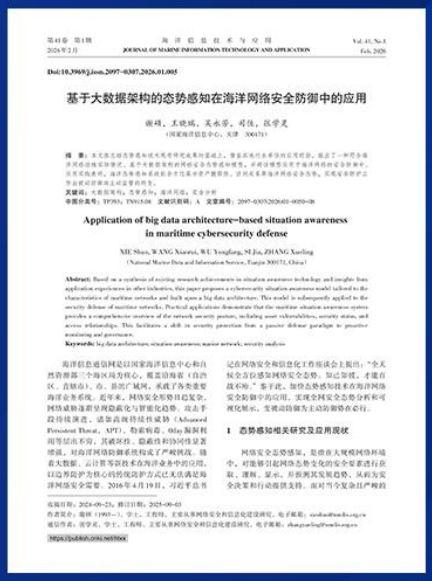
海洋信息技术与应用

Journal of Marine Information Technology and Application

基于大数据架构的态势感知在海洋网络安全防御中的应用



第40卷 第1期 海洋信息技术与应用 Vol. 40, No. 1
2026年2月 JOURNAL OF MARINE INFORMATION TECHNOLOGY AND APPLICATION Feb. 2026

Doi:10.3969/j.issn.2097-0307.2026.01.005

基于大数据架构的态势感知在海洋网络安全防御中的应用

谢硕，王晓瑞，吴永芳，刘佳，张学灵

（国家海洋信息中心，天津 300171）

Application of big data architecture-based situation awareness in maritime cybersecurity defense

XIE Shuo, WANG Xiaorui, WU Yongfang, SI Jia, ZHANG Xueling

（National Marine Data and Information Service, Tianjin 300171, China）

国家海洋信息中心
谢硕、张学灵团队

核心观点

· 本文针对海洋网络的安全防御需求，提出了一套基于大数据架构的网络安全态势感知模型，通过数据采集、智能分析与可视化应用，实现了对全网资产、威胁和访问关系的主动监控，推动安全防护从被动防御转向主动监管。

创新点

· **模型架构创新：**设计了一个三层（数据采集与处理、数据分析与存储、业务应用）的态势感知模型，专门适配海洋信息通信网的环形架构与业务特点，实现了安全数据的统一汇聚与智能处理。
· **分析引擎创新：**在数据分析层引入了“三重判定智能引擎”，融合有监督/无监督学习等AI算法与增强型规则匹配，形成AI+规则的闭环迭代，显著提升了对未知威胁（如0day、Webshell）的检测能力。
· **系统实施创新：**提出了以旁路部署潜伏威胁探针收集流量、在国家中心部署“安全大脑”平台的具体方案，并设计了分析、处置、监控等六大功能中心，实现了检测、可视、响应、溯源的闭环管理。

· 本文为大型行业专网提供了一套可落地、见实效的网络安全态势感知系统建设方案，对构建主动、智能的海洋网络综合防御体系具有重要参考价值。

专注海洋信息学科前沿的中文学术期刊

电话：022-24011918　邮箱：hyxx@nmdis.org.cn

期刊网址：https://publish.cnki.net/htxx

扫码阅读全文