MARITIME SECURITY

DETER

Discouraging access

Preventing unauthorized or hostile access to systems, infrastructure and strategic zones in both civilian and military contexts. Conceptual, physical and digital.

- Continuous patrol and perimeter enforcement (surface, air, underwater) – mix of platforms; need for integrated sensors in air, surface and underwater domains to avoid blind zones.
- Deterrence through visible and invisible presence (autonomous systems and surveillance) by strengthening physical and digital barriers.
- Digital defensive capabilities against spoofing, jamming and data manipulation become critical. Establishing resilient, robust IT & OT systems with redundancy.

DETECT & IDENTIFY

Early detection of anomalies and suspicious activities above, on and below the water

- Detection: Multidimensional detection of threats below, on and above water through fixed and mobile sensors (radar, sonar, drones, underwater robotics), including detection of digital sabotage or electromagnetic interference.
- Identification: Sensor fusion and AI-based pattern recognition are crucial for early and autonomous identification of anomalous behaviour, objects and digital threats (data from combined sensor networks (radar, lidar, sonar, cameras, …), AI-driven pattern recognition, interoperable systems).
- Data integration across civilian, industrial and military sensor networks, with AI models trained on tactically relevant anomalies.
- Optimising underwater detection by reducing acoustic noise and deploying mobile sensors.
- Intelligence sharing to improve situational awareness and shorten response times.

RESPOND & REPAIR

Rapid and coordinated deployment of assets in case of incidents or conflict situations, rapid repair following incidents

- Readiness: Rapidly deployable (autonomous) response assets (drones, UUVs, robotics) for tactical actions such as mine detection, interception or response to sabotage.
- Execution: Improved coordination between autonomous systems in air, surface and underwater domains (swarm operations).
- AI-supported command and control and real-time data fusion (human–machine teaming and multi-agent operations in complex threat scenarios).
- Repair: Mobile repair capabilities at sea (e.g. autonomous inspection and repair robots), redundant infrastructure and digital resilience for critical systems.
- Cybersecurity: Detection of and recovery from attacks (e.g. spoofing, data manipulation), security-by-design and failover mechanisms.
- Civil–military coordination and communication, and interoperable protocols (uniform analysis and interpretation) for rapid response and repair.