

风险提示 | 黑客“登船”升级，从加密敲诈勒索到安全系统夺权

作者：张盼龙



摘要：

过去十年间，航运业的数字化转型深刻重塑了船舶的技术架构与运营模式。电子海图显示与信息系统、集成化驾驶台系统、主机遥控装置以及货物管理系统已普遍实现网络互联。依托卫星通信技术，船舶不仅接入船公司内部网络，更深度融入全球互联网体系。在显著提升运营效率与协同能力的同时，其网络安全暴露面亦随之急剧扩大。船舶已由传统意义上的信息孤岛演变为一个持续在线、具备远程访问能力的移动网络节点。此外，地缘政治冲突的外溢效应加剧了海上网络安全风险，商船正日益面临具有国家背景的高级持续性威胁、导航信号干扰与欺骗、以及恶意软件植入等新型攻击手段。攻击者的动机亦从传统的经济利益驱动，逐步扩展至战略施压、关键基础设施破坏及地缘博弈等多重维度，网络攻击的趋势正在逐步从岸上走向船上，船舶网络安全的风险防范工作已被提升至前所未有的战略高度。

一、网络袭击事件频度烈度上升

岸基网络袭击事件的共性一般停留在锁数据和停业务的层面，而真正的质变是攻击者开始直接触碰船舶本身。从授权测试到真实入侵，船载操作技术层面的事件接连发生。回顾近年来具有代表性的网络安全事件，可清晰识别出威胁态势的演进路径。

1. 2017 年 6 月，马士基遭遇 NotPetya 恶意软件攻击，全球业务系统大面积瘫痪，损失估计约 3 亿美元，航运业第一次领教了网络攻击的破坏量级。

2. 2017 年 12 月，以色列海事网络安全公司 Naval Dome 在一艘营运船舶上开展授权渗透测试，仅凭一封发给船长的钓鱼邮件，测试人员便先后接管了全船系统，篡改 GPS 船位，生成雷达虚假目标，瘫痪机舱监测，夺取燃油与压载泵控制权。测试证明，船舶网络攻击绝非单纯的数据安全问题，而可以直接威胁船舶、船员与货物的物理安全。

3. 2019 年 2 月，一艘驶往新泽西港的国际航行船舶的船长报告，船上网络遭恶意软件严重破坏。美国海岸警卫队牵头调查后发布第 06-19 号海上安全警报称，恶意软件使船上计算机网络显著降级，所幸关键控制系统未受波及。但调查发现该船几乎没有有效的网络安全措施，多数船员共用登录口令、未安装杀毒软件、码头传递货载数据的 U 盘不经扫描直接插入船上电脑。

4. 2023 年 1 月，全球最大船级社之一的 DNV 的 ShipManager 船队管理软件服务器遭勒索软件攻击，约 70 家客户、近 1000 艘船舶受到影响，服务器环境被迫整体重建。

5. 2025 年 12 月，意大利 GNV 公司载客逾 2000 人的渡轮 Fantastic 号在法国塞特港停靠期间，经意大利情报部门提示被发现船上系统疑遭植入远程访问木马（RAT）。法国当局登轮清查，一名拉脱维亚籍船员被以“为外国势力入侵计算机系统”等罪名起诉羁押，法国国内政部长公开表示案件涉嫌外国干涉。船舶经全面安检后获准复航，GNV 称入侵已被识别并消除。

6. 2026 年 8 月，装载约 230 万桶原油的 VLCC VL Prosperity 轮在通过直布罗陀海峡时疑遭网络入侵，船舶通信中断约 30 小时。8 月 21 日，美国海岸警卫队网络保护小组与 FBI 网络行动组联合登轮，对船载 OT 与 IT 系统开展全面网络安全检查；8 月 24 日，另一艘 LNG 运输船也因疑似网络攻击接受检查。该轮管理公司确认船舶其后已恢复正常营运。

7. 2026 年 9 月，17.4 万立方米 LNG 运输船 Vivit Africa 轮在承运美国 LNG 驶往意大利途中，船员报告失去部分内部控制系统的访问权限，怀疑遭遇网络攻击。船员称攻击者一度控制了蒸汽压力与安全阀系统，并干扰货舱压力控制和蒸发气（BOG）管理循环系统，此类干扰会显著增加液舱破裂甚至爆炸的风险。该轮最终未能在意大利罗维戈的 Adriatic LNG 接收站卸货，改道驶往西班牙阿尔赫西拉斯。

二、网络攻击引发的安全与责任问题

船舶网络袭击事件并不是简单的 IT 技术问题，以目前呈现的风险和结果来看，最终会以传统海上风险的形式呈现出来。

1. 人身与船舶安全后果最为严重

LNG 船的罐压控制、BOG 管理、安全阀系统一旦被干扰，直接后果是液舱超压、破裂乃至爆炸起火。主机、舵机、侧推控制系统被入侵，则可能在狭水道或港内酿成碰撞、搁浅。Vivit Africa 轮船员所报告的情形，无论最终调查结论如何，都说明攻击者理论上已具备触碰船舶关键安全系统的路径。

2. 运营中断带来的经济损失立竿见影

船舶改道、绕航、停航待检，产生额外的燃油、港口使费和船期损失。岸上系统瘫痪则造成码头停摆、货物积压。DNV 事件中服务器环境被迫整体重建、近 1000 艘船舶的船队管理服务一度中断，马士基则为全球业务停摆付出了约 3 亿美元的代价，都是直观的注脚。

3. 第三方责任后果正是保赔险的核心关切

网络攻击引发的碰撞触碰、油污损害、货损货差、人身伤亡、港口设施损坏以及相关行政处罚款，本质上仍属于保赔险承保的传统责任范畴。致损原因是网络攻击，并不当然改变责任的性质。但需要提醒的是，事故的发生、处置和索赔过程会因“网络”因素而变得复杂。

三、构建船岸一体的纵深防御体系

与威胁升级相对应，监管框架正从倡导走向强制。IMO 第 MSC. 428 (98) 号决议早已要求将网络风险管理纳入安全管理体系，自 2021 年起的首次 DOC 年度审核即须满足，IMO 于 2025 年进一步发布了新版海事网络风险管理指南。在造船端，IACS 统一要求 UR E26（船舶网络韧性）和 UR E27（船载系统与设备网络韧性）已对 2024 年 7 月 1 日及以后签订建造合同的新造船强制适用。目前对于航运企业壳落地的措施可归纳为以下几点。

1. 网络风险管理真正嵌入 SMS

网络风险不应是 IT 部门或相关负责人的私事，而应作为安全管理体系的正式组成部分。由指定人员牵头，岸基 IT/网络安全团队提供技术支撑，明确船长的报告责任。基础工作是建立船载 IT/OT 设备资产清单与风险登记册，对驾驶台导航、动力定位系统、安全系统、推进与电站、通讯、货控、报警、监测等设备逐项登记、分级管理。行业通行的做法是将系统按失效后果分为三级：导航、动力定位系统、安全系统、推进等一旦失效即危及船舶安全的列为最高级（Category III），通信、货控、报警监测次之（Category II），行政办公类再次之（Category I），防护资源按级别配置。新造船还应核查是否满足 IACS UR E26/E27 的强制要求。

2. 筑牢船岸技术防线

网络分段是第一要务是将驾驶台、集控室等 OT 网络必须与船员 Wi-Fi、办公网络物理或逻辑隔离，关键系统之间设置防火墙和入侵检测。不少大型船舶的导航、推进、操舵系统共用同一网络、仅靠单一道防火墙防护，边界一旦被突破便门户洞开；船载系统账号一人一密、定期更换，远程运维通道启用多因素认证并限时开通、用完即关；卫星通信终端和 VSAT 管理端口是已知的薄弱环节，应纳入重点加固范围。制定适合船舶营运节奏的补丁管理计划，杀毒软件保持更新。ECDIS 航线与配置、控制系统软件、重要文件均应保留离线备份，并定期验证可恢复性。

3. 管好变更与第三方

大量入侵经由合法通道进入。如，供应商的维护笔记本电脑、随手插入的 U 盘、长期不关闭的远程访问账号。建议参照变更管理制度执行，任何软件安装、系统配置修改、硬件更换均须申请、评估、审批并留存记录。外来 U 盘和笔记本电脑上船前须经扫描确认，接入关键网络需专门授权，服务商远程访问逐次审批、全程留痕。

4. 守住人员这道防线

钓鱼邮件仍是最常见的入侵入口。应按对象分层开展培训并留存记录，普通船员侧重识别钓鱼邮件、口令管理和移动介质纪律；驾驶员和轮机员侧重 OT 系统异常识别与手动备份操作；岸基管理人员侧重商务邮件欺诈防范。培训之外，还应定期开展实战化演练，ECDIS

失效、船岸通信中断时的备用信道启用、主机舵机控制异常时的手动接管。这些科目应像消防救生演习一样进入年度计划。

5. 备好应急响应预案

每艘船都应有一份简明可用的网络事件响应计划，核心是识别、隔离、报告、处置、恢复、复盘这六个步骤。船员发现终端异常弹窗、文件被加密、系统失控等症状后，第一时间将受感染设备断网隔离、停止使用任何移动介质；船长立即按预案向岸基网络安全联系人报告（附照片等证据）；岸基按敏感数据、计算机系统、船舶通信、第三方 OT 应用（如 ECDIS）等类别分级响应；处置过程保留日志、邮件等证据以备取证；系统恢复坚持先取证再重装、重装必改密、上线必打补丁；事后必须复盘并修订预案。同时配套标准的网络事件报告表，记录事发时间、船位、受影响系统、严重程度和已采取措施，确保向公司、船旗国、港口国和保险人的报告口径一致、有案可查。



四、结束语

从 2017 年马士基因网络攻击遭受约 3 亿美元经济损失，到 2026 年疑似网络干扰事件导致 LNG 运输船被迫变更航线，航运业在不足十年间经历了网络安全威胁层级的显著跃升，由初期以数据窃取为主的低阶攻击，演进为可直接操控关键航行与动力设备的高阶定向攻击。网络攻击并不会因船舶处于远洋环境而自动规避。相反，通信链路冗长、工业控制系统普遍老化、船员网络安全意识参差且轮换频繁等现实因素，共同加剧了船舶网络空间的脆弱性，使其日益成为高级持续性威胁组织及专业化黑客团伙重点瞄准的高价值目标。对船岸一体化管理体系而言，将网络安全风险管理全面纳入企业安全治理体系，实现责任到岗、制度到人、演练常态化，已非一项可选项，而是关乎运营连续性、资产安全与合规底线的刚性要求。

以上仅供会员参考，如需具体建议请联系协会相关人员。