CRITICAL INFRASTRUCTURE PROTECTION - HOMELAND SECURITY & MILITARY ASSETS

BUILT ON AIR AND MARITIME DEFENSE. ENGINEERED FOR CRITICAL INFRASTRUCTURE

Threat Picture Has Gone Military Grade

Twenty years ago, a desalination plant a presidential compound, a forward operating base, and a power grid were defended as physical sites. Fences, patrols, and access control. The threat was a determined intruder with the right cover story.

That threat still exists. But it is no longer the most dangerous one.

A small drone with a commercial airframe now carries a military-grade payload. Loitering munitions of drones reach hundreds of kilometers from launch. A boat probes a perimeter while another follows behind it. A diver enters a water intake, and a contamination event reaches every household in the city within hours.

This is the operational repertoire of both state and non-state adversaries, deployed against assets where most critical infrastructure is secured with conventional commercial security platforms - platforms that was never build for this threat picture.

Today, a new level of protection is needed. The defensive systems must be built to match the complexity and capabilities of your adversaries.

Critical Infrastructure Under Military Protection

The operators of critical national infrastructure are almost never civilians.

A water desalination plant is run by industry but defended by the National Guard. A state or palace compound is run by the royal household but secured by presidential guard. A power station is operated commercially but is monitored by homeland security forces with a uniformed chain of command.

That distinction shapes the system requirement: the asset has a civilian function but the defenders must work to a military standard. Security officers with military background expect a protection platform that meets them in their own register.

A desalination plant or a military installation near the coast illustrates the demand perfectly, because the threat picture spans four domains at once:

- Surface, a small boat approaching the seaward edge
- Sub-surface, a diver carrying explosive or chemical payload toward the water intake
- Land, a vehicle probing a perimeter at the back of the site
- Air, a drone descending toward the chlorination plant or the control building.

The defending force cannot afford a separate detection system for each domain. They need one operational picture across all four – and a picture that can dynamically adapt to current threats if i.e. intelligence reports a credible plot, the perimeter extends and the detection rules and sensitivity tightens.

In a modern protection system, this shift happens in seconds – no new hardware, just one change of profile.

A Harder Perimeter for a Harder Threat

The security calculus around military bases, munitions sites, and national borders has changed dramatically. Perimeters once considered adequate for peacetime operations are no longer enough.

Today's threat includes drone-borne reconnaissance, hybrid sabotage, and stand-off attacks. Bases are hardening, border patrols are extending their surveillance reach, and forward-deployed fuel and munitions sites are now treated as potential targets.

Today's threat includes drone-borne reconnaissance, hybrid sabotage, and stand-off attacks. Bases are hardening, border patrols are extending their surveillance reach, and forward-deployed fuel and munitions sites are now treated as potential targets.

Success depends on detecting threats at range while distinguishing routine activity from genuine danger. Border patrols cannot investigate every wildlife movement or commercial overflight, just as base operators cannot respond to every flock of birds crossing a radar sector.

The system must do the cognitive work - automatically classifying threats and presenting operators with only the events that require action.

Whether protecting a military base, munitions depot, or national border, the mission remains the same:

- Multi-domain coverage
- Adaptive threat profile
- An intuitive interface operators can master with ease
- Forensic-grade event handling that stands up to post-incident scrutiny

A C2 Platform Built on Air and Maritime Defense Heritage

T.react CIP is Terma's Command and Control (C2) platform for critical infrastructure protection. It fuses data from radars, electro-optical and infrared cameras, sonar, hydrophones, perimeter sensors, ADS-B/AIS, access control, and other surveillance systems into one operational picture for the security operator.

Built on Terma's proven air and maritime defense technology, its fusion engine correlates multiple sensor inputs into a single, validated track -even as targets move between sub-surface, surface, land, and air domains. The result is the precision and situational awareness expected from a military-grade command system.

Unlike many commercial platforms adapted for today's threat environment, T.react CIP was developed for military operations and optimized for critical infrastructure protection.

Its sensor-agnostic architecture integrates existing third-party equipment alongside Terma sensors and scales from a single site to a network of bases and facilities.

When threat conditions change, operators can instantly switch between predefined security postures with a single action. Each profile automatically applies the appropriate detection thresholds, alarm rules, and escalation procedures without reconfiguration or new installations.

Supporting global deployments, T.react CIP offers multilingual operation together with built-in forensic recording, replay, and one-minute incident reporting with screenshots and video.

Designed Around the Operator

Modern security operations generate more information than ever before. The challenge is not collecting data, it is helping operators make better decisions.

T.react CIP was designed with this principle at its core.

Advanced sensor fusion, automated threat classification, intelligent camera tasking, and adaptive threat management work together to reduce cognitive workload and streamline operations. When a potential threat is detected, the system automatically presents relevant information and visual confirmation, allowing operators to assess situations faster and respond according to established procedures.

Rather than overwhelming users with multiple displays and competing alerts, T.react CIP provides a clear and intuitive operational environment that supports decision-making under pressure.
The platform's highly automated workflows and operator-centric interface allow personnel to become operational in less than 15 minutes, significantly reducing training requirements and minimizing dependence on highly specialized operators.

T.react CIP Unique Capabilities

Security teams operate in environments where threats rarely appear in isolation. A drone approaching restricted airspace, an unidentified vessel entering a security zone, or suspicious activity near critical assets may each seem routine when viewed separately. The challenge is understanding when they are connected.

Advanced Data Fusion

Security personnel cannot afford to make decisions based on fragmented information. T.react CIP correlates data from radar, AIS, ADS-B, cameras, sonar, drone detection systems, and other surveillance sources into one unified operational picture. Built on more than 20 years of multi-sensor fusion expertise, the platform presents a single validated track for each detected object, reducing uncertainty, improving situational awareness, and helping operators identify coordinated threats faster.

Enhanced Video Tracker

When an unidentified drone, vessel, or vehicle approaches a protected area, operators need visual confirmation quickly. T.react CIP automatically directs available long-range cameras to search, detect, classify, and track potential threats based on information received from radar and other sensors. By combining intelligent camera tasking with advanced video analytics, operators gain visual identification faster, providing valuable time to assess, escalate, and respond according to established security procedures.

Threat Level Engine

Security operations must adapt as the threat environment changes. T.react CIP allows organizations to define multiple threat levels, each with its own set of detection rules, alarms, and escalation procedures. When a threat level is activated, the system automatically applies the appropriate security posture, ensuring that operators work with the right level of surveillance and response without manual reconfiguration of the platform.

Features

Integrates with Your Existing Infrastructure

T.react CIP integrates seamlessly with existing radars, cameras, AIS, ADS-B, access control systems, and third-party technologies. Its open, sensor-agnostic architecture protects previous investments, minimizes deployment costs, and eliminates vendor lock-in.

One Operational Picture

T.react CIP combines data from multiple sensors into a single operational picture across air, surface, perimeter, and sub-surface domains. Operators gain a unified view of activity, enabling faster threat assessment and more informed decision-making.

Operational Continuity Through Fewer False Alarms

By combining intelligent sensor fusion, cooperative target identification, and advanced analytics, T.react CIP reduces nuisance alarms and unnecessary interventions. Security teams can focus on genuine threats while minimizing operational disruptions and maintaining continuity.

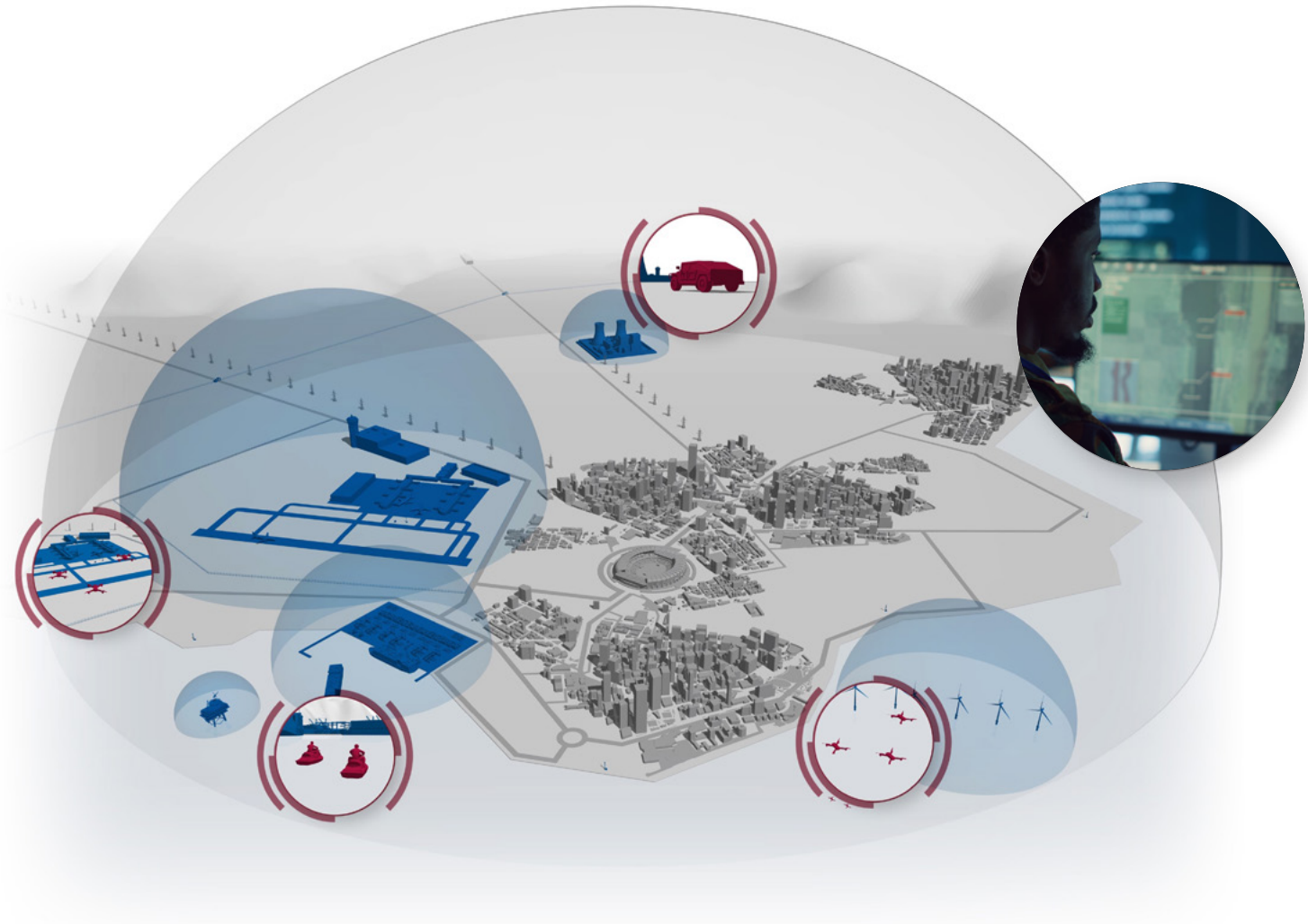
Key Benefits

- Military-grade sensor fusion and correlation, derived from Terma's air and maritime defense systems
- True multi-domain coverage of air, land, surface, and sub-surface in one operational picture
- Adaptive threat profile, switchable on intelligence in a single action
- Sensor-agnostic open architecture, integrating existing infrastructure with no vendor lock-in
- Forensic-grade scenario recording and replay with one-minute incident reporting
- Multi-language operator interface
- Operator-centric design with highly automated workflows, enabling personnel to become operational in less than 15 minutes

Proven Terma Expertise

Terma's Command and Control solution leverages the operational experience and counter-drone expertise of both Terma and OSL, now part of the Terma Group, strengthening the combined platform's ability to detect, track, classify, and manage emerging threats also leveraging different effectors.Additionally, Terma has been protecting critical infrastructure for more than 30 years. We know how a critical infrastructure protection system should be designed, integrated, and maintained, because we have already done it at scale, across continents and threat environments.

- 50+ critical infrastructure installations worldwide
- 30+ years of military-grade surveillance solutions
- 3,500+ Terma radar installations globally



Operating in the aerospace, defense, and security sector, Terma supports customers and partners all over the world. Our dedicated and talented global workforce develops and manufactures mission-critical products and solutions that meet rigorous customer requirements.

At Terma, we believe in the premise that creating customer value is not just about strong engineering and manufacturing skills. It is also about being able to apply these skills in the context of our customers' specific needs. Only through close collaboration and dialog can we deliver a level of partnership and integration unmatched in the industry.

Our business activities, products, and systems include: command and control systems; radar systems; self-protection systems for ships and aircraft; space technology; and advanced aerostructures for the aircraft industry.

Terma has decades of hands-on know-how in supporting and maintaining mission-critical systems in some of the world's most hostile areas. Terma Support & Services offers through-life support of all our products to maximize operational availability, enhance platform lifetime, and ensure the best possible cost of ownership.

Headquartered in Aarhus, Denmark, Terma has subsidiaries and operations across Europe, in the Middle East, in Asia Pacific as well as a wholly-owned U.S. subsidiary, Terma Inc., with offices in Washington D.C., Georgia, and Texas.

www.terma.com

TERMA
ALLIES IN INNOVATION