

## STRATEGIC WHITEPAPER



### *Public Critical Infrastructure Monitoring and Surveillance*

---

Persistent surveillance, decision support and response coordination  
for transport, energy, water, communication and other critical infrastructure.

**Published by Net Group Estonia — Germany**

[www.netgroup.com](http://www.netgroup.com) | [sentinelq.netgroupdigital.com](http://sentinelq.netgroupdigital.com)

*2026 Edition*

**Modern societies depend on a dense, interdependent web of public critical infrastructure: U-Bahn/metro systems, railways, roads, bridges and tunnels; rivers, dams and flood-control structures; gas and fuel pipelines; electricity transmission and distribution lines; heat and electricity generation; industrial parks; drinking-water networks, pumping stations, sewage pipes and channels, wastewater and water-treatment facilities; secure telecommunications; and the digital systems that bind them together. When a crisis hits — a mass-casualty incident, flood, wildfire, industrial accident, cyber attack, infrastructure failure or hybrid disruption — the difference between a contained event and systemic failure is measured in minutes.**

**To prevent unexpected disruptions, anticipate emerging risks, plan and simulate different scenarios, and enable effective cooperation between stakeholders across the critical-infrastructure ecosystem, modern and integrated surveillance capabilities are essential.**

SentinelQ® is an AI-powered surveillance, command and decision-support platform developed by Net Group for the protection, condition awareness and continuity of public critical infrastructure. It fuses critical infrastructure assets and emergency signals with geospatial and Earth-observation feeds, infrastructure telemetry and digital twins, transport and utility data, field-unit positions, authorised public-camera feeds, specialist inspection data from drones and underground robots, and verified citizen observations into a single resilience picture for civil-protection authorities, infrastructure operators and regional command centres.

*SentinelQ turns fragmented public- and private-sector feeds into one verified, defensible decision in real time.*

SentinelQ is designed for non-kinetic protection, maintenance and continuity of critical infrastructure: to monitor, detect, coordinate and document incidents that threaten safety; to manage the health of the critical infrastructure, plan the maintenance, repair activities and predict risk scenarios in the escalation of weather conditions or other external influence.

This whitepaper outlines the strategic context, the platform architecture, and the value SentinelQ delivers to possible stakeholders like regional emergency services, operators of critical public infrastructure and external service providers and society in general.

# 1. Strategic Context

## 1.1 A contested civil domain

German's critical infrastructure is increasingly exposed to compound and cascading shocks: extreme weather, floods, droughts and wildfires; energy and telecommunications outages; cyber incidents and physical sabotage; industrial accidents; and failures of ageing or stressed infrastructure. Because electricity, gas, water, wastewater, telecommunications, transport and industrial systems are deeply interconnected, disruption in one infrastructure domain can rapidly propagate into others and across municipal, regional and national borders. So the threat envelope has shifted from isolated incidents to persistent, overlapping pressure on the civil systems citizens depend on every day.

- Disasters — floods, wildfires, industrial accidents — demand multi-agency coordination across civil protection, EMS, aviation and utilities.
- Telecommunications, GPS and power outages can degrade response precisely when it is most needed.
- Underground and surface transport systems — including U-Bahn/metro tunnels and stations, railways, roads, bridges and tunnels — can suffer structural degradation, flooding, obstruction or service interruption with cascading effects across a city.
- Energy continuity depends not only on power plants but on transmission and distribution lines, substations, district-heating assets, gas pipelines and fuel logistics whose physical condition must be continuously understood.
- Water security spans rivers, dams, reservoirs, intake points, drinking-water plants, pumping stations, distribution pipes, sewage networks, drainage channels and wastewater-treatment facilities; disruption at one node can rapidly affect public health and essential services.
- Industrial parks and concentrated production zones combine hazardous materials, logistics, energy demand and large workforces, making early detection of abnormal conditions and access disruptions particularly important.
- etc...

## 1.2 The capability gap

*National and EU programmes have strengthened individual pillars — Copernicus emergency services, eCall, EU Civil Protection Mechanism — but a persistent, fused operational picture across several critical infrastructure elements, aviation and stakeholders remains a gap addressable only through AI-assisted, interoperable platforms.*

Most civil operators today rely on siloed systems: separate CAD/dispatch platforms, GIS viewers, aviation tools and broadcast channels. None of these alone provide continuous, fused awareness of what is the health of the critical infrastructure and how an unfolding event is consuming the capacity of the wider public-service network.

## 2. The SentinelQ as a Platform

SentinelQ is a layered command-and-control and infrastructure-observability architecture that connects strategic decision-makers — critical infrastructure owners and operators, civil-protection authorities — to field units, transport and utility control systems, authorised third-party inspection providers and trusted public observations through a single resilience backbone.

### 2.1 Persistent civil surveillance

- Earth-observation and Copernicus emergency-mapping feeds identify floods, wildfires, infrastructure damage and population exposure.
- German Open Data feeds about the critical infrastructure, the assets, the map layers giving valuable input into the project.
- Online data about air- and sea traffic situations (active transponders).
- AI models flag anomalous incident clusters, risk areas, traffic disruption and weather hazards along response corridors.
- Infrastructure telemetry and asset-management feeds expose the operating state and condition of U-Bahn/metro infrastructure, railways, roads, bridges, tunnels, rivers, dams, gas pipelines, electricity lines, substations, heat and electricity producers, industrial parks, water and sewage networks, channels, pumping stations, and water and wastewater-treatment facilities.
- Authorised drone operators can contribute scheduled or event-driven inspection imagery and sensor data — for example, identifying corrosion, damaged insulators, vegetation encroachment or other visible deterioration along electrical lines and hard-to-access infrastructure.
- Underground inspection robots can contribute structural, environmental and condition data from U-Bahn/metro tunnels, service corridors, pipes, culverts and other confined infrastructure where routine human inspection is difficult or hazardous.
- Where lawful and authorised, public video-camera networks can contribute real-time situational evidence about street conditions, traffic, access routes, crowd density and visible incidents. SentinelQ should ingest relevant event metadata and selected evidence under purpose limitation, retention controls and human oversight rather than defaulting to unrestricted population tracking.
- The SentinelQ mobile application can provide a controlled public-reporting channel: an individual can place a geolocated pin, add text, photographs or video and describe what they observe — for example, a suspected break-in at a water-treatment facility. Citizen reports enter the platform as unverified observations, with provenance, time and location metadata, and are corroborated against other sources before escalation.

### **3. The SentinelQ as a management system for emergency and critical infrastructure monitoring**

#### **4.1 Trusted Observation & Third-Party Sensing**

The observation layer is governed by source identity, contractual or statutory authority, role-based access and evidence provenance. SentinelQ distinguishes sensor telemetry, professional inspection findings, public-camera observations and citizen reports by confidence and verification status. AI may prioritise anomalies and recommend corroboration, but it does not silently convert an allegation or a visual pattern into a confirmed incident.

Third-party contributors may include utility maintenance contractors, certified drone operators, robotics inspection providers, transport operators, municipalities, camera-system operators and other authorised service partners. Each contributor exposes only the data needed for the agreed resilience purpose, using defined interfaces, retention periods and audit rules.

#### **4.2 Open-Data feed combined with Private-Data feed**

The SentinelQ integrates multiple information layers available through open-data and public-sector data sources, creating a common baseline for critical-infrastructure monitoring and situational awareness.

At the same time, private companies, municipalities and critical-infrastructure operators can operate their own secure and isolated SentinelQ instance, enriching the platform with proprietary operational and infrastructure data that does not need to be exposed outside their organisation. For example, a water utility can integrate detailed GIS maps of its pipeline network, pumping stations, reservoirs, treatment facilities, sensor telemetry, maintenance records and other asset-specific information.

By combining common external information layers with an operator's own trusted data, SentinelQ can create organisation-specific monitoring and risk-management environments. Each operator can configure dedicated monitoring views, define critical assets and dependencies, establish risk indicators and alert thresholds, and model scenarios relevant to its own infrastructure.

This enables organisations to move beyond simply observing individual assets toward understanding how external events may affect their infrastructure, where vulnerabilities and dependencies exist, and how different disruption scenarios could propagate through their network — while maintaining control and sovereignty over sensitive infrastructure data.

#### **4.3 Threat detection and data fusion**

SentinelQ correlates emergency signals, GIS and Earth-observation imagery, transport and utility telemetry, infrastructure digital twins, weather feeds, field-unit positions, professional drone and robotic inspection results, authorised camera observations and citizen-submitted map pins. AI classifiers transform raw signals into ranked operational hypotheses: possible failure of critical infrastructure elements (dams, bridges), infrastructure deterioration, service interruption, abnormal access to protected facilities, degraded communications cells, possible casualty situations and evacuation pressure points. Every hypothesis retains links to its source evidence, confidence and verification state.

## 4.4 Response layer

SentinelQ provides predictive warnings of emerging abnormalities, deterioration and potential failures across critical infrastructure. By continuously correlating infrastructure telemetry, environmental conditions, historical patterns, inspection data and external information sources, the platform can identify developing risks before they become critical incidents.

Beyond detecting an abnormality, SentinelQ is designed to assess what may happen if a critical asset degrades or fails. The platform can model potential cascading consequences across interconnected infrastructure — identifying which assets, services, geographic areas and communities may be affected and providing operators and authorities with an early indication of the expected impact.

For example, SentinelQ can provide predictive, cross-regional flood warnings by correlating upstream weather conditions, precipitation, snowmelt, river levels, reservoir status and hydrological data with downstream terrain and critical-infrastructure locations. If weather conditions change significantly in the Alps, SentinelQ can assess how those changes may affect connected river basins downstream, estimate potential inundation areas and identify exposed infrastructure such as dams, bridges, railways, roads, substations, water and wastewater facilities, industrial sites and telecommunications assets.

Affected infrastructure operators and municipalities can receive early warnings directly within SentinelQ, together with a map-based impact assessment showing what is at risk, where the impact is expected, when it may occur, and which infrastructure dependencies could be affected. Where population areas are exposed, the same analysis can support decisions on protective measures and potential evacuation zones.

The objective is to move critical-infrastructure protection from reactive incident detection toward predictive risk awareness — enabling stakeholders to recognise developing threats, understand their potential consequences and coordinate preventive actions before infrastructure failure produces cascading effects.

The warnings are presented either within SentinelQ, providing operators with a unified view of detected abnormalities, predicted risks and potential consequences or onconfigurable workflows can also be triggered automatically to integrate SentinelQ warnings with external information systems, enabling infrastructure operators, municipalities and other authorised stakeholders to initiate their existing risk-management, maintenance, incident-management and notification processes.

## 5. Strategic Value

### 5.1 For infrastructure owners and operators

- Continuous capacity, integrity and condition monitoring across transport, energy, heating, water, wastewater, flood-control, industrial and communications infrastructure.
- Early warning of surge events, supply-chain disruption and infrastructure damage.
- Reduced cost and friction compared with ad-hoc, manually coordinated multi-agency response.
- A tool for supporting NIS2 compliance, operational resilience and continuous readiness.

### 5.2 For civil protection and emergency services

- Sovereign awareness of public critical infrastructure status in peacetime and crisis.
- Resilience through persistent, attributable monitoring — making degradation visible, recorded and addressable.
- Faster decision cycles through unified GIS data fusion.
- Audit-grade evidence trail for after-action review, accountability and continuous improvement.

### 5.3 For the third party service providers

- Creates opportunities for specialised service providers to add value by integrating their services into the critical-infrastructure management ecosystem — for example, drone- and robot-based monitorings, remote sensing, predictive maintenance and other specialised services.

## 6. Team & Delivery Capability

SentinelQ is developed and delivered by a multidisciplinary team of Estonian–German engineers, emergency-services practitioners and systems architects with backgrounds in internationally recognised digital-health, public-safety and mission-critical technology programmes. The team combines deep expertise in data science, secure data integration, AI-enabled situational awareness and the delivery of command-and-control systems for civil-protection and military environments.

Its members have practical experience integrating complex multi-layer sensor, clinical and operational data systems across sovereign, civilian and public-infrastructure domains while maintaining strict cybersecurity, GDPR and citizen-data-governance requirements. Drawing on Estonia's globally recognised digital-government ecosystem and operational experience across both Estonia and Germany, the team brings strong capabilities in cyber resilience, secure infrastructure operations and trusted cross-domain information sharing between civilian agencies and other possible stakeholders.

*Awareness across the network. Accountability across the response.*

**For more information, contact Net Group — [www.netgroup.com](http://www.netgroup.com) | [sentinelq.netgroupdigital.com](http://sentinelq.netgroupdigital.com)**