

Can Cyber Crucible protect ships and remote or disconnected operations?

Short answer: Yes, and it has. In a maritime deployment, Cyber Crucible operated autonomously across multi-day voyages with no IT staff aboard, adapting to low-bandwidth satellite links and long disconnected stretches while protecting everything from passenger terminals to mission-critical maritime controls.

What the deployment demonstrated

- **Autonomous response** with no IT team present for days at a time.
- **Satellite-aware** operation across bursty, low-bandwidth, weather-interrupted links.
- **Forensic retention** — rich logs preserved through disconnection for post-voyage analysis.
- **Resilience under attack** — it held when adversaries tried to shut it down or degrade its performance.

The unusual part

Logs revealed activity consistent with nation-state involvement, and the targeting was selective: only vessels operating in international waters were affected, while domestic sightseeing vessels were untouched.

When conventional intrusion attempts failed, the adversaries escalated — hijacking Windows login credentials, then reaching BIOS-level settings to lock systems before boot. Even with systems halted before the operating system could load, the deployment continued to hold the line where traditional security stacks had already failed.

Revision #3

Created 2026-07-20 19:24:13 UTC by Dennis Underwood

Updated 2026-07-21 19:32:27 UTC by Dennis Underwood