NAVAL PROTECTION DIVISION

MARITIME SECURITY & INTEGRATED PROTECTION

The maritime security landscape is evolving at pace. Piracy, armed attacks at sea, port infiltration, and cyber threats are no longer isolated incidents — they are systemic risks that demand a unified, technology-driven response. This presentation outlines how our Naval Protection Division delivers a seamless ecosystem of vessel, facility, personnel, and IT security, anchored by proprietary autonomous drone technology that sets us apart from conventional security providers.

Our goal is not simply to present services — it is to demonstrate operational value, reduce your risk profile, and move you toward a concrete security assessment or pilot programme tailored to your highest-priority routes and ports.

THE THREAT LANDSCAPE: WHAT MARITIME OPERATORS FACE

Piracy and armed attacks at sea remain among the most significant operational risks facing commercial shipping today. From the Gulf of Guinea to the Strait of Malacca and the waters off the Horn of Africa, vessels carrying cargo, crew, and critical infrastructure are exposed to coordinated attacks, hijackings, and ransom demands. These are not low-probability events — they are recurring, well-documented, and increasingly sophisticated.

But the threat does not begin or end at the horizon. Vessels at anchor in harbour are vulnerable to theft, sabotage, and unauthorised boarding. Port facilities face infiltration risks that can compromise entire supply chains. Key personnel — captains, logistics managers, and executives — are increasingly targeted both ashore and at sea. And beneath the surface of every physical threat lies a growing digital vulnerability: IT systems, navigation networks, and communication infrastructure are prime targets for cyberattack, with the potential to disable or redirect vessels remotely.

The cost of these gaps is measured not only in ransom payments and cargo losses, but in insurance premiums, operational delays, crew welfare, and reputational damage. Many operators rely on fragmented security arrangements — private guards for ports, ad hoc escort vessels, and legacy communication systems — that leave critical windows of vulnerability unaddressed. The question is not whether a threat will materialise, but whether your current posture can detect, deter, and respond before it escalates.

🏴‍☠️ PIRACY & ARMED ATTACK

Coordinated boarding attempts, hostage situations, and cargo theft on open sea and in transit corridors.

⚓ HARBOUR VULNERABILITY

Vessels at anchor are exposed to theft, sabotage, and unauthorised access during loading and port operations.

👤 PERSONNEL RISK

Crew, captains, and logistics executives face targeted threats both at sea and in port environments.

💻 CYBER & IT THREATS

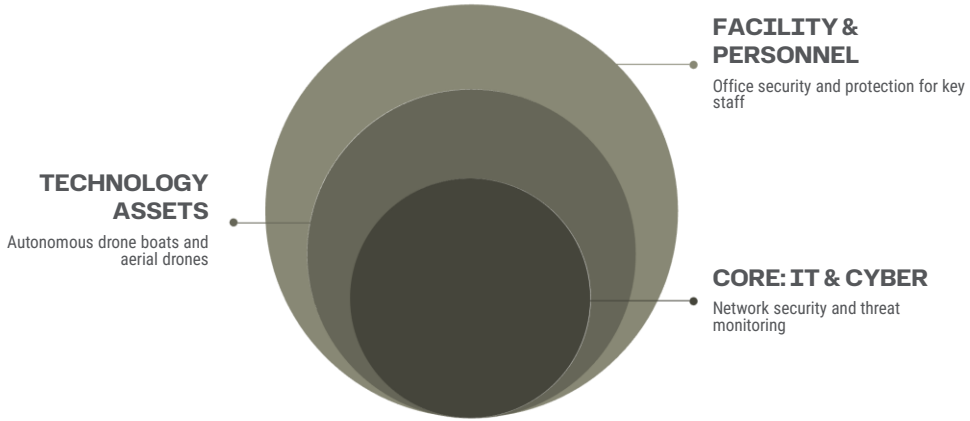
Navigation systems, communications, and cargo management networks are increasingly targeted by hostile actors.

OUR INTEGRATED SOLUTION: A UNIFIED SECURITY ECOSYSTEM

Most security providers offer disconnected services — a guard company for ports, a separate contractor for vessel escorts, and an IT firm for cyber protection. The result is a patchwork of responsibilities, communication gaps, and slow response times when threats materialise. Our Naval Protection Division was built to solve this problem at its root.

We position maritime, facility, personnel, and IT protection not as a menu of options, but as a unified system. Every layer communicates, every asset is coordinated, and every response is informed by a shared operational picture. When a drone detects a suspicious vessel approaching your ship at anchor, that intelligence simultaneously alerts your onboard security team, your port facility command, and your cyber operations centre — because a physical threat and a digital intrusion may be two vectors of the same attack.

This integration is not a marketing claim. It is an operational architecture. Our command-and-control infrastructure ties together autonomous drone boats, aerial surveillance drones, ground-based facility security, close protection teams, and cyber monitoring into a single, coherent response framework. The result is faster detection, faster decisions, and faster intervention — reducing the window in which a threat can cause harm.



Each layer reinforces the others. Maritime protection reduces exposure at sea; facility security closes the gap in port; personnel protection safeguards the people who make operational decisions; and IT security ensures that the systems coordinating all of the above cannot be compromised by a hostile actor. Together, they form a security posture that is greater than the sum of its parts.

MARITIME PROTECTION: ON-SEA & IN-HARBOUR CAPABILITIES

ON-SEA VESSEL PROTECTION

Our on-sea protection capability provides continuous, layered security for vessels in transit through high-risk corridors. Autonomous drone boats patrol ahead and alongside your vessel, creating a visible deterrent perimeter that is difficult for hostile craft to penetrate. Aerial drones provide over-the-horizon surveillance, identifying approaching threats before they enter engagement range.

In the event of a piracy attempt, our drone assets can interdict, track, and delay hostile vessels while alerting naval authorities and coordinating a structured response. The goal is not merely to react — it is to deny the attacker the element of surprise that every piracy operation depends upon.

IN-HARBOUR VESSEL PROTECTION

A vessel at anchor is not a vessel at rest from a security perspective. Harbour environments present unique vulnerabilities: reduced manoeuvrability, proximity to shore-based threats, and the complexity of port operations that can mask hostile activity. Our in-harbour protection establishes a continuous security cordon around your vessel during loading, unloading, and lay-up periods.

Drone boats maintain a persistent patrol perimeter, while aerial drones provide elevated surveillance of the vessel and surrounding dock areas. Any unauthorised approach is detected, logged, and responded to before it becomes an incident. This capability is particularly valuable in ports with known security gaps or in regions where port authority resources are stretched.

MEDICAL EMERGENCY RESPONSE

Beyond security, we provide medical emergency response and backup for vessels — ensuring that crew welfare is protected even in remote or high-risk waters where conventional medical evacuation is not immediately available.

TECHNOLOGY & ASSETS: WHERE WE ARE DISTINCTIVE

Technology is not a supporting feature of our service — it is the foundation. Our proprietary autonomous drone boats and aerial surveillance drones create a competitive advantage that conventional security providers simply cannot match. These are not off-the-shelf products; they are purpose-built assets designed for the specific demands of maritime threat response and deterrence.

AUTONOMOUS DRONE BOATS

Our small autonomous drone boats operate as both a deterrent and a rapid-response asset. Deployed ahead of or alongside a protected vessel, they create a physical barrier that hostile craft cannot cross without detection. Equipped with real-time communication, GPS tracking, and onboard sensors, they can intercept, shadow, and delay approaching threats while coordinating with human operators and naval authorities. Their small footprint and high manoeuvrability make them effective in both open water and congested harbour environments. Critically, they provide visible deterrence — a hostile actor who sees drone boats patrolling a vessel's perimeter must reconsider the feasibility of an attack.

AERIAL SURVEILLANCE DRONES

Our aerial drone fleet extends your situational awareness far beyond the horizon. Capable of long-range reconnaissance, thermal imaging, and real-time video transmission, these assets provide the early warning that every effective maritime security operation depends upon. A piracy skiff approaching at speed can be identified minutes before it enters visual range — minutes that translate directly into options: evasive manoeuvre, alert to authorities, deployment of countermeasures, or coordinated interdiction. In harbour environments, aerial drones provide elevated surveillance of the vessel, the dock, and the surrounding area simultaneously, closing the blind spots that ground-based security cannot address.

Key Differentiator: Our drone assets are not reactive tools — they are proactive deterrents. The visible presence of autonomous systems fundamentally changes the risk calculus for any potential attacker, often preventing an incident before it begins.

FACILITY & PERSONNEL PROTECTION: CLOSING THE GAP ASHORE

Maritime security does not end when a vessel docks. The facilities, personnel, and information systems that support your operations are equally critical — and equally vulnerable. A sophisticated threat actor does not limit their attention to the sea; they exploit weaknesses wherever they exist. An executive travelling through a high-risk port, an office facility housing sensitive logistics data, or an unsecured IT network can all become vectors for disruption, theft, or coercion.

OFFICE & FACILITY SECURITY

Your operational headquarters, logistics centres, and port-side offices house the information, personnel, and infrastructure that keep your fleet moving. A breach at any of these locations can compromise vessel schedules, cargo manifests, crew assignments, and strategic routing decisions. Our facility security provides layered protection — from physical access control and perimeter surveillance to integrated alarm systems and rapid response protocols — ensuring that your shore-based operations are as secure as your vessels at sea.

KEY PERSONNEL PROTECTION

Captains, logistics directors, and senior executives are high-value targets for kidnapping, coercion, and intelligence gathering. Our close protection services extend security to the individuals whose decisions drive your operations — whether they are travelling through high-risk port cities, attending industry events, or transiting between facilities. Protection is discreet, professional, and calibrated to the specific threat profile of each individual and location.

IT SECURITY & CYBER PROTECTION

A vessel's navigation system, cargo management platform, and communications network are only as secure as the IT infrastructure that supports them. Cyberattacks on maritime operators are increasing in frequency and sophistication — from ransomware that locks operational systems to GPS spoofing that can redirect a vessel off-course. Our IT security and cyber protection services monitor, defend, and respond to digital threats across your entire technology stack.

We integrate cyber monitoring with physical security operations, recognising that a cyber intrusion may be the precursor to a physical attack — or that a physical breach may be intended to plant digital malware. This unified approach ensures that no attack vector is addressed in isolation.

- Network monitoring and threat detection
- GPS and navigation system integrity
- Incident response and recovery protocols
- Staff awareness and access management

THREAT SCENARIOS: MAKING THE OFFERING TANGIBLE

Abstract security capabilities are difficult to evaluate. Concrete scenarios make the value clear. The following realistic threat situations illustrate how our integrated approach responds to the specific risks your operations face — and why a fragmented security posture leaves dangerous gaps.

SCENARIO 1: PIRACY ATTEMPT IN TRANSIT

A high-speed skiff approaches your vessel in a known piracy corridor at dusk. Conventional response: the crew spots the vessel visually, raises the alarm, and hopes naval authorities are within range. Our response: aerial drones detect the approach 15 minutes earlier; autonomous drone boats deploy to intercept and delay; your command centre is alerted in real time; naval authorities are pre-warned with live tracking data. The attack is deterred before it begins.

SCENARIO 2: HARBOUR INFILTRATION AT NIGHT

Your vessel is anchored in a port with limited security resources. A small boat approaches under cover of darkness, intending to board and steal cargo or equipment. Ground-based guards have limited visibility and slow response times. Our response: drone boats maintain a continuous patrol perimeter; aerial drones provide elevated thermal surveillance; any approach is detected, illuminated, and logged before the intruders reach the hull. The incident is prevented, not discovered after the fact.

SCENARIO 3: COORDINATED CYBER-PHYSICAL ATTACK

A hostile actor compromises your vessel's AIS system to obscure its position while simultaneously attempting a physical boarding. Conventional security treats these as separate incidents. Our integrated operations centre correlates the cyber anomaly with physical surveillance data, identifies the coordinated nature of the attack, and deploys both digital countermeasures and physical response assets simultaneously — closing both vectors of the threat in a single coordinated action.

SCENARIO 4: EXECUTIVE TARGETING IN PORT

A logistics director is travelling through a high-risk port city for a scheduled meeting. Intelligence suggests a kidnapping attempt is being planned. Our close protection team, informed by the same intelligence network that monitors vessel threats, adjusts the travel route, provides secure transport, and maintains communication with the maritime operations centre throughout. The executive arrives safely; the threat is neutralised without incident.

NEXT STEPS: MOVING TOWARD A SECURITY ASSESSMENT

The question is not whether your operations face maritime security risk — they do. The question is whether your current posture is sufficient to detect, deter, and respond before that risk becomes an incident. A structured security assessment is the most effective way to answer that question with evidence rather than assumption.

Our assessment process is collaborative, not prescriptive. We begin by understanding your highest-priority routes, your most vulnerable ports, your current security arrangements, and the specific metrics that matter to your decision-makers — whether that is insurance cost reduction, crew safety compliance, cargo integrity, or operational continuity. We then map your threat exposure against our capability set and identify where a pilot programme can deliver measurable value with minimal disruption to your operations.

01

INITIAL CONSULTATION

A structured conversation to understand your risk profile, priority routes, current security gaps, and the decision-makers who need to be engaged. We explore your risk tolerance, deployment timeline, and whether you are seeking visible deterrence, rapid response capability, or both.

02

THREAT & GAP ANALYSIS

We assess your current security posture against the specific threats facing your operations — identifying where gaps exist, what those gaps cost, and how an integrated approach would close them. This analysis forms the basis of a tailored proposal.

03

PILOT PROGRAMME DESIGN

We design a focused pilot — typically covering a single route, port, or vessel — that demonstrates our capabilities in your actual operating environment. The pilot is structured to generate clear, measurable outcomes that inform a broader deployment decision.

04

FULL DEPLOYMENT & INTEGRATION

Following a successful pilot, we scale the solution across your fleet and facilities, integrating maritime, facility, personnel, and IT protection into a single, coordinated security ecosystem that reduces your risk and operational complexity.

QUESTIONS WE WILL EXPLORE TOGETHER

- What is your risk tolerance and timeline for security deployment?
- Which maritime route or port region is your highest priority?
- Are you seeking visible deterrence, rapid response, or both?
- How do you currently handle security gaps, and what is the cost?
- Who are the decision-makers, and what metrics matter most to them?

WHY MOVE FORWARD NOW

Every day without an integrated security posture is a day in which your vessels, your people, and your operations are exposed to threats that are preventable. The maritime security environment is not becoming less complex — it is becoming more so. Operators who act now to assess and upgrade their security infrastructure will be better positioned to protect their assets, their crews, and their commercial relationships than those who wait for an incident to force the decision.

We are ready to begin that conversation when you are.

PLEASE CALL US FOR A SECURITY AND FULL PHYSICAL RISK MANAGEMENT CONSULTATION. OUR CAPABILITY STATEMENT IS ALSO ATTACHED AS A SEPARATE DOCUMENT