Building resilience

strategies for securing core Internet functions in the Nordics

Kaj Kjellgren
Technical Ambassador
Netnod

What do we mean by resilience?

- Removes single points of failure
- Provides security by diversity
  - diverse technologies, nodes and locations → resilience and security
- Ensures very high uptime
  - multiple, redundant nodes → 100% uptime possible
- Built secure by design
  - Designed with security as a priority → Proactive security

What do we mean by resilience?

- Uses systems with redundant layers
  - Multiple layers of redundancy → service can handle failures without intervention
- Designed with full awareness of dependencies
  - Full understanding of dependencies → potential issues managed proactively
- Rock-solid 24/7/365
  - Resilient every second, not just when under pressure → the light never goes out!

Wha lience?

Example 1

Large Swe ll DHCP-service for the whole

When that could get an IP address!

What ence?

Example 3:

Around 2008-20

Swedish operat

traffic through S

Sweden is long (

(20 ms+)

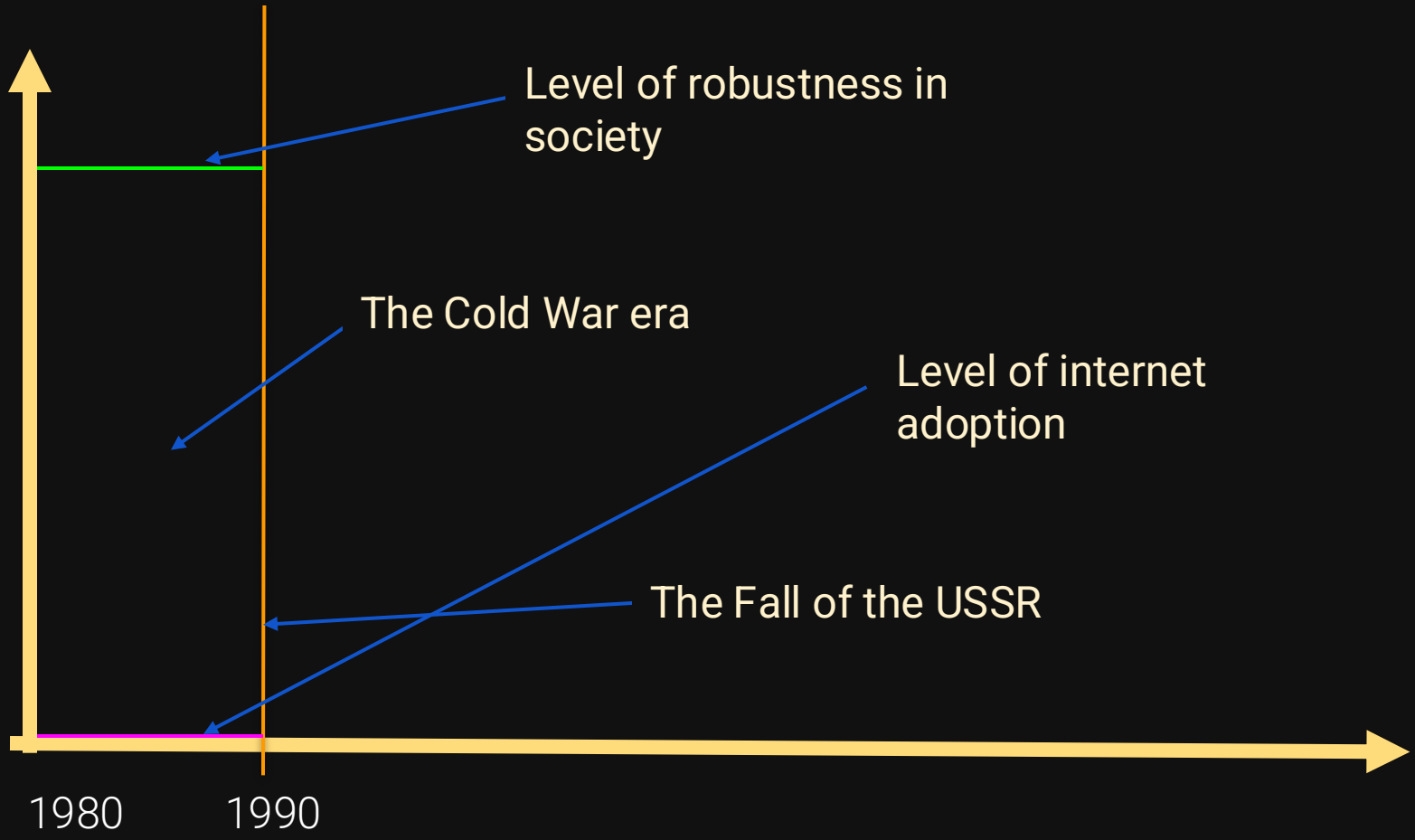
If Stockholm go

Why wa from the star

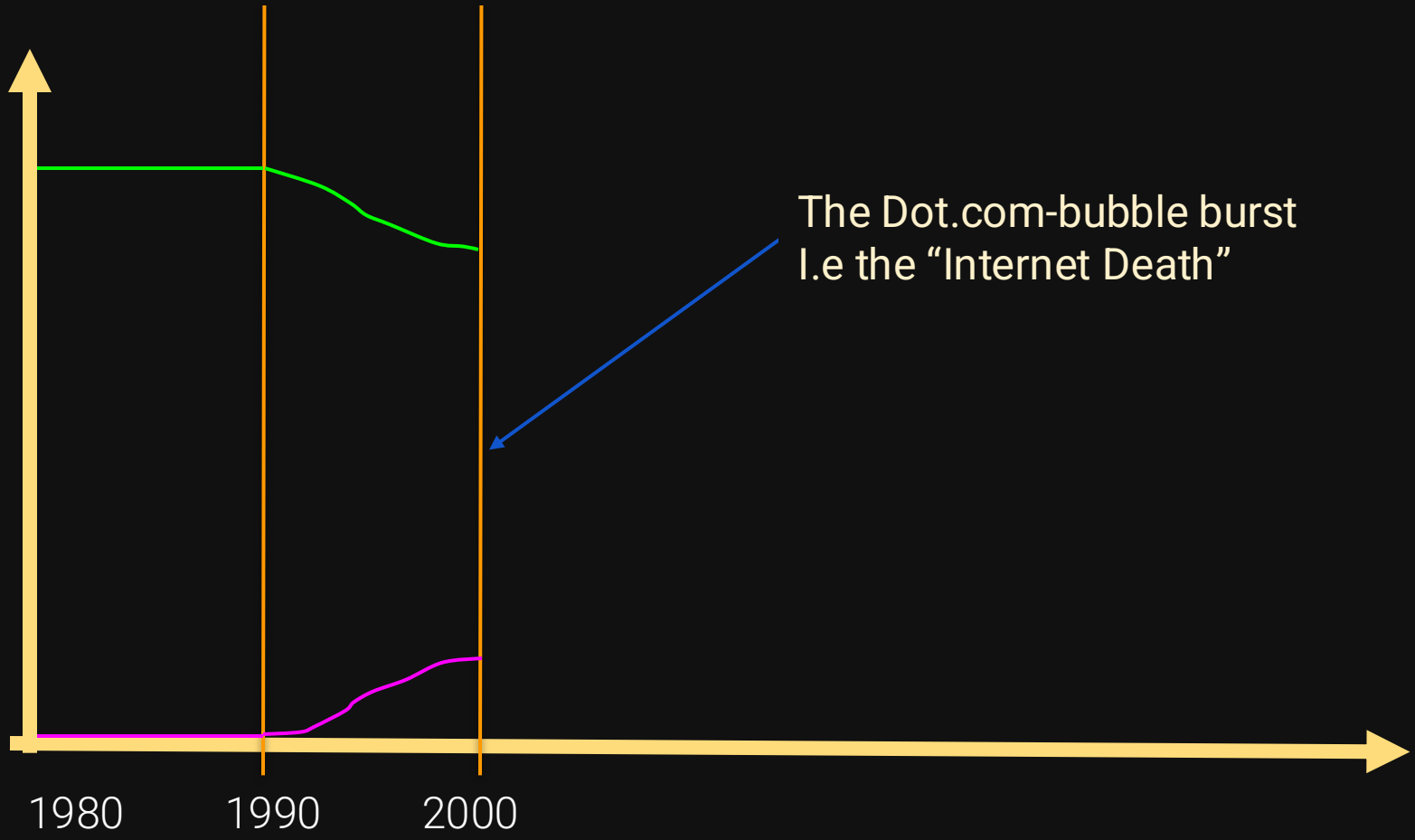
- Cost - no bus t willing to pay more f
- ISP's built eve e.
- Geopolitics wa crisis situations as th

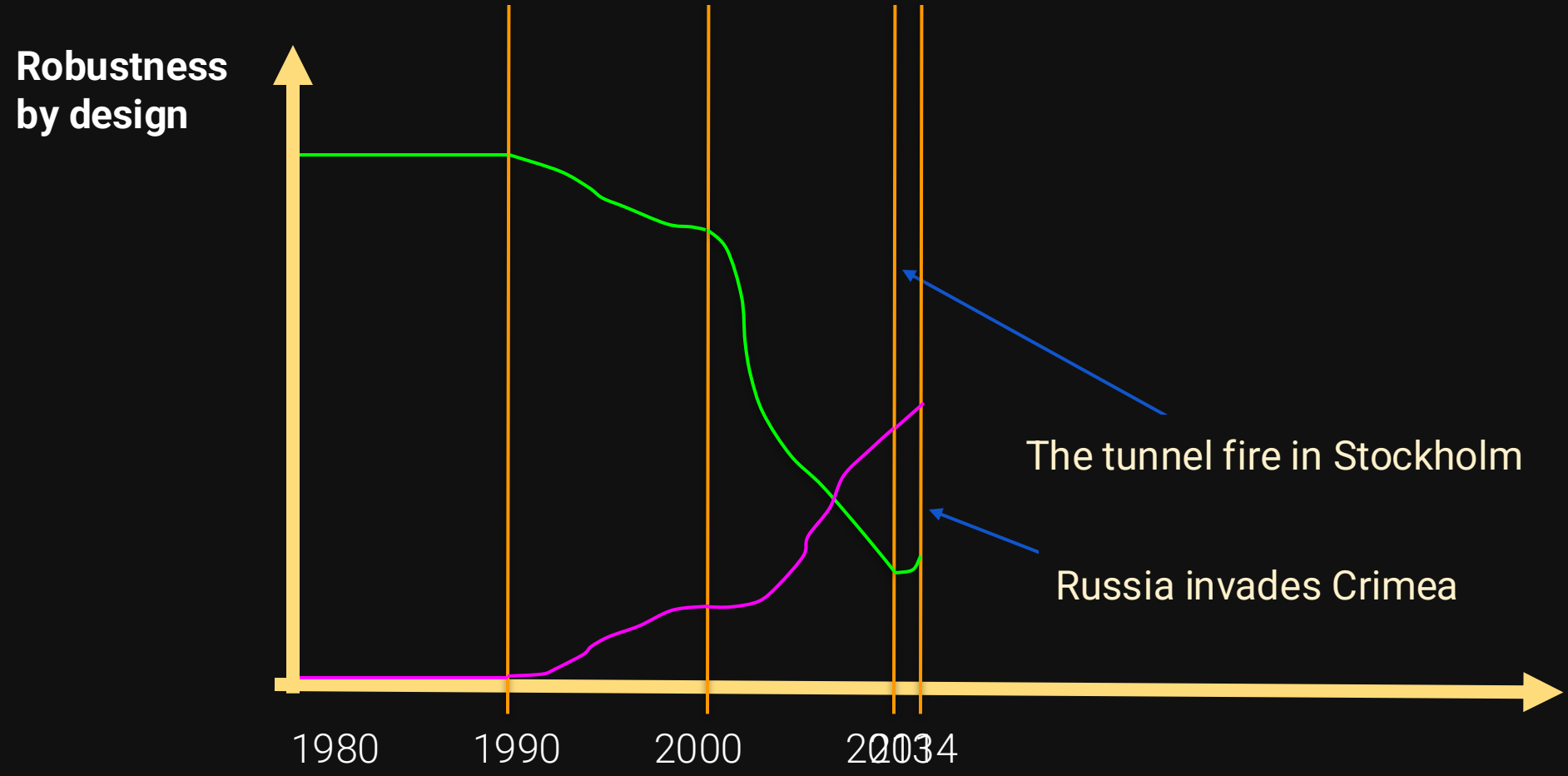
→ centralised

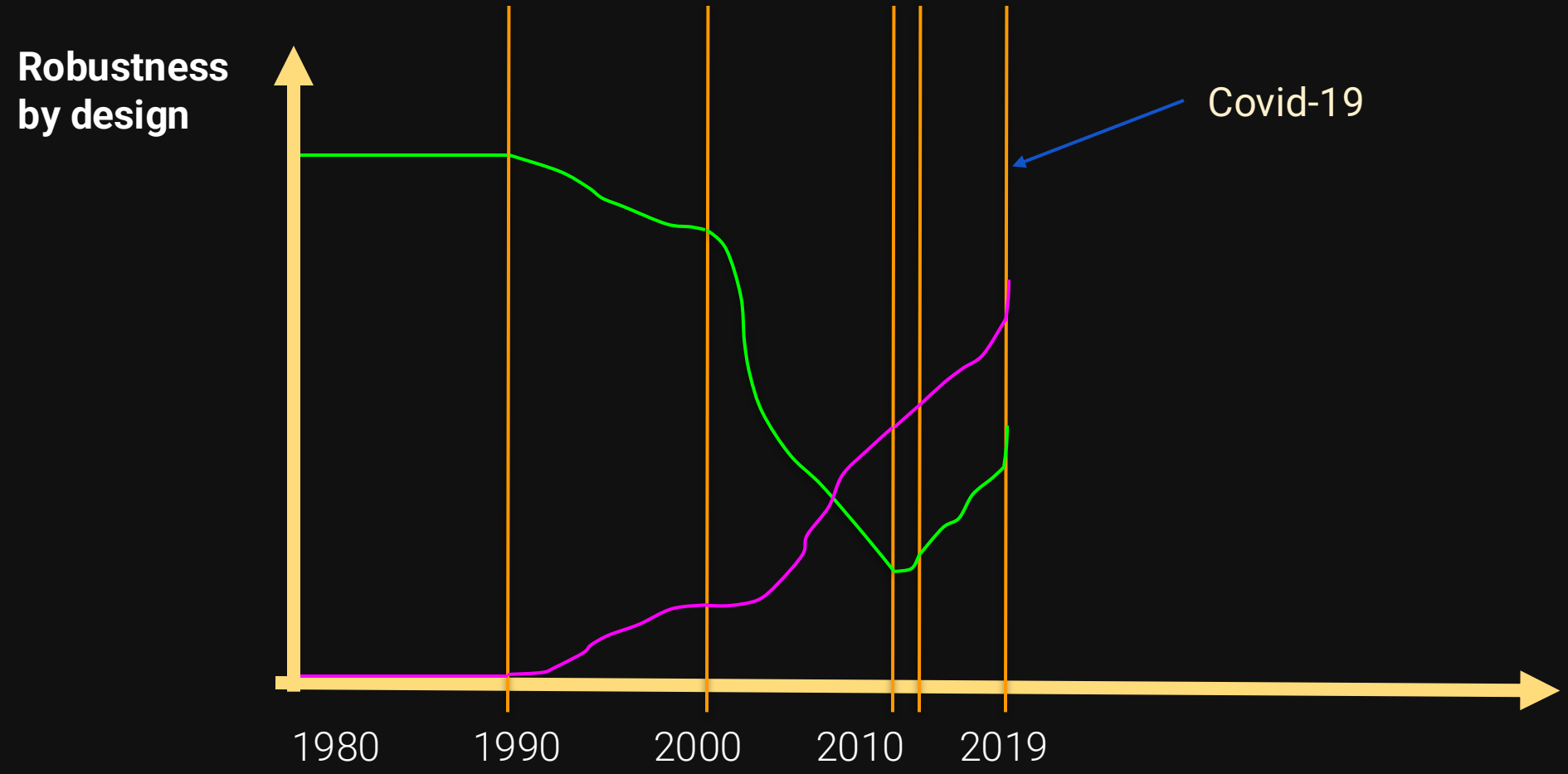
Robustness by design

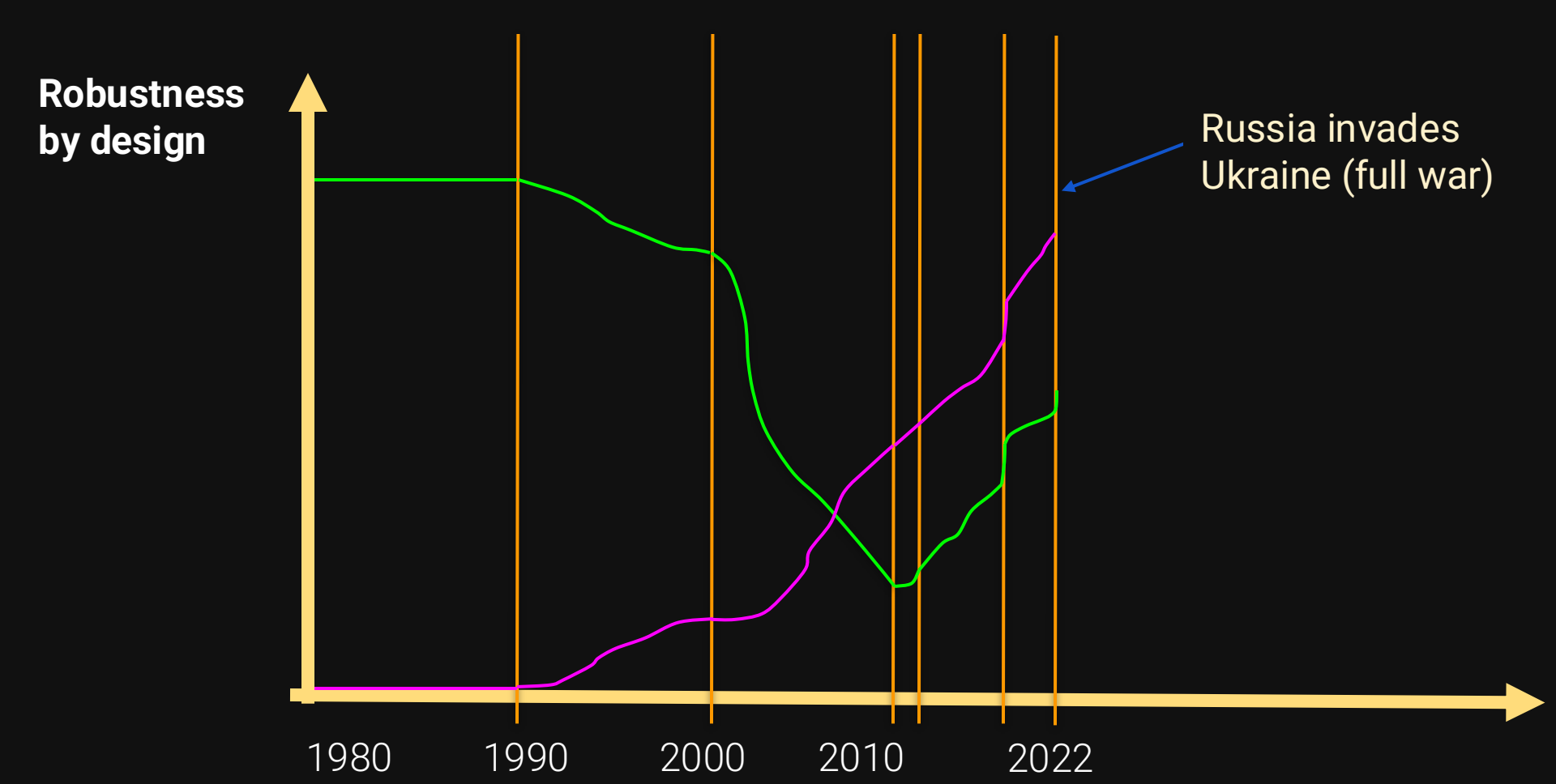


Robustness by design

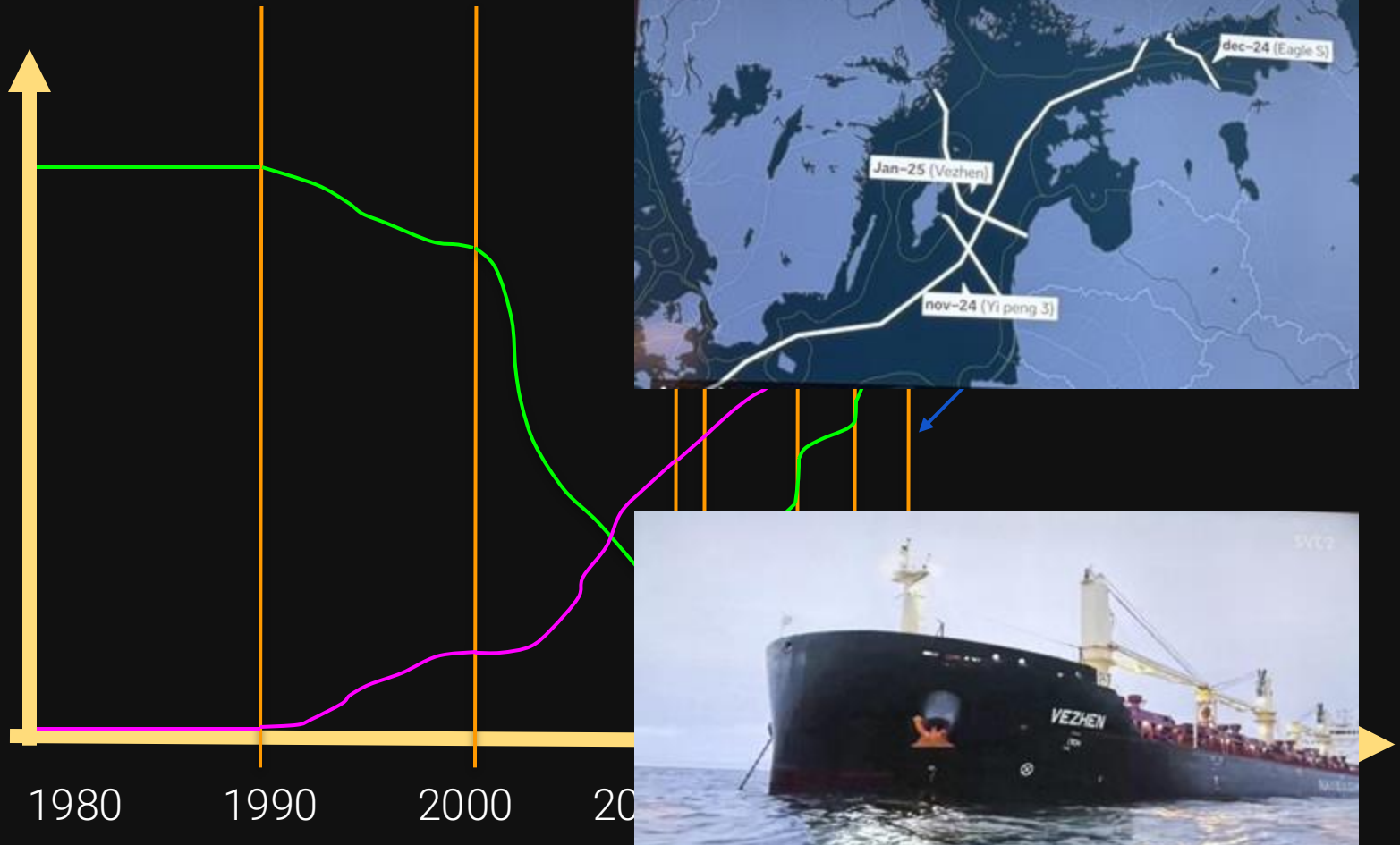


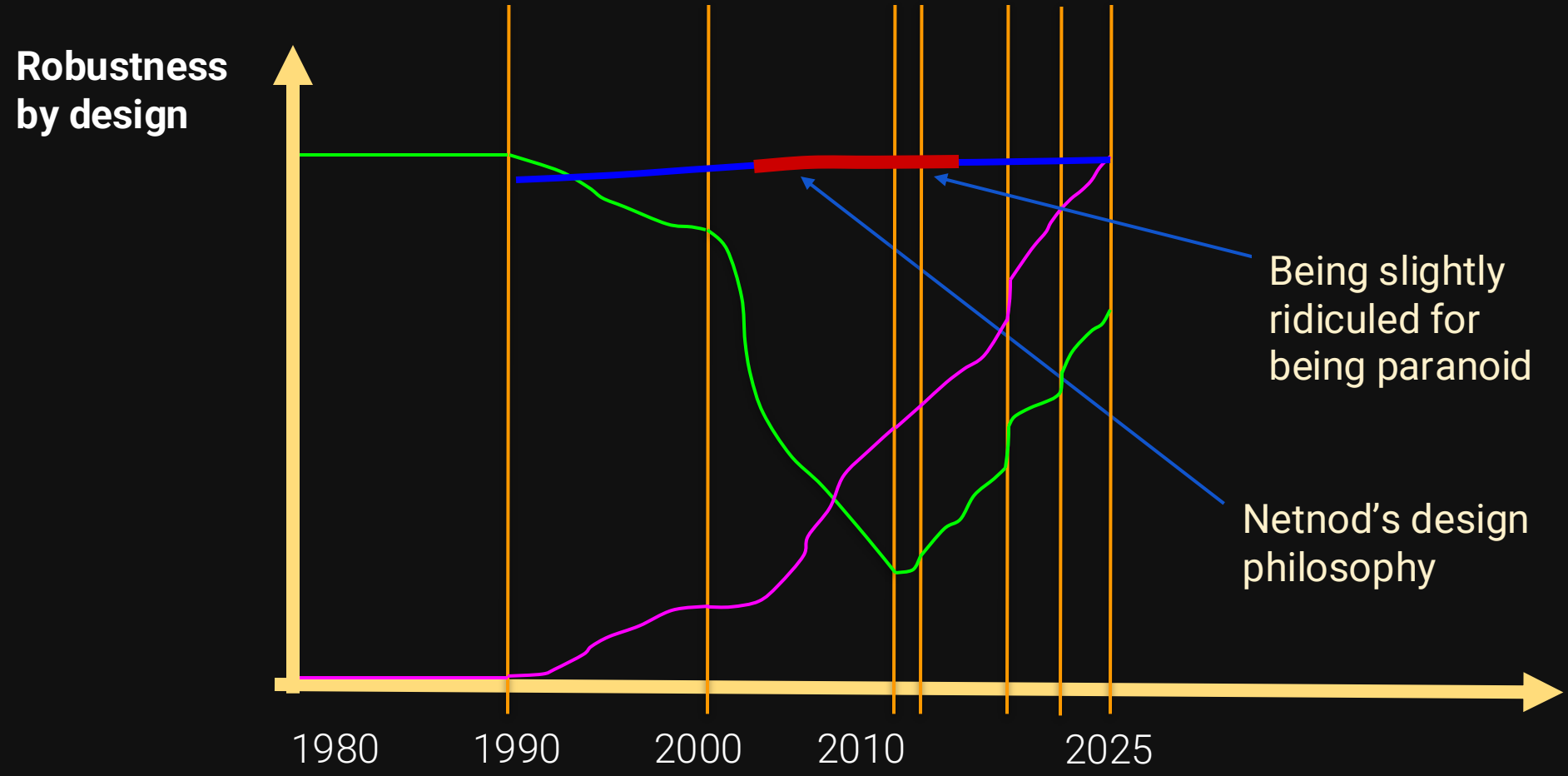

Robustness
by design
The tunnel fire in Stockholm
Russia invades Crimea
1980
1990
2000
2014


Robustness
by design
Covid-19
1980
1990
2000
2010
2019


Robustness
by design
Russia invades
Ukraine (full war)
1980
1990
2000
2010
2022

Robustness by design



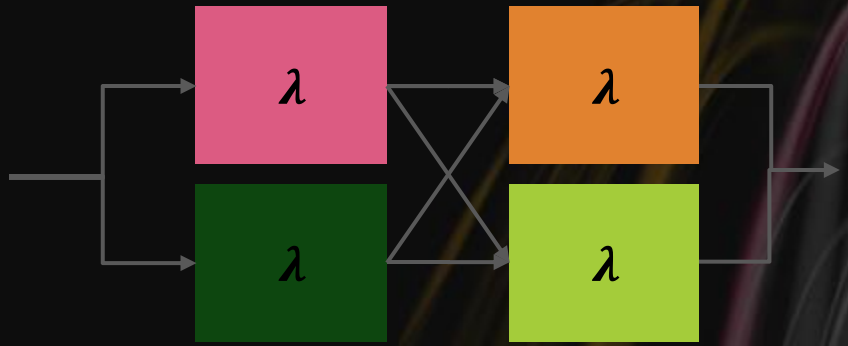

Robustness by design
Being slightly ridiculed for being paranoid
Netnod’s design philosophy
1980
1990
2000
2010
2025


“Everyone has a plan
until they get punched in the mouth”
– Mike Tyson

Building resilience: interconnections

Example: IX’es (and more)

- Fully redundant design
  - Multiple switches
  - Multiple routes
  - Multiple BGP (routing) implementations
  - Proactive monitoring
  - Critical hardware kept in VERY secure locations
  - Robust organisation with long term commitment
  - Should work with the “Good of the Internet” as a goal
- Provides multiple ways to interconnect
  - Make sure to promote all kinds of interconnections



Building resilience: Time

Time and socially critical functions

Accurate and secure time is fundamental for socially critical infrastructure and functions such as:

- Mobile networks
- Financial transactions
- Energy grid

These depend on **synchronised, accurate and secure time.**

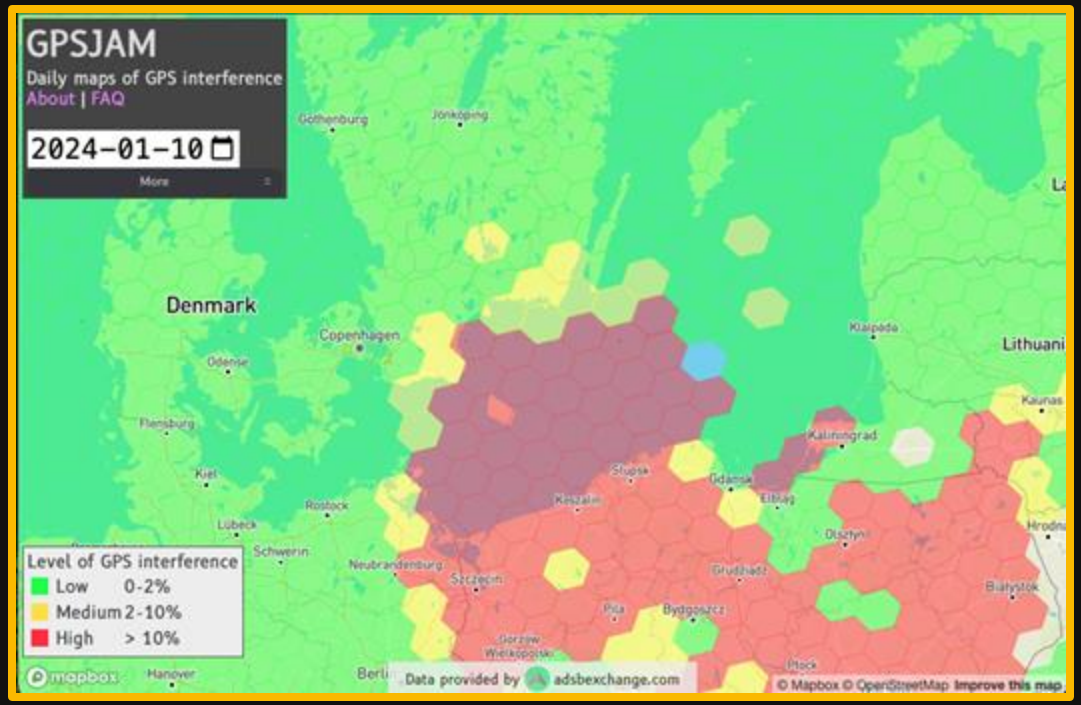
No security without time security

Many security critical protocols need accurate time:

- DNSSEC, secure domain name lookups
- TLS, the basis of many other protocols
- HTTPS, everything on the web
- SMTPS, IMAPS, POP3S, secure mail

Without secure and reliable time, the **entire network is at risk.**

GNSS – The weak link in critical infrastructure



https://gpsjam.org/?lat=55.64583&lon=15.60824&z=5.3&date=2024-01-10

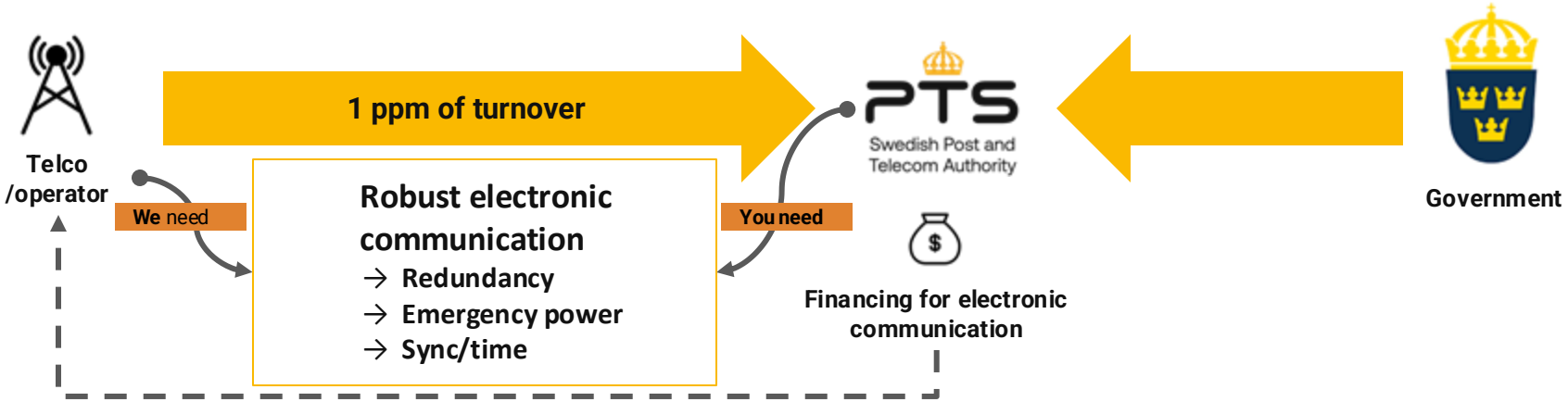
(source: https://gpsjam.org/)

Clock nodes for Sweden's time service

- 6 time nodes placed in secure bunkers throughout Sweden (Stratum-1 time servers)
- Dual nodes with all critical equipment duplicated for redundancy (2x caesium clocks)
- Dedicated battery backup for all time components
- NTP/NTS servers use a custom-built FPGA-based hardware implementation

Funding resilience: the Swedish model

Robust financing



What can operators do to ensure resilience at organisational level?

1. Design for resilience
2. Look at what is happening elsewhere and talk about how this applies to your own region
3. Engage with government/regulator in discussions about resilient infrastructure. Public/Private cooperation is essential and you need to understand requirements from all sides
4. For socially critical infrastructure, make sure you are involved in the long-term planning
5. Make sure that your organisation/leadership stays true to the goal of resilience also when it comes to staffing and taking care of the employees. Losing critical staff is… bad

What can operators do to ensure resilience at technical level?

1. Check your clocks! There is no security without time security.
2. Make sure you have robust DNS (especially for mission-critical zones).
3. Look at your connection strategy.
    a. Do you have diverse paths to your most important peers?
    b. How much traffic are you getting over the IX route server? What happens if you lose access, e.g. do you have redundant connections to the IX route server?
    c. IX'es and PNI's are a good thing. They add to robustness.
4. Secure your routes! e.g. use RPKI and ROAs.

Thanks for listening!

Visit ut at netnod.se