Government
Office for Science

Foresight

Future of the Sea: Cyber Security

Foresight – Future of the Sea
Evidence Review

Foresight, Government Office for Science

Future of the Sea: Cyber Security

Professor Siraj A. Shaikh

August 2017

This review has been commissioned as part of the UK government's Foresight Future of the Sea project. The views expressed do not represent policy of any government or organisation.

Contents

Executive Summary

The UK's reliance on a secure and stable maritime sector makes maritime cyber security a key concern. This is particularly true for the security of seaborne trade, which makes up the vast majority of UK imports and exports. The UK National Cyber Security Strategy has clearly identified maritime infrastructure and vessels, as a class of cyber-physical systems, to be potentially vulnerable to interference from cyber threats. This potential vulnerability stems from a combination of increased connectivity and reliance on digital components, increased levels of autonomous control, and globally accessible navigation systems.

The scope of this review includes evidence accumulated to describe cyber security needs within the maritime sector, accounting for publicly reported cases of successful cyber attacks against the maritime infrastructure. A range of sources have been consulted including peer-reviewed publications, industry reports, government reports, and media sources vetted for credible reporting. The key findings are summarised below.

- Within the maritime sector, three broad categories of cyber attacks have been identified with a range of demonstrable impacts. These categories are defined by the target of the attack; enterprise and information assets, GPS and navigation systems, or critical control systems.
- Across these three types of attacks, a rise in criticality has been observed in terms of threat motivation, technical competence of attackers and complexity of employed attacks. The published evidence for the maritime threat landscape is sparse beyond the reported attacks.
- Some potential technological developments for the maritime industry merit special attention as they are expected to occur during the next 3–5 years. These include advances in communication, improved sensing, and intelligent and autonomous control systems. All three pose cyber security challenges as they build over existing digital technologies, allowing for broader access to ships and vessels, as well as making potential software-dependent weaknesses easier to exploit for malicious gain.
- Traditional engineering has focused on safety-critical design and development. Safety, however, is distinct from cyber security. Lessons from other sectors with parallel challenges suggest that both security and safety need to be incorporated across the engineering lifecycle to ensure such systems are safe from accidents and secure from deliberate threats.
- Enterprise IT systems used for typical office functions within the maritime sector need to be better protected with previously existing security mechanisms to counter commonly known threats.
- Navigation systems, which are critical to the maritime sector, should be paid particular attention in order to protect against skilled and targeted attacks.
- Advanced and sophisticated attacks may target a range of electronic and control systems for ships, vessels, offshore units and port systems. These need particularly highly coordinated responses including support from national technical authorities such as the UK's National Cyber Security Centre (NCSC).
- Other responses to mitigate against cyber security risks are also required to be cross-sector, including threat sharing and attack reporting systems, coordinated incident

response and capability development, and assurance and compliance regimes for sector adoption.

Acknowledgments

This review has benefited from discussions with the following people.

Luis Benito	Lloyd's Register
Tania Berry	Lloyd's Register
Chris Chung	Lloyd's Register
Ilesh Dattani	Assentian Partners
Tim Kent	Lloyd's Register
Bryan Lillie	Qinetiq
Joseph Morelos	Lloyd's Register
Paolo Scialla	Lloyd's Register
Melvyn Scott	Qinetiq
Vittorio Vagliani	Qinetiq
Adrian Venables	Royal Navy
Tom White	Lloyd's Register

1. What is Cyber Security?

The global maritime sector faces an increasing number of cyber threats, stemming from the sector's acknowledgement of its critical reliance on advances in technology (such as fully autonomous ships) and the growing state and non-state actors who challenge the sector with malicious intent. Cyber security for the maritime sector is therefore an important concern for the UK, which is reliant on shipping for trade and, with the inclusion of its overseas territories, has jurisdiction over a large area of ocean.

This review brings to the fore evidence, available in the public domain, to shape an informed view of the relevant priorities. Cyber security is taken to be defined as per the recently released National Cyber Security Strategy of the UK:

> Cyber security refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.
>
> HM Government (2016)

The strategy has also clearly identified 'cyber-physical systems' to be 'potentially vulnerable to interference' from cyber threats. Cyber-physical systems are usually engineered systems that bring together a mix of traditional electronics, advanced sensing and connectivity, and physical components (such as maritime infrastructure and vessels). This vulnerability is particularly so due to increased connectivity and reliance on digital components, increased levels of autonomous control and globally accessible navigation systems.

The Engineering Council's definition, relevant to our scope here, further serves to address what security means for systems like those increasingly seen in the maritime sector:

> Security can be defined as the state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts. It operates on a number of levels ranging from national security issues to countering crime. It includes preserving the value, longevity and ongoing operation and function of an enterprise's assets, whether tangible or intangible, and the handling of privacy issues such as the protection of personally identifiable information.
>
> Engineering Council (2016)

Cyber security measures need to protect assets against a range of low-level crime to national security concerns. Such assets could be tangible, for example ships, vessels, rigs, port equipment and navigation aids; or could be intangible, for example data, information services and supply chain elements. At an operational level, it is a mix of both types of assets that underpin the maritime sector. Therefore cyber security measures need to protect a complex set of assets.

The aim of this review is to bring together a diverse range of evidence that offers value going forward and allows for informed prioritisation in terms of policy making. The current scope of

such sources includes academic peer-reviewed publications (drawn from journals and conference proceedings), industry reports (drawn from credible industry organisations), consultancy house reports (drawn from a mix of UK and non-UK consultancy houses, specialising in cyber and maritime domains), government department and agency reports (where relevant content may be referenced), and wider public media and internet sources (vetted for credible reporting and plausible content).

2. Types of Cyber Attacks and their Impact

Any evidence from the maritime domain, in terms of reported cyber attacks, has to be evaluated for the nature of assets targeted and the level of disruption achieved. This in turn points to the type of response needed and associated needs for the UK. Three broad categories of attacks, identified below, give the available evidence for the maritime sector.

2.1 Attacks on Enterprise and Information Assets

Traditional IT systems, also known as enterprise systems, support organisations with data processing, communication and storage services. Enterprise systems are designed to achieve efficient digitisation of information services. Attacks on such systems aim to disrupt enterprise activities but could potentially result in theft of information that is far more damaging in terms of organisational services and objectives. The risks posed by such attacks are therefore low to medium, as enterprise data, operations and procedural aspects may be potentially violated, with no or very little physical disruption, and no loss of life. For the maritime sector, a number of such attacks have been reported including:

- A few maritime security and vetting firms targeted by Somali pirates and associates, resulting in web service disruption and information theft, with a view to aiding piracy (Frodl, 2012);
- Antwerp Port IT Systems breached, resulting in information breach, and on-premises theft of containers and disruption (Bateman, 2013);
- Automatic Identification System (AIS) shown to have inherent flaws resulting in disruption, spoofing and manipulation of information (Arnsdorf, 2013); and
- Islamic Republic of Iran Shipping Lines (IRISL) targeted with reports of operational data theft and loss (Torbati and Saul, 2012).

Such cyber attacks are usually low in sophistication, realising ‘commodity’ threats in cyber space, and commonly result from lack of a good organisational cyber ‘hygiene’. These kinds of attacks take advantage of common technological weaknesses and, with the number of tools that have emerged over the years to automate such attacks combined with increased connectivity, it takes increasingly little skill to launch such attacks.

2.2 GPS and Navigation Attacks

Certain virtual-technology-driven attacks take advantage of design issues and inherent vulnerabilities, exploited to undermine services dependent on such technologies. GPS and navigation technologies, given their acute use in the maritime sector, are a particular target that have come under close attention. The risks posed by any such attack is medium to high as, alongside data and operation protocol violation, there is potential for physical damage. A number of attacks are reported that attempt to abuse this set of technologies including:

- GPS signals spoofed to alter the course of a vessel without any alarms going off to warn of any manipulation of the system (Vass, 2013);
- Reported GPS Jamming around Incheon in South Korea, reportedly instigated by North Korea, affecting navigation for planes, ships, buoys (GPS World, 2016); and
- US oil company offshore drilling unit, in the Gulf of Mexico, suffered an accidental malware upload through an employee to affect communication links with the navigation system (Roberts, 2013).

Such cyber attacks are generally medium to high in sophistication, realising the inner workings of a certain set of technologies (in this case, communication message formats and timing details), and result from the design and standards involved in providing GPS and navigation systems.

2.3 Advanced Persistent Threats

With the aim of disrupting national security, advanced cyber attacks typically target control systems and other complex systems (that bring together advanced electronics, software and mechanical technologies) to cause maximum damage, including actual physical disruption or damage. These originate from either state or non-state actors often driven by motivation to achieve political goals. The intent is established through the level of preparation and resources deployed, typically including intelligence gathering using a mix of digital and other means, theft of state secrets and location of assets, industrial espionage to subvert technological safeguards, and the level of skills and know-how used to deliver the attack.

The maritime infrastructure offers a number of critical assets that could be targets for such attacks. These include ports and related land-based assets, ships and smaller vessels, as well as satellite communication, positioning and navigation systems. The risks involved here are very high as the nature of systems violated means that physical disruption or damage is likely to occur, with possible loss of life, alongside sensitive state, infrastructure and personal data theft or exposure. Three examples of such attacks are found in the maritime sector:

- Japanese and Korean maritime and shipbuilding concerns suffered targeted and advanced phishing attacks, exfiltrating valuable and sensitive information over an extended period (Coast Guard Maritime Commons, 2015);
- Control systems on a drilling rig being constructed in South Korea were infected with malware resulting in rig being moved off shore and shutting down for several days (Shauk, 2013); and

- US Transportation Command (Transcom) contractors compromised by several advanced cyber attacks, targeting onboard systems with potential loss of confidential data (Stamford, 2014).

Overall, the above lists are a selection of ten attacks that have been reported. The categorisation is deliberate to highlight the increasing criticality in terms of threat motivation, technical competence and complexity employed to conduct the attacks. While it is hard to judge the level of impact from what is reported, the potential impact in terms of disruption and damage grows as the level of sophistication increases across the three categories.

The assessment based on reported attacks is important to account for technological dependencies across the maritime infrastructure and to provide an initial assessment of where known cyber threats and risks lie. It should be noted that evidence for the maritime threat landscape is sparse beyond the reported attacks.

3. How are Maritime Cyber Security Needs Projected to Change?

Some technological developments for the maritime industry merit special attention as they are imminent over the next 3–5 years and would be almost entirely driving the landscape of cyber security threats for the sector. Of particular interest here are three categories of technology including communication, sensing, and autonomous control. As the availability and adoption of such technologies grow (Lloyd's Register, 2015), their integration is expected to converge across the maritime platforms. This will be a step change in the nature of design and engineering involved to ensure safety and cyber security. This sections attempts to address this challenge and refers to lessons from other sectors with parallel challenges.

The National Cyber Security Strategy makes clear that the industrial and regulatory landscape needs to acknowledge the responsibility and liability that such a trend would bring with it:

> Organisations and company boards are responsible for ensuring their networks are secure. They must identify critical systems and regularly assess their vulnerability against an evolving technological landscape and threat. They must invest in technology and their staff to reduce vulnerabilities in current and future systems, and in their supply chain, to maintain a level of cyber security proportionate to the risk. They must also have tested capabilities in place to respond if an attack happens. For the CNI [Critical National Infrastructure], they must do this with government bodies and regulators so we can be confident that cyber risk is being properly managed and – if it is not – intervene in the interests of national security.
>
> HM Government (2016)

An important element of this digital revolution is increasing reliance on digital communication. With the mix of heightened sensing and more data processing, a range of data communication scenarios come to fore including satellite navigation systems, weather reporting, electronic aids

for docking and manoeuvre, diagnostic systems and platform health monitoring, and weather reporting. Such communication links need to be therefore better protected, as such:

> Information will help determine whether these systems are working correctly and in the most efficient manner possible. When a critical part starts to fail, preventative maintenance can be scheduled at the next port of call or, if need be, by dispatching people to make repairs while the ship is still at sea.
>
> (Levander 2017)

Cyber security challenges only add to the above as their interconnected nature means that such isolated subsystems serve together to make critical functions open to abuse. Successful attacks against similar environments have been carried out against tyre pressure wireless sensors (Lemos, 2010) and more critical components (Greenberg, 2015) within the automotive industry. This has already brought legal challenges for the industry, with a class action lawsuit last year to hold Toyota, GM and Ford accountable for “dangerous defects” (Stanley Law Group, 2015). The lawsuit has since been unsuccessful and dismissed, but has raised debate within the automotive industry around product liability and manufacturing practices around cyber security.

Advances in sensing and intelligent control systems are driving the development of autonomous ships (Levander, 2017) and underwater vessels (Nicholson and Healey, 2008). In a wider context, this is an opportunity to push the boundaries of design, performance and operational safety. Remote vessel control can lower the risk from pirates due to uncrewed vessels and have light and sleek designs as certain elements, such as crew occupancy, ventilation and heating, could give way to greater cargo capacity. This could ultimately cut fuel consumption, as well as reducing operating and construction costs. The engineering reality of autonomous control is one of complex physical and software integration with a potentially high cost of failure, such as in the case of the fatal accident of a Tesla Autopilot-driven car in 2016 (Ackerman, 2016a).

What does this mean for the technology integration and platform engineering needs of the future? Traditional engineering methods have coped with safety-critical systems engineering of such ships and vessels with modelling and design techniques focused entirely on safety and with little thought to security. Not only are accidents to be avoided but systems need to be designed to defend against malice and manipulation with intent (to cause damage). Early research suggests that designing secure safety-critical systems poses a substantial challenge (Oates *et al.*, 2013; 2014) with a view that engineering “complex embedded-and cyber-physical systems requires a holistic view on both product and process” (Schlingloff, 2016). This implies a clear need for best practices and compliance standards, alongside rigorous engineering, that incorporate both security and safety. The notion of ‘risk-based systems engineering’ (Oates *et al.*, 2016) is therefore one way forward that acknowledges cyber security risks in the systems engineering lifecycle.

Lessons borrowed from other divisions such as the automotive sector, which is having to deal with similar challenges, affirm that despite rigorous functional safety standards, both security and safety need to be incorporated across the engineering lifecycle. Traditional approaches as proving grounds for testing security and safety concerns do not address the increasing complex design of such cyber-physical platforms. These platforms require greater integration complexity, which ultimately leads to more difficult testing (BBC News, 2016); software-related product recalls (Dixon, 2014) are a testimony to that. Indeed three of the main implementation needs for autonomously controlled ships, acknowledged by the maritime industry (Rolls-Royce, 2016), include:

- Errors and malfunctions in software;
- Disturbances, malfunctions and vulnerabilities in data communication connections; and
- Undue trust on the capability and flawlessness of ICT systems.

Beyond the technical, the human and legal dimensions take over. Some potential cyber security challenges would emerge when human error results in data breach, or data protection has to be enforced strictly across some of the advanced maritime platforms and services. However, such use cases are yet to emerge.

Autonomy brings with it also the challenge of jurisdictional liability and responsibility in international waters. How do current treaties and legislative frameworks govern autonomous operations, including the accidents and violations that may arise from this? The ethical dimension of autonomy (Goodall, 2016) is yet another question mark over the design dynamics (Ackerman, 2016b) that potentially plays out in autonomously controlled transport.

4. Evidence and Existing Guidance to Inform the UK's Cyber Security Response for the Maritime Sector

The maritime sector's growing cyber security needs are likely to require a response at various technological and policy levels in the UK. Based on available guidance and the expert opinions presented in this document, this review has identified a number of potential ways to protect against the types of attack described above[1].

4.1 Protection against Threats to Traditional IT Systems and Information Breaches

Protection is generally seen to require:

- Secure enterprise IT and operational systems, with robust information and resource access control;
- Robust design and deployment of information exchange services and supporting infrastructure to ensure integrity, availability, authentication, and privacy; and

[1] It is worth mentioning here the existing sector-wide high-level guidelines that serve to address a mix of socio-technical risks that emerge from the maritime cybersecurity. Notably these include:

- The guidelines for cybersecurity onboard ships by the Baltic and International Maritime Council (BIMCO), addressing risk assessment, technical and procedural risk reduction, incident response, investigation and contingency planning (BIMCO, 2016); and
- The analysis of cybersecurity aspects for the maritime sector by the European Network and Information Security Agency (ENISA), which place an emphasis on raising awareness, maritime governance and regulation, and cross-sector collaboration (ENISA, 2011).

- A minimum level of user awareness and training to ensure compliance and operational vigilance.

Appropriate regulation and legislation may be required across the sector to incentivise the areas mentioned above. Such enterprise-level incidents need best practice and security baselines enforced to counter against known common threats, examples of which include the NCSC's Cyber Essentials scheme .

4.2 Securing Navigation Systems

Specific, operation-critical, technology platforms, such as navigation systems, are vulnerable to cyber attacks. They can be strengthened against attacks through:

- Well-designed secure and resilient communication systems;
- Built-in redundancy for safe operation even in case of failures; and
- Manually driven response, navigation and control in case of total loss of service.

Navigation and associated communication critically underpins the maritime sector. Protecting them requires coordination across the sector to ensure a collaborative response to ensure safety of all entities that may be affected. Such systems also require secure design and development to instil rigour and robustness.

4.3 Countering Advanced Persistent Threats

The high-level threats described above require:

- Highly capable monitoring and detection deployed to protect and provide early warnings;
- Critical systems designed with advanced measures to counter malware infections, alongside measures in place to minimise physical damage and disruption; and
- Incident reporting, response and management in place to efficiently escalate risk mitigation, forensics and law enforcement coordination.

Stealthy and state-sponsored attacks need close cooperation with national threat and intelligence agencies to mitigate and coordinate against attacks. The UK's NCSC (BIMCO 2016), including CPNI , are well placed to play a central role for this purpose. Sector-led reporting, resilience and deterrence efforts are also likely to be required to counter advanced threats.

4.4 Cross-Cutting Priorities for Securing the Maritime Sector

Three further cross-cutting issues emerge from the evidence above and industry consultation:

- The importance of instant and efficient feedback on cyber attacks to reduce the risk of repeat attacks by ensuring that lessons are immediately learnt and preventative practices are adopted by all within the sector;
- Coordination of incident response and cyber capabilities, to assist with incident management (in terms of capability, knowledge and advice); this is likely to be particularly important in cases where a number of inter-dependent infrastructure and vessel operators are affected;
- Security assurance and compliance regimes, particularly for safety-critical components onboard vessels, rigs and port infrastructure (Lloyd's Register, 1995). Such regimes become particularly important as technological advancement is combined with increasingly critical tasks. The maritime sector is reliant on two particular areas:
    - Complex software systems, such as GPS navigation, where a combination of large amounts of data, algorithmic complexity and distributed processing results in increased difficulty in implementing secure design, development and operation; and
    - Cyber-physical systems, such as sophisticated and autonomous cargo ships (Levander, 2017), which comprise of a heterogeneous array of different systems that combine physical components (electronic or mechanical) alongside typical software components. This makes it challenging to protect for physical safety against cyber attacks that manipulate software parts of such systems.

References

Ackerman, Evan (2016a) Fatal Tesla Self-Driving Car Crash Reminds Us That Robots Aren't Perfect. 1 July, *IEEE Spectrum*. http://spectrum.ieee.org/cars-that-think/transportation/self-driving/fatal-tesla-autopilot-crash-reminds-us-that-robots-arent-perfect

Ackerman Evan (2016b) People Want Driverless Cars with Utilitarian Ethics, Unless They're a Passenger. 23 June, *IEEE Spectrum*. http://spectrum.ieee.org/cars-that-think/transportation/self-driving/people-want-driverless-cars-with-utilitarian-ethics-unless-theyre-a-passenger

Arnsdorf, Isaac (2013) Phantom Ships Expose Weakness in AIS Vessel-Tracking System, 29 October, *Bloomberg*. https://www.bloomberg.com/news/articles/2013-10-29/phantom-ships-expose-weakness-in-vessel-tracking-system-freight

Bateman, T. (2013) Police Warning after Drug Traffickers' Cyber-Attack. 16 October, *BBC News.* http://www.bbc.co.uk/news/world-europe-24539417

BBC News (2016) Google's Self-Drive Cars had to be Stopped from Crashing. 13 January, *BBC News.* http://www.bbc.co.uk/news/technology-35301279

BIMCO – Baltic and International Maritime Council (2016) The Guidelines on Cyber Security Onboard Ships. Bagsvaerd, Denmark: BIMCO. https://www.bimco.org/news/press-releases/20160104_cyber_security_guidelines

Coast Guard Maritime Commons (2015) Coast Guard Commandant on Cyber in the Maritime Domain, 15 June, United States Coast Guard, http://mariners.coastguard.dodlive.mil/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain

CPNI – Centre for Protection of National Infrastructure (UK) website. HM Government. https://www.cpni.gov.uk

Cyber Essentials (UK) website. HM Government. https://www.cyberaware.gov.uk/cyberessentials

Dixon, Hayley (2014) Toyota Recalls Every Third Generation Prius over Software Glitch. 12 February, *The Telegraph.* http://www.telegraph.co.uk/motoring/car-manufacturers/toyota/10632703/Toyota-recalls-every-third-generation-Prius-over-software-glitch.html

Engineering Council (2016) Guidance on Security. London: Engineering Council (UK). http://www.engc.org.uk/security

ENISA – European Network and Information Security Agency (2011) Analysis of Cyber Security Aspects in the Maritime Sector. November. Heraklion, Greece: ENISA https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/dependencies-of-maritime-transport-to-icts

Frodl, Michael G. (2012) Pirates Exploiting Cybersecurity Weaknesses in Maritime Industry. *National Defense magazine*, May. https://www.safety4sea.com/pirates-exploiting-cybersecurity-weaknesses-in-maritime-industry

Goodall, Noah J. (2016) Can You Program Ethics into a Self-Driving Car? 31 May, *IEEE Spectrum*. http://spectrum.ieee.org/transportation/self-driving/can-you-program-ethics-into-a-selfdriving-car

GPS The Global Positioning System, US Government. http://www.gps.gov

GPS World (2016) State Department Issues Notice on North Korean Jamming, 8 April, http://gpsworld.com/state-department-issues-notice-on-north-korean-jamming

Greenberg, Andy (2015) Hackers Remotely Kill a Jeep on the Highway – With Me In It. 21 July, *WIRED*, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

HM Government (2016) National Cyber Security Strategy 2016 to 2021 (UK). https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Lemos, Robert (2010) Wireless Car Sensors Vulnerable to Hackers. 10 August, *MIT Technology Review.* https://www.technologyreview.com/s/420168/wireless-car-sensors-vulnerable-to-hackers

Levander, Oskar (2017) Forget Autonomous Cars – Autonomous Ships Are Almost Here. 28 January, *IEEE Spectrum*. http://spectrum.ieee.org/transportation/marine/forget-autonomous-cars-autonomous-ships-are-almost-here

Lloyd's Register (1995) Software Conformity Assessment: Procedure SC94. London: Lloyd's Register of Shipping. https://goo.gl/a4dekm

Lloyd's Register (2015) Global Marine Technology Trends 2030. 31 August, Lloyd's Register, Qinetiq and University of Southampton, http://www.lr.org/en/news-and-insight/news/global-marine-technology-trends-2030.aspx

NCSC – The National Cyber Security Centre (UK) website. HM Government. https://www.ncsc.gov.uk

Nicholson, J.W. and Healey, A.J. (2008) The Present State of Autonomous Underwater Vehicle (AUV) Applications and Technologies. *Marine Technology Society Journal* 42 (1), 44-51.

Oates, R., Thom, F. and Herries, G. (2013) Security-Aware, Model-Based Systems Engineering with SysML. BCS Learning and Development Ltd. Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research, 78-87. https://pdfs.semanticscholar.org/15b5/aba68745dada600e031160fdde1b003e5cce.pdf

Oates, R., Foulkes, D., Herries, G. and Banham, D. (2014) Practical Extensions of Safety Critical Engineering Processes for Securing Industrial Control Systems. System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International. http://ieeexplore.ieee.org/document/6725793

Oates, R., Malysz, V. and Melville, R. (2016) Cyber Security Risk Management of Maritime Systems. *Engineering & Technology Reference.* http://digital-library.theiet.org/content/reference/10.1049/etr.2016.0015

Roberts, John (2013), GPS flaw could let terrorists hijack ships, planes. 26 July, *Fox News Tech*. http://www.foxnews.com/tech/2013/07/26/exclusive-gps-flaw-could-let-terrorists-hijack-ships-planes.html

Rolls-Royce (2016) Safety and Security in Autonomous Shipping – Challenges for Research and Development, in *Remote and Autonomous Ships: The next steps*. London: Rolls-Royce, plc and Advanced Autonomous Waterborne Applications (AAWA), 56-73. http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf

Schlingloff, B.-H. (2016) Cyber-Physical Systems Engineering. In Z. Liu and Z. Zhang (eds) Engineering Trustworthy Software Systems. *Lecture Notes in Computer Science*, vol. 9506. Switzerland: Springer, 256-289. https://link.springer.com/chapter/10.1007/978-3-319-29628-9_5

Shauk, Zain (2013) Malware Offshore: Danger Lurks Where the Chips Fail. 29 April, *fuelfix.* http://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail

Stamford, Eric M. (2014) Sophisticated Scams Highlight Growing Cyber Risk to Shipping. 10 October, *TradeWinds*, 12. http://www.tradewindsnews.com/weekly/346334/Sophisticated-scams-highlight-growing-cyber-risk-to-shipping

Stanley Law Group (2015) Class Action Lawsuit Filed to Hold Toyota, Ford and GM Accountable for Dangerous Defects Allowing Cars to be Hacked and Drivers to lose control. 10 May, *PR Newswire*, http://www.prnewswire.com/news-releases/class-action-lawsuit-filed-to-hold-toyota-ford-and-gm-accountable-for-dangerous-defects-allowing-cars-to-be-hacked-and-drivers-to-lose-control-300048163.html

Torbati, Yeganeh and Saul, Jonathan (2012) Iran's Top Cargo Shipping Line Says Sanctions Damage Mounting. 22 October, *Reuters World News.* http://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022

Vass, Lisa (2013) $80 Million Yacht Hijacked by Students Spoofing GPS Signals. 31 July, Naked Security (Sophos). https://nakedsecurity.sophos.com/2013/07/31/80-million-yacht-hijacked-by-students-spoofing-gps-signals

This publication available from www.gov.uk/go-science

Contacts us if you have any enquiries about this publication, including requests for alternative formats, at:

Government Office for Science
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000
Email: contact@go-science.gsi.gov.uk