

Boost resilience by embedding cyberspace into the Extended Common Operational Picture

Connecting stakeholders, data
and domains for holistic
situational awareness

Executive summary

Today's threat landscape is increasingly complex, with cyberattacks often forming part of broader, multi-dimensional campaigns that combine digital disruption, physical impact, misinformation, operational pressure, and other destabilising activities.

For organisations in public safety and critical infrastructure, and mission-critical operations, cybersecurity can no longer be treated as a purely technical discipline. It must be understood as a strategic and operational resilience issue that directly affects service continuity, public trust and mission performance.

This whitepaper highlights the need to extend the traditional Common Operational Picture into a cyber-enabled Extended Common Operational Picture (eCOP). By integrating cyber situational awareness with operational data, external intelligence and organisational context, an eCOP provides stakeholders with a shared understanding of risks, dependencies and potential impacts on their safety-critical services.

This holistic approach helps operational teams, security operations centres, executive leadership and external partners to enable a shared, trusted view of risks and impacts. It improves coordination and decision-making during cyberattacks, sabotage, physical disruptions and misinformation campaigns, helping organisations respond faster and maintain continuity of safety-critical operations.

The paper further recommends establishing a dedicated incident responder role with oversight of both operational and technical risks. Combined with secure communications, data fusion and decision-support capabilities, this approach strengthens resilience against hybrid threats and helps protect continuity in safety-critical operations.

Strengthen operations against growing security threats by integrating cyber situational awareness

In today's increasingly complex and serious threat landscape, cybersecurity attacks are much more diverse and sophisticated, especially in the context of public safety and critical infrastructure. Often strategically orchestrated and politically motivated, many attacks extend across multiple dimensions, going beyond pure cybersecurity threats to encompass social media and physical disruptions.

From the organisational perspective, this implies the need for closer links between cyber-physical systems, information security and physical threats to understand their influence on the required organisational capabilities.

To ensure safe and reliable operations in public safety and mission-critical work, organisations must therefore enrich and extend their Common Operational Picture (COP) by integrating a holistic view, embedding cyberspace and cybersecurity into it. By uniting what is currently a fragmented set of systems, people, policies and technologies, organisations can use these insights to inform strategic, operational and tactical decision-making, and to improve communication and collaboration with both internal and external stakeholders.

Protecting critical operations against multidimensional threats

In this age of geopolitical tension, where sophisticated state-sponsored actors pose a growing threat to critical infrastructure and public safety, siloed approaches to protecting physical and digital assets are no longer sufficient. Cyberattacks increasingly go hand-in-hand with attempts to disrupt physical operations, and attacks in one domain can quickly spread to others. These orchestrated threats are designed to disrupt operations, compromise sensitive data and destabilise organisations by exploiting vulnerabilities across multiple domains.

The emergence of orchestrated, multi-dimensional threats implies that cybersecurity must no longer be viewed as a technical activity at the edge of the corporate network, but as a strategic imperative that touches every part of the organisation. Equally, the organisational and systemic barriers between information technology (IT), operational technology (OT), and the required operational capabilities must be removed so that vital information can flow freely between them.

Fragmented views

Most organisations struggle to gain a clear and unified view of the threats they face because the relevant information comes from multiple unconnected sources and is managed by different teams of people. The resulting gaps in visibility and inter-departmental coordination can hinder timely and intelligent responses to threats and incidents, putting organisations at risk of disruption to their core operations. In particular, threats in the cyber domain have a huge impact on the overall organisation and its capabilities.

Without real-time information on the combined status of cyber-physical systems, operational

capabilities and hybrid threats, decision-makers miss opportunities to mitigate risks. This increases the likelihood of contagion, such that relatively small attacks can snowball into operational disruptions, financial losses and reputational damage. Indeed, many attacks are designed to work across multiple dimensions – such as social media, cyberspace and the physical environment – over a sustained period precisely to exploit the gaps in the typical organisation's security posture.

Slow detection and response

Speed and agility are critical factors in any organisation's ability to face up to complex security challenges. Organisations need to be able to identify attacks, determine the root causes, decide on the appropriate counter-measures, and communicate instructions to the relevant teams. This all needs to happen as rapidly as possible, especially when operational capabilities are at risk of disruption.

Where a cyberattack is particularly sophisticated, the first sign may be its impact on operations, and this highlights the need for a more connected and integrated approach to security. When an organisation's teams (for example: operational teams, SOC teams) work in their own silos, using their own systems, it is easy for multi-dimensional attacks to have a serious impact before the organisation as a whole is even aware of them. For example, fake news spreading on social media about damage to railway infrastructure could cause a sudden decrease in the number of passengers. Without an organisation-wide ability to see this operational trend and communicate it to the appropriate teams, the organisation's core mission could be severely disrupted.

Embedding cyber awareness into operational decision-making

It is standard practice for many organisations working in safety-critical industries to have a Security Operations Centre (SOC) that is responsible for cybersecurity threat detection, defence measures, and the monitoring of both IT and OT environments. However, the SOC is usually seen as part of the technology infrastructure, separate from the operational domain. Its outputs are typically not integrated into the organisation-wide Common Operational Picture (COP) and are limited to cybersecurity incident management, being the first line of defence for the organisation.

The best-practice approach today is to create an extended COP (eCOP) that includes real-time information and analysis from the cyberspace domain, as well as information on operational capabilities and demands. By combining this operational context with cybersecurity insights from SIEM platforms and relevant external sources, organisations gain a more comprehensive understanding of potential threats and their operational impact.

For organisations that need to combine strategic, operational and governmental perspectives into a single, unified view of the threat landscape, an eCOP can provide:

360-degree situational awareness across IT, OT and operations

Faster, better-informed decisions that take operational constraints into account

Greater resilience against hybrid attacks

Stronger crisis management

Built-in documentation and recording for compliance

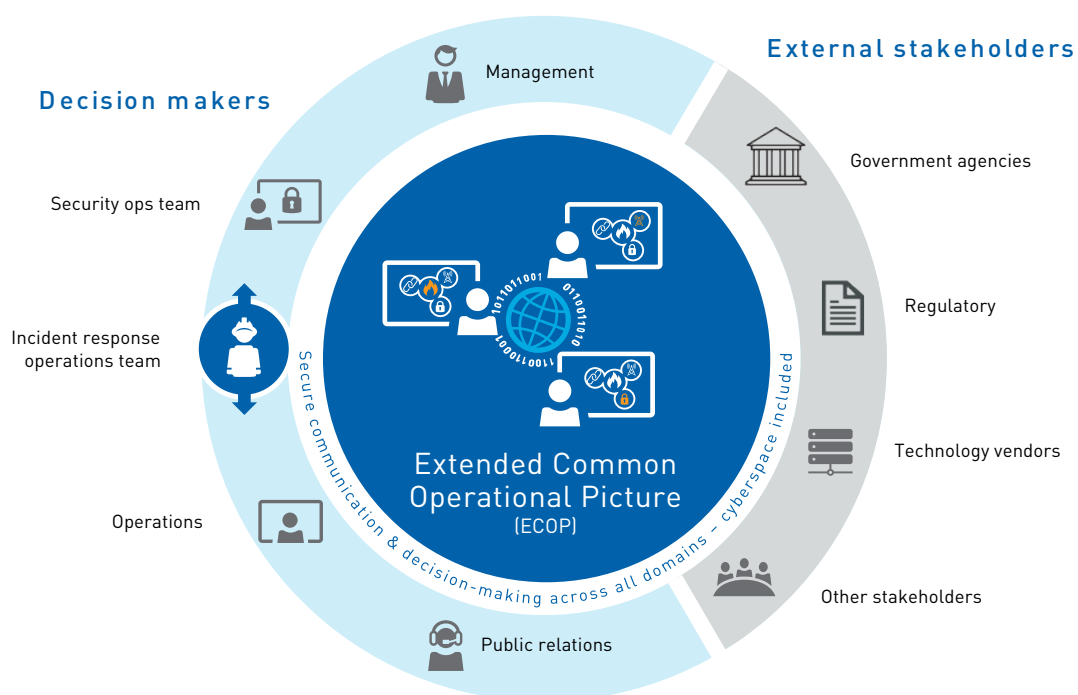
Enabling a coherent understanding of the risk landscape

The key value of an eCOP is to enable a coherent understanding of how cyberthreats intersect with strategic risk, organisational stability and long-term resilience by revealing the connections between strategic objectives and day-to-day operational realities. An eCOP provides a layered view of all potential threats to operational stability and capacity. It covers not only cybersecurity but also other segments like staffing, public sentiment, operational capabilities and so on – essentially anything from the virtual or physical worlds that could impact operations. The consolidated perspective provided by an eCOP helps translate complex information into actionable insights that allow organisations to assess potential impacts on business continuity, evaluate operational dependencies, coordinate cross-functional response measures, and guide risk-informed decision-making, investment planning, and organisational prioritisation. Particularly during large-scale incidents, reliable and secure communication capabilities

are vital. Information will typically need to be shared not only with operational and security decision-makers, incident-response teams and crisis-management personnel, but also with board members, executive leaders, government cybersecurity centres/national Computer Emergency Response Teams (CERTs), and the general public. The information will often flow in both directions; for example, CERTs will contribute authoritative external insights, including early warnings, threat intelligence and regulatory expectations.

Integrating operations and cyber security in a new role

Organisations in safety-critical industries must establish a holistic eCOP that incorporates the cybersecurity domain, seamlessly blending operational data with internal assessments and external perspectives to support informed decision-making in high-pressure situations. In addition to gaining the ability to fuse and analyse data from multiple domains and sources, public-safety organisations should consider creating a new incident responder role with oversight of both the operational and



Connecting decision-makers against holistic cyber threats

technical risks. This role would be responsible for maintaining a comprehensive overview of detected threats, operational performance, and surroundings (media, relationships). The incident responder would use the eCOP to enable early identification of emerging issues and ensure organisational readiness to tackle challenging situations.

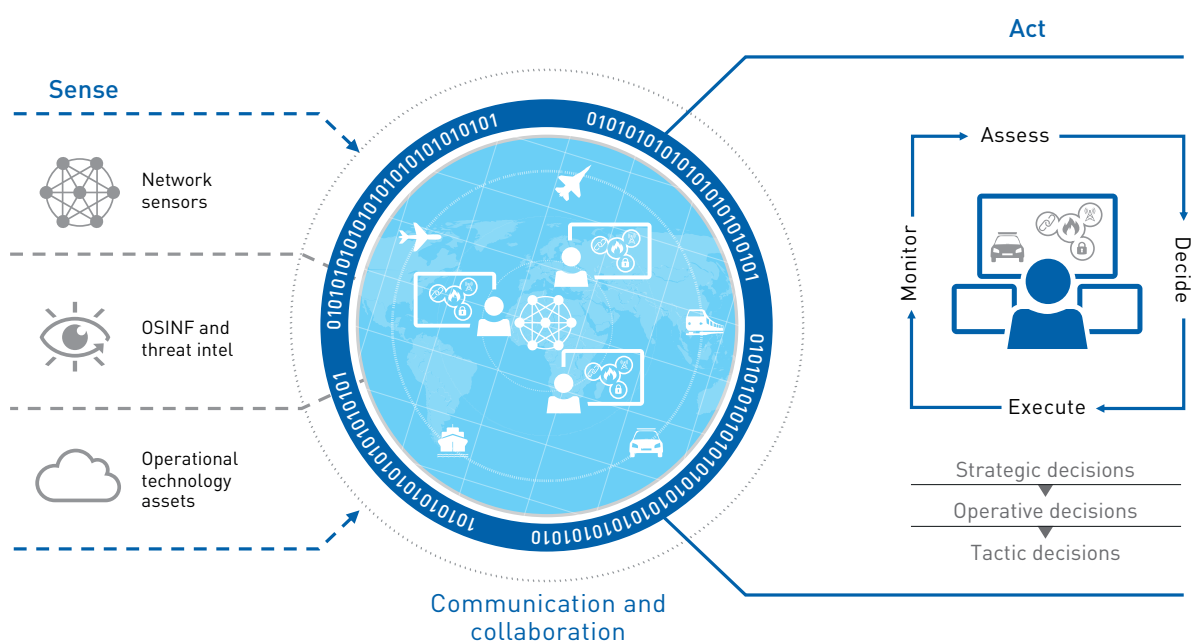
By monitoring operational activities, technical systems and relevant social media signals, an incident responder would support and reinforce the work of the SOC, allowing cybersecurity specialists to remain focused on their role as the primary line of defence—while enjoying enhanced situational awareness and operational context.

Introducing a holistic approach to security threats

Maintaining operational resilience in the face of multi-dimensional threats depends on both technical and operational discipline. An eCOP provides the foundation for understanding threats holistically and acting decisively under pressure to protect safety-critical operations. From the organisational perspective, bringing together the people, policies and processes

relating to both security and operational management will enable the effective use of the eCOP to support safe and reliable operations. Building these capabilities and organisational structures will typically start as a consulting engagement to determine the as-is and to-be processes, as well as the data that is available to support them. In addition to integrating existing sensors across the extended network, during ongoing system evolution it may be necessary to deploy new sensors and integrate additional sources of information from outside the organisation. The next step will be to fuse and analyse the available data to support multiple different workflows and perspectives, present it to different internal and external audiences, and build appropriate automations into the sense-to-act cycle. By choosing an external partner with a deep understanding of safety-critical industries and long experience in cybersecurity for OT systems, data fusion, data presentation, decision-support systems and secure communications, organisations can layer new capabilities on top of their existing cybersecurity measures to enable a holistic view of security threats.

Extended common operational picture – incl. cyber domain



Targeted Measures through Shared Situational Understanding

Take the next step

For more information on how Frequentis can help your organisation face up to complex security threats, contact us today.



FREQUENTIS AG
Innovationsstraße 1
1100 Vienna, Austria
Tel: +43-1-811 50-0
www.frequentis.com

The information contained in this publication is for general information purposes only. The technical specifications and requirements are correct at the time of publication. Frequentis accepts no liability for any error or omission. Typing and printing errors reserved. The information in this publication may not be used without the express written permission of the copyright holder.