全球大流行病中的網絡安全問題

雖然國際海事組織（IMO）已經敦促船東和船舶營運人在 2021 年前將網絡風險納入船舶安全管理體系，但網絡罪犯早已悄然而至。尤其在新冠病毒這樣的全球大流行病的危機下，不懷好意的網絡罪犯往往會乘機通過各種惡意的方法來獲取利益。

為解決“拒絕物理訪問”、“船舶被隔離”和“旅行限制”等實務操作上的問題，船東目前正在積極開放遠程訪問，對船舶使用遠程數字勘察工具，並鼓勵岸上人員在家遠程工作。

同時，公司還越來越多地使用移動設備訪問船舶上的操作系統和核心業務系統。在這種狀況下，未受保護的設備可能導致數據丟失、隱私洩露和系統被劫持的風險。因此切實保護作為寶貴資產的數據需要在機密性、完整性和實用性之間保持良好的平衡。

在一個遍布網絡的時代，隨著更多的技術改造、“雲”技術的廣泛使用，以及更普及的船舶聯網能力，使得安全威脅不斷增加。網絡罪犯將以高度複雜的方式同時攻擊操作系統和備份能力，以造成有破壞性的網絡攻擊。網絡安全不僅取決於公司和船上的系統和流程是怎樣設計的，還取決於它們如何被使用——即人的因素。

網絡風險可能不易識別

基於行業特點，航運業中船舶及其船員的組織合作良好，且運作方式在不斷優化，但網絡犯罪分子對此是虎視眈眈。這總體上也反映了網絡風險不斷演變的本質。網絡風險管理方法應當是基於公司和船舶，但也必須遵循相關國家、國際和船旗國法規中的要求。

對於還未做好應對的船東和船舶營運人，應首先進行風險評估，同時把應對網絡風險的措施納入其船舶安全管理體系（SMS）和船員意識培訓裡。船東和船舶營運人還應將網絡風險意識文化融入公司和船上的各級部門。其目的是為營造一個靈活的網絡風險管理制度，以確保制度體系才能持續運作，並能通過有效的反饋機制不斷進行評估改進。

大部分船級社以及若干海事諮詢公司都發布過關於船舶網絡安全的指南和建議。船級社作為船旗國當局認可的組織，現在也可以進行包括網絡風險在內的 ISM 審核。

船級社還提供了一套基於自願原則的網絡安全船級理念，以應用於驗證安全船舶的設計和操作，以及網絡安全類型的認證，來支持製造商使用網絡安全系統和組件。船級社作為顧問，還可以為船上和辦公室提供網絡安全風險評估、改進、滲透測試和培訓支持。

在 Gard，我們努力通過最佳途徑保護會員和客戶的利益。我們的建議是對網絡風險採取全面的方法，通過涵蓋流程、技術和最重要的人員的措施，保護 IT 和 OT 系統的機密性、完整性和可訪問性。對於網絡犯罪分子來說，最容易又最常見的入侵目標，就是通過疏忽大意或缺乏訓練的個人。

建議 1：專注於政策、流程和風險評估

最新的船舶網絡安全指南預計，網絡事故會對現實產生影響，並導致潛在的安全以及污染事件。因此，公司不僅需要評估 IT 設備的使用所帶來的風險，還需要評估船上 OT 設備的使用所帶來的風險，並建立適當的防範措施，防止其中任何一種可能帶來的網絡事故影響。

公司的網絡風險管理計劃和流程，必須與公司政策裡 ISPS 和 ISM 規範中的現有安保和安全風險管理要求保持一致。關鍵網絡系統的培訓、操作和維護的相關要求也應包含在船上的相應文件中。

國際海事組織海事安全委員會（MSC）於 2017 年 6 月通過了關於*安全管理體系中海事網絡風險管理*的 MSC.428（98）號決議 。決議規定，經批准的安全管理體系應包括符合 ISM 準則目標和要求的網絡風險管理，且不得遲於 2021 年 1 月 1 日，對公司合規性文件的首次年度驗證。

基於 MSC-FAL.1/Circ.3《海上網絡風險管理指南》中的建議，該決議確認，應採用現有的風險管理做法，解決因日益依賴網絡系統而產生的運營風險。該指南規定了以下可採取的行動來支持有效的網絡風險管理：

1. ***識別***：定義負責網絡風險管理的角色，識別系統、資產、數據和能力，評估如果它們被中斷時將對船舶運營構成的風險。
2. ***保護***：實施風險管控流程、措施和應急計劃，以防止網絡事故，並確保航運業務運作的連續性。
3. ***檢測***：制定並實施能及時檢測網絡事故所需的流程和防禦措施。
4. ***響應***：制定和實施有恢復能力的活動和計劃，以恢復因網絡事故而中斷的航運業務或服務所需的系統。
5. ***恢復***：確定如何備份和恢復受網絡事件影響的航運業務所需的網絡系統。

DOC 證書持有人是確保船上網絡風險管理的最終負責人。由第三方管理船舶時，建議船舶管理人與船東協商好責任歸屬。雙方都應重視責任劃分，確定符合實際的預期、對船舶管理人的具體指示達成一致。盡可能參與採購決策以及預算要求的製定。

除 ISM 體係要求外，此類協議還應考慮其他適用法律，如歐盟《通用數據保護條例》（GDPR）或其他沿海國家的特定網絡條例。船舶管理者和船東應考慮將這些指南作為基礎，以公開討論如何最好地實施有效的網絡風險管理制度。任何有關網絡風險管理責任的協議都應是正式的和書面的。

公司還應在供應商協議和合同中，涵蓋並評估服務供應商的物理安全和網絡風險管理流程。同樣，協調船舶挂靠港口是一項非常複雜的任務，包含了全球性和地方性諸多特性。其中包括船舶代理的消息更新、與所有港口供應商的協調信息、港口國管制、處理船舶和船員的要求，以及船舶、港口和岸上機構之間的電子通信等多方面的工作。

另外，船舶代理的選定的質量標準十分重要，因為和所有其他企業一樣，代理商也是網絡罪犯的目標。網絡犯罪：如電子電信欺詐和虛假船舶預約，以及網絡威脅：如勒索軟件和黑客攻擊，都要求船東和代理人雙方採取協同的網絡戰略並加強彼此之間的網絡關係，來減輕這些風險。

建議 2：確保系統設計和配置的安全性、並被貫徹理解和執行

程序的問題在於，良好的意圖可能會變成紙上談兵。因此，如何確保負責執行涉及網絡安全任務的人員，充分了解該等程序的目的是防止未經授權的訪問，而非僅僅是應對監管機構或其直接上級的要求就變得尤為重要。

與傳統的可參照過往經驗的安全/安保領域不同，網絡風險管理由於缺乏相關事故的事實和影響而變得更具挑戰性。在我們掌握有關證據之前，網絡攻擊的規模和頻率都往往未知的。

航運業和其他商業部門（如：金融機構、公共管理部門和航空運輸）的經驗表明，既遂的網絡攻擊可能導致由於服務無法正常運轉而造成的重大損失。

現代科技帶來便利的同時也可能會給船舶管理增加漏洞，特別是當船舶置於不安全的網絡之中，並被允許自由訪問船舶的互聯網。此外，岸上和船上人員可能沒有意識到一些設備製造商保留和維持了對船舶相關設備和網絡系統的遠程登陸訪問權限。對於船舶而言，對不明且不協調的遠程登陸權限的管理應該是風險評估的一個重要部分。

Gard 建議公司充分了解船舶的 IT 和 OT 系統，以及這些系統是如何與岸上連接和整合的（包括公共當局、海事碼頭和裝卸工）。這需要對船上所有基於計算機的系統，以及網絡事故如何危及安全、運營和業務進行了解。

一些 IT 和 OT 系統可以遠程訪問，並且可能持續連接互聯網，進行關聯遠程監控、數據收集、維護、安全和安保。這些系統可以是“第三方系統”，因此承包商可以在遠程位置監控和維護系統，並且可以是雙向數據流或僅上傳數據。

具有遠程控制、訪問或配置功能的系統和工作站包含以下幾種：
- 船舶艦橋和機艙計算機以及船舶行政網絡上的工作站，
- 帶冷藏溫度控制系統的集裝箱或可遠程跟踪的特化貨物，
- 穩定性決策支持系統
- 船體應力監測系統
- 導航系統，包括電子導航圖（ENC）航行數據記錄器（VDR）
- 動態定位系統（DP）
- 貨物裝卸和存放、發動機、貨物管理和裝載計劃系統
- 安全和安保網絡，如閉路電視（CCTV）
- 專業系統，如鑽井作業、防噴器、海底安裝系統,
- 油輪緊急關閉（ESD），海底電纜安裝和維修

以下是一些常見的網絡漏洞，可能在現有船舶和一些新造船舶上出現：
- 淘汰且不受維護的操作系統，
- 淘汰或已缺失防病毒，防惡意攻擊的軟件，
- 安全配置和正確操作不足，包含無效的網絡管理和使用默認的管理員帳戶和密碼，
- 船載計算機網絡缺乏邊界保護措施和網絡劃分。
- 安全關鍵設備或系統始終與岸上連接。
- 缺乏對包括承包商和服務提供商在內的第三方的訪問控制。

建議 3：提供恰當的船上安全防範意識和培訓

當前，網絡安全最薄弱的環節仍然是人為因素。因此，對船員進行適當培訓，幫助他們識別和報告網絡事件十分重要。

最新的網絡安全調查顯示，業界對這一問題的認識有所提高，並增加了網絡風險管理培訓，但仍有改進的空間。這一點也得到了 Futurenautics Maritime 集團與其合作夥伴進行的 "2018 年船員連通性調查" 的證實，只有 15%的海員表示接受過網絡安全培訓，且僅有 33%的海員表示，他們最近一間工作的公司有定期更改船上密碼的政策。

在評估網絡風險時，外部和內部網絡威脅都應當加以綜合考慮。船上人員在保護 IT 和 OT 系統方面起著關鍵作用，但疏忽大意在所難免，例如：使用可移動媒體端在系統之間傳輸數據時不採取防止惡意軟件傳輸的措施。培訓和培養意識應根據包括船長、高級船員和普通船員在內的船上人員進行程度的調整。

Gard 此前曾與 DNV-GL 一起發布了一個免費下載和分享的 **網絡安全意識活動**，針對日常工作和日常事務，為 "普通人" 揭開網絡問題的神秘面紗，並建立和培養船員和其他人的相關素質和能力。此等行動的目的並不是為了改變任何行業規則，而旨在改變人們的行動和行為方式。

最後，我們建議每個人保持網絡警惕，避免所有有關 "COVID-19" 釣魚程序：• 要謹慎處理任何包含 "COVID-19" 相關的主題行、附件或超鏈接的電子郵件，並小心與 COVID-19 相關的社交媒體請求、文本或電話。
- 使用可靠的資源—比如來自合法的政府網站的最新的，基於事實的網絡安全和 COVID-19 信息
- 不要在電子郵件中透露個人或財務信息，也不要回复此類信息的郵件請求。
- 請謹記在完成工作後，斷開或關閉任何外部端口的臨時遠程訪問。

More resources

Gard

August 2019 - Maritime industry targeted by cyber criminals

July 2019 - Ship operators cannot afford to turn a blind eye to cyber security

Jan 2019 - Denmark identifies cyber threats in its maritime sector

December 2018 - It is time to strengthen your onboard cyber security procedures

June 2018 – Cyber security awareness campaign

Full 20 mins video for crew awareness and training (MP4 - 635Mb)

Short 3 mins teaser of the full video for creating interest (MP4 - 102Mb)

Loss Prevention Poster Cyber security

Loss Prevention Poster Think before you click

Loss Prevention Poster Is your download free of malware?

BIMCO

BIMCO together with the International Chamber of Shipping (ICS) have, October 2019, published a new "Cyber Security Workbook for On Board Ship Use" meant to serve as a guide for the master and officers on board ships and thereby help them prepare for a potential cyber incident.

BIMCO together with Safety at Sea publish a cyber security white paper, in September 2019, containing advice based on results and findings from Cyber Security Surveys produced over the last four years, as well as on feedback and knowledge from experts at roundtable events.

BIMCO together with other leading shipping organisations have in August 2019, published version 3.0 of the Guidelines on Cyber Security onboard Ships (commonly referred to as the BIMCO Guidelines), which offer guidance to shipowners and operators on how to assess their operations and develop the necessary procedures and actions to improve resilience and maintain integrity of cyber systems onboard their ships. The guidelines have been aligned with the recommendations given in the IMO Guidelines on Cyber Risk Management. See also this useful poster which can help prevent the most common cyber incidents.

US Coast Guard

The US Coast Guard published its *Cyber Strategy* in July 2015 in response to what it perceives is one of the greatest threats to US economic and national security interests. The Coast Guard's cyber security website provides access to the strategy document and other cyber-related information, e.g. their *Cyber Maritime Bulletins*, and can be viewed by using the link: *http://homeport.uscg.mil* and the following path: Missions > Cybersecurity

The US Coast Guard published version 3 of its Guidelines for Cybersecurity Onboard Ships on 13 December 2018. These guidelines were developed to mitigate the potential safety, environmental, and commercial consequences of a cyber incident and are designed to assist companies in formulating their own approaches to cyber risk management onboard ships.

UK Department of Transport (DfT)

The DfT published its Code of Practice: Cyber Security for Ships on 13 September 2017, providing a management framework that can be used to reduce the risk of cyber incidents that could affect the safety or security of a ship, its crew, passengers or cargo. The Code of Practice is intended to be used together with DfT's Good practice guide: cyber security for ports and port systems, latest edition issued on 27 January 2020.

Although the Code of Practice refers to Maritime Security Regulations in the UK, its provisions are complementary to those of the SOLAS Convention, the ISM Code and the ISPS Code and it is therefore considered as a useful guidance document for all nationalities of ships.

Classification Societies

ABS Cyber insight: A Simple approach to understanding cyber risk in OT assets

ABS Cyber insight: Cyber Security Solutions for Operational Technology

ABS Application of Cybersecurity Principles to Marine and Offshore Operations - CyberSafety Volume 1

DNV GL Maritime cyber security insight (including ISM guidance)

DNV GL Recommended practice: Cyber security resilience management

Lloyd's Register Cyber insight - Tackling an evolving threat

Lloyd's Register Procedure for the Assessment of Cyber Security for Ships and Ships Systems

作者: Jarle Fosen
高級防損主管