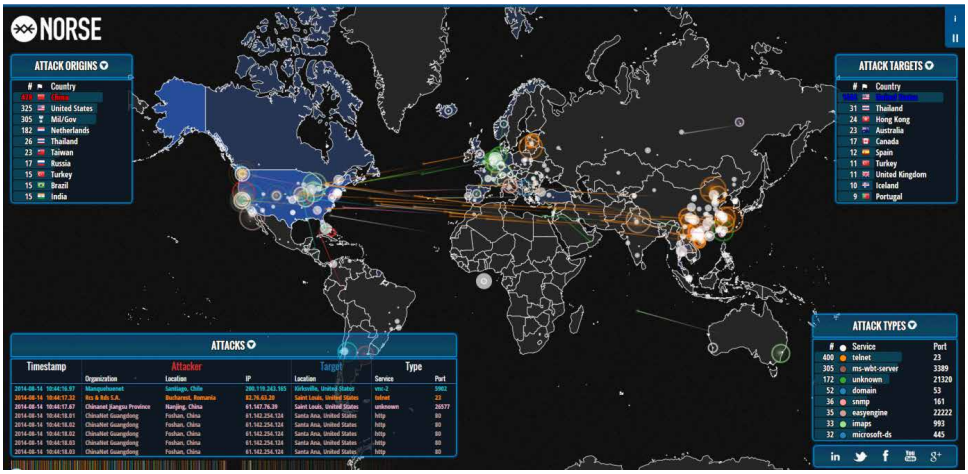
For ports, two distinct trends of digitization are dominant: terminal and vessel automation. ***Terminal automation*** encompasses terminal operation and container terminal management systems. Automated container terminal entrance, for instance, increasingly becomes fully automated with sensors (registering weight), RFID (Radio Frequency Identification), barcodes (cataloguing cargo details) and cameras (capturing truck license plates, drivers and registration codes using so-called Optical Character Recognition/OCR and detecting process anomalies using Computer Vision/CV). OCR and CV help port authorities keeping track of containers, vehicles and detecting damaged containers. It also increases a supervisor's awareness about dangerous cargo that must be separated or receive special treatment in case of fires or other accidents. This enables port authorities and customers to track their cargo, receive updates about container processing status, current position and access information about the status of the cargo (humidity, temperature or other data). Terminal automation also digitizes on-site security by featuring an ID card system for personnel, vehicles and containers and CCTV systems. CCTV systems allows tracking involved employees or unauthorized personnel in case of cargo theft, damage or in cases of violations of operational safety. In addition, ports increasingly rely on autonomous vehicles and crane systems to manage, store, load and transport containers. Next to port and terminal automation ***vessel automation*** has been introduced to ships over the last decades. Radar, automatic identification systems, electronic chart display information systems, GPS, radio

and satellite communications, ship collision avoidance systems as well as internet access are considered vital components of modern navigation. On state-of-the-art ships all those systems are interconnected in integrated bridge systems. Vessel automation outsources basic communications (such as positioning, routing, schedule and radar data) to automatic systems that relay this information to traffic systems and maritime authorities. In navigation, the International Maritime Organization (IMO) introduced an e-navigation strategy and this indicates that the future of navigation will depend on secure information technology to facilitate communication between the sea and shore. With the future of seafaring characterized by e-navigation, digitization will further dominate maritime traffic and transport. For a more thorough discussion of technologic aspects of vessel automation see Günther (2015: p. 27-46) following this article.

Further attempts to address the increasingly digital future of the maritime domain have been made. The 2010 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) - Manila Amendments introduced Electro Technical Officers (ETOs) on every cruise ship, indicating the need for on-board professionals handling cyber-related tasks. Thus, the maritime fields related to cyber security encompass multiple areas ranging from maritime information and surveillance systems as well as traffic control and navigation systems to port and cargo database security in harbors and the protection of critical infrastructure by enhancing cyber security and installing redundancies. While vessel and terminal automation as well as e-navigation is intended to increase safety and benefit productivity, efficiency, and the ability to process and distribute more and more cargo, both lead to increased cyber risks and security vulnerabilities that endanger ports and vessels. Coupled with the "zero-inventory" ideology in modern maritime commerce a disruption of the flow of basic resources, spare parts, consumer goods, and essential materials could lead to both, empty warehouses for producers as well as empty shelves for consumers in grocery stores. Next to ports and in more general terms sea lines of communication, maritime-based critical infrastructures that encompass off-shore wind energy facilities, oil and gas rigs are similarly vital. Energy infrastructures depend on sophisticated ICT that controls vital systems, communications and production procedures. Malicious software infestations thus can limit productivity of energy outputs, cause environmental pollution (i.e. oil spills) and ultimately even lead to the loss of human lives (by triggering an explosion in cases where safety systems are overridden).

3. Risks and Vulnerabilities for Ports, Vessels, Critical Infrastructures and Maritime Economy

Both state and private actors will have to address the emerging risks and vulnerabilities that arise in conjunction with increased digitization in a holistic manner. Classic security risks and vulnerabilities originate in relation to cargo, vessels, critical infrastructures, economic assets, trade flows and people involved. They range from the misuse of ships as weapons, cargo theft, smuggling, money laundering, and illegal migration to direct attacks on vessels, ports, and personnel, anthropogenic environmental disasters, and piracy. The relationship of those physical security threats and cyber risks is crucial with access to critical systems exponentially increasing the likelihood of a successful attack or disruption. Subsequently, a consideration of cyber security aspects in developing a maritime security strategy is relevant for state and private actors alike that seek to prevent and mitigate different types of threats to commercial, civilian and military naval operations. State and private actors require cyber security strategies to protect vital assets and harden their resilience in cases of third-party digital interference. According to the IBM Cyber Security Index 2013 the majority of cyber attacks originate from opportunists (49%), industrial espionage, terrorism, financial crime and data theft (23%) or from disgruntled employees (15%). The main tools are usually malicious code (such as malware planted inside the security perimeter) (35%) or investigative scans (external probing outside the security perimeter) (28%) that analyze weak points of targeted systems. It is important to note that the majority of elements that contributed to vulnerability and risks and subsequently to breaches of company systems originated from misconfigured systems (42%) and end-user errors (31%).



Given the increasing frequency of cyber attacks in the maritime domain, cyber assets in need of protection first and foremost encompass (1) critical digital traffic/communication systems, (2) critical information/databases, (3) automated terminal and vessel systems, and (4) critical infrastructures.

(1) Organized crime, terrorist groups, pirates, and other malevolent actors active in the maritime domain can interfere with vital systems and access databases. Hacking, cracking or hijacking of critical traffic and guidance systems can facilitate the misuse or misdirection of vessels in maritime chokepoints or the vicinity of ports with grave consequences. It can also be used to disguise cargo or ship movements of specific vessels used to transport illegal cargo, such as weapons, drugs or other contraband. Next to the physical damage ship collisions or environmental pollution can cause, the seizure of digital traffic systems would result in incalculable economic damages and logistical chain disruptions. In addition, accessing ship tracking data and shipment information could allow malevolent actors to single out particularly high-value targets for attacks or use that information for targeted hijackings. Recent analysis of existing maritime traffic systems revealed (see Günther 2015) that key technologies such as GPS, Automatic Identification System (AIS), and the system for viewing digital nautical charts (Electronic Chart Display and Information System/ECDIS) are prone to hacking attacks and feature poor cyber security standards (Reuters 2014). For instance, "[…] researchers have discovered that flaws in the AIS vessel tracking system can allow attackers to hijack communications of existing vessels, create fake vessels, trigger false SOS or collision alerts and even permanently disable AIS tracking on any vessel" (Security Intelligence Blog 2014). Using such exploits of the AIS infrastructure

to their advantage pirates have impersonated maritime authorities and lured ships into changing its course or seize all communications, concealed their ships with fake (or coast guard) IDs, sent false weather reports to incite course changes or sent out false distress signals to lure ships into dangerous waters. In conjunction with GPS spoofing malevolent actors can alter the course of any vessel, anytime anywhere (see figure 2).

Fugure 2: Course information of fake vessel in the Adriatic Sea after an AIS-hack[4]

(2) The data can also be used to harm a particular company by blackmailing it, providing peer competitors with cargo information, prices, ship schedule and speed or destinations and engage in other related activities that diminish the profitability or even survival of a shipping company. In addition, illegally acquired personal information can enable malevolent actors to target vital individuals (such as security personnel or senior management) and blackmail or bribe them for their purposes. In such cases crackers can access vital systems unnoticed and extract information that relates to port or vessel security or company information. Such actions are far from fiction as a recent example remarkably shows. In 2011, two companies operating in the port of Antwerp were targeted by hackers in employment of organized crime. The group awaited concealed cocaine that had been hidden in legitimate containers transporting bananas and timber from South America to Europe. By accessing transport and position information criminals were able to steal containers unnoticed before the legitimate owners arrived at the port or attacked specific trucks on

[1] Available at: http://www.portvision.com/news---events/press-releases---news/bid/343898/AIS-Hacking-Buzz-Hype-and-Facts [Accessed on: 30.09.2015].

highways with assault rifles in order to acquire the respective containers. When the system breaches were discovered, the hackers installed key logging devices in order to extract entry codes and then seized the cargo disguised as legitimate lorry drivers. After operating almost two years, the group was tracked down by Europol in 2013 (BBC 2013). Currently, the majority of ports and maritime traffic information systems do not possess the necessary cyber security infrastructure and lack the required data protection capacities. Furthermore, the background checks for vital personnel are seldom extended to the point of encompassing cyber vulnerability. This owes to the fact that the worldwide political and social awareness about cyber security has not reached the maritime domain yet.

(3) The same dynamics of vulnerability apply to terminal and vessel automation. The hijacking of digitized vessel and port systems can be used to conceal information about cargo in order to facilitate smuggling activities, to disrupt supply chains, to conduct espionage, distort the functionality of critical infrastructure and to put a port out of business by deliberate database destruction or data confusion.

(4) Regarding the hijacking or hacking of critical infrastructures worst-case scenario draw a catastrophic picture. A hacked security system on an oil rig can, as a recent example of worm infestation on a rig in the Gulf of Mexico shows, ultimately reduce the oil production to zero for several weeks. Depending on the targeted systems malware can render central components inoperable and in some cases even lead to physical damage. A coordinated attack of critical maritime infrastructures can thus put companies out of business or even limit the availability of energy (wind farms) and resources (oil, gas) for states in the targeted region. In addition, to productivity losses, infected systems may lead to the failure of safety protocols and lead to oil spills or even explosion of the facility generating massive environmental pollution. Finally, due to the remoteness of some oil rigs hacked systems can in fact endanger the lives of the personnel working on such platforms by distorting the functionality of safety systems. Infection can originate either directly by downloads through satellite connections (as in recent cases from online sources featuring movies or pirated music sites), or be brought aboard on laptops, external hard drives and USB drives that were infected on land.

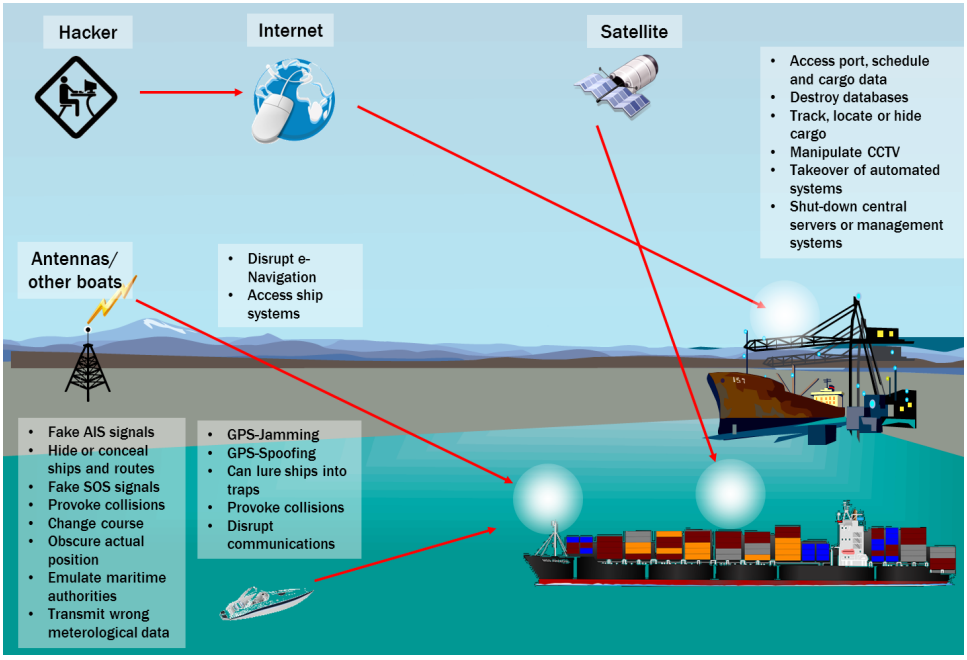


Figure 4: Potential threats against vessels and ports by cyber attacks[5]

In sum, the potential risks emerging from allegedly "soft" maritime security issues are diverse:

› Information misuse that leads to maritime attacks (organized crime, terrorism, piracy) as well as information misuse by peer business competitors (i.e. business espionage, influencing price fluctuations, accessing proprietary company data as well as details of vessel schedules)

› Concealing ship movements or cargo data by cracking related systems/ databases

› Distortion of critical infrastructure architecture (i.e. port automated cargo systems or off-shore energy producing facilities)

› Losing information sovereignty on ship position and distance to ports/coast guard/military vessels

› Disruption of communication, traffic and navigational systems

› Infiltration of key personnel (Electro Technical Officer - ETOs) on ships by organized crime or other actors

› Distortion of navigational data leading to accidents, hijackings and environmental pollution

[5] Own creation by the authors.

In light of the aforementioned cyber-related risks and vulnerabilities the adoption of numerous approaches and practices by private and public actors are necessary. In the following section measures to increase cyber security and awareness as well as policy recommendations are directed at, both, private and public actors in the maritime domain.

4. Necessary Steps to Port and Vessel Cyber Security

The first step to increase cyber security for ports begins with an industry-wide cyber security strategy. In the best case it is fully embedded in and compatible to a national cyber security strategy of the respective host nation. The following recommendations are based on the IBM Essential Practices for Cyber Security and should be considered as vital by any actor, whether port or shipping company, in the maritime domain.

- **Increase cyber risk awareness:** On the basis of such strategy private actor decision makers are required to build and ensure a risk-aware cyber culture amongst the employees of an organization. This can be achieved by targeted seminars, security briefings, establishing of a cyber risk and security department and by hiring specialists (either directly or as contractors). Cyber risk awareness should be implemented in a top-down approach until a security guard and a CEO of a company share the same awareness culture.
- **Cyber security by design:** Most ports and vessels originate from an era where digitization was less common and were retrofitted without cyber security being a top priority. Thus, ports need to implement modern cyber security systems ex-post or update older ones. Bearing in mind the lifecycle of ports and vessels this approach is unavoidable. However, when companies update their fleet and their equipment steps should be made to implement cyber security systems in conjunction with the upgrade process. With security built-in by design a plethora of risks and vulnerabilities can be reduced significantly. Security considerations affect design decisions from the beginning. They can rule out certain design paths that would seem attractive if security is not a priority. Therefore, consultations of cyber security expert should be a part of every design step. As no design implementation can be completely secure, future security flaws should be considered, a fault tolerant included that can be fixed quickly and with low-effort in case of a security breach. Security research will be much more effective if open-source thus increasing the chance of a security flaw being found first by researchers and not by actors with malevolent intentions. While open design standards ease the process of securing infrastructure, the actual implementation of the design should be diverse. A monoculture of hard- and software could endanger not only one part of an organization, but the organization as a

whole and to some degree affect the whole industry.

- **Workplace protection:** Digital assets of a company require the best possible protection to ensure cyber security. Every digital device can be used as a Trojan horse to enter a protected network or system. Critical systems therefore should be redundant and separated from any infrastructure available to untrusted personnel. Every company laptop, smartphone and workplace should fulfill the same security standards as the company's main server room. Guidelines for device configuration should be implemented and restricted and business-related usage only defined in order to reduce risks.
- **Network and intranet access:** A secure network setup is necessary to isolate malicious software and attacks quickly and prevent the spreading other parts of a system's infrastructure. Restricted and separated channels, supervised access points and selected user rights provide a suitable environment for a comprehensive cyber defense.
- **Detection mechanisms:** Automated detection mechanisms to thwart cyber attacks are crucial. Depending on the size of a company or systems and data under management, intrusion detection provides the necessary warning tools that monitor undesired behavior and enable companies to respond quickly to cyber threats.
- **State-of-the-art and updates:** For a secure system transparency is vital. Administrator should be able to oversee every program that is currently running on the system and be able to ensure that it is up-to-date. Running a multibillion dollar port on Windows 98/NT server may be convenient but far from safe. Updates and patches are crucial in eradicating exploits and backdoors and should be installed as soon as they are available. All systems should be updated simultaneously since a hardened network can be compromised by just one overlooked system component. Also, long-term maintenance of dedicated software must be ensured. A powerful piece of software can originate from a small contractor and therefore its security depends on the state of this contractor which is often unknown to the customer. This can be avoided by the customer when having full access to all documentation and source code and by publishing security risk through constant internal or external review of the software and its updates.
- **Cloud security:** If an organization uses cloud services it should be aware of the risks and threats and capable of protecting its data by isolating it from other users in the cloud and the inherent access of the cloud provider. Encryption can overcome some of those risks but it is not always practicable. Crucial encrypted data that is secure today, can be snapshot and decrypted tomorrow (forward secrecy).

- **Protect crucial assets:** It is vital for companies to identify its critical assets (conditional documents, inventory and employee databases etc.) and direct special attention for their protection. A common practice of modern-day crackers is to attack several servers with denial-of-service attacks (DoS) and while a company's cyber security team is distracted by this evident threat, the crucial assets/data are scanned and stolen. Therefore, critical assets require priority attention even if they are not under obvious attack.
- **Keep track of your employees:** With 15% of all cyber attacks originating from disgruntled or ex-employees it is vital to revoke access permission once the respective individual has left the company or is engaged in a different department.
- **Analyze your environment:** The degree of interconnectedness of modern businesses in the maritime domain requires companies to extend the preceding recommendations and best practices to cooperating companies, sub-contractors, supplies, customers and on-site neighbors. Ports, for example, are used by various companies with different backgrounds and potentially different risk cultures. The safety of a company's system may be nullified if one's contractors, neighbors or customers are negligent to potential cyber threats. Standardization in this regards cannot only increase security but also contributed to reduced operating costs.

5. Policy Recommendations for (State) and Private Actors

Necessity to Increase Awareness on Maritime Cyber Security

- Participate in and sponsor awareness campaigns for governmental, military and maritime authorities
- Participate in guidance and training programs on the impact of maritime cyber security threats and their mitigation
- Establishment of cyber security programs for ports and maritime traffic control systems

Intra-, Intergovernmental, International and Private Cooperation

- Participate in and sponsor the development of national and international standards, protocols, and systems for the implementation of maritime ICT systems
- Implementation of national maritime cyber security guidelines
- Coordination with regional and international organizations (e.g. IMO, IMB) and establishment of regional cyber security systems in the maritime domain
- Establish a reporting culture for recognized or thwarted cyber attacks on an international, national, academic and business-wide level

› Increasing private-public partnerships on the basis of national and regional cyber security guidelines and best practices
› Support development and implementation of critical infrastructure redundancy (operating Systems, GPS, etc.)

Modification of Maritime Regulations in Light of Cyber Security

› International Ship and Port Facility Security (ISPS) should be expanded beyond safety and physical security aspects
› Revisions to national and international legal regulatory frameworks necessary to adapt to cyber-related maritime threats
› Clarification of responsibilities and tasks between governmental and private key stakeholders in maritime security

National Economic Incentives to Private Stakeholders and ICT Research

› Provision of economic incentives to private stakeholder and businesses in the maritime domain to invest into port and maritime cyber security systems
› State and private funding for the development of open-source maritime-related cyber security systems (software and hardware)
› State and private actor sponsored cooperation with research institutions for the development of resilient port and maritime cyber security systems and programs

Short and Medium Term Requirements for Maritime Cyber Risk Mitigation

› Stimulate dialogue and information exchange between key stakeholders in the maritime sector and associated stakeholders
› Navigational chart updates should be certified, include encrypted data and digital electronic signatures to verify their source
› Define roles and responsibilities towards cyber security in this sector on regional and national levels
› E-navigation systems need to be secured to avoid data distortion or misuse
› Develop appropriate cyber security training programs for port and traffic control personnel
› Consider the establishment of company-wide cyber security officers and the hiring of ETOs for vital assets
› New training and certification requirements for ETOs and improved measures to prevent fraudulent practices relating to modern technology such as electronic charts and information systems

6. Outlook

Recent recorded cases of successful cyber attack on ports (such as Antwerp), critical infrastructures (oil rig in the Gulf of Mexico) and single vessels (such as the experimental GPS-spoofing attack on the "White Rose of Drachs") as well as the sophistication with which terrorists, organized crime and pirates are employing modern technology to hijack, takeover, spy on or lure vessels off course requires the industry's full attention. The evident weaknesses of established maritime traffic and communications systems (such as AIS and GPS) offer ample exploitation opportunities for malevolent actors, both governmental and non-state, and highlight existing vulnerabilities. Only a coordinated effort by international and corporate decision makers can increase international maritime safety and security standards to confront cyber-related threats to maritime trade and commerce. In addition, ports as the portals to a globalized world need to be hardened, both physically and digitally, to reduce the risks of cyber attacks and ultimately avoid disruption of global supply chains. Companies in the maritime sector as well as the respective governments should establish digital redundancies, countermeasures and procedures to protect critical infrastructure and vessels. This can only be achieved if an appropriate risk awareness culture is promoted and cultivated to fit the contemporary challenges of the digital information age. Ignoring these developments is perilous for both the state and private sector. States risk functionality disruptions of valuable economic trade hubs, may face environmental pollution of enormous proportions if ships are steered deliberately off course and could get exposed to severe economic consequences in the aftermath of successful cyber attacks on ports and critical maritime infrastructures. Maritime companies are in danger of forfeiting their economic competitiveness, risk the loss of critical business-related information or valuable vessels and ultimately may be thrown out of business by one successful cyber attack causing billions in damage.

7. References

BBC (2013): Police warning after drug traffickers‘ cyber-attack. 16.10.2013. Available at: http://www.bbc.com/news/world-europe-24539417 [Accessed on 01.08.2014].

Enge, Hans-Christoph/Göge, Dennis (eds.): Maritime Domain Cyber: Risks, Threats & Future Perspectives, Bremen.

ENISA (2011): Analysis of Cyber Security Aspects in the Maritime Sector. Workshop on Cyber Security Aspects in the Maritime Sector. European Network and Information Security Agency.

Günther, Christoph (2015): Design of Maritime Cyber Security Systems, in:

- IBM (2014): The 2013 IBM Cyber Security Intelligence Index. Somers, NY.
- IBM (2014): IBM Essential Practices Security Workshop. Somers, NY.
- IBM (2013): The 2013 IBM Cyber Security Intelligence Index. Somers, NY.

***ICC International Maritime Bureau (2013)*:** Piracy and Armed Robbery against Ships. Report for the period 1 January – 31 December 2013. London.

***Norse (2014)*:** Live Attack Intelligence. Available at: http://map.ipviking.com/ [Accessed on: 14.08.2014].

Reuters (2014): All at sea: global shipping fleet exposed to hacking threat. 23.04.2014. Available at: http://www.reuters.com/article/2014/04/23/us-cybersecurity-shipping-idUSBREA3M20820140423 [Accessed on: 01.08.2014].

Security Intelligence Blog (2013): Vulnerabilities Discovered in Global Vessel Tracking Systems. 15.10.2013. Available at: http://blog.trendmicro.com/trendlabs-security-intelligence/ vulnerabilities-discovered-in-global-vessel-tracking-systems/ [Accessed on: 01.08.2014].

World Economic Forum (2012): Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience. Available at: http://www3.weforum.org/docs/ WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf [Accessed on: 01.08.2014].

World Economic Forum (2014): Hyperconnected Travel and Transportation in Action. Available at: http://www3.weforum.org/docs/WEF_Connected_World_HyperconnectedTravelAndTransportationInAction_2014.pdf [Accessed on: 01.08.2014].

Design of Maritime Cyber Security Systems

Christoph Günther

A safe, efficient and environmentally friendly maritime traffic is crucial to the functioning of the world economy. Concepts supporting these goals are currently developed in e-navigation initiatives. They strongly rely on electronic sensing and data exchange in order to develop a joint situational awareness and to enable joint decision making. This is the basis for optimally navigating ships in dense traffic and constrained water ways under all weather conditions. The surveillance implicit in e-navigation additionally supports law enforcement (contraband, fraud in fishery, disposal of chemicals) and helps identifying preparations for terrorist actions. This introduces a security aspect in e-navigation which shall be addressed in the present paper.

1. Introduction

The size of ships has steadily increased over the years, with the largest container ships measuring more than 400 meters in length and carrying more than 19,000 twenty-foot containers. These ships need to maneuver in locks with margins that sometimes are not more than a few fingers. The precision in maneuvering became possible due to a number of propellant screws, often mounted on pods, as well as due to advanced electronic control systems for steering. Container ships are not in isolation. The largest cruise ships reach 362 meters and carry more than 6,200 passengers. This involves a significant responsibility. Also Liquid Natural Gas (LNG) tankers (345 meters for Q-Max class) and tankers (458 meters for the Knock Newis) have substantial sizes. In the latter cases, it is the risk emanating from their loads, which is particular critical. Besides this, the density of maritime traffic and the diversity of ship classes are increasing as well. Very large ships are highly inert and need long distances to maneuver. Other ships are highly agile and extremely fast. These ships mix sometimes in confined spaces such as near Rostock-Warnemünde in the Baltic Sea. The situation is further worsened under adverse weather conditions. In the

whole Baltic Sea, this leads to 100 collisions and grounding events every year (Helcom, 2014), fortunately, most of them minor. Half of these events are due to navigation errors. The increasing complexity of maritime navigation, which is present everywhere, led the International Maritime Organization (IMO) to initiate its e-navigation initiative for avoiding collisions and groundings, reducing fuel consumption, and easing the control of vessels (IMO, e-Navigation, 2006). It plans to heavily rely on satellite and inertial navigation, radar and sonar as well as on communications amongst ships and with shore. The interworking of these systems shall ensure the necessary situational awareness and support collaborative decision making amongst all parties involved. The associated radio systems, electronic equipments, and information systems are to be designed for robustness against known natural impairments, such as signal distortions and fading due to multipath, ionospheric propagation, unintentional interference and the like. The same systems shall also serve law enforcement and security by monitoring maritime movements. This includes the protection of fishing grounds, the identification of ships that dump materials at sea, and the prevention of contraband, e.g. the smuggling of arms. The parties acting against laws have a strong interest in evading any form of surveillance and will thus aim at manipulating e-navigation. Thus security becomes an important aspect of e-navigation. Finally hostile states at war and terrorists might aim at disrupting "sea transportation." They might aim at causing collisions that block routes intentionally or that even cause a large number of casualties. Although this is currently not a significant threat, the new e-navigation system should be designed in such a manner that it would be difficult to cause such harmful actions. The cost of including adequate protections is minor now. For this reason, we recommend to address the cyber security threats of the companion article by Masala and Tsetsos (Masala, 2015).

The rest of this article is structured as follows: section 2 introduces our view of e-navigation; section 3 addresses the threats and counter-measures associated with the estimation of the own position and attitude; section 4 discusses the specifics of the Automatic Identification System (AIS) and its evolution; section 5 addresses the sounding of the environment

by radar and sonar; Section 6 discusses the security of communications, and section 7 concludes with some remarks on telecontrol.

2. E-Navigation – System Description

In the best of all worlds a ship reliably knows its position and its heading. It furthermore has a complete and up-to-date picture of the status of water ways, as well as of shore lines, the sea bed topography, tides, weather, water currents, the height and direction of waves and the location of ice-fields. Most importantly, it also knows about the position and heading of all other ships. All this information is used to compute an optimal route in the sense of a quantified and acceptable risk as well as including economic and environmental considerations.

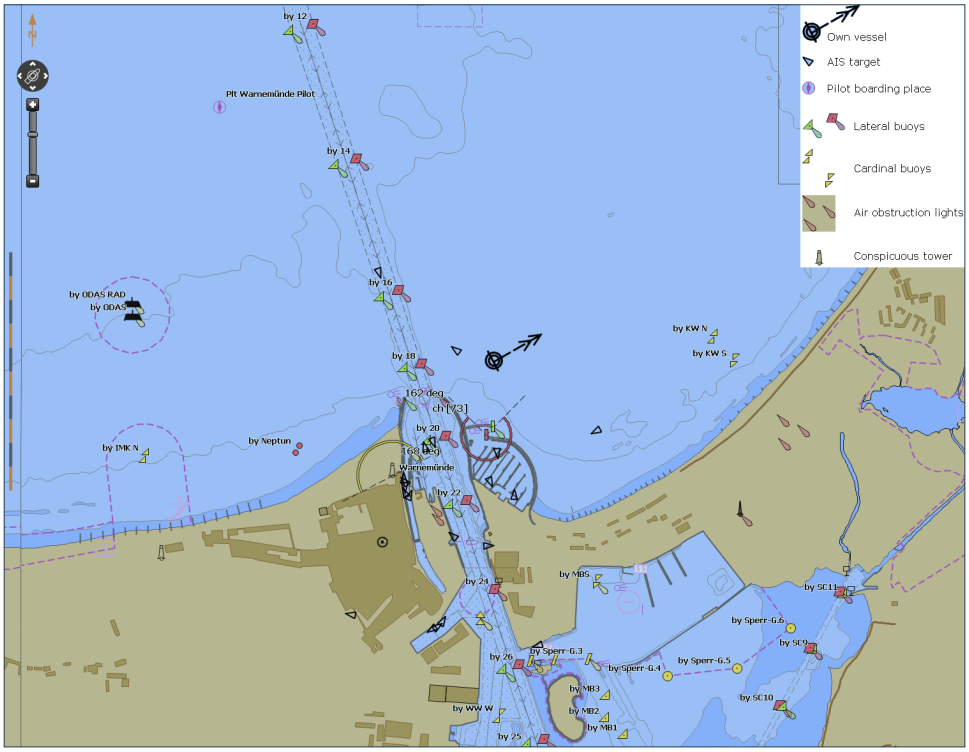


Figure 1: ECDIS chart of the entrance of the port of Rostock-Warnemünde, showing the own ship, AIS equipped ships and navigation aids. E-navigation will add integrity, improved situational awareness and maneuver support. [Courtesy: P. Banys, DLR]

The aim of e-navigation is to achieve this in a manner that is user-friendly for all people involved on-board and ashore, see figure 1. The information just described shall be collected by a number of means, which include the ships themselves, shore equipment, and satellites. The ships carry sensors, which allow them to estimate their position and heading over ground (satellite navigation, gyros), the local direction and velocity of the wind and water currents (previous ones, anemometer, and speed logs), the height of tides and local sea bed topography (with depth and imaging sonar in addition) and wave patterns (again satellite and inertial navigation as well as gyros). Satellites are an ideal source for ice maps and maps of the coast lines. They provide information about weather and wave fields, as well as about maritime traffic for a short period of time. Finally, coastal radars also map ship movements. Coastal systems, such as Vessel Traffic Service (VTS) systems additionally play an important role in the integration and distribution of information. They furthermore have a control role. In their absence, all of this has to be handled by the ships autonomously. So in our view e-navigation shall not rely on the availability of coastal systems but shall smoothly integrate with them when they are present, and shall support whatever priorities maritime regulations imposes. It is obvious that the above vision requires all information to be reliable. This is a critical and difficult endeavor, currently addressed by the use of several different sensors, a careful modelling of their error characteristics, and an appropriate integration of the resulting information using probability theory to produce desired outcomes, such as a probability of collision or grounding under the assumption of a certain set of movement hypothesis. All of this requires that the systems are certified in the manner claimed and that they have not been artificially manipulated. The latter manipulation can be in the equipment itself, by disrupting its function through external jamming, and or by injecting artificial signals to obtain a measurement that does not reflect the physical reality (spoofing).

A large variety of manipulations at equipment level can be prevented by a tamper proof design of the hardware and a strict control of software changes. Any output of such equipment must be cryptographically authenticated using a key that is irrevocably deleted whenever a manipulation is detected. This requires the authentication of the measurement data transmitted between the sensors and the processing facility, as well as a tamper proof packaging of the sensors themselves and of their mounts. The overall system must however remain stable if some equipment fails to provide the necessary authentication. Such a failure must lead to an increased attention. In some cases, the information might be replaced by an alter-

native one. In other cases, there is no alternative source of information and the answer must involve game theoretic approaches for identifying potential strategies of malevolent parties and for choosing routes that avoid high risks such as the ramming of a pier by a gas tanker.

3. Positioning and Navigation

The central piece of information in e-navigation is the own position over ground $\vec{r}$. Four more quantities are of similar importance – they are the vessel's velocity over ground $\vec{v} = d\vec{r}/dt$ and the absolute time t, as well as the attitude $\vec{\alpha}$ and its derivative $d\vec{\alpha}/dt$. In maritime navigation, the latter two quantities can be reduced to heading and rate of turn. The full attitude is, however, needed in order to map sonar measurements, to estimate the response to waves and wind, as well as to control antennas for communications and navigation. The position, velocity, heading and rate of turn are used to avoid groundings and collisions with locks, piers, and other fixed objects. Time is additionally needed to coordinate the own movement with that of other ships. These quantities or a subset of them are sometimes logged for documentation purposes in fishery, for example. They are also reported by the Automatic Identification System (AIS) for collision avoidance and traffic coordination amongst ships. In both contexts, the ship's position becomes observable to authorities. Thus, there is an incentive for criminal actors to modify its content. Assuming that the manipulation of information has been made difficult on-board, the manipulation has either to be performed in the signals of the Global Navigation Satellite System (GNSS) or in the signals transmitted by the AIS. The latter is addressed in a separate section.

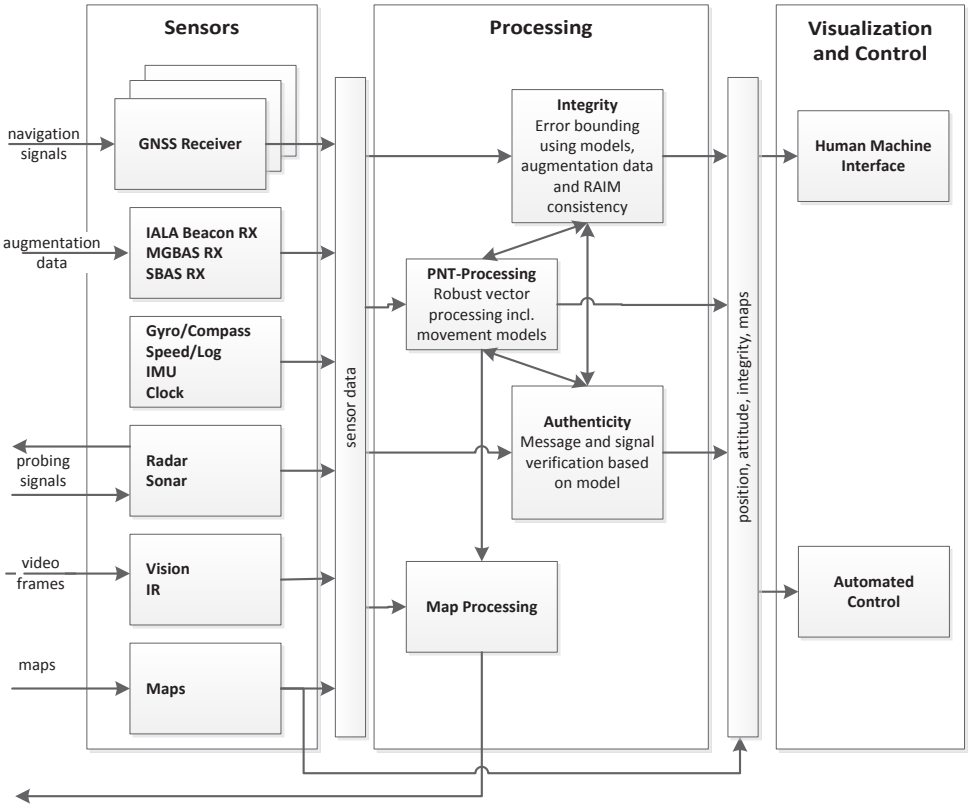


Figure 2: Generic Multisensor Receiver. DLR's current PNT unit estimates position and error bounds using GNSS, inertial, and speed log sensor data.

The specification of GNSS systems is public, see e.g. (GPS Wing, 2012) for the GPS C/A and (Galileo-OS-SIS, 2010) for the Galileo open service, see also (Misra & Enge, 2006). These specifications are needed for the design of receivers. At the same time they are used to build simulators, which perfectly reproduce the signals transmitted by the satellites, so that receivers can be tested during development and production. Unfortunately, this is also the basis for the design of spoofing equipment which aims at misrepresenting the position, typically, in one target receiver. This is easiest, when the criminal actor, the so-called spoofer, has access to the antenna interface, which is the case presently. The spoofer then disconnects the antenna and injects signals from his simulator and can thus substitute the true route by a synthetic one. Three types of countermeasures are considered; see also (Günther, 2014):

› The first one is to authenticate the satellite signals. It is very likely that Galileo will integrate such a protection in its I-Nav message, see Fernández-Hernández et al. (Fernández-Hernández, Rijmen, Seco Granados, Simón, Rodriguez, & Calle, 2014).
› The second one is to integrate the antenna and receiver in a tamper-proof manner.
› The third one is to continuously run the positioning system and to evaluate measurements from other sensors as well.

With the decreasing size of receiver chips, it is no more difficult to integrate the analog front-end and the pre-processing in the antenna – first modules which at least partially implement this program exist, see e.g. the sensor module of ANAVS (ANavS, 2015). The simulator could still capture the receiver by injecting the signal into the antenna in a very careful manner. In this case, the third defense, the evaluation of other sensors would constrain the trajectories to remain in the error budgets of the other sensors. Inertial measurements provide accelerations and turn rates. They are nearly impossible to manipulate. The high-end of such equipment includes laser gyro and supports autonomous navigation over long periods of
time - unfortunately they are very expensive. Recent developments in the low price sector are very promising. First products have announced drift rates of 6 degrees per hour. This permits to constrain the manipulation of the GNSS signal and even to bridge short GNSS outages. The position uncertainty grows linearly with speed logs, while this is with the third power for inertial measurements. This makes speed measurements attractive whenever the water currents are known. From a security perspective one has to consider the possibility of influencing speed log measurements by using small propellers under the ship's hull. Doppler sonars could solve that problem by taking profiles at random distances. In shallow waters with a stable sea bed, they could even be used for measuring "absolute" movement. Although, rogue mariners can misrepresent their position, the design of countermeasures is easier and the cost of countermeasures is lower than the cost of spoofing. Figure 2 shows a generic setup of a multisensory receiver for Position Navigation and Time (PNT). DLR's development of a PNT unit integrates GNSS, inertial, and speed log information to generate a robust solution (Ziebold, Dai, Lanca, Noack, & Engler, 2013).

Figure 3: Antenna array in two different sizes (upper right), mounted on a ship under a radom (left), and multi-antenna receiver (lower right). [Courtesy: Dr. Achim Hornbostel DLR]

A second scenario is that terrorists aim at disrupting the navigation of a ship in a critical situation, e.g. of an LNG at the entrance of a port. Since GNSS signals are extremely weak, more than one million times weaker than mobile radio signals, they can easily be jammed. "Jamming" means superposing a signal to the received signal, in order to prevent the receiver from being able to estimate its position. Jammers typically disrupt signal reception in a whole area, but sophisticated jammer could also direct their interfering signal to a particular ship. The ship under attack can defend itself by nulling out the jammer, e.g. using an antenna arrays to suppress the signal coming from the direction of the jammer. DLR's Galant receiver, see Figure 3, achieves the best published performance in this respect (Hornbostel, et al., 2013). Its most advanced version uses a dual approach, which suppresses the jammer before correlation (jammer above the noise) and after correlation (residuals in the noise). The jammer can overcome this barrier by increasing its signal power. In this case, the vessels positioning algorithm has to de-weight the satellite measurements in the multisensory receiver and to rely on other sensors. Short jamming periods can be easily bridged using inertial measurements. Speed-logs are sometimes helpful as well. Additionally, in critical shore areas, straights, and ports, radars have a sufficient number of characteristic reflectors to also support navigation.

Jamming of GNSS is considered a critical threat. It is applied by the military in conflict situations. North Korea is reported to have jammed GNSS reception in South Korea a number of times (Gallagher, 2012). Jamming also happened in peaceful environments. In Newark NY, USA, so-called Personal Privacy Devices (PPD) jammed the GPS Landing

System. The PPDs are used to protect against being tracked by data loggers, e.g. those installed in the vehicles of logistic companies. They are illegal and often much more disruptive than intended.

Due to the sensitivity of GNSS to jamming, the UK, South Korea and recently the US are reconsidering the use of LORAN as a backup system. LORAN is a terrestrial short wave radio navigation system with a number of virtues. Its ground installation consists of transmitters with a power of 100-4,000 kW and antennas that are 100 and more meters high. This is the system's strength, since it makes it difficult for jammers to generate significant disturbances. On the downside, the operation of such infrastructures is very expensive. The same applies to the investment needed to extend LORAN to a global scale. The so-called R-Mode aims at using Medium Frequency (MF) communication signals for navigation (Johnson, Swaszek, Alberding, Hoppe, & Oltmann, 2014). R-mode promises to provide a cost-effective backup solution. The principle of using communication signals for navigation could also be extended to other communication standards. The aim is to jointly use all available signals in order to obtain a very robust and reliable position estimate.

Another class of threats is the misleading of a vessel's satellite navigation system by injecting artificial signals through the antenna. It is unclear whether it ever happened, except for demonstration purposes (Spoofing a Superyacht at Sea, 2013). Spoofing would be a highly aggressive act. The aim could be the hijacking of a ship with a precious load by pirates, the sinking of a ship in a harbor entrance during war or the use of a ship as a weapon in an act of terrorism. In these cases, the authentic satellite signals are be substituted by artificial ones. Like in the case of on-board spoofing, the inclusion of other sensors in the solution is a central element in the countermeasures. Additionally, there are a number of methods for detecting spoofing signals, as well as for eliminating them. The most powerful of all is obtained by using the DLR Galant receiver to estimate the direction of arrival of the signals. This forces the spoofer to reconstruct the complete wave field, which is a difficult task. The associated complexity and know-how is unlikely to be managed by pirates or terrorists. The suitable combination of a multi-antenna receiver with inertial sensors, a stable clock and a speed log can be considered safe with respect to all practical threats.

4. Automatic Information System (AIS)

AIS is a system designed to provide the own position and course to neighboring ships in order to prevent collisions. The own position can either be determined using GPS or using a multisensory receiver. Additionally, AIS may also be used by coastal systems to mark the location of buoys, rocks or shallow waters, so-called Aids to Navigation (AtoN). In this case, the information is transmitted by a centralized installation. Finally, AIS marks locations of ships in distress or of men over board. The associated equipment is called AIS Search and Rescue Transmitter (AIS-SART).

Beyond this, AIS is used for surveillance purposes as already exposed. The latter is the primary incentive for manipulations. Such manipulations have been described and performed by Balduzzi, Pasta, Wilhoit (Balduzzi, Pasta, & Wilhoit, 2014). In our view the most important ones are:

- Be in another location,
- Be another ship,
- Disappear,
- Piracy/hijack ships, and
- Confuse (other) vessels for causing a collision.

In the first two cases, we assume that the ship's installation is protected against spoofing, which means that the spoofer cannot misuse the ship's authentic AIS. He has to install a spoofing AIS next to it. With this second installation, he overpowers the authentic signal in a manner that does not trigger a slot reallocation in the AIS protocol. This requires the spoofing signal to never be earlier than the authentic signal. Two options for the spoofing signal exist: it might overlay the authentic AIS with a signal of greater power and of a different content to capture the receiver or it might simply jam the transmission by generating a cluster of false AIS messages and create a new message at another time delay and/or frequency. In this manner, the spoofer can pretend to be in another location or to be associated with a different ship. The first approach could be detected by the receiver, due to the imperfect suppression of the authentic signal. The second approach is more difficult to detect if the spoofer is smart. This allows for the mentioned frauds such as fishing in forbidden areas, dumping material at sea, smuggling, and the like. The countermeasure to the second threat is to authenticate the message. Specifically, every vessel has a private and a public key. Each transmitter signs its messages using its private key, and each receiver

verifies it with the public key. The latter one is published and authenticated by a public authority such as IMO. The list of public keys is continuously updated, e.g. over satellite by interrogating each ship whether its security system has been tampered. The protocol is a challenge response scheme, which involves the private key. The private key is erased, whenever a tamper attempt was made. This mechanism also protects against spoofing from on-shore or from another nearby ship when it aims at moving the ship in the AIS situational awareness of the other ships and VTS systems.

It is always possible to disappear from AIS monitoring by cutting electricity, destroying the transmitter or by covering the antenna with aluminum foil. The two countermeasures are the continuous tracking of ships even at sea as well as independent means of observation. The former is supported by the deployment of AIS receivers on satellites. There are currently 19 units in space under the control of different operators and administrators. Another 17 are due to be launched very soon. Additionally, aircraft can also be used for such tasks. The integration of corresponding reception capabilities is not complex from a technical point of view and could thus be considered on a broad scale. The overlay of aeronautical and maritime routes is such that more than 95% of the ships could be covered. On major routes the update rate would be several times per hour (Plass, Poehlmann, Hermenier, & Dammann, 2015). Radar is the primary independent means of observation. Many vessels are equipped with radars. Additionally space-born radars observe the scene intermittently. In both cases ship locations without AIS signals – so-called dark targets - are easily spotted and the information about them can be communicated to law enforcement and other ships. Pirates can use AIS in different ways. The first one is to learn about the course of victim vessels. This is favored by the information from AIS, which includes the destination port, the load of the ship and the like. The risk of being hijacked causes vessels to switch/off their AIS transmitters in certain regions of the world. This puts them at risk, however, since the intended collision protection disappears. Any protection against this threat is a critical trade-off between safety and security. A possible compromise is that ships indicate their sole presence in a certain sector, potentially via satellite in order to escape triangulation. As a consequence of this, other ships know about their presence. In a second step ships enter into a mutual authentication and key exchange procedure. This leads to the provision of instantaneous public keys available to all trusted ships, which normally are all ships. The vessels then encrypt their messages using their instantaneous private keys. The receiving parties can decrypt them using the corresponding instantaneous public keys. Contrary to the vessels public key, the instantaneous public key is only known to parties that entered

into a pairing procedure, which is a trusted process. A second approach to capture ships is to involve them in a search and rescue operation by transmitting AIS-SART
messages – ships are obliged to participate in such rescue operations and are thus vulnerable to this threat. Authentication prevents messages from being planted too easily but there is still the option to sink a real ship in order to capture a fat pray.
Finally, vessels can be confused by manipulating AIS messages reporting about ships, rocks, and navigation aids or by generating artificial ones. A judicious choice of false AIS information may induce the crew to perform a sequence of maneuvers that ends in a collision. This threat needs again be protected by authentication.
In conclusion, message authentication and the consistency of data with other measurements such as radar plots are effective methods to detect manipulations. Authentication increases the data volume. The associated capacity problem is addressed in Section 7.

5. Radar and Sonar

Radars are currently the primary means of navigation required by COLREGS, i.e. the IMO's collision avoidance regulation (IMO, COLREGS - International Regulations for Preventing Collisions at Sea, 1972). Radars transmit a pulsed waveform which is reflected by the target ship and by objects surrounding that ship. The distance of the ship is estimated from the round-trip delay. The relative velocity is obtained from the Doppler-shift of the echo. The estimation of position and velocity required different pulse repetition frequencies in the past. Thus different radars or at least modes were used. Modern systems with appropriate waveforms and digital correlation can combine both modes more easily. The antennas of radars are highly directive in order to maximize the signal to noise ratio of the signal received after reflection by the target. A complete picture of the surroundings is obtained by spinning the antenna at a rate of a few cycles per minute. The various echoes are thus aligned on a ray for each value of the azimuth angle, resulting in the usual polar plots seen on radar screens; see (Skolnik, 2001). Modern radars have an "Automatic Radar Plotting Aid" (ARPA) function, which automatically tracks objects, shows their trajectory, and computes the closest point of approach. Radar visibility can be increased by using radar corner retroreflectors. They are used on navigation aids or on wooden ships, for example. The signals of maritime radars are in one of two frequency bands: the S- and the X-band. The longer wavelength of the S-band allows for a slightly longer range. Typical ranges are up to 35-50 nm. Harbor operations are performed using reduced power settings.
Radars have the enormous benefit of locating any object with a sufficient cross section at a

certain distance. Radars are, however, affected by spurious reflections (clutter), e.g. caused by a rough sea or by strong rain. The accuracy of the estimation of the attitude, location and velocity is a function of the clutter surrounding the target, the distance of the target and its radar cross section. Finally, ships might be hidden beyond other ones or might appear as a single target although they are two. Besides collision avoidance radars are also used for surveillance purposes. For this reason, certain navigators want to hide from radar signals. A first option is to design stealth ships. This is an option used by the military and by some coast guards. It is costly and hardly accessible to criminals. The latter are more likely to resort to electronic countermeasures. The two main countermeasures to evade radar detections are again jamming and spoofing. Jamming means that the reflected signal is drown in a sea of noise, which makes it impossible to retrieve useful distance information. The angular location of the jammer is more difficult to hide.

Alternatively, the opponent might also induce the radar in error by generating false echoes. This might prevent a surveillance ship from moving any further towards the spoofer since it is expecting an obstacle between itself and the spoofer. It might also cause a regular ship to change its course and enter unsafe waters. This can be prevented if the radar uses waveforms under control of a cryptogenerator. In this case, the spoofer can no more predict the shape of the echoes. Radars are and should remain a central element for maritime collision avoidance, since they can also detect ships that are not transmitting AIS signals but their signals should be hardened in the manner described.

At DLR, Heymann is fusing AIS and radar information; see e.g. (Heymann, Banys, & Noack, 2014). This means that the AIS information is matched with radar targets. The augmented information is then displayed in an ARPA like manner on the ships display. Additionally, dark targets, i.e. targets that do not transmit AIS signals, can be marked by the transmission of an AIS message, which describes their navigational data. This prevents ships that are not equipped with radars from colliding with such objects.

In a future networked maritime world, radars can be further enhanced by using the multi-static principle. In this case, several radars cooperate: one radar is transmitting while several others are receiving the echoes. The measurement results are then exchanged and jointly processed. In the next cycle, another radar illuminates the scene and so on. This leads to a much better resolution in complex situations (Bethke, Röde, & Schroth, 2002) but requires a high rate link between the cooperating radars.

Sonars are similar to radars. They operate under water using acoustical waves. Sonars are typically used in shallow waters to prevent grounding. They might just be echo sounders

for determining the depth or they might image some portions or the whole sea floor under the ship. In the latter case, they could be used for navigation in areas with a stable sea floor. Since many harbors have a sea access through a river and a highly variable sea floor this is currently not considered. Sonars are not very suitable to locate other ships since the propagation along the surface is often unpredictable. Submarines are an obvious exception, here propagation is in the bulk of the water volume, and sonars are correspondingly used by submarines and by surface ships to locate each other.

6. Communications and Traffic Awareness

The above developments suggest that cryptographically secured radio links amongst ships should play an important role in e-navigation. Furthermore, the current data rates of a few kilobits at best must be increased substantially to cover the needs of a safe, secure and route optimizing system.

System	Use	Areas	Links	Technology
Navtex (Navigational Telex)	Navigation and meteorological warnings and forecasts, urgent safety information	All	All	**Digital**, Frequency Shift Keying (FSK) Medium (MF) and High Frequency (HF) 100 Bd
Maritime Very High Frequency (VHF) (Voice communications)	Vessel Traffic Service (VTS), general communications, search and rescue	All	Only ship-to-ship on high seas	**Analog**, Frequency Modulation (FM), Frequency division multiple access (FDMA) VHF: 156-162 MHz 25 kHz analog channels
Automatic Identification System (AIS)	Collision avoidance, also traffic awareness information, Aids to Navigation and Search and Rescue	All	Only ship-to-ship on high seas	**Digital**, Gaussian Minimum Shift Keying (GMSK), Self-Organized Time Division Multiple Access (SOTDMA) VHF: 161.975 and 162.025 MHz 9.6 kbps
Digital Selective Calling (DSC)	Distress signaling	All	Only ship-to-ship on high seas	**Digital,** FSK MF, HF, VHF 1.2 kBd
COSPAS/SARSAT	Distress beacon	All	GEO/MEO/LEO satellites in polar regions only MEO/LEO	**GPS-Positioning/Digital** UHF: 406.022-406.076 MHz Location Msg with 15,22, or 30 characters additionally Doppler positioning from LEO and MEO satellites
VHF Data Exchange (VDE)	Multiservice, bidirectional terrestrial and satellite system	All	All	**Digital:** Phase Shift Keying, FD-TDMA VHF: 156-162 MHz terrestrial: 300 kbps satellite: 240 kbps

Table 1: Maritime communications systems for voice and data (IALA, Maritime radio communica tions plan edition 2, October 2012). The areas are: port, coastal, high seas and polar. The links are ship-shore, ship-ship and ship-satellite.

Today communications are typically specialized for a particular application and narrow band. A VHF Data Exchange (VDE) System (IALA, Technical Characteristics for a VHF Data Exchange System in the VHF Maritime Moble Band, 2015) is a first promising step to change this situation. The request for a frequency allocation at the next World Administrative Radio Conference (WRC) in 2015 is under preparation (ITU, 2014). VDE shall have a ship-to-ship, a ship-to-shore and ship-to-satellite component. The associated satellites shall be Low Earth Orbiting (LEO) satellites. The terrestrial and satellite components shall share a piece of spectrum in a judicious manner. In the long-term, the whole maritime communication shall be migrated to generic digital channels using the frequency bands best adapted to the range that the signal, have to travel for reaching their destination. Besides collision avoidance, the main services used today include

› Dissemination of weather information, location of icebergs, lost containers and the like
› Distress signaling and beacons
› Coordination amongst ships, as well as with shore

Besides this, communication links are used by ship owners for logistics and for staying in contact with their crews as well as by passengers for telephony, internet access, and entertainment. Today, weather information is textual and Navtex - the system used – is a telex. This servive shall be migrated to VDE broadcast from shore or LEO satellites. Distress signaling is well covered: it might be by voice on VHF channel 16, by digital signaling through the Digital Selective Calling (DSC) system or by COSPAS/SARSAT beacons. The functions of coordination by Vessel Traffic Systems (VTS), of remote pilotage, and of joint decision making are currently handled by analog voice in the VHF band. They shall additionally be supported by VDE in the future. The latter system has the potential of taking-over an important role in all three functions (dissemination, distress signaling and coordination). VDE system is currently in the concept phase and is the most promising option for introducing security. Ship-owners have the option to communicate by any wide area standard, including geostationary (GEO) L-band systems, LEO L-band systems, and in the future VDE over LEO satellites. But even this information should be encrypted, not only for protecting ths shipowner's business but also for preventing pirates and terrorists to learn about the ship's position and load. Finally, passengers will use any system available. Large cruise ships provide on-board cellular and the like and use backhauling via GEO or MEO satellites. Table 1 lists the most important current and future systems relevant to maritime traffic coordination.

The establishment of trust in maritime traffic coordination is a central task that needs to

be solved. Trustworthiness is critical for most forms of deep cooperation – since such co-operation might put people, ships, and their cargo at risk if a malevolent party can either falsify or inject erroneous information. AIS can be seen as a first prototype for the exchange of sensor data. Some ideas for creating trusted reports were discussed in the context of AIS. The question will be how to keep track of trustworthiness or more precisely: how to identify pirate ships or ships that intend at harming others. Alarms triggered by the crew or by any form of tampering are certainly meaningful means for isolating information flows from and to ships. Departures from expected behaviors are other indicators that must be carefully analyzed as well. They may also be due distress situations. Pirates and rogue captains will do the outmost to not unintentionally trigger such alerts. Thus it is important that the whole sensor and communication system is built in a manner which prevents external manipulation.

7. Telecontrol

With telecontrol, pilots do not necessarily need to be on-board of ships while entering a port or passing a water way such as the panama channel. This would allow for a more effective use of the human resource "pilot", since they would not loose time for transfers and would not be locked-up with a ship during uncritical parts of the itinerary. The same shortage of resources also exits for captains and other skilled crew members. Automation might be a solution in this context. The EU has financed the project MUNIN to address these issues (MUNIN Project Web Page, 2012). Additionally, telecontrol could also reduce the chance that pirates take control of ships. In this context all systems would have to be secured in a manner that prevents a cyber capture of the ship.

For a serious consideration of telecontrol, the latter must be designed in such a way that the radio links are highly available, that radio link outages can be bridged by autonomous control and that the controls cannot be manipulated by breaking the cryptosystem. There is still quite some work to be done to achieve that.

8. Conclusion

E-navigation is a big opportunity for significantly reducing the number of collisions and groundings. It bears a huge potential for reducing the cost of operations and the environmental impact of maritime traffic. Furthermore, it provides means for surveillance in fishery, contraband, and most importantly for reducing the risk of piracy and terrorism. These goals can be achieved if the systems are properly designed from the start. In this case, the

cost impact of the additional functionality would not be very significant. We thus recommend that the specification of a secure e-navigation system and its deployment receive a high priority.

9. Acknowledgements

I would like to thank Thoralf Noack and Dr. Simon Plass, both at DLR, for their templates to Figure 2 and Table 1, respectively, as well as for critical discussions and comments on the article. I would also like to acknowledge interesting discussions with Dr. Frank Heymann from DLR on methods for the verification and complementation of AIS by radar.

10. References

ANavS. (2015). Retrieved 4 15, 2015, from http://anavs.de/products/

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A Security Evaluation of AIS Automated Identification System. ASAC'14. New Orleans, LA, USA.

Bethke, K.-H., Röde, B., & Schroth, A. (2002). Combination of Low Power Radars and Non-Rotating Sector Antennas for Surveillance of Ground Moving Traffic on Airports. Sensors 2002, Proc. of IEEE, 2, pp. 1690-1695.

Fernández-Hernández, I., Rijmen, V., Seco Granados, G., Simón, J., Rodriguez, I., & Calle, J. (2014). Design Drivers, Solutions and Robustness Assessment of Navigation Message Authentication for the Galileo Open Service. Preprint (see also ION 2014, Tampa Florida).

Galileo-OS-SIS. (2010). Galileo Open Service Signal-In-Space Interface Control Document. European Union.

Gallagher, S. (2012, May 10). North Korea pumps up the GPS jamming in week-long attack. Retrieved March 5, 2015, from Ars Technica: http://arstechnica.com/information-technology/2012/05/north-korea-pumps-up-the-gps-jamming-in-week-long-attack/

GPS Wing. (2012). GPS Interface Specification 200F. USAF.

Günther, C. (2014). A Survey of Spoofing and Counter-Measures. ION J. of Navigation, 159-177.

Helcom. (2014). Annual Report on Shipping Accidents in the Baltic Sea in 2013. Helsinki, Finland.

Heymann, F., Banys, P., & Noack, T. (2014). A pilot study of the advantage of radar image data over ARPA based position and bearing. Proc. ENC-GNSS 2014. Rotterdam, Netherlands.

Hornbostel, A., Cuntz, M., Konovaltsev, A., Kappen, G., Hettich, C., Mendes da Costa, C., et al. (2013). Detection and Suppression of PPD-Jammers and Spoofers with a GNSS Multi-Antenna Receiver: Experimental Analysis. ENC GNSS 2013. Vienna, Austria.

IALA. (2015). Technical Characteristics for a VHF Data Exchange System in the VHF Maritime Mobile Band.

IALA. (2012). Maritime radio communications plan edition 2.

IMO. (2006). e-Navigation. Retrieved March 5, 2015, from http://www.imo.org/OurWork/Safety/Navigation/Pages/eNavigation.aspx

IMO. (1972). COLREGS - International Regulations for Preventing Collisions at Sea.

ITU. (2014). Working document toward a draft new Report ITU-R M. [VDES] "Selection of the channel plan for a VHF data exchange system (VDES)" under WRC-15 agenda item 1.16. ITU-R WP5B Contribution 587.

Johnson, G., Swaszek, P., Alberding, J., Hoppe, M., & Oltmann, J.-H. (2014). The Feasibility of R-Mode to Meet Resilient PNT Requirements for e-Navigation. ION GNSS 2014, (pp. 3076-3100). Tampa, FL, USA.

Masala, C., Tsetsos, K. (2015). Maritime Cyber Security – Adapting to the Digital Age, in: Enge, Göge (eds.): Maritime Domain Cyber: Risks, Threats & Future Perspectives. Berlin.

Misra, P., & Enge, P. (2006). Global Positioning System, Signals, Measurements, and Performance (2nd Ed.). Lincoln: Ganga-Jamuna Press.

MUNIN Project Web Page. (2012). Retrieved 03 03, 2015, from http://www.unmanned-ship.org/munin/

Plass, S., Poehlmann, R., Hermenier, R., & Dammann, A. (2015). Global Maritime Surveillance by Airliner-Based AIS Detection: Preliminary Analysis. The Journal of Navigation, 1-15.

Skolnik, M. I. (2001). Introduction to Radar Systems (3rd Ed.). New York: McGraw-Hill.

Spoofing a Superyacht at Sea. (2013, 7 30). Retrieved 5 3, 2015, from http://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea

Ziebold, R., Dai, Z., Lanca, L., Noack, T., & Engler, E. (2013). Initial Realization of a Sensor Fusion Based Onboard Maritime Integrated PNT Unit. Transnav: Int. J. on Marine Nav. and Safety at Sea Transp., 7, pp. 127-134.

The Authors

Beckmeyer, Uwe

Uwe Beckmeyer holds the office of Parliamentary State Secretary at the Federal Ministry for Economic Affairs and Energy and is the German Government‘s Maritime Coordinator. Mr. Beckmeyer, who was born in Bremerhaven, has been a Member of the German Bundestag since 2002. From 2004 to 2011 he was spokesman for transport policy; since 2011 he has been coordinator for maritime affairs in the SPD parliamentary group in the German Bundestag. From 1987 to 1999 Mr. Beckmeyer was a Member of the Senate of the Free Hanseatic City of Bremen.

Klöcker, Georg

Georg Klöcker holds a Magister in political science, history and philosophy. He started his career within the German Army where he served the mountain troops in Mittenwald. After finishing university, Georg Klöcker worked as a research associate at the Center for European Integration Studies (ZEI) in Bonn where his work was focused on the consultancy of the three Baltic states and their way into the European Union and NATO. Between 2001 and 2006 he worked as Head of a Private Family Office in Zurich with a strong focus on Risk Management, before working as a senior risk consultant until 2011. Since 2012, Georg Klöcker acts as Managing Director of Marine Risk & Quality, a subsidiary of the Lampe & Schwarze Group in Bremen as well as Senior Advisor for Security Risk Management and Business Enablement matters for Lampe & Schwartze Marine Underwriting. He is a member of the Commission on Customs and Trade Facilitation at the International Chamber of Commerce (ICC) as well as speaker of the consortium Alliance for Risk Awareness & Solutions (ARAS).

Masala, Carlo

Prof. Dr. Carlo Masala, born March 27, 1968 in Cologne, studied political science, German and Roman philology at the university Cologne/Bonn from 1988-1992. Prof. Masala was a research associate at the institute of political science and European studies at the University of Cologne from 1992 to 1998. In 1996 he completed his dissertation on German-Italian relations from 1963-1969. In 1998 he was named academic council for life at the institute of political science and European studies at the University of Cologne. In the course of his work in the field of political science he received the venia legendi. In 2004 he was appointed research advisor at the NATO Defense College in Rome an in 2006 he was promoted to Deputy Director. During the last ten years, Prof. Masala was guest professor in Ann Arbor, Chicago, Washington, Monterey, in Shrivenham, UK, in Slovakia (Matje Belt University), in Italy (Rome and Florence) as well as at the Eastern Mediterranean University on Cyprus. In 2007 Prof. Masala was named professor for international politics at the Bundeswehr University in Munich. Since 2009 Prof. Masala is member of the academic board of German Ministry of Education and Science for the social studies in relation to security research. Together with Prof. Stephan Stetter he was the editor of the German scientific journal Zeitschrift für Internationale Beziehungen (ZIB) from January 2010 to June 2014. His research interests concentrate on theories of international relations, security studies, transatlantic relations as well as security-related developments in the wider Mediterranean region.

Tsetsos, Konstantinos

Dr. Konstantinos Tsetsos, born October 1, 1981 in Munich, studied political science, modern history and international law for social scientists at the Ludwig-Maximilia- University Munich from 2002 to 2008. He is a research associate at the institute of political science (professorship of international relations) at the University of the Bundeswehr Munich since April 2008. In the course of his academic work he participated and led various research projects concentrating on public security, maritime security, future studies, crisis early warning and political risk management. Dr. Tsetsos received a grant from the Hanns Seidel Foundation from 2010 to 2012 und completed his dissertation on conflict outcomes in asymmetric conflict in November 2014 with „summa cum laude". Next to his engagement at the University of the Bundeswehr Munich, Dr. Tsetsos is also lecturer at the Central European University in Skalica, Slovakia and the George C. Marshall Center in Garmisch-Partenkirchen. His research interests concentrate on maritime security, causes of war, theories of war, future studies, crisis early warning mechanisms as well as crisis management.

Günther, Christoph

Prof. Dr. sc. nat. Christoph Günther studied theoretical physics at the Swiss Federal Institute of Technology in Zurich. He received his diploma in 1979 and completed his PhD in 1984. He worked on communication and information theory at Brown Boveri and Ascom Tech. From 1995, he led the development of mobile phones for GSM and later dual mode GSM/Satellite phones at Ascom. In 1999, he became head of the research department of Ericsson in Nuremberg. Since 2003, he is the director of the Institute of Communication and Navigation at the German Aerospace Center (DLR) and since December 2004, he additionally holds a chair at the Technische Universität München (TUM). His research interests are in satellite navigation, communication, and signal processing.

Lampe & Schwartze KG
Herrlichkeit 5-6 | 28199 Bremen | Germany
P + 49 (0)421 5907-01 | F +49 (0)421 5907-139
mailbox@lampe-schwartze.de | www.lampe-schwartze.de/en

ISBN: 978-3-00-051014-4