
NET
NOD

From Compliance to Survivability

Building Resilient Digital Infrastructure

Patrik Fältström · Netnod

CAETS 2026, Munich

Bridging Perspectives – Earth Observation for Decision-Making, Security, and Resilience

Where do I come from?

- Netnod – operator-neutral, 30 years at the core of the Internet
- The largest Internet Exchange (IX) in the Nordics
- i-root – one of the world's thirteen DNS root name servers
- Swedish time and frequency is distributed by Netnod on behalf of the Swedish Post and Telecom Authority
- Various security services
- Co-author, IVA (Royal Swedish Academy of Engineering Sciences) report *Cyber Risks and Vulnerabilities in Nuclear Command, Control and Communication Systems* (July 2024)

Satellite: a diversity mechanism, not a core network

Its real value is path diversity

- A route no terrestrial network can replicate

But access is only access

- Ground station or mast — the path onward to the service still runs on fibre

Diversity moves the last mile — it does not replace the core

- You still need a resilient, fibre-connected core

Satellite sits inside the nuclear chain, not at its edge

- DSCS and AEHF carry presidential and nuclear-force traffic to air and ICBM crews

DSCS — Defense Satellite Communications System · AEHF — Advanced Extremely High Frequency · ICBM — Intercontinental Ballistic Missile

Satellite adds a path — it does not remove the need for a resilient core.

Targeted, not stochastic: KA-SAT, 2022

24 February 2022 — one hour before the invasion

- A misconfigured VPN appliance into KA-SAT's management network, then AcidRain wiper malware bricked tens of thousands of modems across Europe

Ground segment only

- Viasat: no evidence the satellite or its ground infrastructure was compromised

The spillover reached Germany

- 5,800 Enercon wind turbines lost remote monitoring — still generating, but blind

The EU called it deliberate

- *"… thus facilitating the military aggression"* — EU declaration, 10 May 2022

This wasn't chance. It was chosen — the moment, the target, the method.

Stochastic failure – or an adversary?

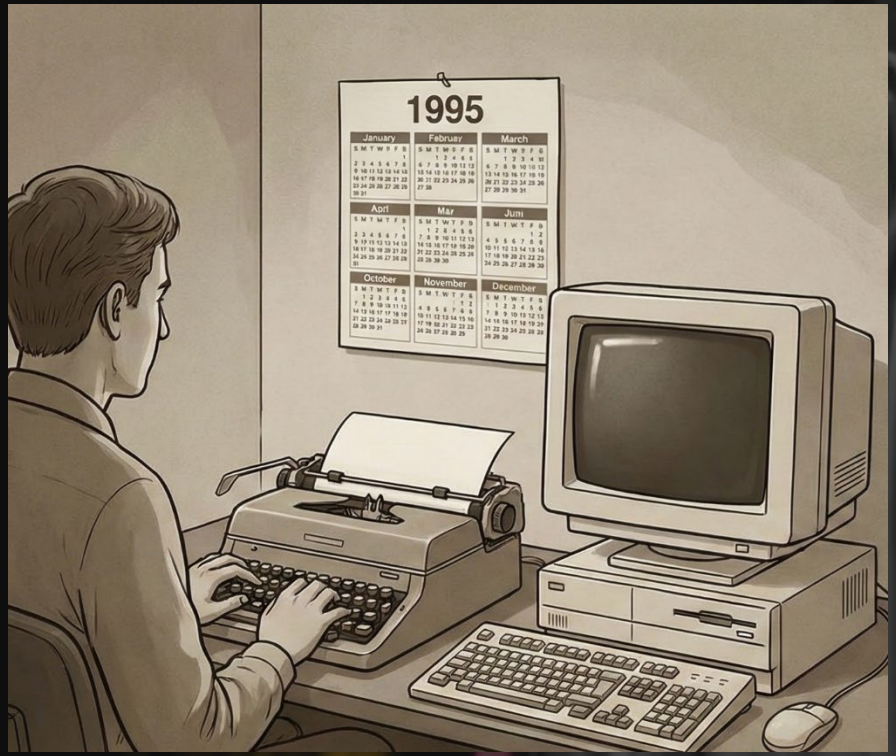
BEFORE — chance

- Natural events, component failures, suppliers closing — chance doesn't care who you are
- History predicts the future: MTBF, statistics, due diligence
- Two independent solutions cut the risk
- Occurs at random, any time

NOW — someone who chooses

- Russia, North Korea, Iran — direct, or via deniable proxies
- The adversary chooses you, based on your value — not chance
- History tells us little; the adversary's intent matters more
- Two similar solutions offer no protection
- Strikes when and where you're weakest

Chance doesn't care who you are. An adversary does.



Before: Digital complements

Now: Digital dependencies

AI compresses the timeline

The attack chain gets shorter, not different

- Recon, phishing, vulnerability analysis, lateral movement – faster and in parallel

Response times assume a timeline that no longer exists

- Alarm at night, call in the morning, action after lunch — attacker in seconds, we in days

Consequence for risk analysis

- How fast we restore, and how much data we accept losing — both set against the wrong clock

Faster than the adversary — anything slower is reaction, not defence.

The legislator cannot answer these for you

- Do you know what you do — and what's expected of you?
- Do you know which IT systems and functions you need to keep running for at least two weeks?
- Does the legislator know your organisation better than you do?

EU Preparedness Union Strategy, March 2025: households should cope alone for at least 72 hours. Sweden goes further — MCF says one week without help from society: food, water, heat, information.

European Commission, 26 March 2025 · mcf.se

The EU says 72 hours. Sweden says a week. Can your organisation do better?

Compliance is not survival.

None of us can fix this alone

Nothing you run stands alone

- You are one link in someone else's chain

An incident that misses you can still stop you

- Contracts move the risk, not the dependency

A chain is no stronger than its weakest link

- Several chains help — but only if they are truly separate

Your own risk analysis isn't enough

- It stops at your perimeter. Your dependencies don't

Patrik Fältström

Senior Security Consultant

paf@netnod.se

Greta Garbos väg 13
169 40 Solna
Sweden

Visit us at netnod.se