

NET NOD

Regelefterlevnad eller överlevnad?

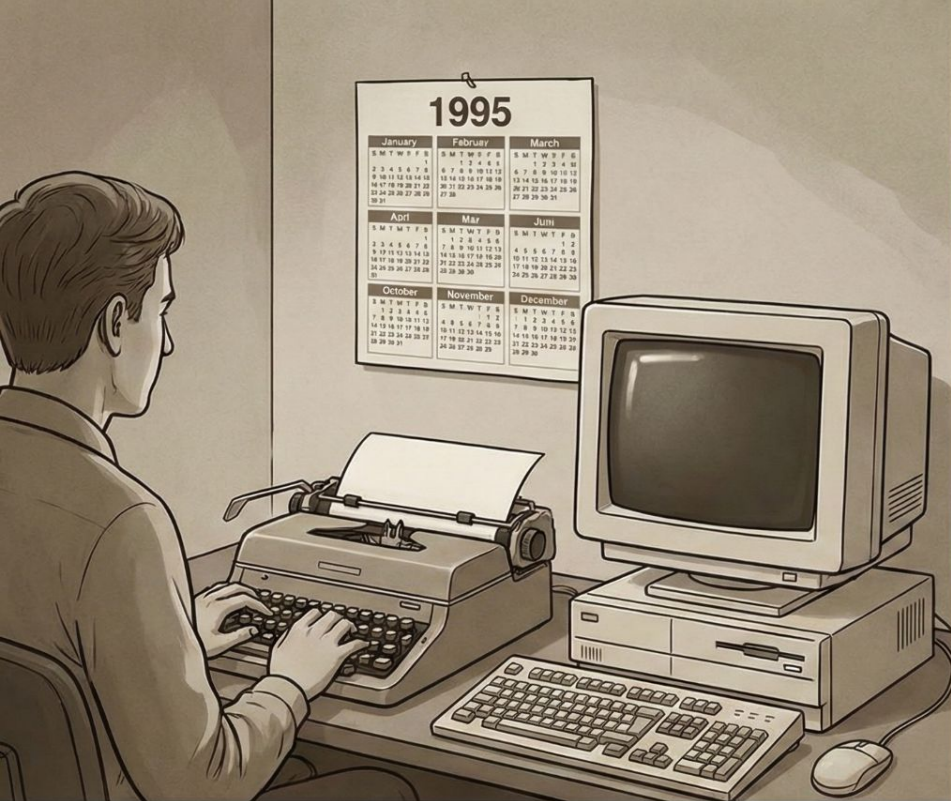
Fredrik Lindeberg, PhD, CISO

Var kommer vi ifrån?

Vi är en operatörsneutral organisation som i mer än 25 år jobbat med centrala delar av Internet

- Vi driftar den största **Internet Exchange (IX)** i Norden
- Vi är rotnamnsserveroperatör, och driftar i-root, en av världens tretton (13) rotnamnsservrar i **DNS**-systemet
- Vi erbjuder **DNS**-tjänster till företag och några världens största toppdomäner (TLD:er)
- Vi utvecklar och driftar **tid- och frekvens**-tjänster med höga krav på precision och säkerhet
- Vi hjälper **digitaliserade organisationer** i deras arbete med **robusthet och resiliens**





FÖRR: DIGITALA KOMPLEMENT



NU: DIGITALT BEROENDE

Digitaliseringen av Sverige

Digitalisering är:

- Möjligheten att omvandla fysiskt till digitalt, och tillbaka
 - Även behandling digitalt -> digitalt
- Kommunikation - överföring av det digitala - Internet
- Hur man gör ovan - metoder

Sverige är idag ett av världens mest digitaliserade länder, men kanske inte alltid på det mest genomtänkta sättet

Digitaliseringen måste vara rock-solid

Digitaliseringen av Sverige

- Idag är Internet jämställt med kommunikation
- Tidigare hade telefonen och radion liknande roll, inkluderat nödkommunikation
- SOU 2024:34, Kommittédirektiv Dir. 2024:74, MSB2263, Ds 2023:34, osv

Internet och den underliggande arkitekturen används för kommunikation till i princip allt som inte är blåljusverksamhet idag

Internet måste vara rock-solid

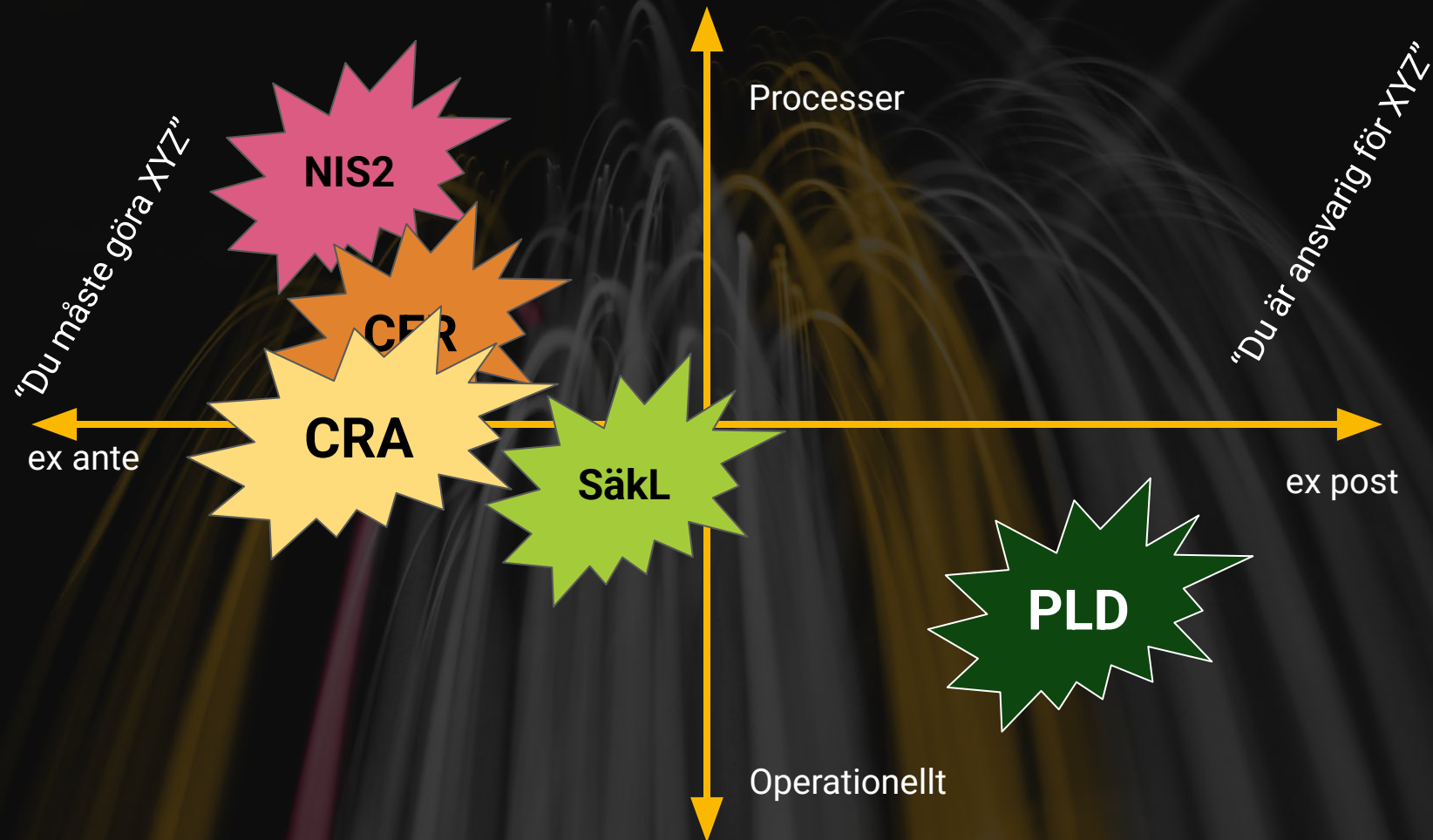
The background of the slide is a dark, almost black, surface. It is decorated with numerous thin, glowing lines that resemble fiber optic cables or data streams. These lines are primarily yellow and orange, with some strands of red and blue. They are arranged in a dynamic, flowing pattern, with many lines curving upwards and outwards from the bottom left and bottom right corners towards the top of the frame. The lines have a soft, ethereal glow, giving the impression of light traveling through the cables.

Internet

Mer än katter och Netflix

En kommunikationsarkitektur för mer än katter

Företagsnät, e-handel, sjukvård, omsorg, civilförsvär,
internationell samverkan, betallösningar....



Omvärldsanalys - regelutveckling

Nya och uppdaterade regelverk kopplade till cybersäkerhet

EU

Gräver ner sig i **ex-ante** reglering kopplat till processöverbyggnad

- CRA, NIS2, CER, DNA osv.
- **ProtectEU**: Idag en otydlig strategi för intern säkerhet. Påverkar elektroniska kommunikationer och operatörsansvar.
- **Regelefterlevnad?**

USA

Ändrad inställning för compliance under 2024 (sept, DOJ ECCP)

- Från *"du skall göra så här!"* till *"fungerar det du gör?"*
- *"Is the program well-designed? Is it adequately resourced and empowered? Does it work in practice?"*
- **Överlevnad?**

A black and white photograph of Mike Tyson in a boxing ring, wearing boxing gloves and boxing trunks. He is shown from the side, leaning forward and punching a man in the mouth. The man being punched is shirtless and has his head tilted back. The background is dark and out of focus.

**“Everyone thinks they have a plan
until they get punched in the mouth”**

– Mike Tyson

Effekt

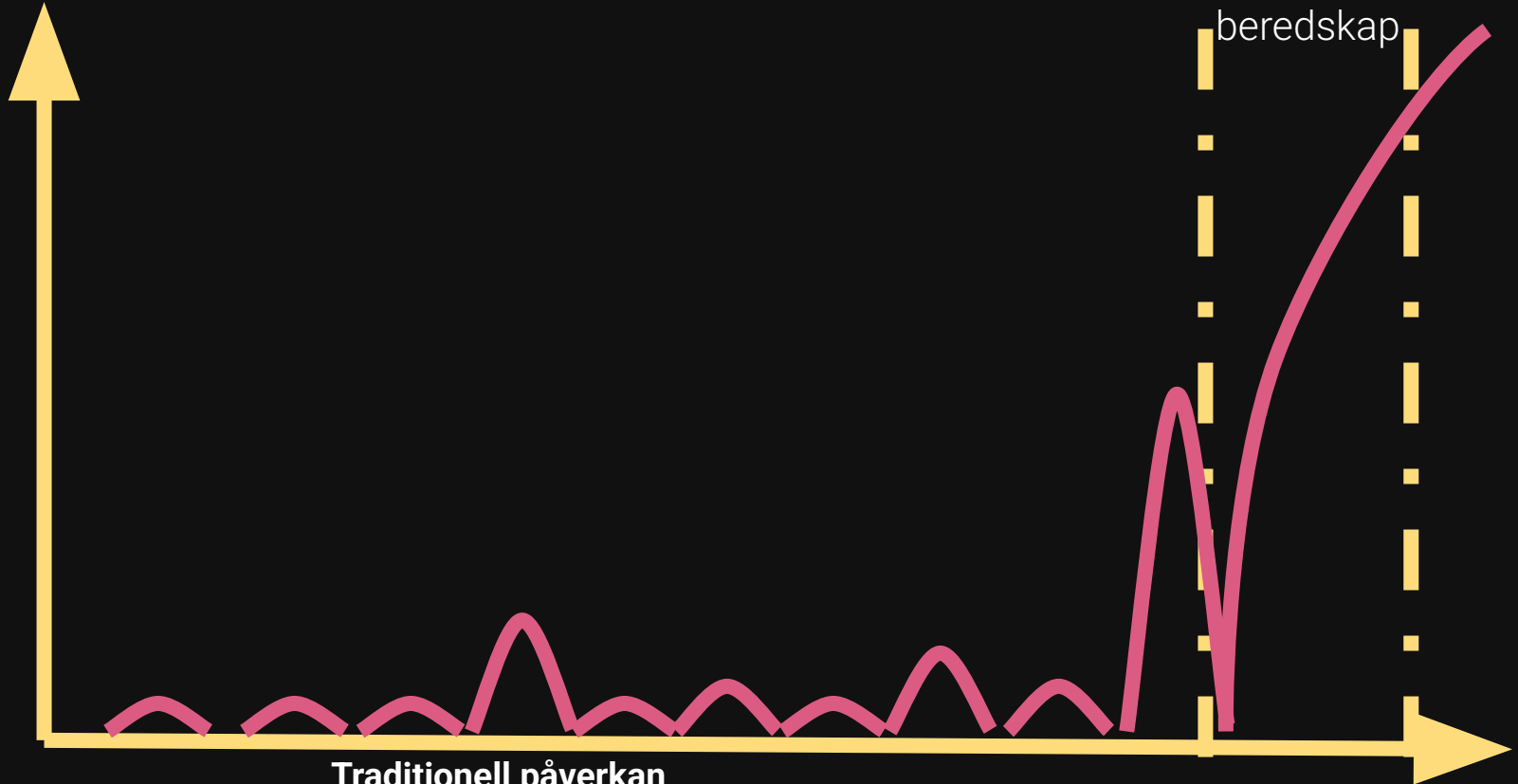
Fred

Höjd
beredskap

Krig

Traditionell påverkan

Tid



Effekt

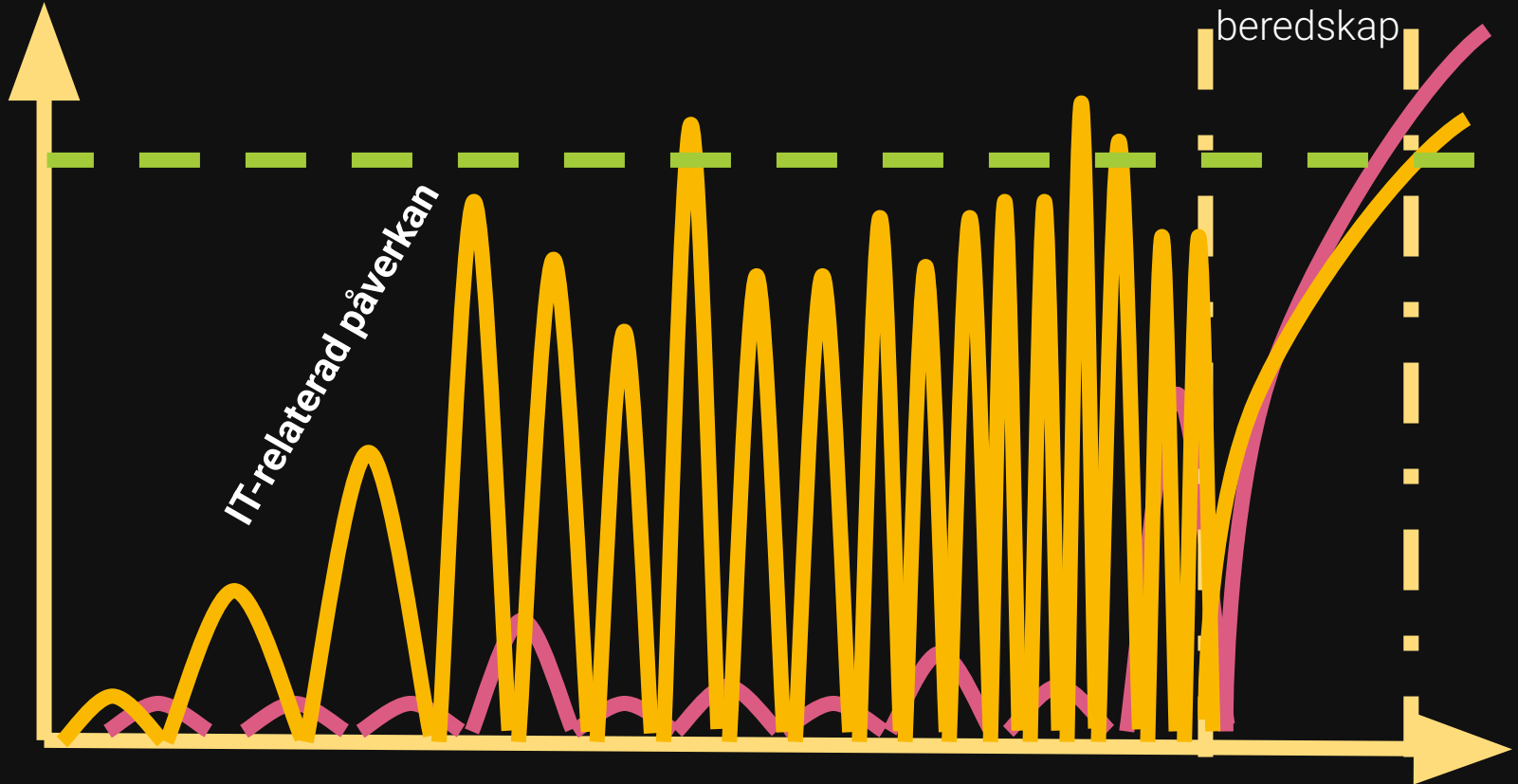
Fred

Höjd
beredskap

Krig

IT-relaterad påverkan

Tid



Internets (tekniska) beståndsdelar

- **Fiber i marken** för att signaler ska nå fram med redundans och robusthet
 - 5G är en accessteknik, inte en transportlösning
- **Trafikutbyte / routing** för att paket och information ska komma rätt
 - Internetknutpunkter / IX
- **Tjänstekataloger** för att användare och system ska kunna hitta rätt tjänst / server
 - Domain Name System / DNS
- **Korrekt och säker tid** för klockor ska ha rätt tid och för att validerings- och säkerhetsprocesser ska fungera
 - Svensk tid distribueras av Netnod på mandat av Post- och telestyrelsen

Internet måste vara rock-solid

Digitaliseringens beståndsdelar

- **Internet** för kommunikation mellan organisationer
 - Upphandlad access, operatörer som kan prata med varandra
- **Datorer och annan hårdvara** som applikationer körs på lokalt
 - Telefoner, laptops, plattor, passagesystem, röntgenmaskiner osv
- **Datorer och annan hårdvara** som körs hos tredje part
 - Onlinetjänster, molnlösningar, VM:ar hos 3:e part, osv
- **Input och output** till verkligheten
 - Styrning av CNC-maskiner, öppning av lås, input av kameror, osv

Digitaliseringen måste vara rock-solid

Säkerhetens dualism



Motsatta Arkitekturer

Tillgänglighet och konfidentialitet kräver (ofta) helt olika tekniska lösningar.

Vad finns det egentligen för krav?



Tillgänglighet

Uppnås bäst genom redundans och diversitet.

Många och varierade noder.



Konfidentialitet

Uppnås genom att samla och skydda informationen centralt.

Få noder, kontrollerad design.



Vad är de egentliga konsekvenserna?

Dessa motstridiga behov skapar en komplex utmaning för robust IT-design.

Uthållighet i praktiken



Planering & Scheman

Att skriva ut scheman för **nästa dag** är görbart; men går det för **två veckor**?



Hårdvarubyten

Central hårdvara byts inte på en dag.



Frekvens då tjänster behövs

Löneutbetalningar behövs bara en gång per månad. Ofta kan samma lön betalas ut flera månader i sträck.



Kritiska frågor

Vad måste fungera hela tiden? Och vad bara ibland?

IT gör IT, inte det verksamheten behöver



Vilka behov är kommunicerade?

Är verksamheten dimensionerande för IT-verksamhet?



Vilka mandat finns?

Vet IT-avdelningen om system är kritiska? Finns mandat och resurser för robusthet?



Exempel – nära

Inga krav på mobiltelefoner ställdes, så IT-avdelningen köpte de billigaste/finaste.



Exempel – längre bort

NIS2 delegeras till IT-chefen; verksamheten kör på som vanligt.

Konfidentialitet, inte tillgänglighet



Fokus på informationsläckage framför driftsäkerhet

- Vad är värst; att journaler läcker eller att akuten stängs ned?
- Tekniska beslut tas ensidigt p.g.a. rädsla för GDPR-överträdelser



Exempel ur verkligheten

Backup-rutiner testas inte för att man är rädd att känslig information ska hamna på villovägar under testmomentet.



Ställ er själva frågan; vet ni vad ni gör?

- Vet ni vilka IT-system och funktioner som du behöver för att fortsätta göra det i minst två veckor?
- Vet lagstiftaren bättre än du vad som krävs för att hålla igång er verksamhet och era system än vad du gör?

Regelefterlevnad är en sak, överlevnad är en annan.

Den bästa vägen framåt



1. Enas om

Vad ni gör och vad som är riktigt **viktigt**



2. Inventera

Hitta funktioner och beroenden som är **livsviktiga**



3. Säkerställ drift

Se till så att dessa fungerar, **när de behövs**



4. Öva kontinuerligt

Öva, öva, öva, och **öva lite till**

IXP-Country-Jedi
Peer-to-Peer Fabric

Fredrik Lindeberg, PhD

CISO

flindeberg@netnod.se

Greta Garbos väg 13
169 40 Solna
Sweden

Visit us at netnod.se