

SoK: Cross-Layer Cyber Attack Surfaces of Unmanned and Autonomous Maritime Systems

Elizabeth Tran, Gary Goodman, Hosam Alamleh, Ulku Clark, and Bilge Karabacak

Why Maritime Autonomy Needs a Cross-Layer Security View

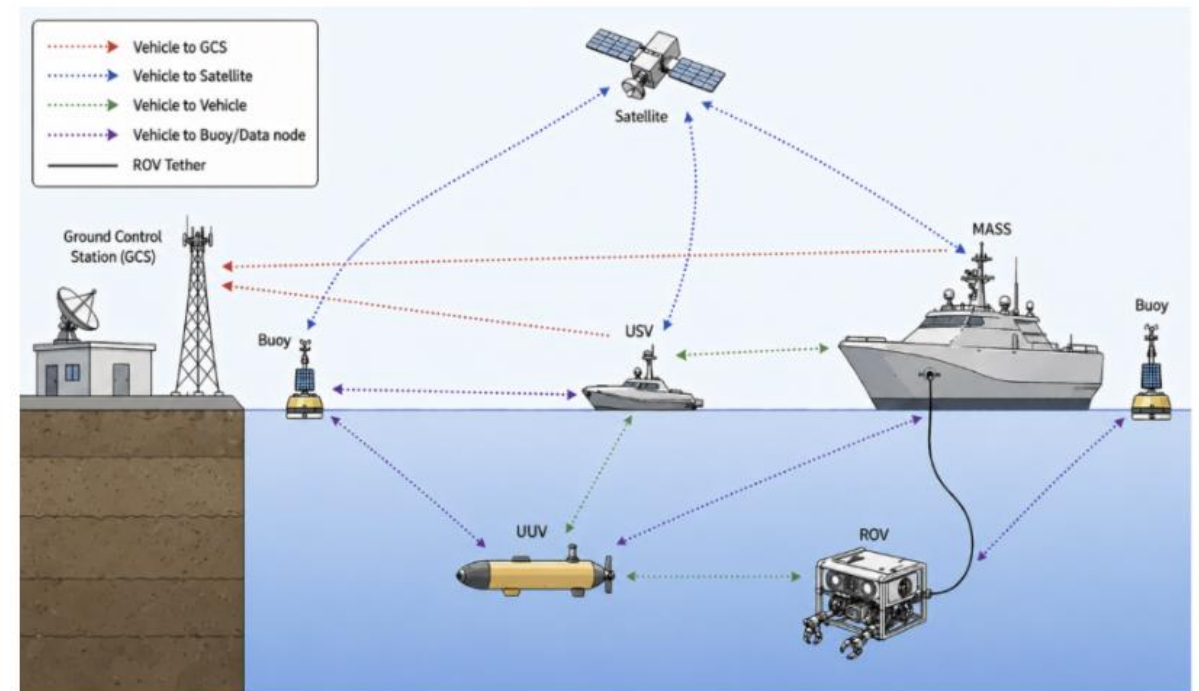
Communication, navigation, perception, and control directly influence vessel behavior.

A compromised sensor or communication channel can affect mission execution and physical safety.

Intermittent connectivity, acoustic delays, and environmental uncertainty complicate attack detection.

Existing research often examines individual attacks, subsystems, or vehicle classes separately.

Our question: How do cyber threats affect different maritime platforms, and where do their effects propagate?



Four Maritime Domains, Different Operating Constraints
Similar attacks can produce different operational consequences across these domains.

Domain	Platform type	Security-relevant characteristics
USV/ASV	Unmanned/autonomous surface vehicles	Wireless links, GNSS navigation, fleet coordination
AUV/UUV	Autonomous/unmanned underwater vehicles	Acoustic links, GNSS-denied navigation, disconnected operation
ROV	Remotely operated vehicles	Operator commands, telemetry, video feedback, tethered links
MASS	Maritime Autonomous Surface Ships	Integrated navigation, ship–shore supervision, ship-scale safety consequences

Structured Review of 212 Studies

- Scopus served as the primary search database.
- Coverage checks used IEEE Xplore, ACM Digital Library, and Web of Science.
- Studies had to address maritime operation, an unmanned or autonomous system, and an explicit cybersecurity concern.
- **Study selection**
 - 2,605 initial records
 - 1,484 records after deduplication
 - 161 studies retained after title and abstract screening
 - 51 additional eligible studies from citation snowballing
 - **212 studies in the final synthesis**
 - Three independent reviewers achieved substantial agreement: **Fleiss' $\kappa = 0.773$.**

A Taxonomy Connecting Platforms, Layers, and Attacks

Affected system layer



Control / actuation



Communication / network



Navigation / perception



Software / AI / operations

Attack family

- Availability
- Integrity / deception
- Navigation and communication disruption
- Software / AI
- Physical-component
- Hybrid cyber–physical

The taxonomy captures where attacks affect the system and supports comparison across platforms.

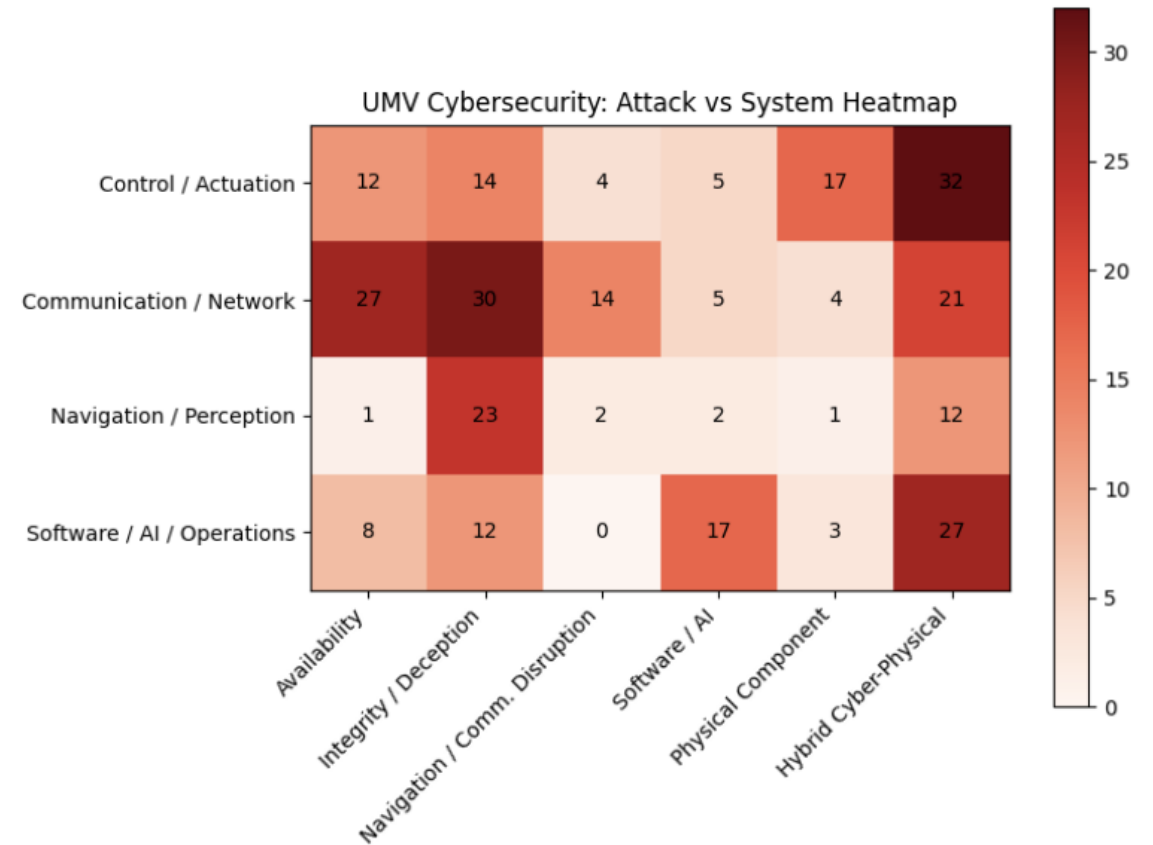
The Evidence Map Shows Uneven Research Coverage

Integrity and deception attacks appear across all four system layers.

Communication/network research strongly covers availability and integrity threats.

Hybrid cyber–physical threats connect technical compromise with control and operational effects.

Sparse categories identify areas that warrant further investigation.



Surface Platforms: Navigation and Communication Shape Safety

USV/ASV

- GNSS spoofing, false data injection, replay, and jamming affect navigation and networked control.
- Consequences include trajectory errors, unstable formations, and degraded fleet coordination.
- Research is comparatively strong in control security.

MASS

- Exposed functions include integrated navigation, waypoint handling, and ship–shore supervision.
- Attacks can compromise collision avoidance and remote intervention.
- Research places greater emphasis on risk, survivability, and safety assurance.

Underwater Platforms: Constraints Complicate Security

- AUVs/UUVs operate without underwater GNSS reception and often with limited external supervision.
- Acoustic communication introduces low bandwidth, delays, and intermittent connectivity.
- Communication disruption can degrade cooperation and distributed control.
- Falsified sensor or localization data can corrupt estimation and path following.
- Much of the evidence relies on simulations or mathematical models.

Security mechanisms must account for long periods of limited communication and autonomous operation.

ROVs: The Operator Feedback Loop Is an Attack Surface

ROV operation depends on trustworthy commands, telemetry, and visual feedback.

Command manipulation can affect thrusters, positioning, or manipulators.

Falsified or delayed video and sensor data can mislead the operator.

A physically functional vehicle can still behave unsafely when its operator receives corrupted information.

ROV-specific cybersecurity remains substantially underexplored.

Cross-Domain Findings

- **Finding 1:** Maritime cyber compromise is cross-layer.
- **Finding 2:** Integrity and deception attacks are especially safety-critical.
- **Finding 3:** Availability threats are domain-specific.
- **Finding 4:** Navigation security is expanding beyond GNSS protection
- **Finding 5:** AI, trust, and human supervision are becoming mission-level attack surfaces

Central Finding: Cyber Effects Propagate Across Layers

Illustrative navigation attack pathway

1. An attacker manipulates positioning or sensor information.
2. State estimation produces an incorrect view of the vessel's location.
3. Planning or collision avoidance selects an unsafe action.
4. Control commands translate that decision into physical movement.

Integrity attacks are especially safety-critical because corrupted information can remain plausible while the system appears available.

Security evaluation must follow the attack through to mission and safety consequences.

Security Extends Across the Full Autonomy Pipeline

Navigation: Protection must include localization, sensor fusion, waypoint handling, and route interpretation.

AI: Poisoning and adversarial inputs can influence perception, planning, and control.

Trust: Compromised identities or malicious nodes can undermine fleet coordination and remote supervision.

Human supervision: Manipulated displays, delayed telemetry, and false alerts can impair intervention.

Each of these functions can influence mission execution and physical safety.

Research Priorities Emerging from the Review

Current gap	Research priority
Limited realistic validation	Shared maritime cyber ranges, representative testbeds, and reusable benchmarks
Underrepresented ROV security	Operator-interface integrity, video deception, and commercial ROV hardening
Fragmented safety-security evaluation	Joint evaluation of detection, control, operator response, and recovery
Limited AI and trust assurance	Measure how compromised models or identities affect complete missions
Isolated attack scenarios and weak lifecycle coverage	Study multistage attacks, secure updates, maintenance, and post-attack recovery

Takeaways

- We organize 212 studies across four maritime domains using a common layer-and-attack taxonomy.
- Cyber compromise can propagate from information channels into control behavior and physical safety.
- Deception can remain dangerous while systems appear operational.
- Availability threats have different consequences across surface, underwater, remotely operated, and ship-scale platforms.
- Priorities include ROV security, realistic validation, AI assurance, and lifecycle protection.

Securing maritime autonomy requires tracing attacks from their initial effects through vessel behavior, operator response, and recovery.



Questions