Forensic Readiness within the Maritime Sector

Kimberly Tam
kimberly.tam@plymouth.ac.uk
University of Plymouth

Kevin Jones
kevin.jones@plymouth.ac.uk
University of Plymouth

Abstract—**Forensic investigation is an essential response strategy following a cyber-related incident, and forensic readiness is the capability to gather critical digital information and maximize its use as evidence. The effectiveness of this data is highly dependent on the readiness, quality, and trustworthiness of the data itself. Far from a passive post-analysis tool, there have been many instances where an organization has benefited from gathering, and using, digital evidence to improve their cyber-security and mitigate future incidents. This article examines the forensic readiness of the maritime sector, a core component of global trade and a unique combination of information/operational technology and people, to understand its investigation and mitigation capabilities. Once the readiness of maritime forensic investigation has been better understood, by comparing it to other sectors and using risk scenarios, this paper proposes actions toward improvement. These steps are built from established attempts to increase investigation capabilities and improve maritime cyber-security, but address the maritime sector specifically.**

Index Terms—**forensic readiness, cyber, maritime, risk**

I. Introduction

Currently 90% of worldwide trade is transported by ships and handled by ports [1], [2]. In terms of value, e-commerce alone was last estimated at £26 trillion in 2018 [3]. As such, maritime transport is an integral part of the global infrastructure and events that damage, delay, or misplace shipments can have significant widespread effects on a nation's economy, stability, and people. In 2011, the first EU maritime-cyber report showed alarmingly low awareness and protection, and more recent studies highlight significant concerns as technology advances faster than it can be fully secured [4], [5]. Other studies have revealed more specific maritime-cyber vulnerabilities [6], [7] or how behind maritime cyber-security is [8]. However, there is currently no wider understanding of the maritime cyber-threat due to the low amount of evidence available both publicly and internally. This gap has not gone unnoticed, as the UK Department for Transport recently released a call to gather evidence in areas like maritime security [9]. This is an indication that the cyber-forensic capabilities within modern shipping are currently insufficient.

While forensic readiness and cyber-related investigations are a regular practice in other sectors, it is less prevalent in maritime, particularly within ship operations. As shipping becomes more technologically advanced, and with the rise of remote-control and autonomy within ports and ships [10], [11], cyber-risks also grow. It is also important to note that port-side and ship-side forensic readiness are not currently equal. As a large part of port infrastructure is more similar to other shore-based IT-based businesses, they can gain forensic capabilities from existing frameworks and protocols. Ship-side systems, however, are both less well understood forensically and unique to maritime, making existing solutions harder to adapt.

The forensic readiness of individual sectors worldwide have not developed similarly over time, as change is heavily influenced by events and sector-specific risks. For example, in a business context like financial banks, there was no incentive or opportunity to actively collect cyber-related evidence (e.g., transactions, logs, emails, network captures) until significant funds were threatened. Banks were initially wary of sharing cyber-vulnerabilities with competitors, and it was not until benefits outweighed the risks did they collaborate [12]. Evidence gathered by the finance sector since then, anonymized to protect individuals, is collected in advance of an incident and serves both the collecting organization and wider sector. Particularly when responding to an event, e.g. data breach, readiness for quick and thorough investigations are pivotal for a quick recovery with minimal financial or reputation damage.

Similarly, transportation sectors airborne or on land (e.g., trains) were somewhat lacking in forensic readiness until significant risks arose. Certain risks, ranging from general concerns to terrorism [13], [14], encouraged these sectors to be forensic ready. Compared to shipping, incidents in these sectors are also more visible to the public, whose opinion can drive decisions. Unlike other businesses primarily based information technology (IT) (e.g., finance), transportation sectors also require operational technology (OT) for physical actions. This mandates forensic capabilities for cyber-physical events as well, an overlap of cyber and physical worlds [14]. In maritime, while forensic readiness for physical events and human error are currently held to high standards, readiness for cyber-related events has yet to reach the same levels.

The paper is organised as follows. Section II establishes what forensic readiness is for maritime, considering ports, ships, IT, and OT. Section III continues to evaluate maritime forensic capabilities today, particularly when facing current risks. This includes a range of cyber, cyber-physical incidents that this industry will likely need to be prepared for. Lastly, Section IV proposes steps for increasing forensic readiness within the maritime sector, similar to previous business IT focused forensic readiness plans [15].

II. Establishing Forensic Readiness

To evaluate the forensic readiness of the evolving maritime sector, i.e. its ability to accurately depict cyber-related events using evidence, we analyse its current capabilities for gathering, storing, and investigating with forensic data. Digital evidence is essential in managing the impact of risks, particularly in this digital age [16], and as both cyber and cyber-physical risks rise at port and at sea. This article define cyber-physical, based on [14], [17], as physical attacks with a cyber-element aid or outcome, cyber-attacks made possible with physical action, or cyber-attacks with physical outcomes.

Despite several known risks [6], [18], surveys show that the sector is, on the whole, not prepared for detailed investigations. Of the 350 individual respondents in [18], 16% have reported their own company was victim of a cyber-related incident within the last 12 months, however, only 56% of participants had a business continuity plan, making it likely that even a smaller percentage of those organizations is suitably forensic ready. Participants also claimed 33% of incident response and recovery took days or weeks, however, as this is based on personal responses and not digital evidence, it is likely that some incidents, particularly sophisticated ones, have gone unnoticed, unreported, or misclassified as human error [11].

Considering accidents and attacks, with outcomes ranging from minor to major, cyber to physical, if digital evidence is not gathered prior and during a maritime incident, it may be too late to do so later. The cyber-element is also not easily seen, particularly when crew are untrained to recognize it (which Section IV tries to improve) and systems are not configured to store digital evidence. For example, navigation ECDIS (Electronic Chart Display and Information System) systems normally have an underlying Windows OS running out of sight [19]. Ship crew, normally, only ever see the ECDIS application running, making human-in-the-loop detection unlikely. Additionally, there are no International Maritime Organization (IMO) requirements for cyber-related ECDIS evidence to be stored, which may illustrate low forensic capabilities [20]. By analysing regulations set by the IMO and others for ships (e.g., sensors, communication, navigation [6]) and ports (e.g., business IT, terminals, industrial control systems, monitoring [10]), there is a low likelihood that the average organisation are using forensic-ready systems. This is dangerous considering the malicious players in existence [7].

A. Forensic Readiness in Ports

Ports globally handle operations off-shore, on-shore, inland, manually, semi-autonomously, and autonomously [10]. Their forensic readiness can be divided into two areas; the well-known IT business and the IT/OT management of cargo and ships. With most IT systems, forensic readiness is relatively standard, centred around on work machines, devices like smartphones, company servers, communication channels (e.g., email, telephone, Skype) and networks (e.g., internet, intranet) [16]. In comparison, OT systems and networks like SCADA [21] may include machinery (e.g., cranes), sensors (e.g., temperature), cyber-physical security (e.g., electronic locks) and other intelligent devices. Digital evidence such as CCTV, digital and physical access logs, and transfer of privileges are also useful. Based on recent events, it is likely that the business side of ports is somewhat forensic ready, as the recent MAERSK and COSCO events [22], [23] showed them able to quickly understand and patch vulnerabilities.

The operational technology of ports, however, is not as well established. This includes the loading and unloading of cargo and the servicing (e.g., mooring, refitting, refuelling) of ships. One example of a gap in forensic readiness was demonstrated in the late analysis port terminal vulnerabilities used to smuggle [10]. Although physical security of these terminals may have been increased to restrict access, and the business side was improved to reduce infection vectors, it does not seem like the forensic readiness of these terminals have been increased. Therefore it is unclear what the current state of digital evidence collection is, however ship-based smuggling (e.g., drugs, weapons) and human trafficking are still massive problems in the modern world [24], [25]. Better evidence, in quantity and quality, is likely needed to improve the situation.

B. Forensic Readiness on Ships

Unlike ports, the risks and forensic needs of ships are highly divergent from traditional systems [6] and past studies [15] do not address the unique aspects of maritime transportation. In addition to the storage of log files etc., it becomes necessary to retain digital evidence on location, cargo status, fuel, and bridge readings from systems like ECDIS and RADAR [26]. While a number of physical-related evidence is stored digitally and used by the UK Marine Accident Investigation Branch (MAIB), there are currently no procedures set in place to even identify the necessary forensic evidence sources for cyber-related events, let alone gather and analyse them.

The MAIB currently investigates physical incidents using evidence stored in the maritime equivalent of an airplane "black-box" [27]. Unfortunately, it does not currently have the ability to store cyber-related evidence as the system interface language used does not support it. Furthermore, individual IMO regulations do not require cyber-related evidence to be made available. Knowing the practices and technical limitations of ship systems, it is safe to establish that ships are not forensic ready for cyber-related events, despite them being found vulnerable [4], [7], [11] and responsible for some of the largest cases in illegal trafficking [24], [25]. An added complexity with evidence stored locally on a ship, often at sea for months, are insider threats which could tamper with evidence [28]. If implemented correctly, however, forensic evidence could help deter the growing number of external (e.g., pirate) [29] and internal crime [30], [31].

III. Maritime Cyber Investigation Needs

One of the foremost issues in assessing this sector's forensic needs is understanding the scope and range of cyber-risks [17]. While there are well-known risk assessment tools like NIST, as currently defined they are unlikely to provide full comprehensive risk views within maritime. Most noticeably, the NIST frameworks primarily considers IT, with little coverage of OT in a maritime setting or interconnected IT/OT [32], [33]. NIST may be applicable to ports, however, on ship IT/OT systems there is an added complexity of frequent changes

TABLE I
SCENARIO NUMBER AND CYBER-RISK DETAILS [17].

1	Malware is introduced to the ship bridge via USB with required chart updates and causes system to lag.
2	Autonomous ship software needs to be updated remotely but satellite connection is vulnerable
3	Localized jamming is used on a ship of high value with the aid of social engineering to install jamming device
4	Shore-based jamming delays operations of a river-ferry that relies on ship-to-shore radio signals to dock
5	Denial of sensor readings for critical operations causes crew confusion and reduces their confidence in bridge sensor readings
6	Traffic jam at geographic choke-point, a tunnel or strait, caused by lost connection with engine
7	GPS spoofing causes incident with a new high-profile ship, causing huge reputation damage to the shipbuilders
8	Navigation misdirection caused by spoofing virtual buoys to increases ship-shore collision risks in low-visibility conditions

in environmental, personnel, and technical factors, as ships move physically and through cyberspace. This also may make NIST less applicable to the range of ship types and crimes (e.g., information theft, physical theft, damage, misdirection). Lastly, isolation and limitations during transit negatively affect ship risks in a way most assessments do not measure, so risk assessment frameworks designed for maritime, like [26], may reveal more risks with more realistic risk profiles. These may better describe the risk impacts and better define the evidence requirements for future investigations, how to obtain the evidence, and how use it to mitigate those risks.

Once maritime organizations fully recognize the need for investigative capabilities to combat risk, its next step is to ensure it is forensic ready across both IT and OT systems. IT/OT convergence is prevalent and growing in this sector [26], as a number of both system types work in conjunction. Compromising one or more of those systems could lead to a number of cyber and/or physical outcomes.

To illustrate how forensic evidence can help investigate maritime-cyber risks, we adapted risk scenarios from [17] into Table I and made Table II. Most cyber-related, and some physical, evidence in Table II are not currently gathered, demonstrating what categories of new evidence would be useful to properly investigate these kinds of risk scenarios. While evidence in some categories (i.e., environmental, video, and audio) are being gathered for investigating human action and physical incidents, new subcategories for cyber will need to be introduced for more comprehensive forensic readiness, e.g. third-party networks. Physical evidence is also not exclusive to OT, for example, scenario 8 would require evidence such as position, but physical evidence in scenario 5 would be derived from the OT systems responsible for engine and fuel.

The last question before discussing potential steps for improving maritime forensic readiness, is whether organizations have the funding for it. In general, companies have been persuaded by the recent, large-scale, and expensive cyber-incidents to raise their security budges by at least 5% in 2019 [34]. It is likely the maritime will follow this trend, if not surpass it, given the most recent and viable incidents recently [22], [23] and current budget trends [18].

TABLE II
EVIDENCE NEEDED TO INVESTIGATE TABLE I SCENARIOS.

Scenario	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Computer	C/P	C			C/P	C/P	C	C
Network/Comms		C		P	C/P	C/P	C	C
Video/Audio	C/P		P		P	C/P		P
Supply chain	C/P	C			C/P	C/P		C
Environment			P	P		P	P	P
Sociotechnical	C		C		C	C	C	

C = cyber evidence   P = physical evidence

IV. STEPS FOR FORENSIC READINESS IN MARITIME

From the content in Sections II and III, this section proposes steps to improve the gathering of cyber-related evidence in the maritime sector, without interfering with shipping operations and business processes. The end-objective is to set in place procedures and evidence standards so maritime organizations, including individuals across this sector, can fully investigate potential crimes, accidents, and disputes to minimize negative impacts and improve general safety in several capacities. As discussed previously, this is only possible if investigations are made using useful, trustworthy data by the proper parties.

To acquire the most effective set of IT/OT evidence in the maritime context, we propose the seven following steps, similar to established patterns of general forensic readiness [15]. Unlike previous studies, the following seven-step procedure is aimed at improving the forensic readiness of ports and ships. It is likely that these will have a more significant impact to ship security due to the current levels of forensic capabilities.

Step 1 Define the range of risk scenarios involving ship and port environments (e.g., [26]) to determine their requirements for readily available digital evidence. This, effectively, is a risk assessment that would consider human, IT, and OT assets. Each organisation should preform the appropriate assessments as a fishing boat will have a different risk profile than a fully autonomous cargo port. Organization should also determine compliance with legal constrains and commercial agreements.

Step 2 Identify sources and endpoints, within IT/OT systems, internally and externally for various types of evidence (e.g., logs, screenshots, network captures, voice). Namely which systems (e.g., IT servers, ship sensors) generate data including format, amount, and frequency and what the end consumers of that data is. The endpoints of data can be categorized in normal business (e.g., shipping efficiency) and incident-related evidence. Organizations may also clearly determine the ownership of certain data to establish responsibilities.

Step 3 Provide secure collection and transfer methods for evidence between established sources and endpoints, such as secure local storage and trusted external parties (e.g., insurance firm). Security is important to prevent data tampering, but collection must also be cost-effective and accessible. For example, many ship engine systems are off-line, but provide critical evidence. An incident may also flood or damage these systems, so a cost effective approach may be to periodically, physically, transfer evidence to the bridge, where it can be stored and retrieved more securely and reliably.

Step 4 Establish cyber, cyber-physical, policy for accessing, handling, and exchanging digital evidence. The engine room scenario would apply, but a more fitting example would be cargo tags which hold data on cargo, sender, receiver, and more, but also physically move a great deal across land and ocean. It is important to ensure cyber evidence policy, e.g. e-signatures, securely collects data in transit or during transfers.

Step 5 Specify circumstances when investigations should be held internally (e.g., ship-based, organization based) or externally (e.g., MAIB) based on incident details, companies and countries involved, loss of life, and data ownership/sensitivity.

Step 6 Train staff, crew to management, in cyber-incident awareness and secure evidence handling by establishing clear responsibilities. For example, if the crew want to access forensic data during a voyage (e.g., unusual internet usage), they should be trained to prevent evidence tainting and how not to break international and national laws, e.g., when pursuing an alleged hacker. Knowing how to process, or securely pass-on, data is also a basis for training at all levels.

Step 7 Establish or modify protocols for evidence-based documentation on cyber-related incidents. This may include internal report formats or anonymized reports to be shared with other maritime industries for sector-wide mitigation.

Of course, each of these steps require more in-depth actions at technical, policy, and training levels. However, these are presented as an initial start to securing better forensic readiness within the maritime sector, as there is a likely need for better investigation capabilities regarding cyber-related events. This is not intended as a protection scheme, although it may help inform better defences. Moreover it is assumed that the appropriate preventative defensive cyber-security measures will be in place with the evidence collectors and storage. It is our intention to continue developing an understanding of the unique nature of maritime risks and to use that understanding to better forensic readiness at port and in transit on ships.

V. Conclusions

While the maritime sector is facing an exciting time of technical and economic growth, the downside is that cyber risks and crime are becoming more prevalent. In this article we believe that forensic readiness is key to understanding and mitigating cyber-related incidents, however, when compared to other sectors, the maritime sector seems behind, particularly ship-side. Currently, there is no capacity or policy to drive cohesive forensic readiness across this sector in order to investigate known, and unknown, risks and concerns. To increase forensic capabilities, this article proposed seven steps to enhance and secure digital evidence collection across ships and ports for cyber-informed investigations, and mitigation strategies. This can begin to improve the current state of forensic readiness and help the maritime community, and those that work with them, to have a better understanding of the scope and scale of cyber-related incidents in their sector, and have the capability to obtain the evidence needed to prevent, prosecute, mitigate, analyse, and recover from incidents.

References

[1] International Chamber of Shipping, “Review of maritime transport,” *United Nations Conference on Trade and Development*, 2017.

[2] ——, “Shipping and world trade,” http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade, 2018.

[3] ——, “Review of maritime transport,” *United Nations Conference on Trade and Development (UNCTAD)*, 2018.

[4] Allianz SE, “Safety and shipping review,” 2018.

[5] ENISA, “Cyber security aspects in the maritime sector,” 2011.

[6] K. Jones, K. Tam, and M. Papadaki, “Threats and impacts in maritime cyber security,” IET Engineering & Technology Reference, 2016.

[7] BIMCO, CLIA, ICS, Intercargo, Intertanko, OCIMF and IUMI, “Guidelines on cyber security onboard ships,” BIMCO 2.0 ed. Bagsvaerd, 2017.

[8] K. Belmont, “Maritime cybersecurity: Cyber cases in the maritime enviroment,” American association of Port authorities, 2016.

[9] UK Department for Transport, “Maritime 2050 call for evidence,” Open Government License, 2018.

[10] G. Wilshusen, “Maritime critical infrastructure protection: Dhs needs to enhance efforts to address port cybersecurity,” GAO-16-116T, 2015.

[11] K. Tam and K. Jones, “Cyber-risk assessment for autonomous ships,” IEEE TCS Cyber Security, 2018.

[12] European Credit Research Institutez, “Cybersecurity in finance getting the policy mix right,” Report of a CEPS-ECRI Task Force, 2018.

[13] J. A. Lewis, “Assessing the risks of cyber terrorism, cyber war and other cyber threats,” Center for Strategic and International Studies, 2002.

[14] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, “Cyber-physical systems: The next computing revolution,” in *Design Automation*, 2010.

[15] R. Rowlingson, “A ten step process for forensic readiness.” *IJDE*, 2004.

[16] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Academic Press, Inc., 2011.

[17] K. Tam and K. D. Jones, “Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping,” Journal of Cyber Policy, Pages 147-164, 2018.

[18] BIMCO, Fairplay, and ABS, “Maritime cyber survey 2018 - the results,” IHS Markit, 2018.

[19] CyberKeel, “Security risks and weaknesses in ecdis systems,” NCC Group Publication, 2014.

[20] ECDIS Info, “ECDIS Regulations,” http://www.ecdisinfo.com/ecdis_regulations.html, 2014.

[21] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, “A review of cyber security risk assessment methods for scada systems,” *Computers & Security*, vol. 56, 2016.

[22] Maersk, “A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year,” *Maersk*, Aug 2017. [Online]. Available: https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017

[23] V. Rajamanickam, “COSCO’s cyber attack and the importance of maritime cybersecurity,” *FreightWaves*, July 2018. [Online]. Available: https://www.freightwaves.com/news/technology/coscos-cyber-attack-and-the-importance-of-maritime-cybersecurity

[24] UNDOC, “World drug report,” United Nations Office on Drugs and Crime, 2015.

[25] SIPRI, “A comprehensive approach to combating illicit trafficking,” Stockholm International Peace Research Inst., 2010.

[26] K. Tam and K. Jones, “MaCRA: A model-based framework for maritime cyber-risk assessment,” WMU Journal of Maritime Affairs, 2019.

[27] International Maritime Organization, “Solas chapter V annex 10 imo resolution msc.214(81),” IMO, 2006.

[28] R. Santamarta, “Maritime security: Hacking into a voyage data recorder (VDR),” IOActive [Online], 2015.

[29] C. Baraniuk, “How hackers are targeting the shipping industry,” BBC News, 2017.

[30] D. Rider, “The maritime security cyber threat,” Maritime Security Review [Online], 2015.

[31] MarEx, “Nigerian navy: Crewmembers involved in pirate attacks,” The Maritime Executive, 2016.

[32] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” NIST 800-30, 2002.

[33] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to industrial control systems (ics) security,” NIST 800-82r2, 2015.

[34] A. Ram, “Data breaches persuade companies to raise cyber security budgets,” Financial Times, 2018.