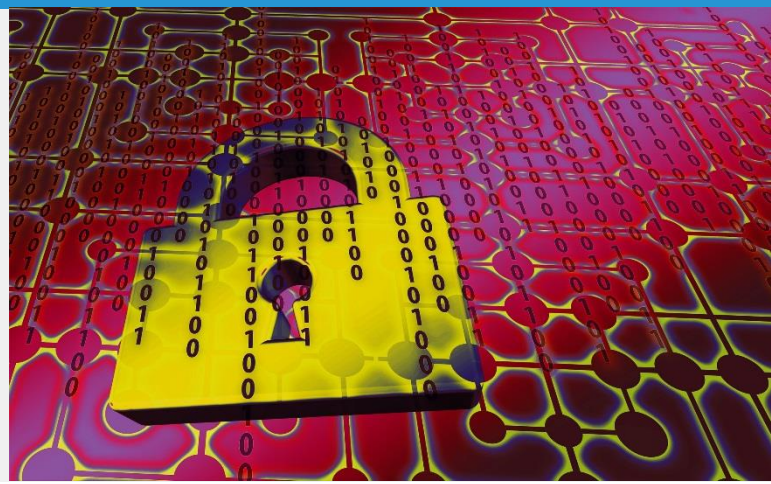
IT-säkerhetsdagen 2016

Jacob Löfvenberg, FOI

Pierre Anderberg, FM



Scandic Ariadne informerar

Bakgrund

– 2013	FOI:s årliga avrapportering av IT-säkerhetsforskning
2014–2015	Fokus ändras till från avrapportering av forskning till konferens. FM/FMV tillkommer.
2016	Försvarsrelaterade IT-frågor för alla relevanta myndigheter.
2017 –	?

Program

09:00 – 09:10	**Inledning** (Pierre Anderberg, FM, Jacob Löfvenberg, FOI)
09:10 – 09:30	**Öppningsanförande** (Fredrik Robertsson, FM)
09:30 – 10:00	**Informationssäkerhetskultur** (Jonas Hallberg, FOI)
10:00 – 10:20	**Rast**
10:20 – 10:50	**RÖS eller Tempest – vad innebär det i praktiken?** (Ove Friman, FM)
10:50 – 11:20	**Erfarenheter från utveckling och underhåll av IT-system** (Daniel Eidenskog, FOI)
11:20 – 11:40	**Rast**
11:40 – 12:20	**Heuristiska datamodeller för förbättrad logganalys** (Robert Carlsson, FM)
12:20 – 13:20	**Lunch**
13:20 – 13:30	**FOI:s verksamhet inom IT-säkerhet (**Peter Stenumgaard, FOI)
13:30 – 14:00	**FRA:s roll i ett nationellt cyberförsvar** (Fredrik Wallin, FRA)
14:00 – 14:30	**Crate 2.0 – Nationell Cyber Range** (Magnus Sparf, FOI, Richard Widh, MSB)
14:30 – 15:00	**Rast**
15:00 – 15:30	**Samhällets informationssäkerhet och robusthet** (Christina Goede, MSB)
15:30 – 16:00	**Cyberforensiska utmaningar och möjligheter** (Martin Karresand, FOI)
16:00 – 16:20	**Avslutning (**Pierre Anderberg, FM, Jacob Löfvenberg, FOI)

Logistik

- Fika med tilltugg ingår kl. 10.00 och kl. 14.30
- Lunchkuponger bör köpas under förmiddagen
- Utvärdering av dagen
  - Webformulär – http://survey.iwlab.foi.se/nov2016
  - (det finns små lappar med adressen)
- Presentationsmatrialet finns i pdf-format
  - och blir tillgängligt när utvärderingen skickats in.
- Något om säkerheten här

IT-Säkerhet

En förutsättning för operativ effekt

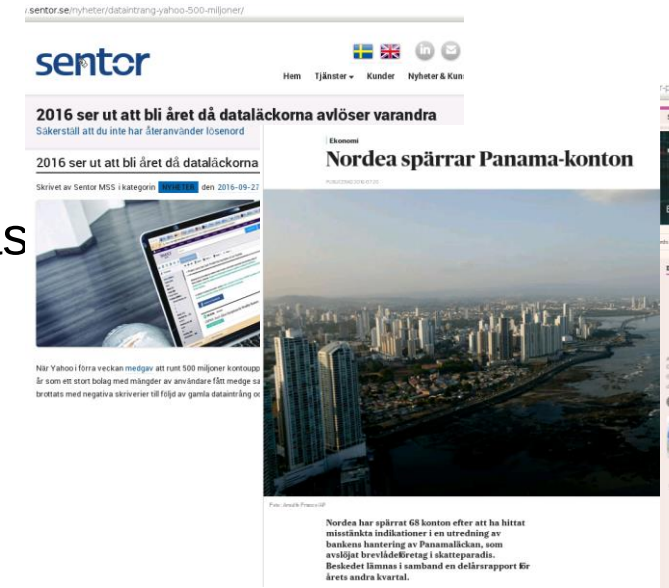
FM CIO Fredrik Robertsson
Generalmajor

Omvärldsförändring

- Europa - Ukraina, Krim och ”Brexit”
- Närområdet – ökad aktivitet, ökande risker
- Informationssäkerhetshändelser
- Samhällets utveckling
- Digitalisering/teknikutveckling

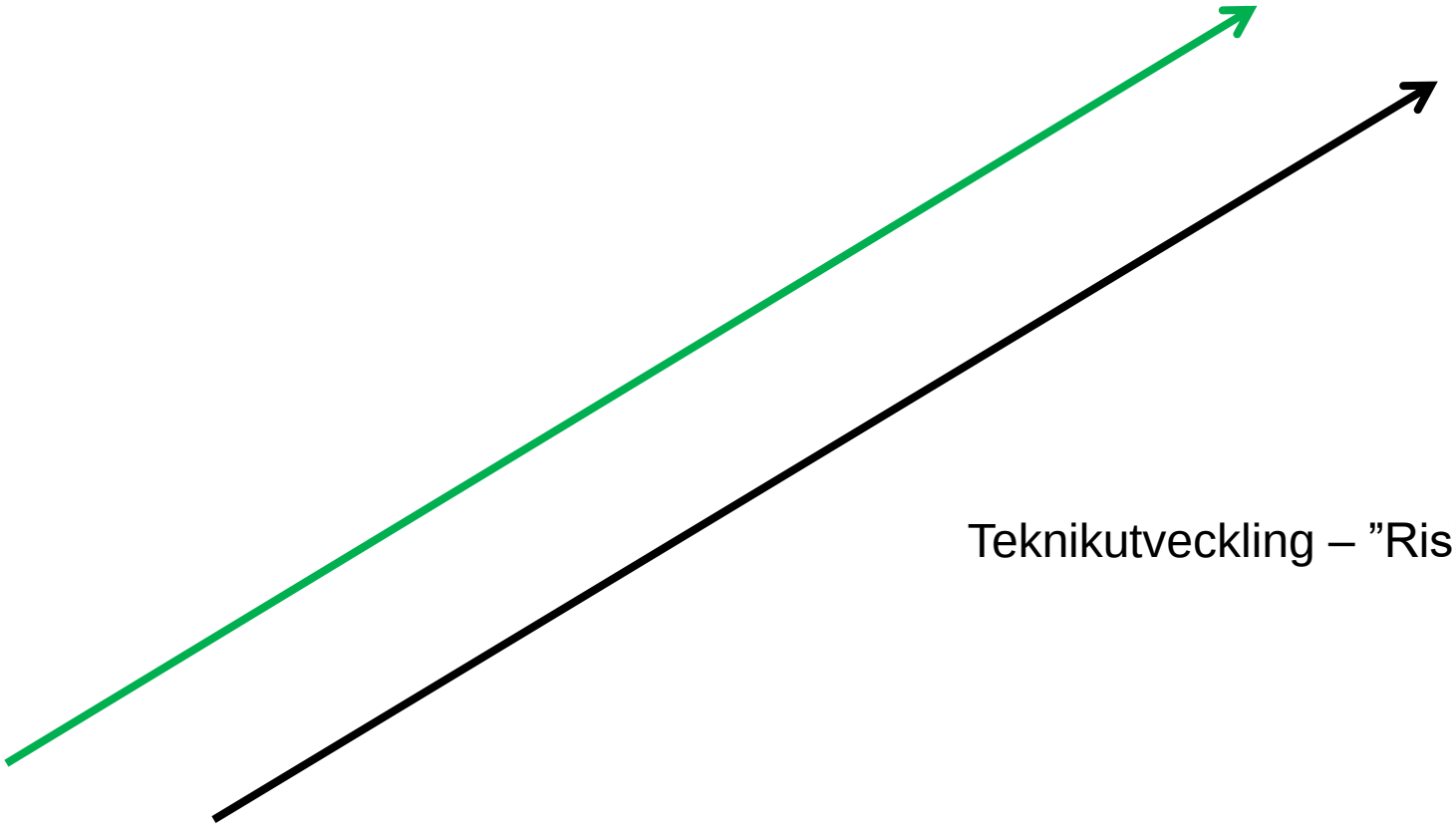
Informationsrelaterade händelser

- Cyberattacker
  - elnät, oljepipeline, industrier, presidentkandidater
- Informationsläckor
  - Edward Snowden, Chelsea Manning, Panamadokumenten
- Störningar
  - SJ bokningssystem
  - Luftfartsverket
  - Avsiktligt fälld sändarmas
  - DNS-tjänst



Operativ effekt

IT-Säkerhet/ Robusthet



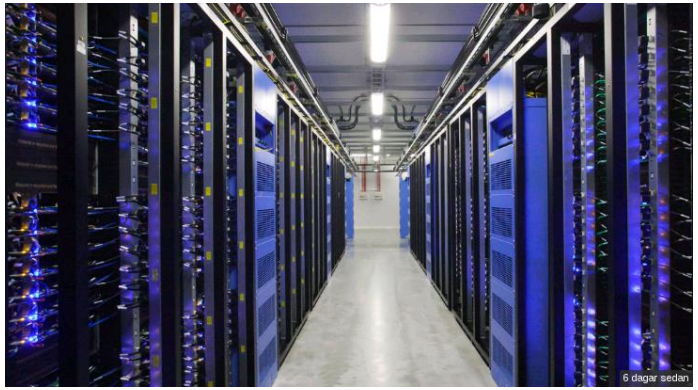
Teknikutveckling – ”Riskexponering”

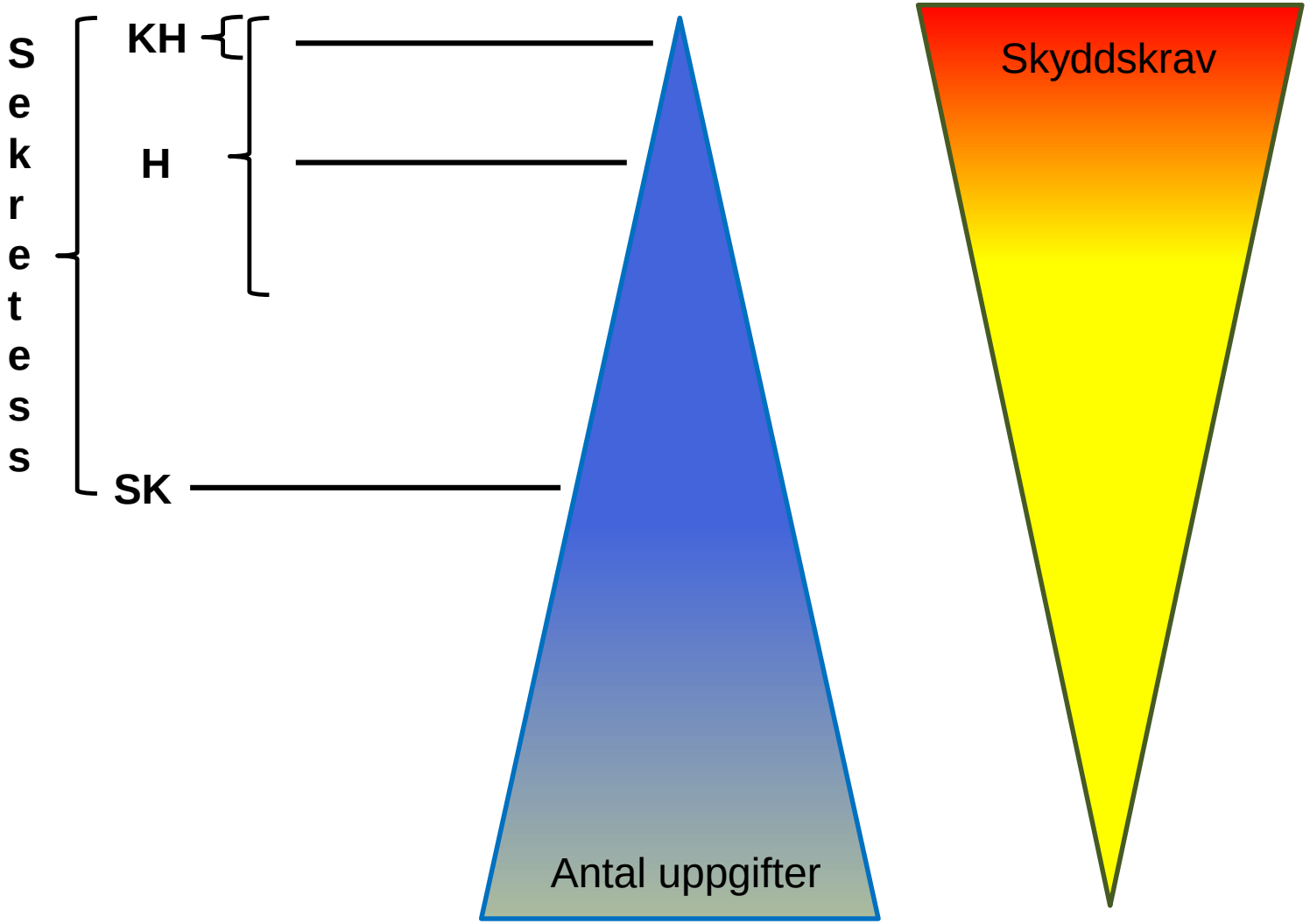
Högre operativ förmåga

- Kan också skapas genom att generera större värde från vår information
- Bygger på god informations- och IT-säkerhet
- Förutsätter robust IT-utrustning, på samma sätt som annan militär utrustning

Resurshantering

- Investeringar i resurser, ekonomi och tid för att bevara informationens sekretess, riktighet, tillgänglighet och spårbarhet
- Balansering genom riskanalys av verksamhet, önskad effekt och hot
- Om balansering inte sker kan andra investeringar ”tappas bort”




Sekretess
KH
H
SK
Antal uppgifter
Skyddskrav

Självgranska dig

Best practice är för dåligt

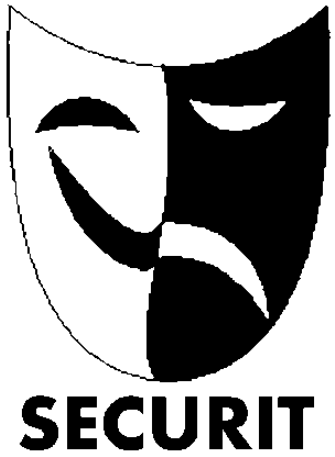
Common Criteria

Sluta underskatta hotet

Ökat fokus på informationssäkerhet inom Försvarsmakten

- Etablering av FM CIO vid Ledningsstaben med tre sektioner
  - Cyberförsvar
  - Strategi och analys
  - Ledning och informationshantering

Frågor?



Informationssäkerhetskultur— forskningsprogrammet SECURIT

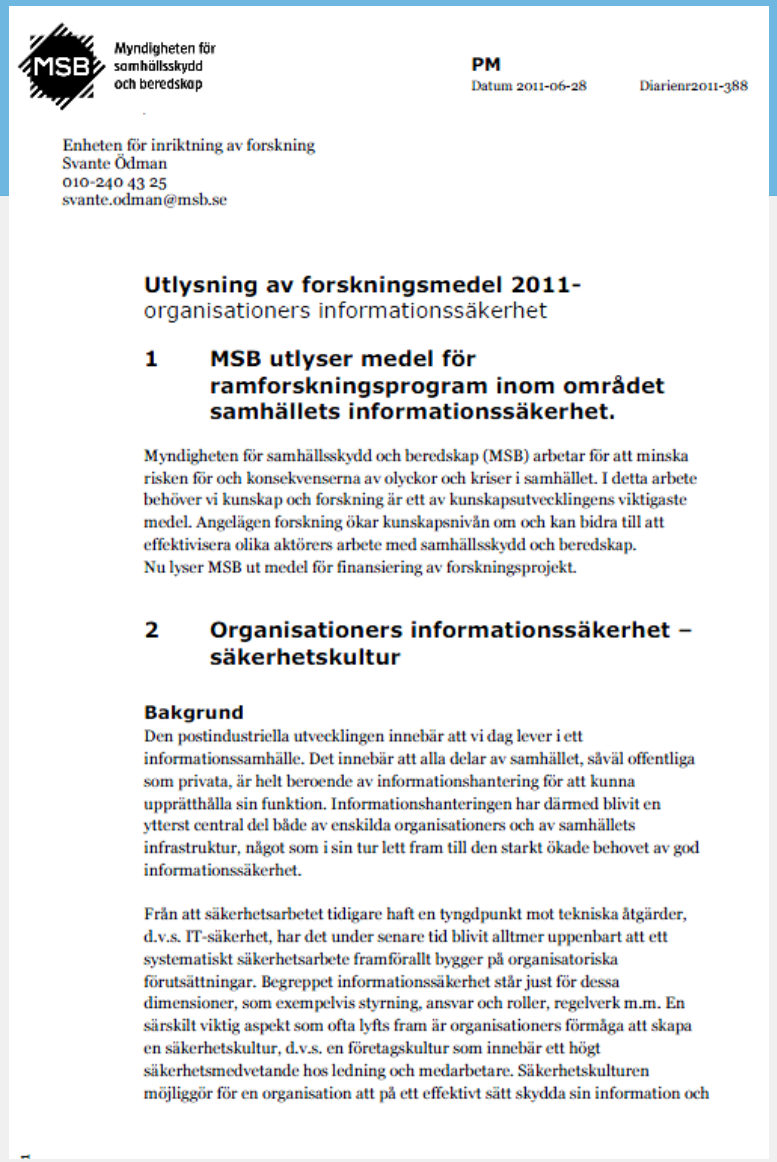
Jonas Hallberg

www.foi.se/securit

FOI

Utgångspunkter

- Behov av förbättrad informationssäkerhet
- Kultur–en central aspekt av informationssäkerhet
- SECURIT studerar
  - säkerhetsrelevanta egenskaper hos individer och organisationer
  - effekter av sociala åtgärder



Myndigheten för samhällsskydd och beredskap

PM
Datum 2011-06-28 Diarienr2011-388

Enheten för inriktning av forskning
Svante Ödman
010-240 43 25
svante.odman@msb.se

Utlysning av forskningsmedel 2011-
organisationers informationssäkerhet

1 MSB utlyser medel för ramforskningsprogram inom området samhällets informationssäkerhet.

Myndigheten för samhällsskydd och beredskap (MSB) arbetar för att minska risken för och konsekvenserna av olyckor och kriser i samhället. I detta arbete behöver vi kunskap och forskning är ett av kunskapsutvecklingens viktigaste medel. Angelägen forskning ökar kunskapsnivån om och kan bidra till att effektivisera olika aktörers arbete med samhällsskydd och beredskap.
Nu lyser MSB ut medel för finansiering av forskningsprojekt.

2 Organisationers informationssäkerhet – säkerhetskultur

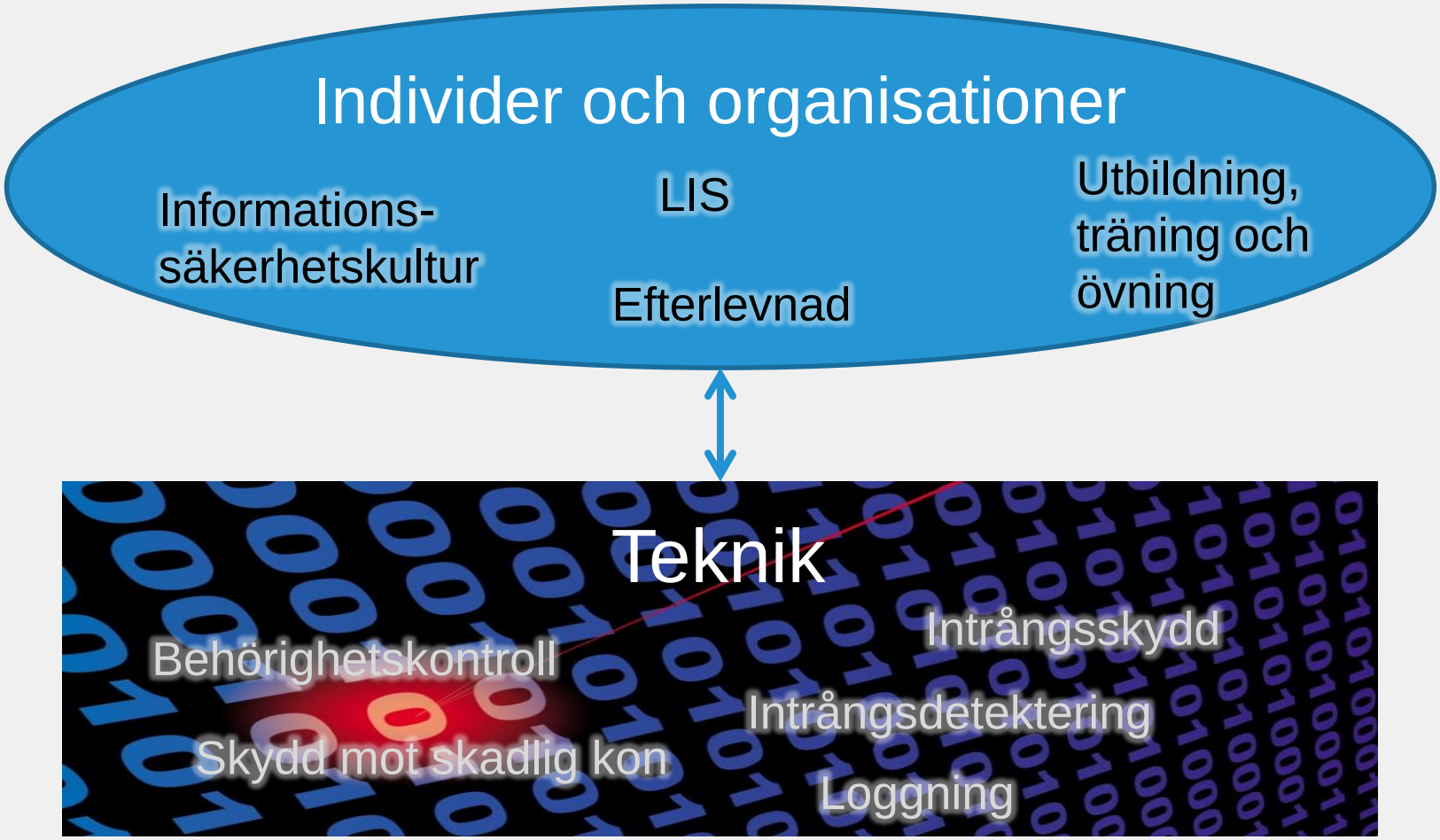
Bakgrund
Den postindustriella utvecklingen innebär att vi dag lever i ett informationssamhälle. Det innebär att alla delar av samhället, såväl offentliga som privata, är helt beroende av informationshantering för att kunna upprätthålla sin funktion. Informationshanteringen har därmed blivit en ytterst central del både av enskilda organisationers och av samhällets infrastruktur, något som i sin tur lett fram till den starkt ökade behovet av god informationssäkerhet.

Från att säkerhetsarbetet tidigare haft en tyngdpunkt mot tekniska åtgärder, d.v.s. IT-säkerhet, har det under senare tid blivit alltmer uppenbart att ett systematiskt säkerhetsarbete framförallt bygger på organisatoriska förutsättningar. Begreppet informationssäkerhet står just för dessa dimensioner, som exempelvis styrning, ansvar och roller, regelverk m.m. En särskilt viktig aspekt som ofta lyfts fram är organisationers förmåga att skapa en säkerhetskultur, d.v.s. en företagskultur som innebär ett högt säkerhetsmedvetande hos ledning och medarbetare. Säkerhetskulturen möjliggör för en organisation att på ett effektivt sätt skydda sin information och

www.foi.se/securit

SECURIT

Informationssäkerhet



SECURIT

Vad är kultur?

Hofstede:

“Culture is the collective programming of the mind distinguishing the members of one group or category of people from others”

http://geert-hofstede.com/national-culture.html

Edgar Schein:

There are three distinct levels

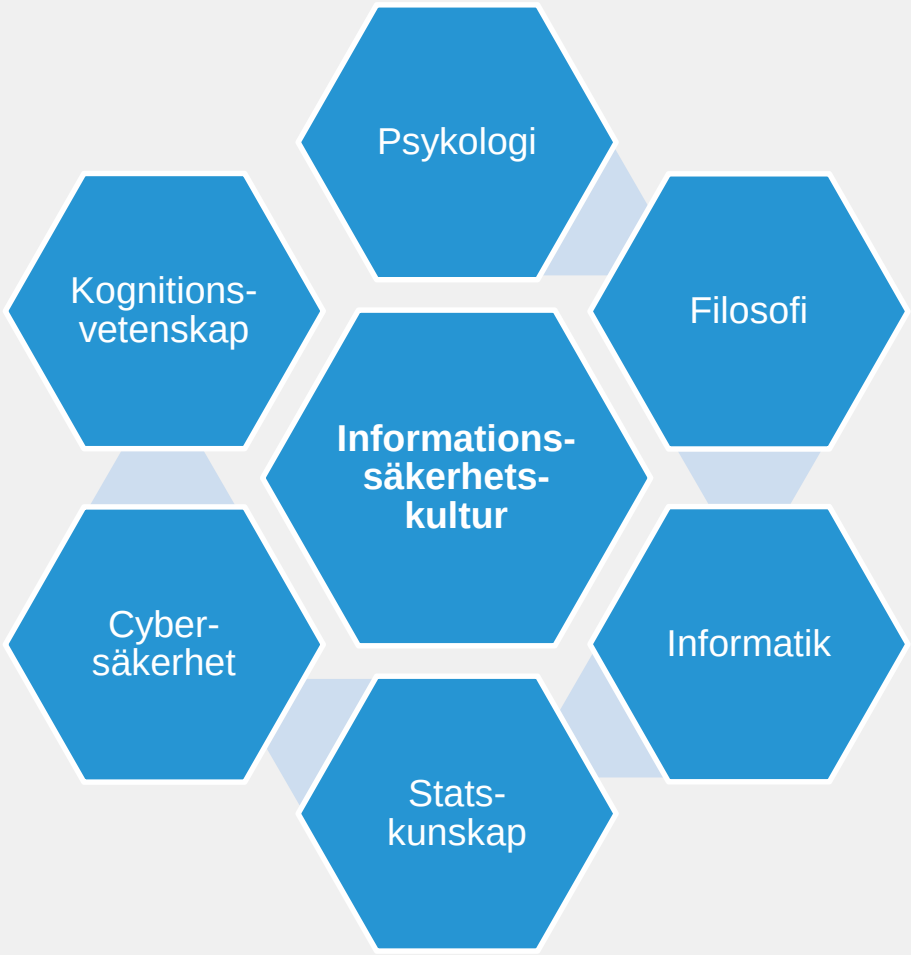
- Artifacts
- Espoused values
- Basic assumptions

Aktörerna bakom SECURIT

www.foi.se/securit

SECURIT

Forskningsprogrammet SECURIT, 2012-2017



www.foi.se/securit

SECURIT

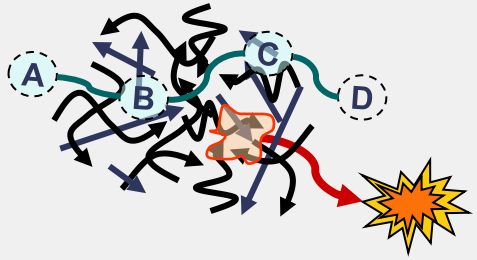
Informationssäkerhetskultur

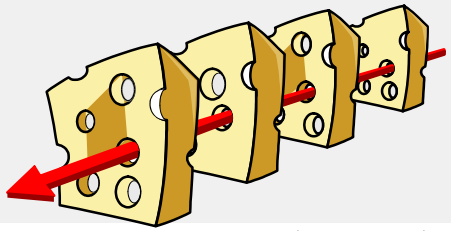
Gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer baserade på inre och yttre krav, som traderas till nya medlemmar och som har implikationer för informationssäkerhet

http://foi.se/sv/Sok/Sammanfattningssida/?rNo=FOI+MEMO+5253

Forskningsprojekten i SECURIT

- Security culture
- User acceptance of information security policies
- Attitude, culture, and information security
- Discourse and security practice
- Balanced IT-based Organizational development
- ATTITUDE
- INTERORG
- CONGRUENCE
- Cultural aspects in information security standard development



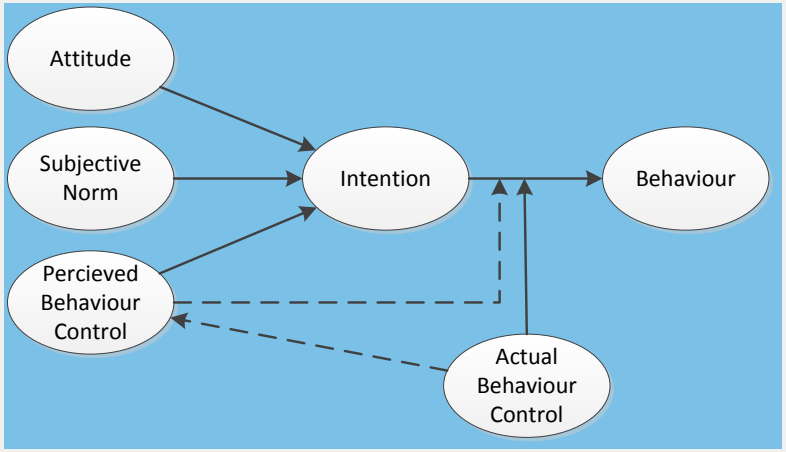


www.foi.se/securit

SECURIT

Exempel: följa bestämmelser

- Vilka faktorer påverkar anställdas intention att följa informationssäkerhetsbestämmelser och faktiska beteende?



- Testa teorin
  - Litteraturstudie
  - Metaanalys
  - Egen datainsamling

	Regression model							
	1	2	3	4	5	6	7	8
Theory of planned behavior	•	•	•	•	•	•	•	•
Threat Appraisal (PMT)		•			•	•	•	
Coping Appraisal (PMT)			•		•	•		•
Anticipated Regret				•		•	•	•
Explained variance (R^2)	0.36	0.40	0.37	0.43	0.41	0.45	0.44	0.44

www.foi.se/securit

SECURIT

TPB-tolkning av en bestämmelse

Norm?

- Ett lösenord till ett IT-system vid FOI ska vara så konstruerat att det inte kan gissas eller knäckas på ett enkelt sätt. För närvarande gäller att lösenord, om inte IT-systemet i sig är begränsande, bör bestå av minst 15 tecken samt innehålla en blandning av Versaler, gemener, siffror och specialtecken. T.ex. FIfs&ish84#snli (FOI Instruktion för säkerhetsskydd & informationssäkerhet har 82 # sidor nyttig läsvärd information). Lösenord ska bytas minst en gång per år.

Stärka beteendekontroll?

SECURIT

Mer TPB-anpassad formulering

Attityd

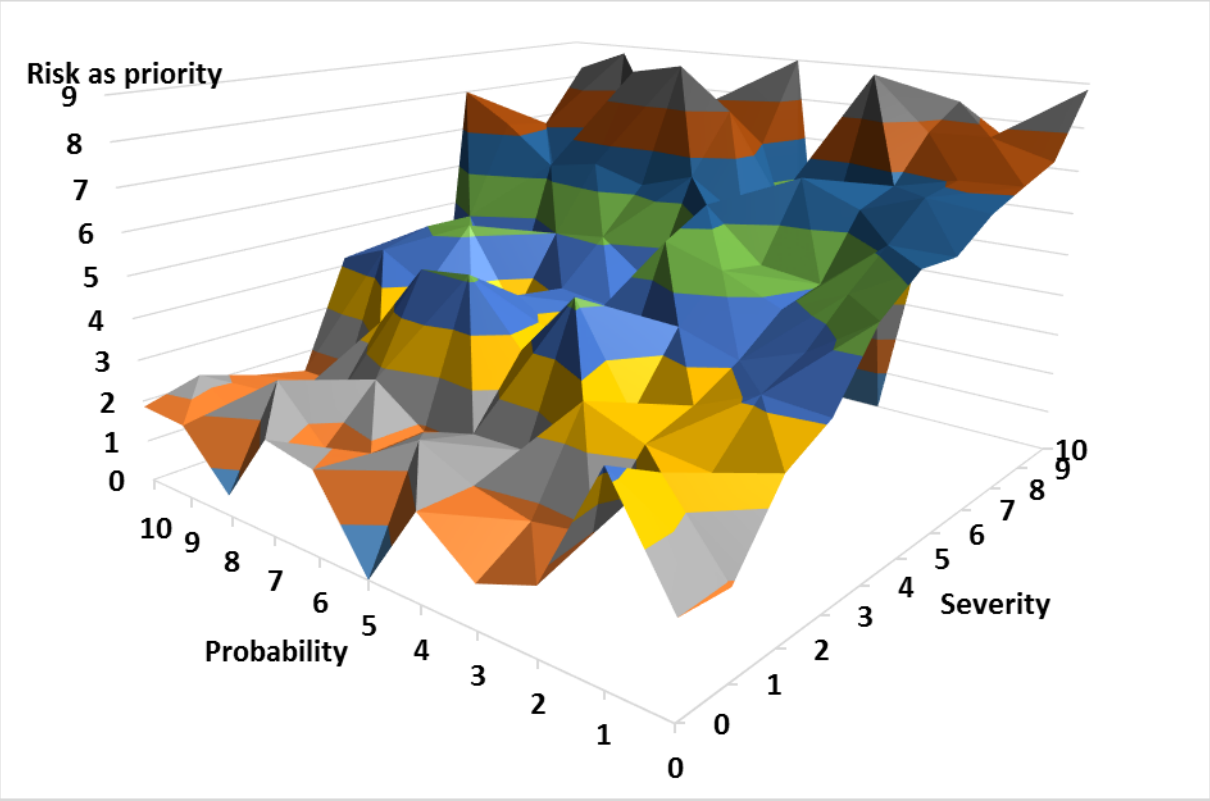
Normer

Att skydda IT-system vid FOI är viktigt. Det förväntas av medarbetare och uppdragsgivare att de lösenord som används till IT-system vid FOI är konstruerade så de inte kan gissas eller knäckas på ett enkelt sätt. Om inte IT-systemet i sig är begränsande bör lösenordet bestå av minst 15 tecken samt innehålla en blandning av Versaler, gemener, siffror och specialtecken. Du kan enkelt skapa ett bra lösenord genom att utgå från en mening. T.ex. kan du skapa ”FIfs&ish84#snli” från meningen ”FOI Instruktion för säkerhetsskydd & informationssäkerhet har 82 # sidor nyttig läsvärd information”. Lösenord behöver bara bytas en gång per år.

Upplevd beteendekontroll

SECURIT

Exempel: bedöma risker



T. Sommestad, H. Karlzén, P. Nilsson, J. Hallberg, (2016) "An empirical test of the perceived relationship between risk and the constituents severity and probability", Information & Computer Security, Vol. 24 Iss: 2

Datainsamling

- SCB-enkät
- Frågor från flera av SECURIT-projekten
- Utskick till
  - 11 000 anställda
  - 6 branscher
  - Organisationer och arbetsställen
- Svarsfrekvens: 33,6 %

Resultat

SECURIT

Security Culture and Information Technology

Forskningsprogrammet Security Culture and Information Technology, SECURIT, har som mål att förbättra organisationers informationssäkerhet. I moderna informationsdrivna organisationer utgör god säkerhetskultur en viktig förutsättning för informationssäkerheten.

För att uppnå målen studerar SECURIT:

- Egenskaper hos individer och organisationer som är relevanta för informationssäkerheten
- Effekter av åtgärder som syftar till att förbättra informationssäkerheten genom att påverka individer och organisationer

SECURIT finansieras av Myndigheten för samhällsskydd och beredskap, MSB, och koordineras av Totalförsvarets forskningsinstitut, FOI. Forskningen genomförs gemensamt av Chalmers, Göteborgs universitet, FOI, KTH och Örebro universitet i samarbete med Linköpings universitet. Karlstad universitet koordinerar och stödjer nätverket Swedish IT Security Network for PhD students (SWITS) inom ramen för SECURIT.

Relaterat material

Rapporter

Definition of information security culture

Dokument

Projektbeskrivning (eng)

Länkar

Forskningsprojekt

Resultat

Resultaten från SECURIT kommer att spridas på flera olika sätt till ett antal olika mottagare. Forskningen kommer främst att dokumenteras i form av artiklar som skickas till vetenskapliga tidskrifter och konferenser. Resultat kommer också att spridas via fackpress, seminarier, fallstudier etc. på så sätt nås forskare, informationssäkerhetsexperter och beslutsfattare inom såväl näringsliv som den offentliga sektorn.

Informationssäkerhetskultur

Gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer baserade på inre och yttre krav, som traderas till nya medlemmar och som har implikationer för informationssäkerhet

Forskningen inom SECURIT syftar till att besvara följande frågor.

- Vad är förhållandet mellan säkerhetskultur och det generella sociala och intellektuella klimatet i organisationer?

www.foi.se/securit

Antologi

SECURIT

RÖS vs TEMPEST

Ove Friman
MUST SÄKK SÄKT

Lite begreppsförvirring

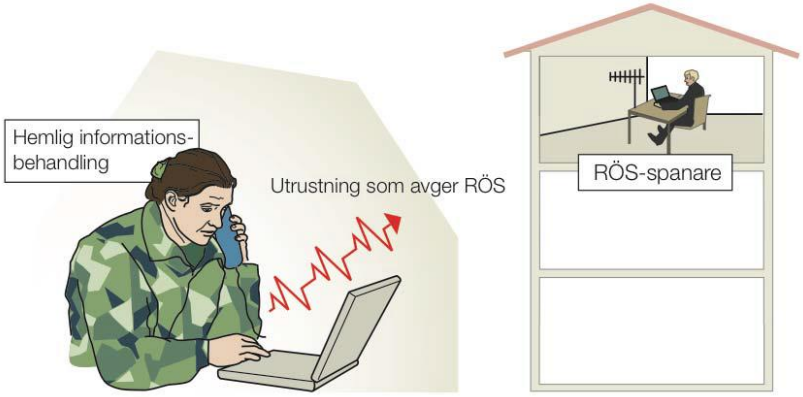
- TEMPEST
- Compromising Emanations (CE)
- Röjande signaler (RÖS)

TEMPEST: **MIL-STD-464C**
An unclassified, short name referring to the investigation and study of compromising emanations.

Compromising emanations (CE): **MIL-STD-464C**
Unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose the national security information transmitted, received, handled, or otherwise processed by any classified information processing system.

Röjande Signaler: (RÖS) ”Icke önskvärda elektro-magnetiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehörig, kan bidra till att sekretessbelagda uppgifter röjs.”

Idag gäller svenska RÖS-normer enligt
”Beslut om krav på skydd mot röjande signaler (RÖS)”
FM HKV 10755:65114 2006-03-24



Två TEMPEST regelverk

NATO - SECAN Doctrine and Information Publication (SDIP)

- SDIP – 27 NATO Requirements and Evalutaion Procedures
- SDIP – 28 NATO Zoning Procedures
- SDIP – 29 Facility Design Criteria and Installation of Equipment for the Processing of Classified Information

EU - Information Assurance Security Guidelines (IASG)

- IASG 7–01 Selection and Installation of TEMPEST Equipment
- IASG 7–02 TEMPEST Zoning Procedures
- IASG 7–03 EU TEMPEST Requirement and Evaluation Procedures

Eftersom 22 av EU medlemstaterna även är anslutna till NATO är båda regelverken innehållsmässigt snarlika då det är orimligt att följa två helt olika regelverk avseende röjande signaler.

Fördelar med TEMPEST-regelverket

Trots att regelverken skiljer sig åt på flera punkter ger båda två ett likvärdigt skydd mot röjande signaler. Ur ett svenskt perspektiv finns det dock flera fördelar med att övergå till TEMPEST-regelverket:

- Redan idag nyttjar vi flertalet NATO-system som har TEMPEST-krav
- För att kunna vara fullt interoperabla vid internationella insatser bör vi följa samma regelverk som resten av våra partners.

- TEMPEST-regelverket är mer pragmatiskt än vår svenska motsvarighet.
- TEMPEST-regelverket möjliggör att vi enklare kan gå utanför Sverige vid anskaffning av IT-materiel där det finns krav på skydd mot röjande signaler. Kostnaden för själva TEMPEST-utrustningen är ofta lägre jämfört med svensk motsvarande materiel.
- TEMPEST-regelverket är mer tydlig och väldefinierat än vår svenska motsvarighet med avseende på dämpningsmätning och installation av materiel.

- TEMPEST-regelverket gör det möjligt för vår inhemska industri att utveckla produkter som är gångbara på den svenska så väl som den internationella marknaden.

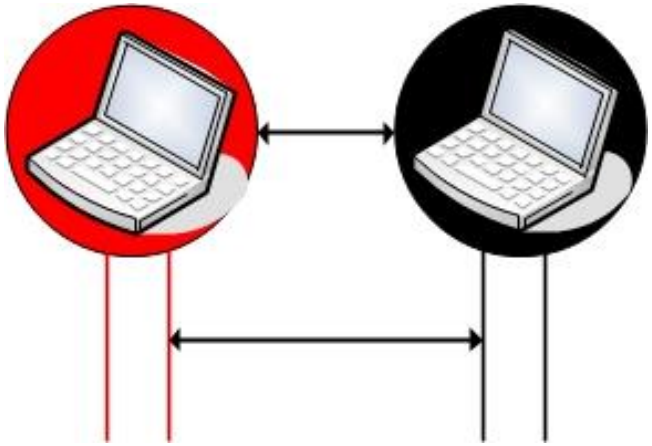
TEMPEST-regelverket reglerar inte endast materielens beskaffenhet utan ställer även krav på:

- **”Zoning” (dämpningsmätning/avståndsmätning)**

  Det måste utföras ”Facility TEMPEST Zoning” på relevanta platser där TEMPEST-utrustning är tänkt att användas. Det finns dock flera undantag, såsom mobila taktiska plattformar, berganläggningar m.m.

- **Installation**

  Det måste finnas fysiskt avstånd mellan hemliga (röda) och öppna (svarta) system, galvaniskt kablage som bär röd respektive svart information, avstånd till radio-sändare, separation av strömförsörjning m.m.



- **Uppföljning**

  Det måste utföras uppföljning på att installationerna inte har förändrats (ex. att utrustningen eller kablaget inte har flyttats, att dämpningsegenskaperna inte har förändrats vid ombyggnation).

Nackdelar med TEMPEST-regelverket

I vårt nationella regelverk finns tre så kallade utrustningsklasser; U1, U2 samt U3 vilket anger hur långt en utrustning strålar. På motsvarande sätt indelas TEMPEST-materiel i nivåerna; A, B och C.

- De klasser som strålar minst, U1 respektive A, skiljer sig relativ mycket med avseende på strålat avstånd där U1 har det kortare avståndet.
- Detta innebär att för signalskyddssystem avsedda för SG C eller högre samt för viss nivå A-utrustning som placeras på särskilt utsatta platser måste dessa ges kompletterande skydd för att motsvara dagens U1-utrustning.

- Krav på att installation sker enligt regelverket medför initialt en ökad kostnad då motsvarande krav inte finns i vårt nu gällande regelverk.

Det omsätts, troligtvis, IT-materiel i en snabbare takt än vad det omsätts byggander, lokaler, fartyg m.m.

Man kan t.ex. lätt tro att krypto- och IT-system som har den högsta graden av skydd mot röjande signaler (U1) kan placeras godtyckligt, men det är en felaktig bedömning då även denna typ av system måste ha en viss separation från bland annat öppna system och radiosändare.

Oaktat om vi övergår till TEMPEST-regelverket eller ej måste det införas tydligare krav på installation inom en snar framtid.

Införande

Regelverket kommer först kunna införas fullt ut då det finns tekniska och organisatoriska förutsättningar och berörd personal har fått nödvändig utbildning inom området.

Det kommer under en övergångsperiod finnas kvar materiel som har skydd mot röjande signaler baserat på nuvarande nationellt regelverk till dess att dessa kommer att omsättas/ersättas till förmån för nya system och utrustningar.

SLUT
FRÅGOR?

ove.friman@mil.se
08 - 788 7904

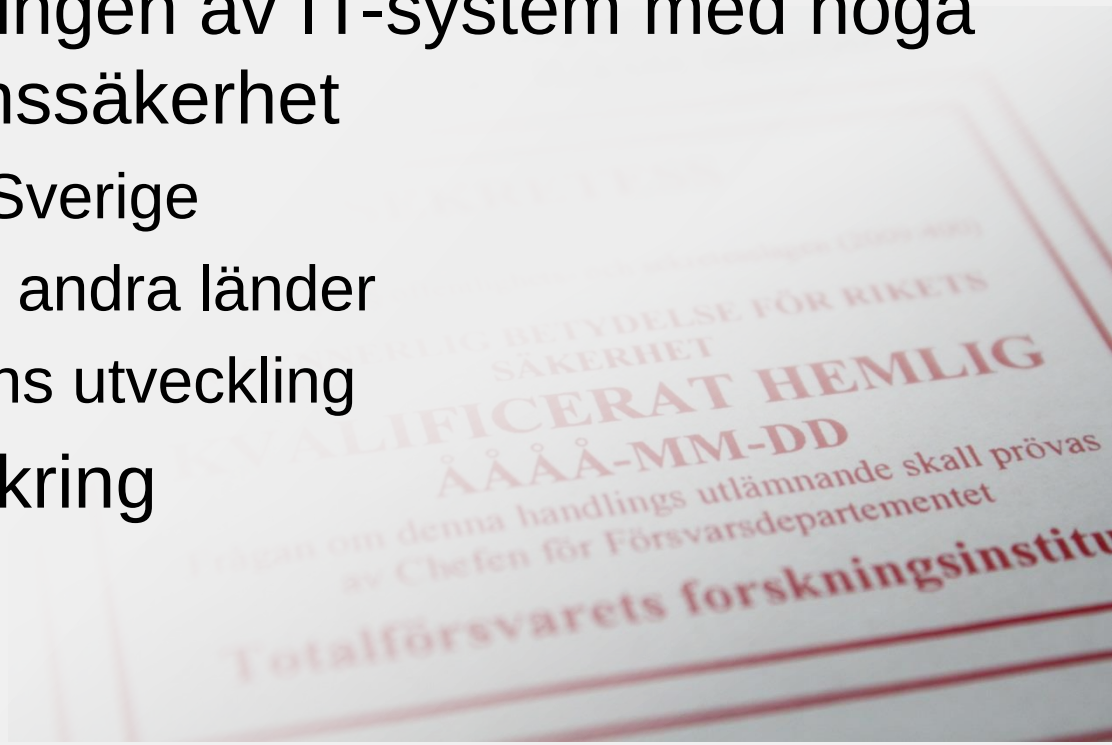
IT-säkerhet i system med höga krav på informationssäkerhet

Daniel Eidenskog

FOI

Bakgrund

- Uppdrag från Försvarsmakten
- Undersöka utvecklingen av IT-system med höga krav på informationssäkerhet
  - Primärt avseende Sverige
  - Vissa utblickar mot andra länder
  - De senaste 15 årens utveckling
- Vetenskaplig förankring



Metod – Intervjuer

- Förfining av frågeställning
  - Projektfrågor – breda och abstrakta
  - Intervjufrågor – fokuserade och konkreta
- Semistrukturerade intervjuer
  - Manus för att guida genom intervjun
  - Undvika ”dåliga” frågor, exempelvis ledande formuleringar
  - C:a 2 timmar per intervju
- Respondenternas svar antecknades

Metod – Efterbearbetning

- Strukturerad tematisk syntes
  - Tematisering av svaren
  - Syntes av svar på projektfrågorna
- Söka andra mönster i svaren
  - Finns det svar på ej ställda projektfrågor?
- Syntes av slutsatser ur svaren

Respondenter

- 11 intervjuer, 17 personer
  - Försvarsmakten, civila myndigheter och näringsliv
  - En internationell näringslivsrepresentant
  - Alla med arbete inom ”högsäkerhetsområdet”
  - Domänkompetens inom IT-arkitektur och informationssäkerhet
  - God kunskap om Försvarsmaktens kravbild på IT-säkerhet
- Vår uppfattning är att respondenterna är representativa

Respondenternas svar

Utvecklingen

- Mer mobilitet och ökad kommunikation mellan olika IT-system
- Komplexiteten i systemen ökar
- Det funktionella gapet mellan Försvarsmaktens IT-system och civila IT-system har ökat
- Allt svårare och dyrare att specialutveckla för Försvarsmaktens krav
  - COTS/MOTS blir allt tydligare som ekonomiskt alternativ men innebär utmaningar vad gäller säkerhet och tilltro

Respondenternas svar

Säkerhet

- Riktighet har fått ökat fokus men sekretess är fortfarande högsta prioritet
- Säkerhetskraven har fått större acceptans hos utvecklare och användare
  - Förståelsen av syftet med kraven har ökat
- Ökad riskavvägning i omvärlden där verksamhetens behov ställs mot säkerhetskraven
  - Annan syn på acceptabel IT-säkerhetsrisk när verksamheten vägs in tydligare

Respondenternas svar

IT-säkerhetsarbetet

- Absolut säkerhet är omöjlig
  - Komplexiteten är alldeles för stor
  - IT-säkerhet har för stor tyngd
  - KSF 3.0 är ett bra steg i rätt riktning
- Godkännandeprocessen är hindrande
  - IT-system som är värdefulla för verksamheten försenas eller stoppas, osäkerhet när system blir klara
- IT-säkerhet kräver kontinuerligt arbete
  - Hot- och sårbarhetsanalyser under driftsfasen
  - Övervakning, logganalys, patchning/uppdateringar, penetrationstester

Respondenternas svar

Situationen

- Idag skapas onödiga kostnader och hinder för verksamheten
  - Strävan mot absolut säkerhet
  - Långa cykler för utveckling och godkännande
  - Nytänkande hindras p.g.a. projektrisker
- Respondenterna önskar se större fokus på riskavvägningar
  - Verksamhetsrisker kontra IT-säkerhetsrisker
  - Nytta kontra IT-säkerhetsrisker

Analys

- Analysen utgår från att respondenternas svar speglar verkligheten och är representativa

Analys – Dagsläget

- Krav på godkännande innebär stora projektrisker idag
  - Oklar kostnad, oklar tidplan
  - Tekniken ska hantera riskerna
  - Nytänkande upplevs som riskfyllt
- Ansvarsfördelningen är komplex
  - Många aktörer, olika intressen
  - Oklara mandat

Vems fel är det?

- Lätt att peka på MUST – men felet är inte deras
  - MUST agerar utifrån den roll och det mandat som de har fått genom förordningar och styrande dokument
  - Olyckligt med resursbrist
- Strukturfel inom Försvarsmakten

Vad borde göras?

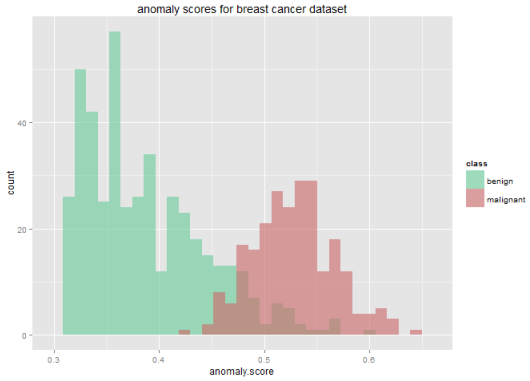
- Den här studien har inte svaret
- Läget bör utredas
  - Varför är läget som det är?
  - Vilka hinder finns?
  - Vilka framgångsfaktorer finns?
  - Hur borde utveckling, godkännande och vidmakthållande hanteras?

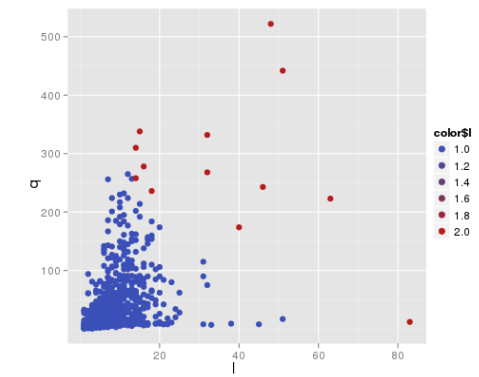
Frågor?

Heuristiska datamodeller för förbättrad logganalys

Upptäck avvikelser i nära realtid

- Upptäck avvikande beteende
- Korrelera olika datakällor
- Strukturera information
- Beskrivning av verksamheten
- Förmåga att dra slutsatser om en instans av ett objekt inom en domän
- Problemlösningsmetoder; Heuristik (upptäcka)





Robert Carlsson
Säkerhetsarkitekt Försvarsmakten

Agenda

- Vad vill vi åstadkomma?
- Hur gör vi det?
- Bakgrund
  - Logganalys /exempel på modellering
  - Information /exempel på modellering
- Modellering
- Varför och vad tillför det?
- Testfall och visualisering (demonstration)
- Slut frågor

Presentationen kommer att ta upp exempel på logganalys, informationshantering och modellering. Det krävs fördjupning för att få en helhet och önskad funktionalitet.

Vad vill vi åstadkomma!

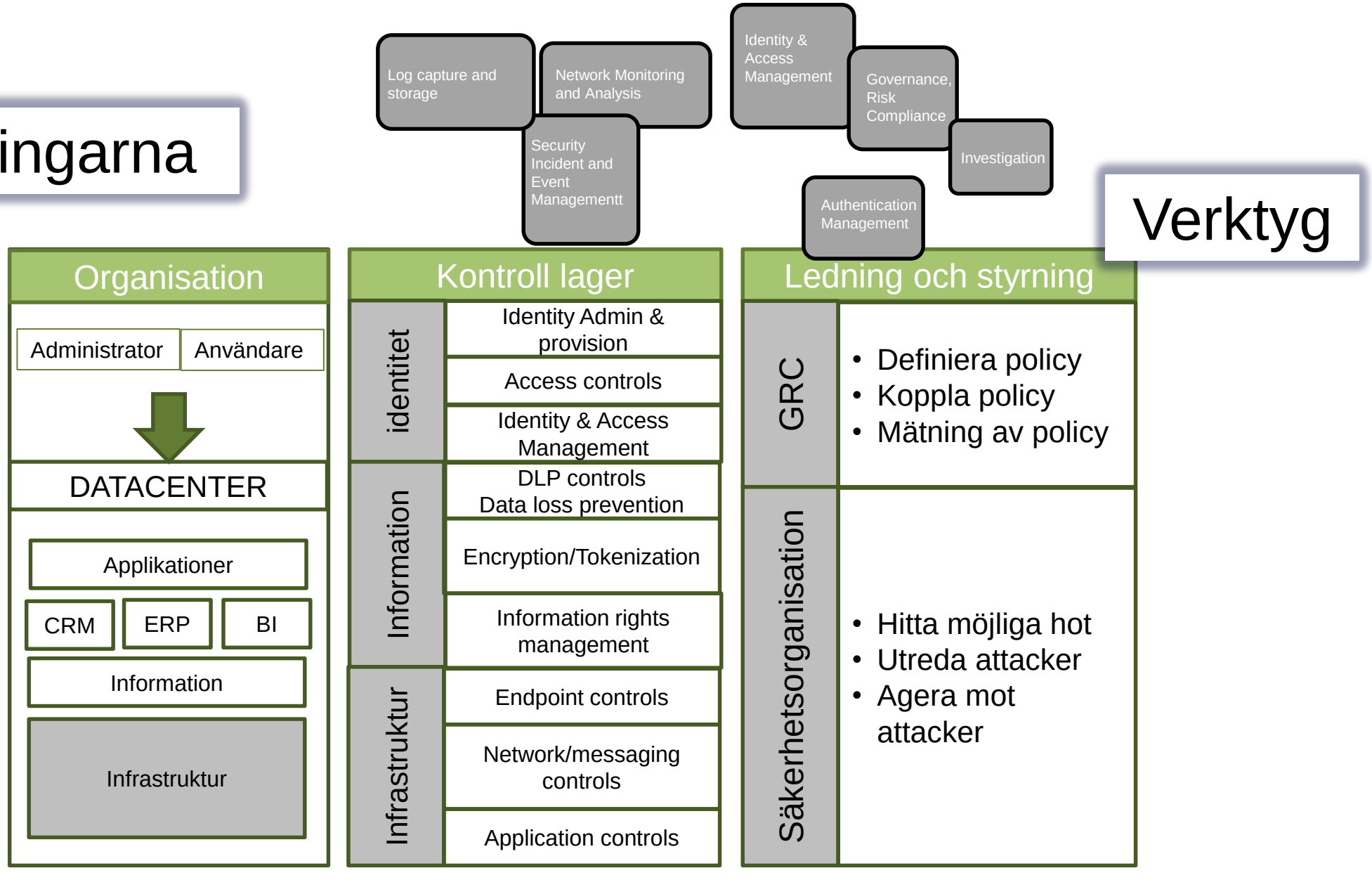
En proaktiv förmåga att upptäcka!

- Proaktivt identifiera, analysera och förhindra hot med snabbhet och skalning
- Undersöka incidenter och hot i en stor mängd data
- Automatiserad analys och förmåga att förutspå händelser

Hur gör vi det?

- Iterativ design och implementation av modelltänkt, och det utgörs bland annat av:
  - Datamodellering (objekt och relationer)
  - Beskrivning av problemstrukturer
  - Framtagning av tekniker för att utveckla lärande system
  - Användning av maskininlärningsmetoder
- Dokumentation av konceptdesign och skapande av krav hanteras i en ”enterprise architecture” miljö (EA) för spårbarhet och kvalitetssäkring.

Utmaningarna

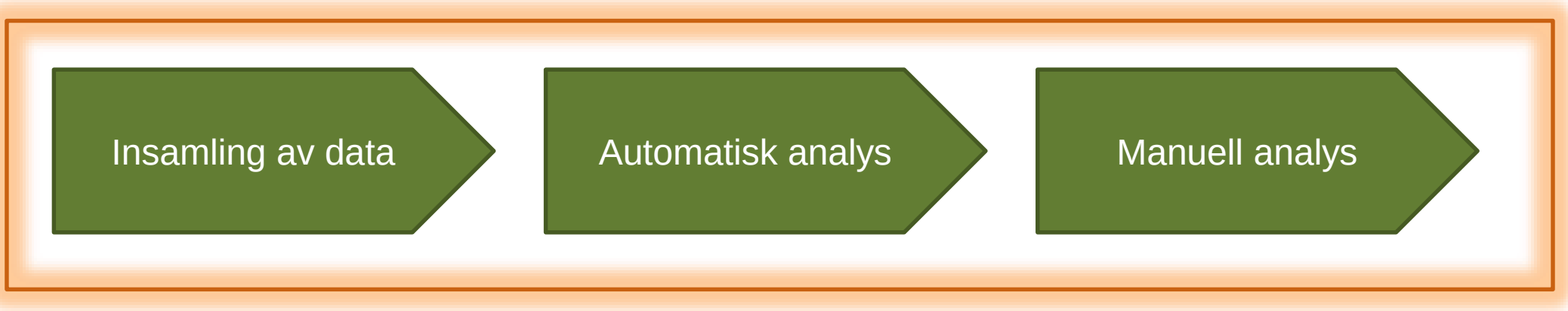


Bakgrund

- Logganalys

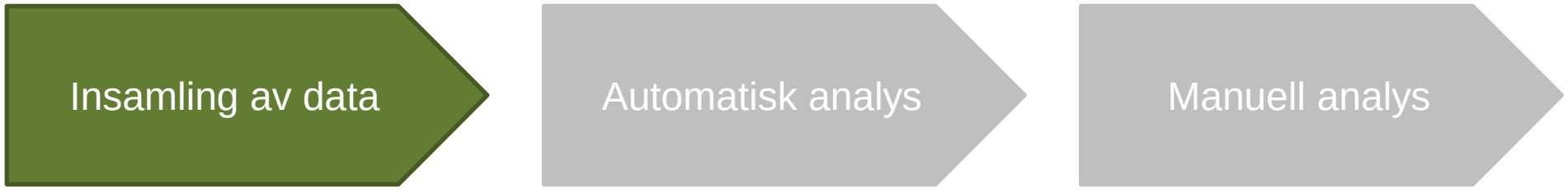
Logganalys

- Logganalytiker samlar in information och genomför analyser! (förenklat)
- Och det syftar bland annat till att identifiera avvikelser, oregelbundna mönster eller andra tecken på hot



Insamling

- Insamling av vad som sker
  - Ett IT-system har många olika platser där det lagras information om vad som händer i systemet.
  - Händelser är centrala för logganalys. Det är nödvändigt att ha en god förståelse för det tillstånd systemet är i och vilka egenskaper det vanligtvis har. Samt vilka olika relationer som finns i och omkring ett IT-system och dess data.



Exempel på relevanta systemhändelser:

- Namn på maskiner och användare i systemet
- Behörigheter i nätverk, dess maskiner och mjukvaror
- Tjänster, applikationer och andra som finns i systemet
- Kända mjukvarusårbarheter och konfigurationssårbarheter i systemet
- Det vanliga beteende som användare och mjukvaror har

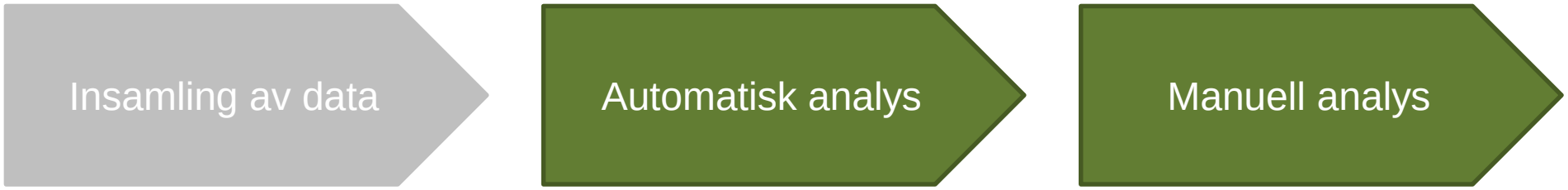
Intressanta områden

- Förutom information om vad som finns i systemet vid en viss tidpunkt kan information om vad som borde finnas i systemet vara av intresse!

Informationskvalitet!

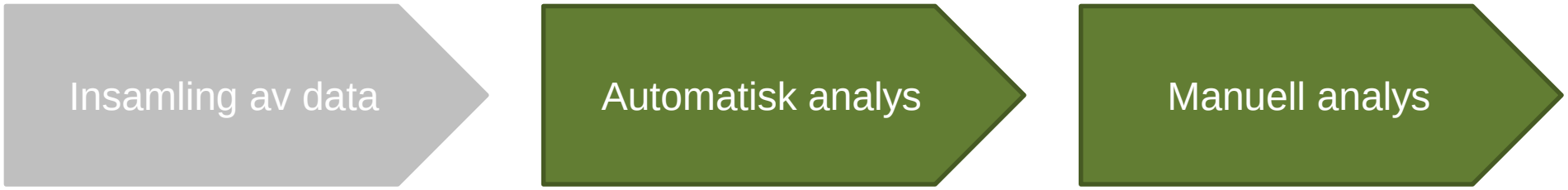
Analyser

- Syftet med insamling av data är att möjliggöra automatisk och manuell analys. ***Insamlingen bör möta de krav analysen ställer***.
- Resultat från automatiska analyser kommuniceras till en logganalytiker som fattar beslut baserat på innehåll.
- Objekt och händelse är något en analytiker bör undersöka



Analyser

- Det manuella logganalysarbetet går till stor del ut på att filtrera bort falsklarm och oviktiga loggposter, identifiera anomalier, konfigurera om sensorer, konsekvensanalyser mm.
- Logganlytikerns jobb kan till del sägas är att komplettera den automatiska analysen.



Exempel på modeller inom logganalys

- Modeller av elakartade aktiviteter (missbruk, angrepp, virusattacker etc) i systemet
  - Hur olika attacker och angrepp hör samman
  - Relationer larm har till varandra

- Modeller av godkända aktiviteter i systemet
  - Systemspecifikationer
  - Kunskap och information
- Modeller över olika komponenter i ett nätverk

Analys av modeller för elakartad aktivitet

- En vanlig metod är att matcha systemhändelser mot en databas med hårdkodade signaturer som beskriver olika elakartade eller riskabla beteenden. (IDS, Antivirus etc.)

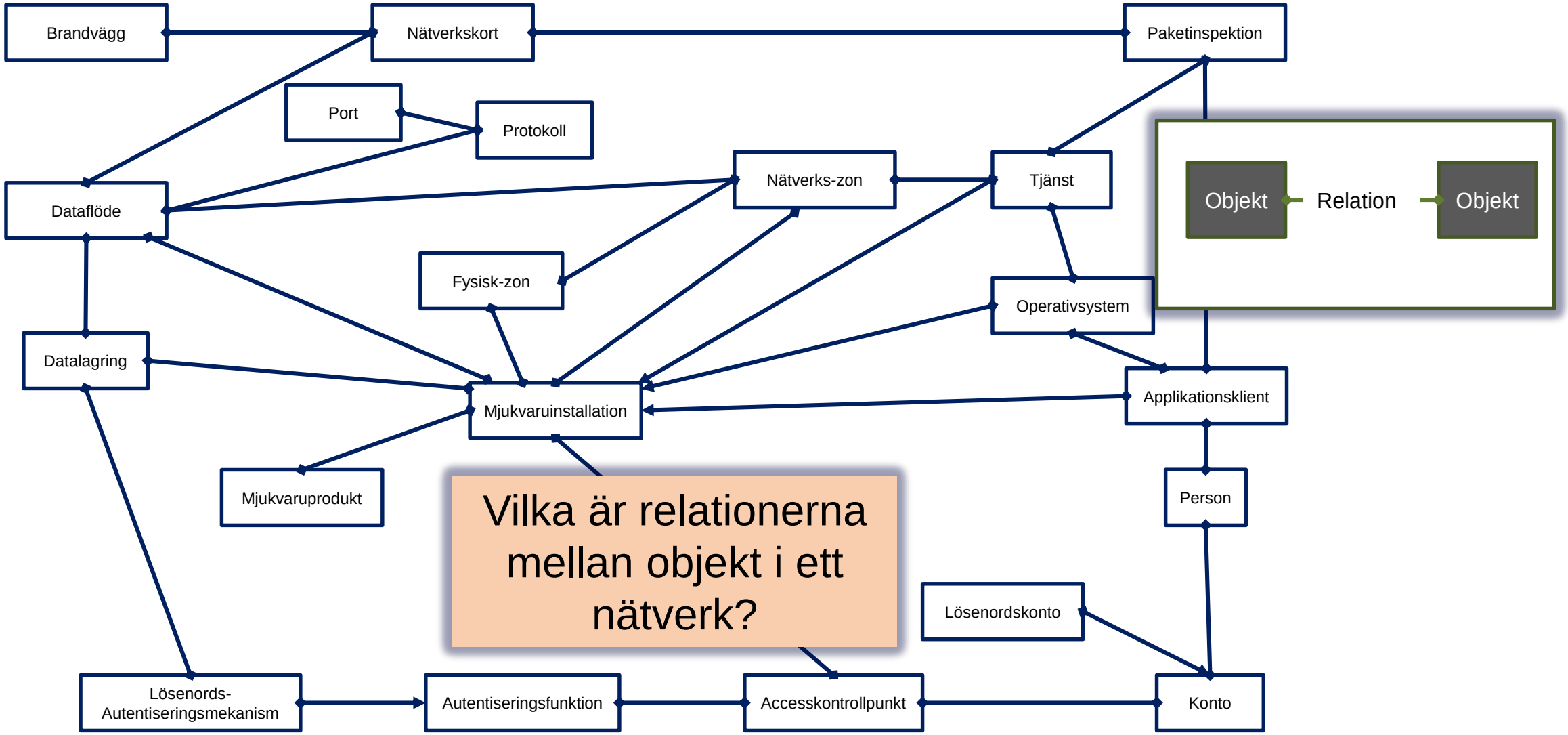
Men när händelsen inte är lagrad i databasen vad gör man då?

Modeller för godartade aktiviteter

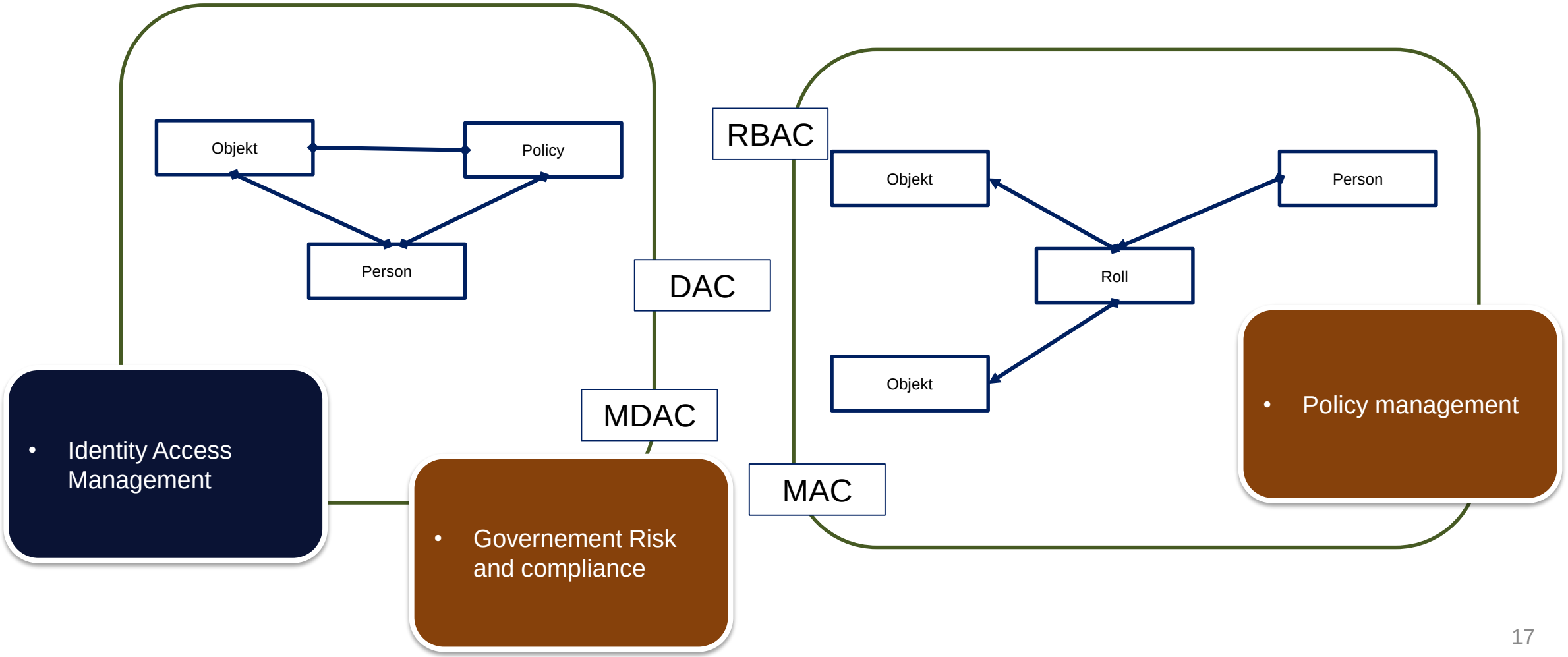
- Detektering kan göras genom att jämföra händelser och tillstånd mot en modell över vad som är godtagbart.
- Stöd till det är trafikmönster, belastningsmönster, normalbeteende!

Vilka egenskaper är godartade händelser?

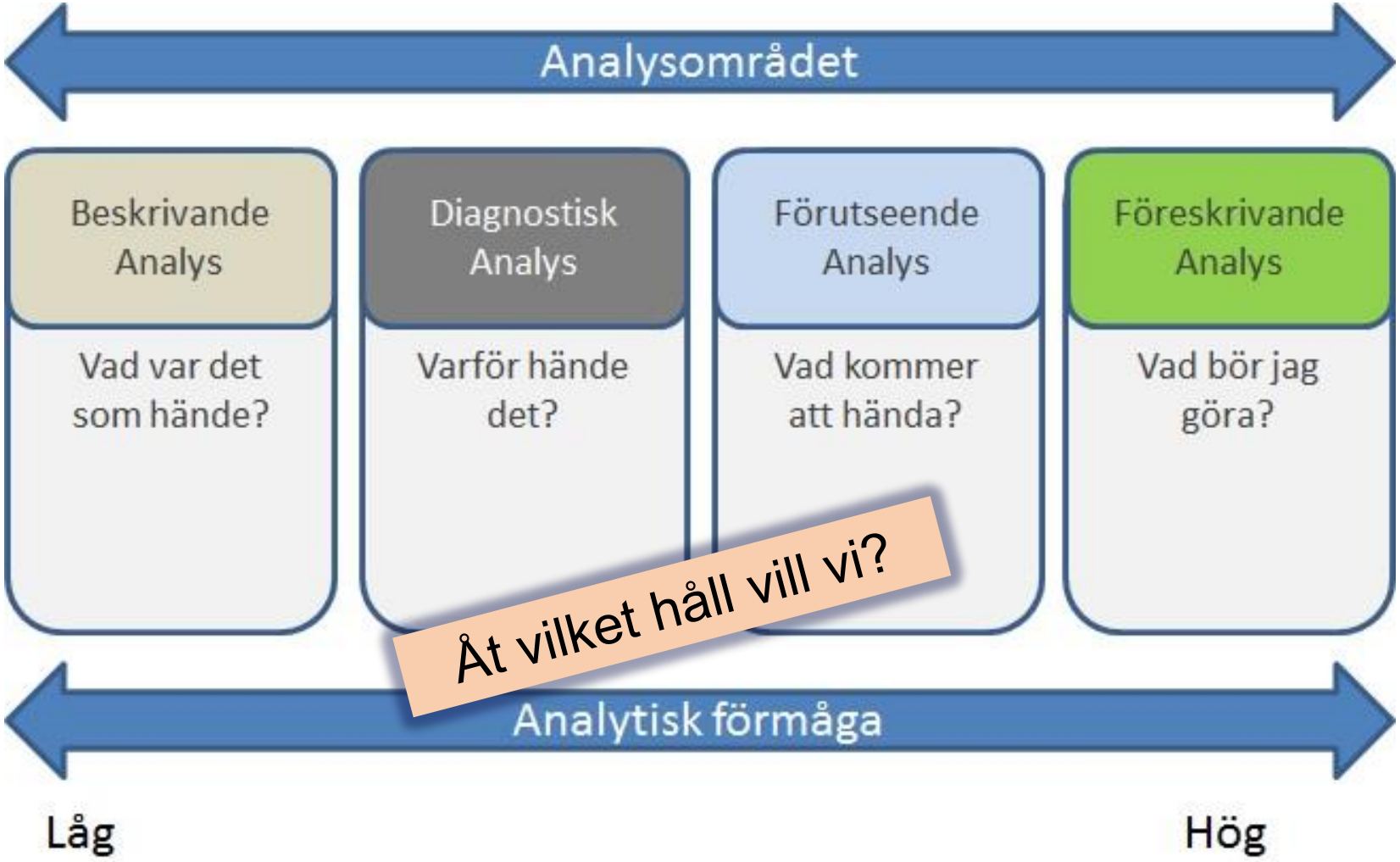
Modellering av ett nätverk



Åtkomst- och behörighetsmodeller



Faser i analysen



Rimlighet i logganalysen

- Hur gör en analytiker rimliga beslut baserat på de data som kommer in.
- Effektiva metoder för att hantera sökningar i stora datamängder är alltså av betydelse för logganalysarbetet

Bakgrund

- Information

Information

- Idag bearbetas, lagras, kommuniceras och mångfaldigas information i större mängder än någonsin.

Information

- Ett första steg mot en bättre styrning och kontroll är att skapa en tydlig bild av vilken information som organisationen är beroende av samt de system och tjänster som används för att hantera informationen

Information

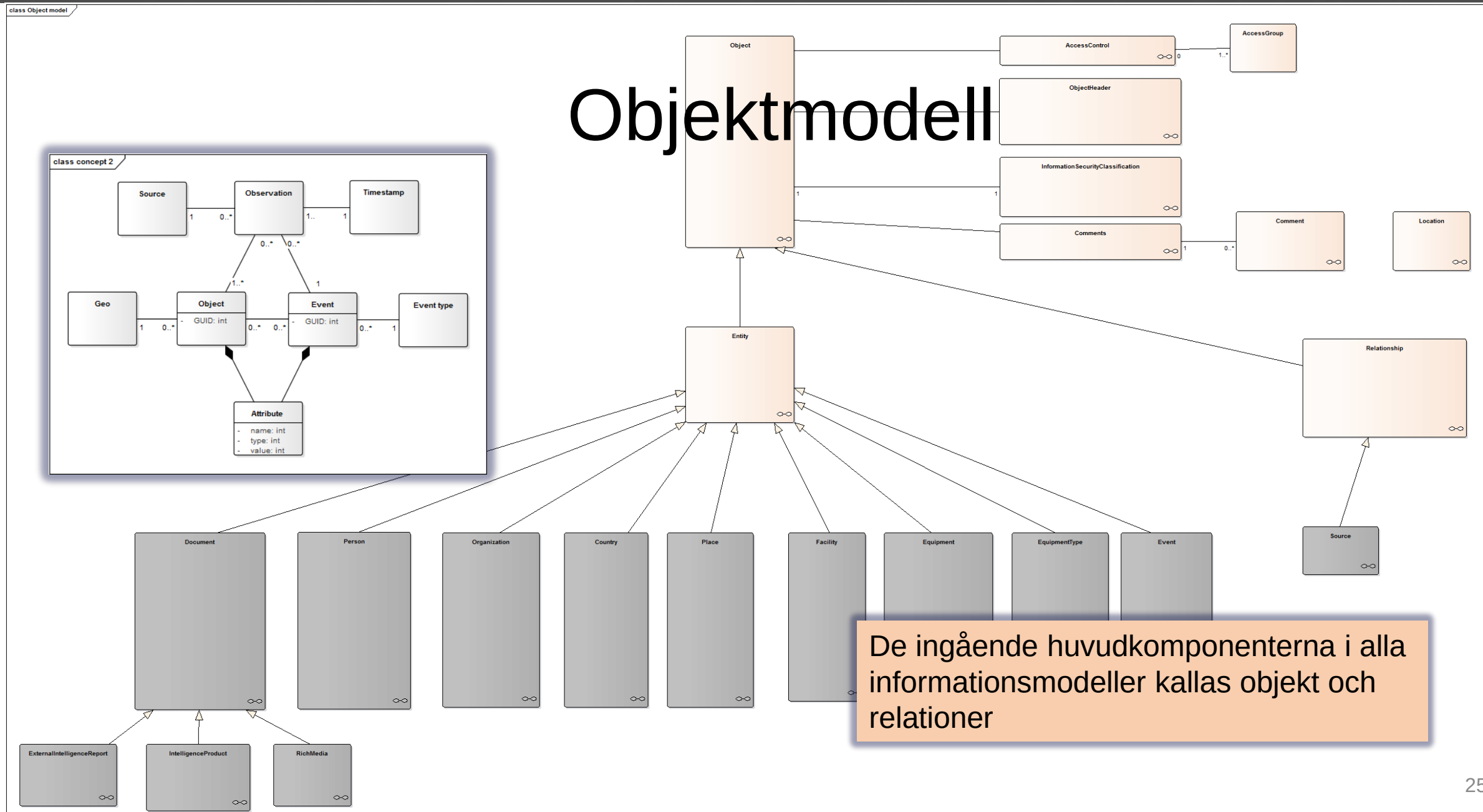
- En kartläggning av information är nödvändig för att kunna vidta rätt åtgärder för skydd och långsiktigt bevarande!

Information

- Ett första steg för att kunna skydda och effektivt nyttja den viktiga resurs som informationen utgör är att kunna analysera vilken information som hanteras och på vilket sätt det sker.

- En kartläggning av informationsflödet måste ta hänsyn till inte bara hur informationen kommuniceras och lagras utan också till vilka resurser som är involverade

Objektmodell



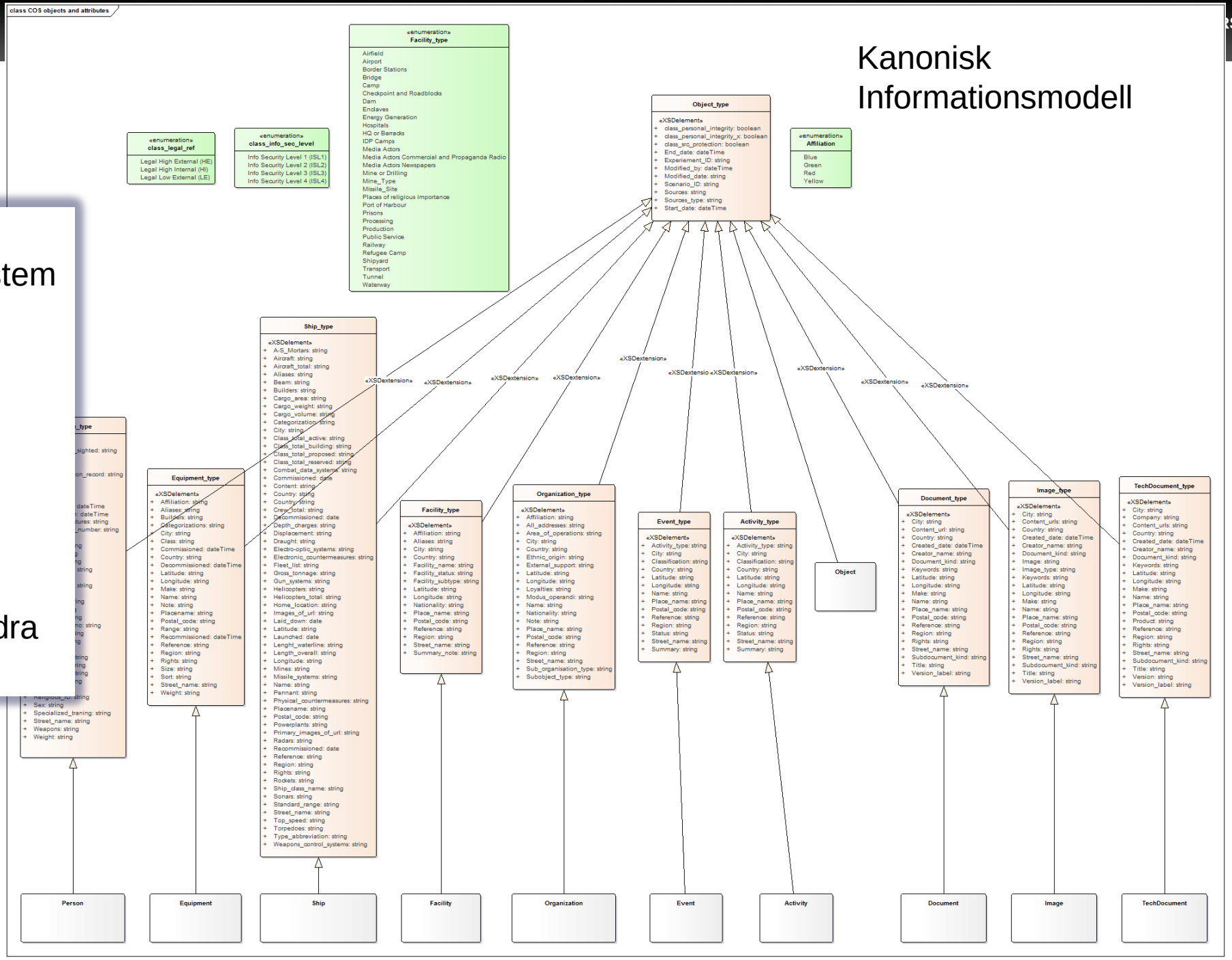
De ingående huvudkomponenterna i alla informationsmodeller kallas objekt och relationer

Kanonisk Informationsmodell

Exempel:
KSUS Konceptsystem underrättelse och säkerhetstjänst

KSUS har en omfattande IT-infrastruktur med komplex IT-miljö.

Ansvarig: Alexandra Larsson



Bakgrund

- Modeller

En modell omfattar

- Semantik- Beskrivningskategorier
- Symbolik- Regler för att göra modellen begriplig
- Syntax- Regler om hur symboler får kombineras

- Alla tre delar är viktiga
- De ingående huvudkomponenterna kallas objekt och relationer

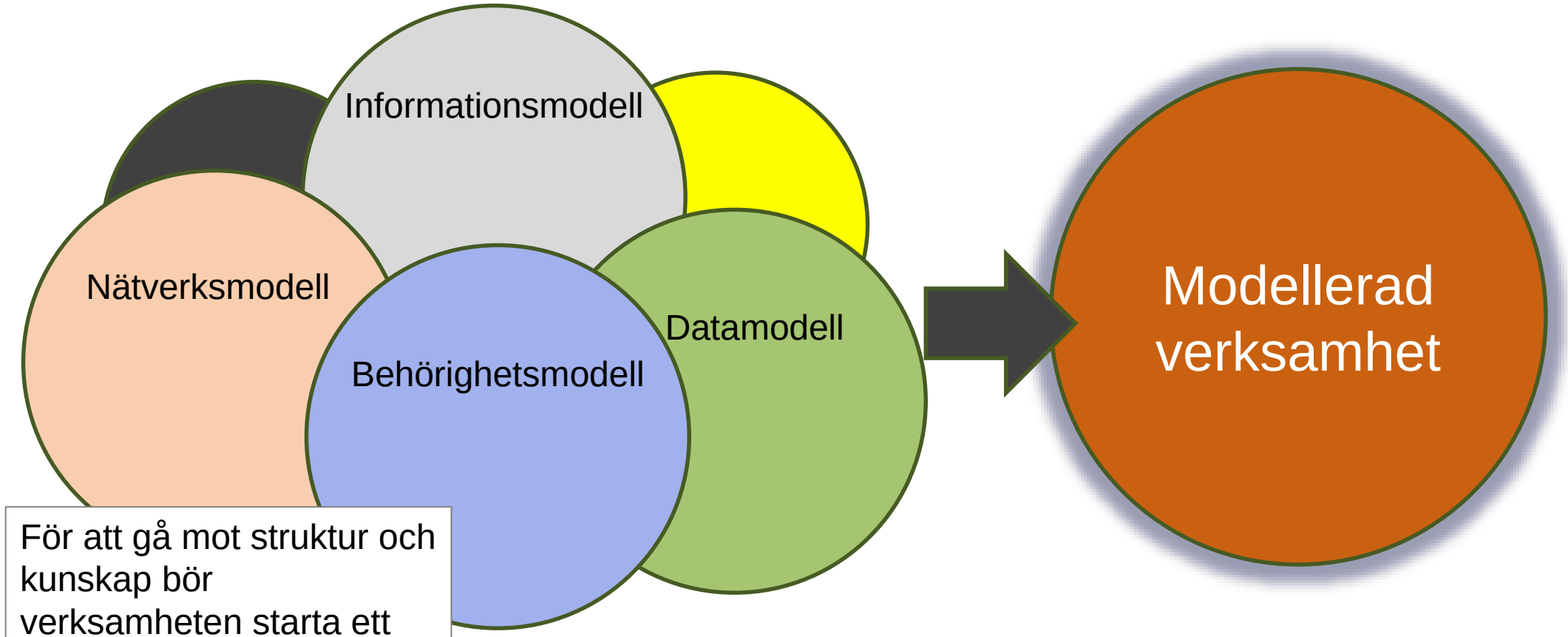
Modeller används för att:

- Beskriva en verklighet eller ett system utifrån en eller flera synvinklar.

Modellering med hjälp av EA

- Enterprise Architecture är verksamhetsdrivet och handlar om att modellera verksamhetsprocesser, medan IT-arkitektur är IT-drivet och handlar om att hitta passande tekniker och standarder.
- Det ska finnas en processbeskrivning från verksamheten. IT-sidans uppgift är att anpassa sig till den- och att hitta tekniska standarder som passar in i modellen.
- Det finns olika ramverk så som:
  - TOGAF, DoDAF, mm

Modellera verksamheten



För att gå mot struktur och kunskap bör verksamheten starta ett modelleringsarbete

Varför och vad tillför det?

- Möjlighet att upptäcka avvikande beteende
- Möjlighet att korrelera olika datakällor
- Möjlighet att strukturera information
- Möjlighet att beskriva verksamheten
- Möjlighet att ge förmåga att dra slutsatser
- Möjlighet att använda maskininlärning
- Möjlighet att analysera med hjälp av algoritmer
- Möjlighet att skapa kunskap om infrastruktur och verksamhet

- Det ger oss en av flera problemlösningsmetoder; Heuristik (upptäcka!)

Testfall och visualisering

Tillvägagångsätt med Neo4j

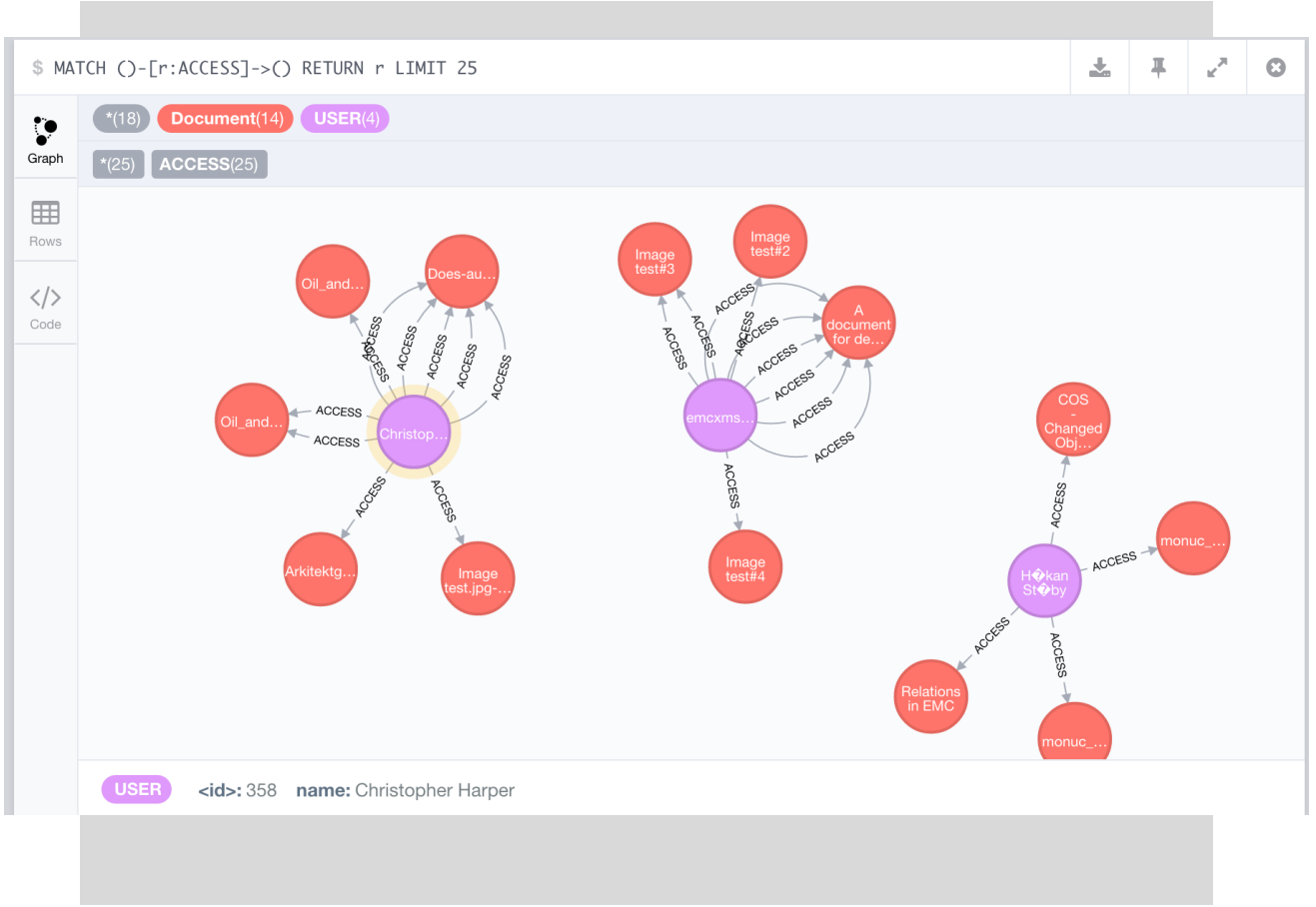
- Användning av Neo4j inbyggda ETL verktyg för att importera strukturerad data enligt informationsmodellen och transformera till Neo4j interna graf representation.
- Sedan användes R med ett R bibliotek för att ställa frågor till Neo4j och bearbeta data för att skapa grundläggande grafer.

Tillvägagångssätt med IBM i2

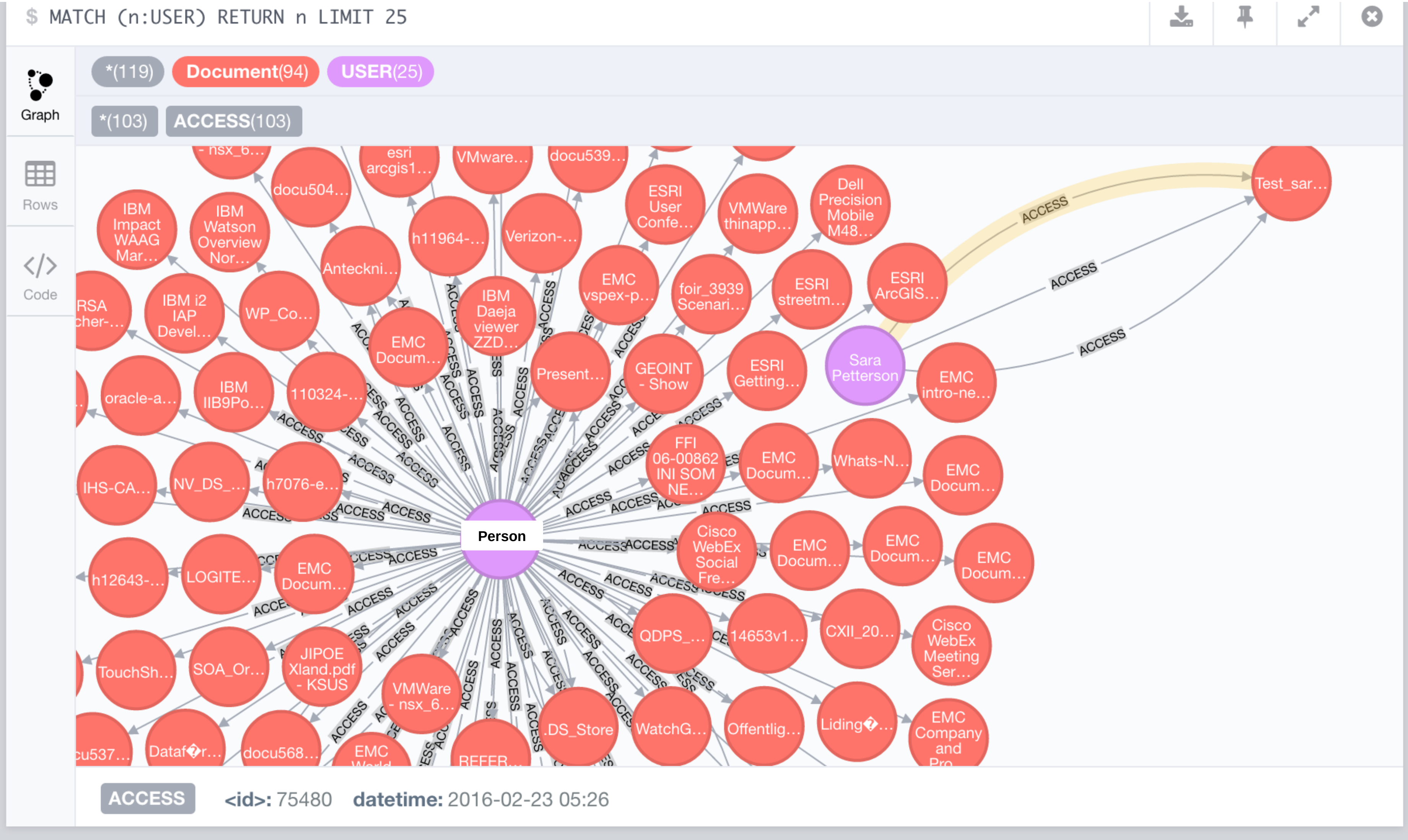
- Användning av IBM i2 inbyggda verktyg för import av strukturerad data enligt informationsmodellen och sedan transformerad till IBM i2 interna representation

- Som en POC, importerades en access-logg från Documentum till Neo4j

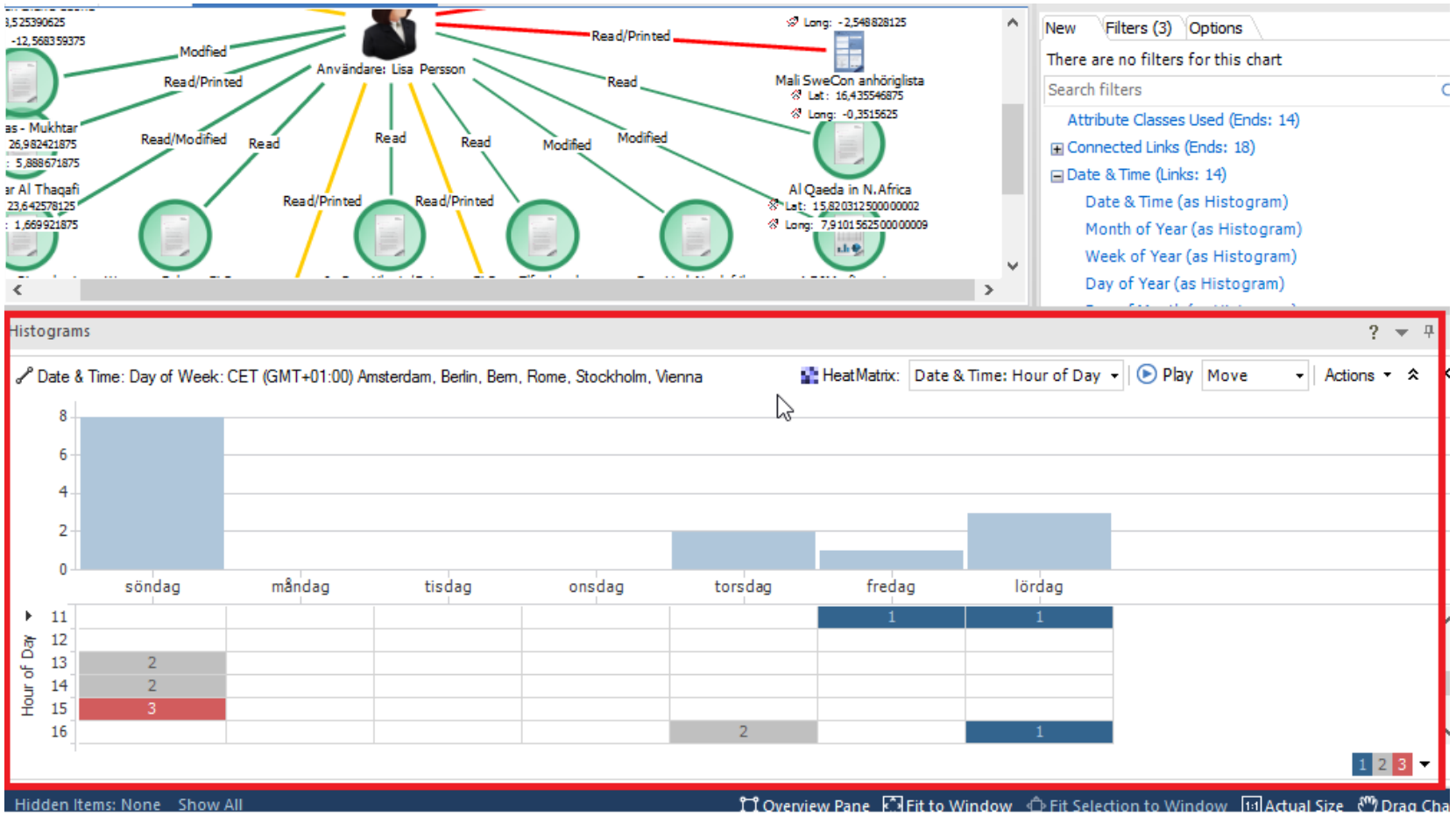
- Syftet var att visa att vi kan relatera datakällor till informationsmodellen, och sedan använda verktyg för att utreda informationen



Vilken access har en person haft vid en viss tid



Temporal vy över access visualiserat med IBM i2



Slut

Frågor?

FOI:s verksamhet inom IT-säkerhet

Peter Stenumgaard
Enhetschef
Informationssäkerhet och IT-arkitektur

www.foi.se/informationssakerhet

Forskning och direktstöd

Kunskapsuppbyggnad och kunskapstillämpning

Forskning

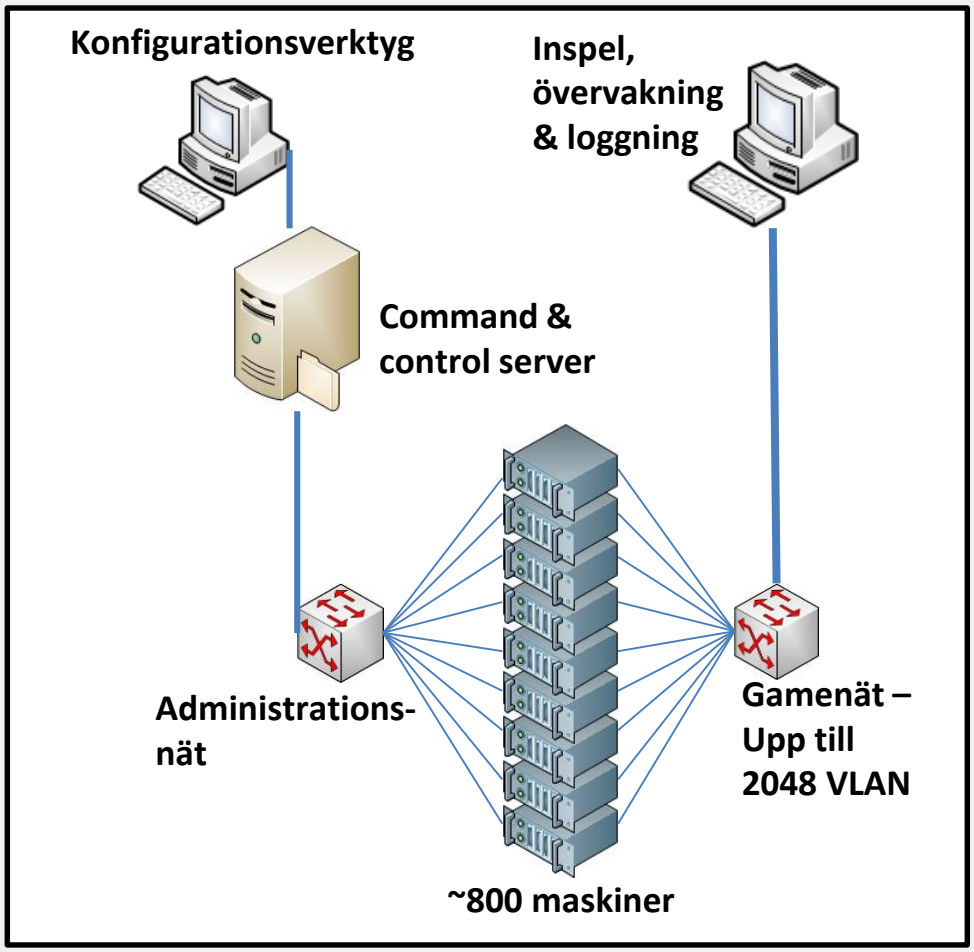
Expertstöd

Utbildning/Träning
/Övning

Delområden

- Utbildning, träning och övning inom försvar av IT-system (medvetande- och förmågehöjande)
- Strategiskt expertstöd
- Teknik för IT-säkerhet
- Bedömning av informationssäkerhetsrisker
- Säkerhet i industriella informations- och styrsystem (MSB)
- IT-forensik
- Sociala aspekter av informationssäkerhet

CRATE – Cyber Range And Training Environment



- Nationella och internationella IT-säkerhetsövningar
- Praktiska moment i kurser för FM och MSB.
- Experiment inom:
  - Sårbarhetsbedömning
  - Intrångsdetektion
  - Övningsuppföljning

FOI


www.foi.se/informationssakerhet

Crate 2.0 – Nationell Cyber Range

Magnus Sparf, FOI
Richard Widh, MSB

2016-11-02

Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

FOI

Defaitistisk (realistisk?) syn på cyberhotet

- Utveckla säker programvara
- Pålitlig leverantörskedja
- Konfigurera programvaror att vara säkra
- Hantera arvet
- Backup
- Utbilda och träna användare och specialister
- …

- Minimera och avgränsa skada
- Fortsatt drift av kritiska funktioner
- Säkerställ bevisning
- …

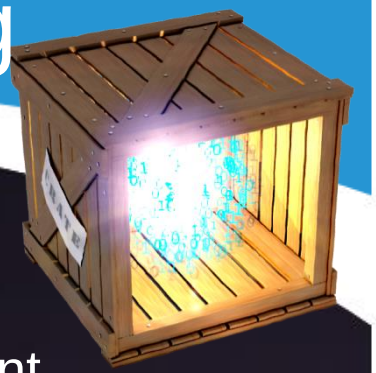
- Forensisk analys
- Återställ infekterade system
- Erfarenhetsåtermatning
- …

Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

FOI

CRATE - **C**yber **R**ange **A**nd **T**raining **E**nvironment



- Designad för cyberförsvarsövningar, utbildning och experiment
- ~750 fysiska servrar
- Förmåga att rulla ut virtuella maskiner (5000+) med olika sårbarheter i olika organisationsstrukturer i en kontrollerad miljö (Windows, Linux)
- Internetinfrastruktur med virtualiserade routrar (BGP, RIP)
- Klientbaserade trafik- och händelsegenererade agenter som simulerar användarbeteende
- Webbaserat verktyg för att designa och hantera utrullning av [illegible] konfigurationer
- Verktyg för att logga, följa, rekonstruera och utvärdera

Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

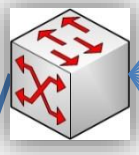
FOI

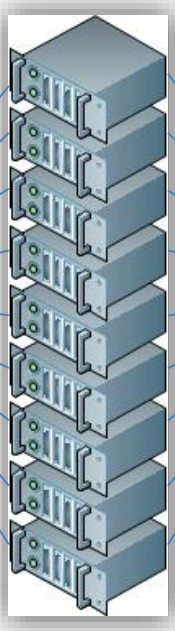
Automatic deployment and configuration

CrateWeb
Configuration and visualization utility

Command and control server
Pushes VM templates and configuration files to servers

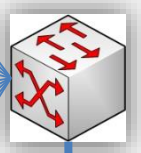
Administrative network





~750 servers

In-Game Internet
2048 networks
(soon 16 million)



Data collection
Log files
IP packets

Router backbone

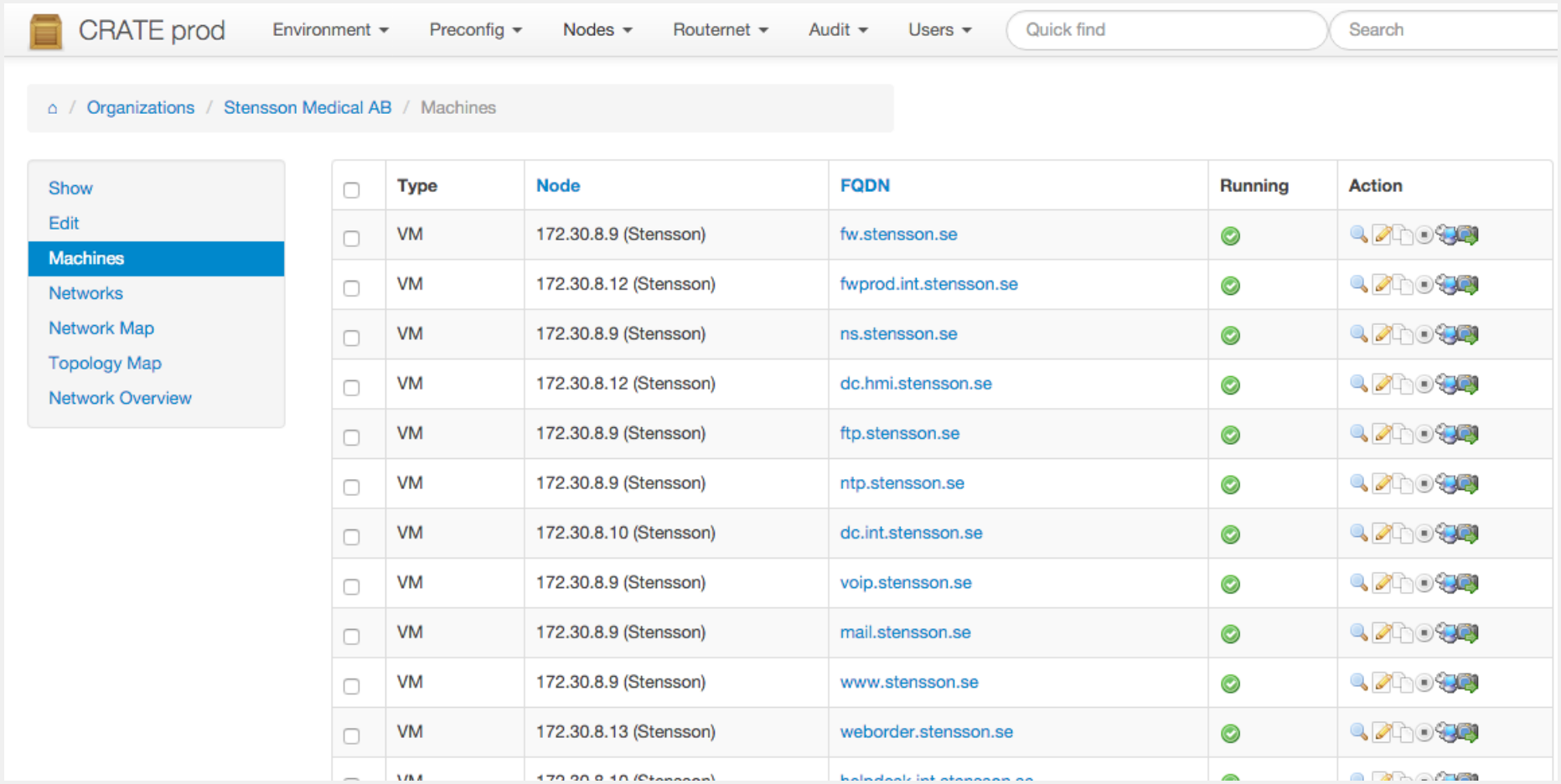
- ✓ 100 core routers
- ✓ All virtualized
- ✓ Can be geo-mapped anywhere in the world

Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

FOI

Management

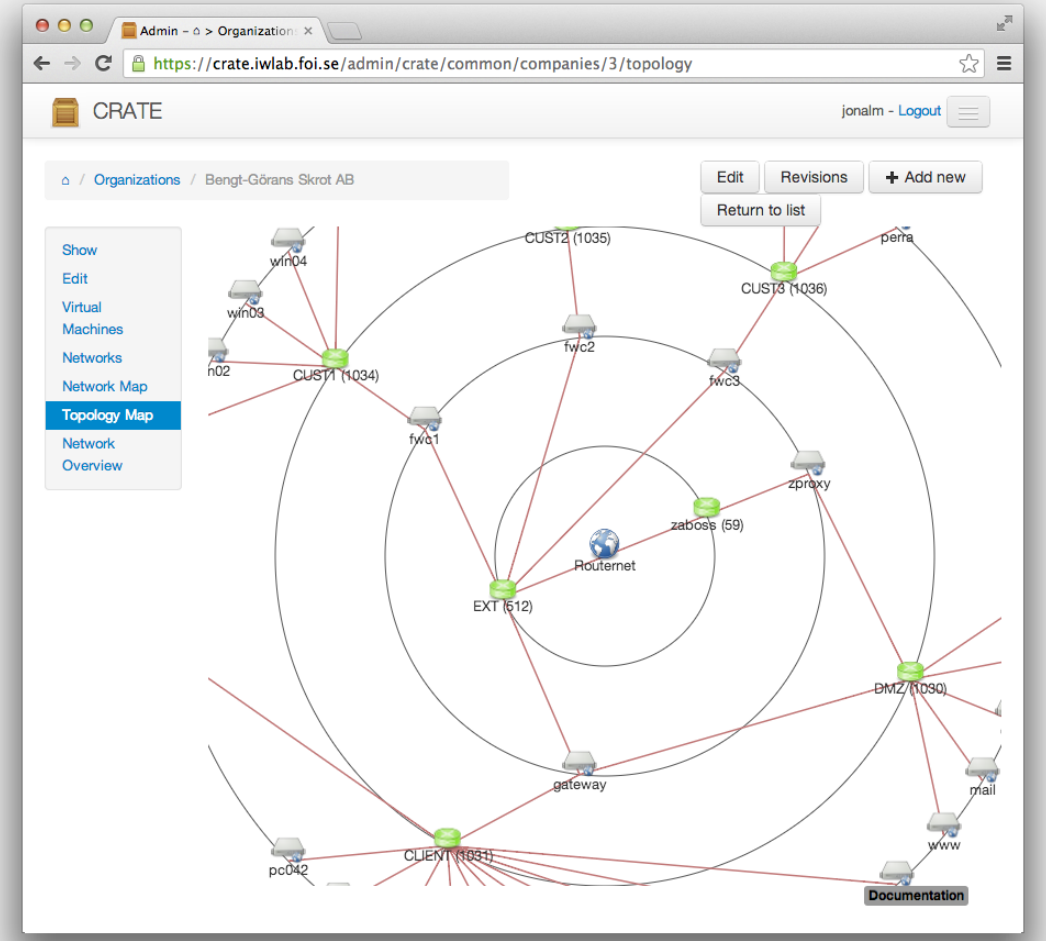


MSB Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

FOI

Management



Myndigheten för samhällsskydd och beredskap

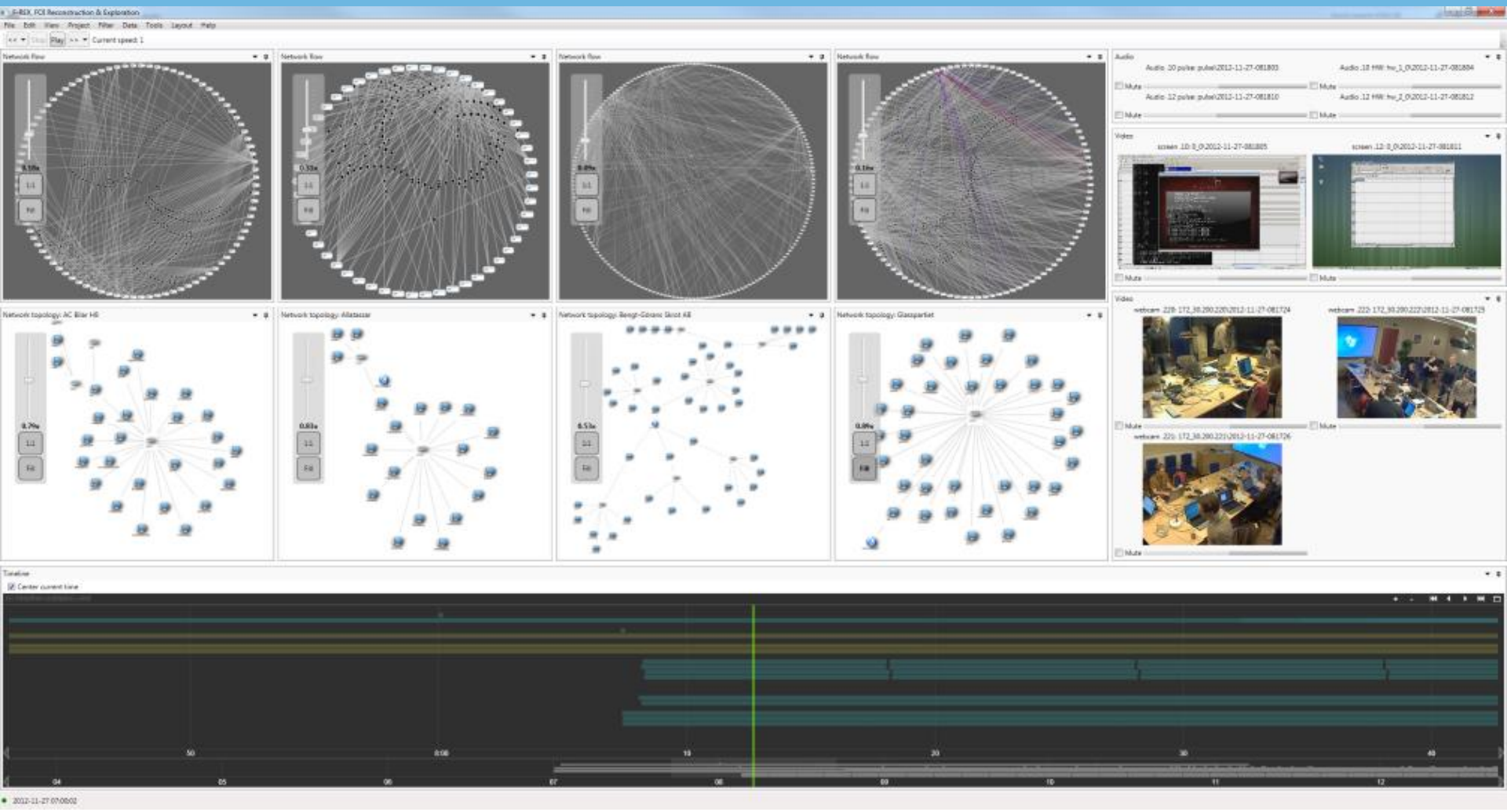
FÖRSVARSMAKTEN

FOI

Automated users (“bots”)

- Generate network “noise”
- Doing common tasks (surfing, reading/sending email, open documents)
- Enable possibility of spear phishing attacks
- Controlled from outside the gaming environment

Evaluation

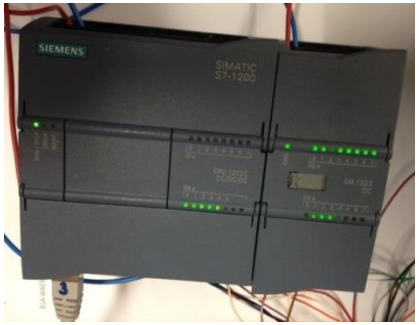


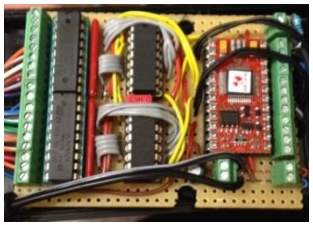
Myndigheten för samhällsskydd och beredskap

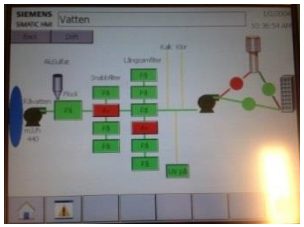
FÖRSVARSMAKTEN

FOI

- Integrering av fysiska artefakter
- Virtualisering
- Emulering
- Simulering

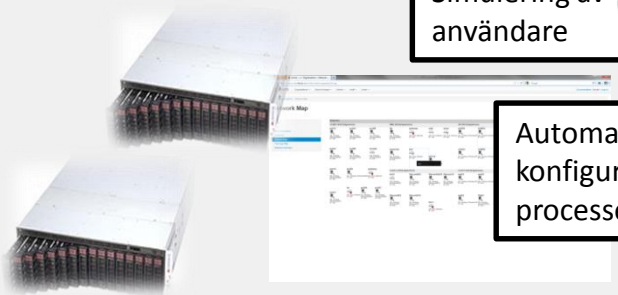






Tidslinjal

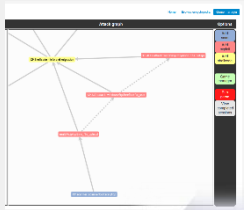
Hårdvara donerat från Superdatorcentrum och SMHI



Simulering av användare

Automation av konfigurations-processen

Ny hårdvara



Automatiserad av inspel

Ny hårdvara

2008 2009 2010 2011 2012 2013 2014 2015 2016 2017

DDoS-övning med Estniska och Svenska studenter.

Baltic Cyber Shield: 6 blå lag och över 100 deltagare från flera länder.

Experiment och tester tillsammans med Försvarsmakten.

Nationella och internationella övningar under ledning av MSB.

FoT-projekt inom logganalys och övningar med ITF.

Stabil finansiering för att vidmakthålla och utveckla CRATE?

MSB Myndigheten för samhällsskydd och beredskap

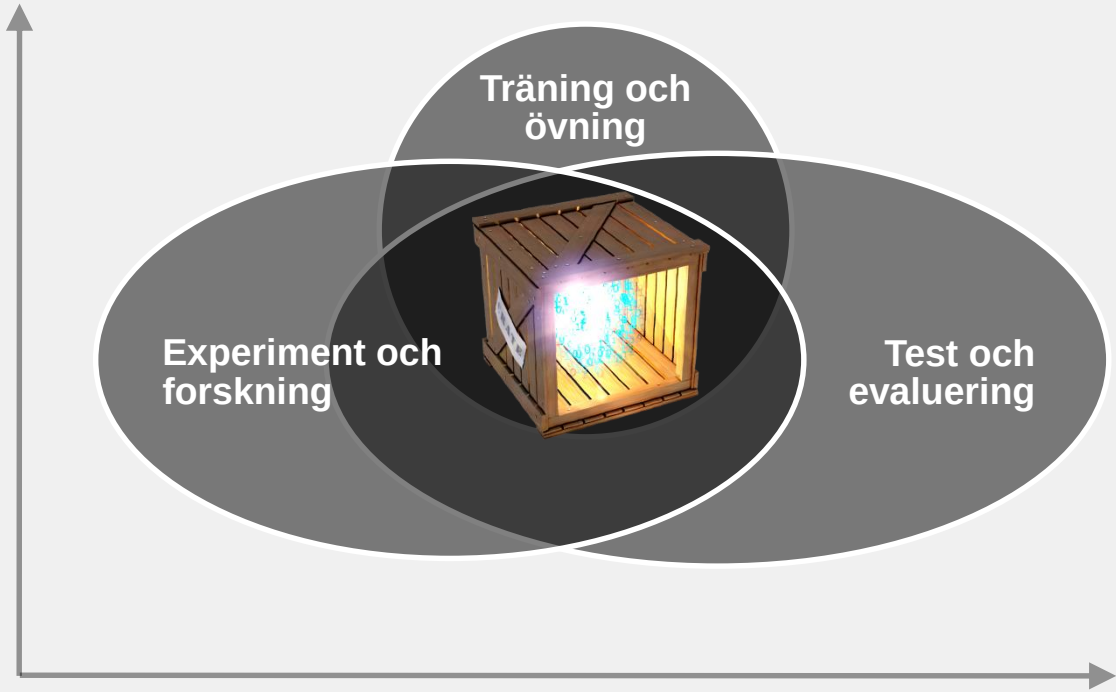
FÖRSVARSMAKTEN

VINNOVA

FOI

Den huvudsakliga idén

- Träning och övning:
  - Realistiska tekniska övningar är kul och medvetandehöjande.
  - Operationer i cybermiljön och dess taktik behöver prövas.
- Test och evaluering:
  - IT-säkerhetsprodukter (IDS, brandväggar, SIEM, mm)
  - IT-avdelningar
- Experiment och forskning
  - Beteende hos grupper, individer och på skadlig kod
  - Algoritmer, Protokoll
  - Värdering av säkerhetsåtgärder och säkerhet i system



Exempel på genomförd verksamhet

Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

FOI

Exempel 1: Nyttan med en operatör

- Från en övning 2011 samlades data om:
  - Angriparnas aktiviteter
  - Alarm från IDS-systemet
  - Alarm från IDS-systemets operatör
- Skript skapade bakgrundstrafik enligt samma användningsmönster som riktiga datoranvändare (på FOI, Universitet, etc.).
- I efterhand kunde alarm markerats som korrekta eller felaktiga.

	IDS	Admin
Alarm skapade	2107	70
Recall **P(Alarm=Ja | Attack=Nej)**	69%	58%
Precision **P(Attack=Ja | Alarm=Ja)**	11%	57%

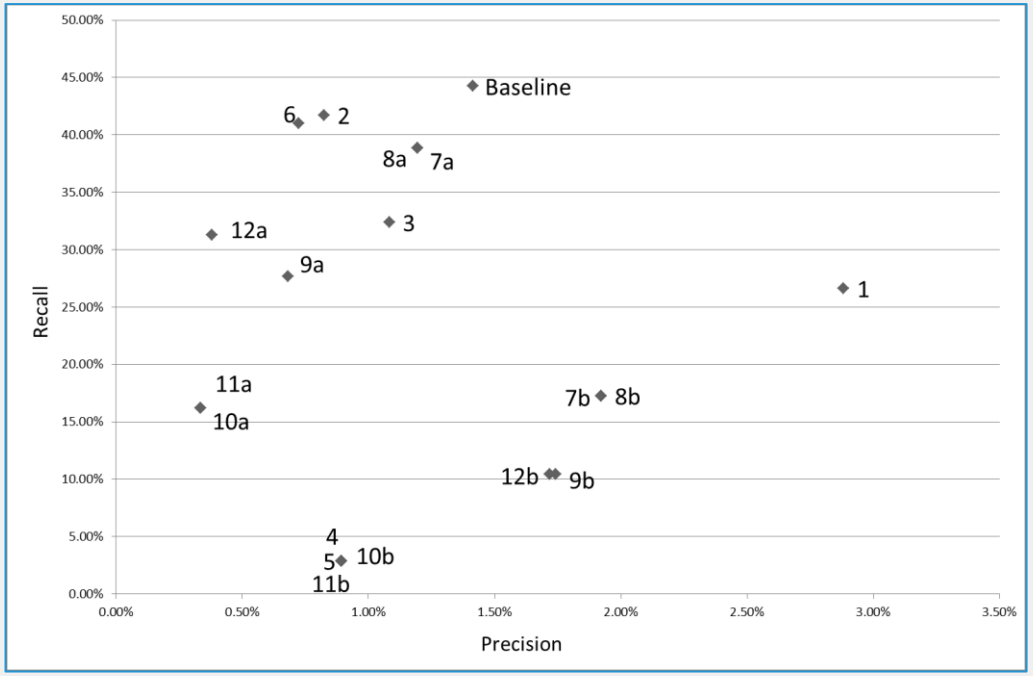
- Administratörens alarm är 5 grr mer precisa.
- Administratören använde kunskap om:
  - Datornätverket
  - Generell kunskap om säkerhet och IDS:er
  - Kunskap om hotbilden

Sommestad & Hunstad, "Intrusion Detection and the Role of the System Administrator", *Information & Computer Security* 21 (1): 30 – 40, 2012.

FOI

Exempel 2: Att automatisera en operatör

- Liknande test som innan, men med data från 2012 med mer komplex miljö.
- Administratörens resonemang om falsklarm automatiseras genom att korrelera larm mot:
  - Systemets arkitektur och tjänster
  - Kända sårbarheter i systemet



- Gick åt skogen!
- Inget av de 18 filtren eller någon kombination av dem presterar bra.

Sommestad & Franke, “A test of intrusion alert filtering based on network information”, *Security and Communication Networks*, *8*(3), 2291–2301, 2015.

FOI

Swedish Civil Contingencies Agency

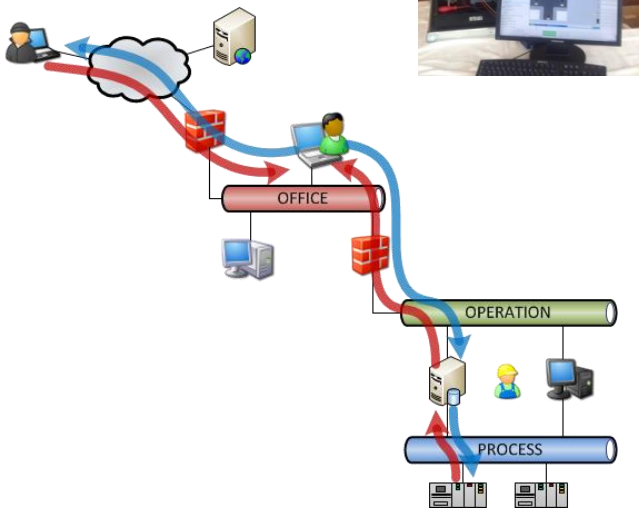
Training, part 1: Basic security in Critical Infrastructure Control Systems

Awareness raising course with practical hands on training.

Participants get education in threats, risks and mitigations.

Participants will perform a step by step attack with real hacking tools against an virtualized ICS environment. (Traffic lights)

Course ends in a workshop how to secure and defend an ICS company. Including mitigations in physical security, information security and IT-security.



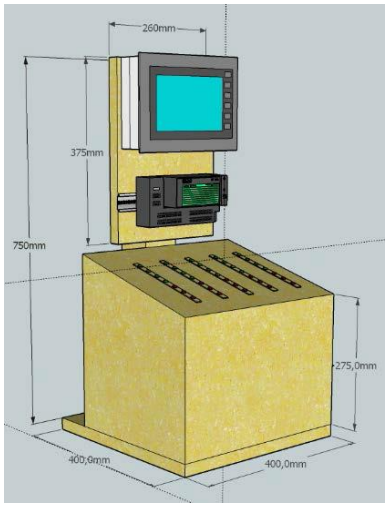
Swedish Civil Contingencies Agency

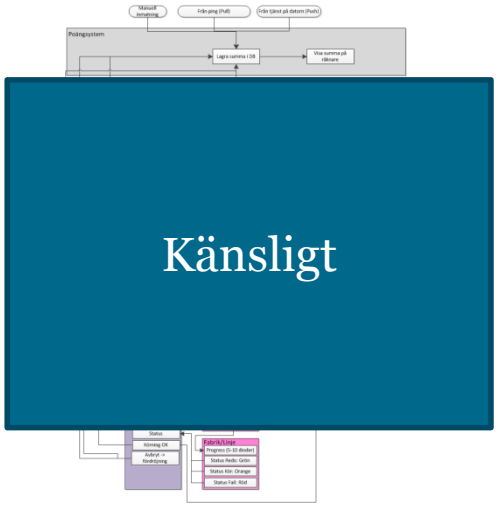
Training, part 2: Practical incident handling in Critical Infrastructure Control Systems

A pharmaceutical company needs help maintaining the production of special pharmaceuticals, but the as the whole team of the regular IT/OT staff is on a conference, a special team (the participants) are called in on extreme short notice to help protect the facility as a cyber threat is imminent.

By using regular IT-security tools the special team needs to dive into the network and perform live incident handling and maintenance without disturbing the ICS systems and at the same time make sure that the production is up and running.

And of course, the hackers are closing in ready to steal recipes and disrupt the production.





Nordic CERT Exercise 2015

Aim of the Exercise

- Strengthen the Nordic National CERT Collaboration (NCC) and the relations between participants

Objectives

- Develop the capability to:
  - share information within the Nordic National CERT Collaboration (NCC)
  - establish a common situational awareness within the NCC
  - cooperate within the NCC to handle IT incidents

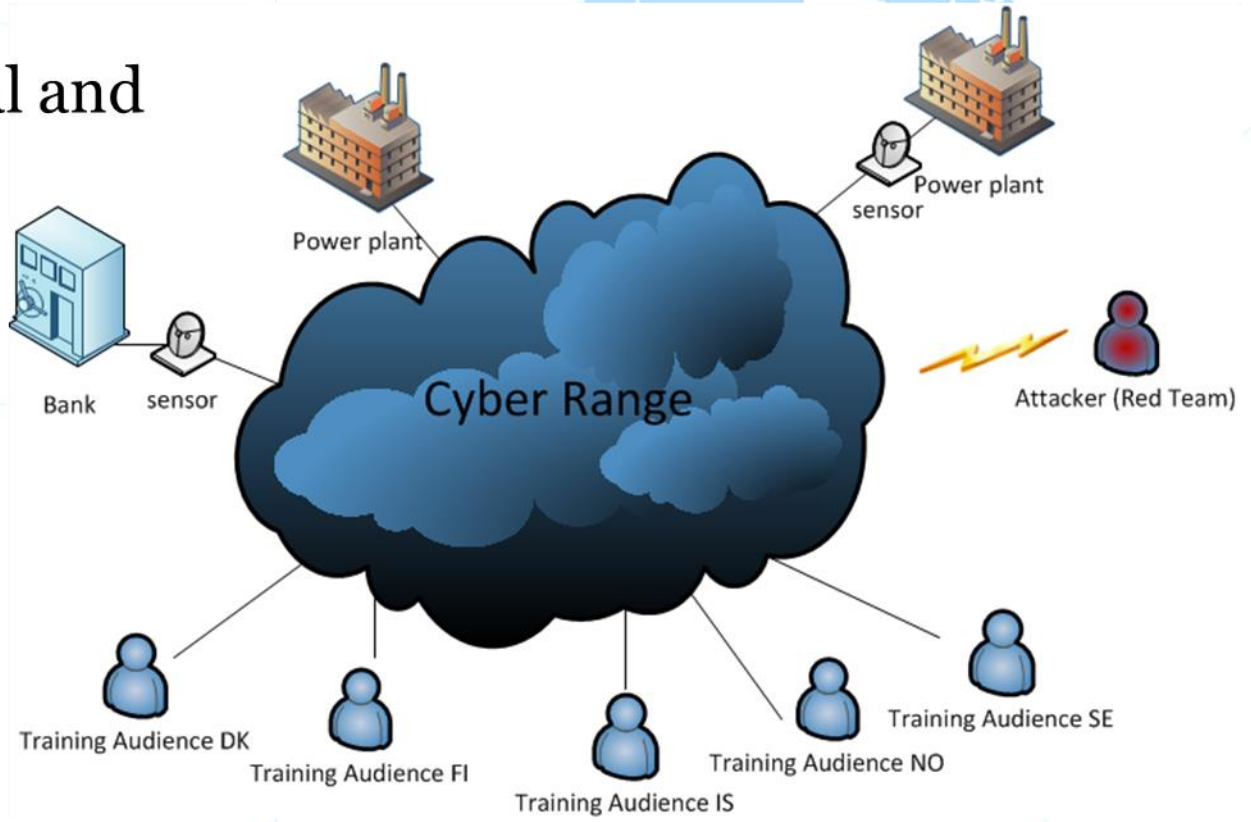
Overarching Concept

Operational aspects

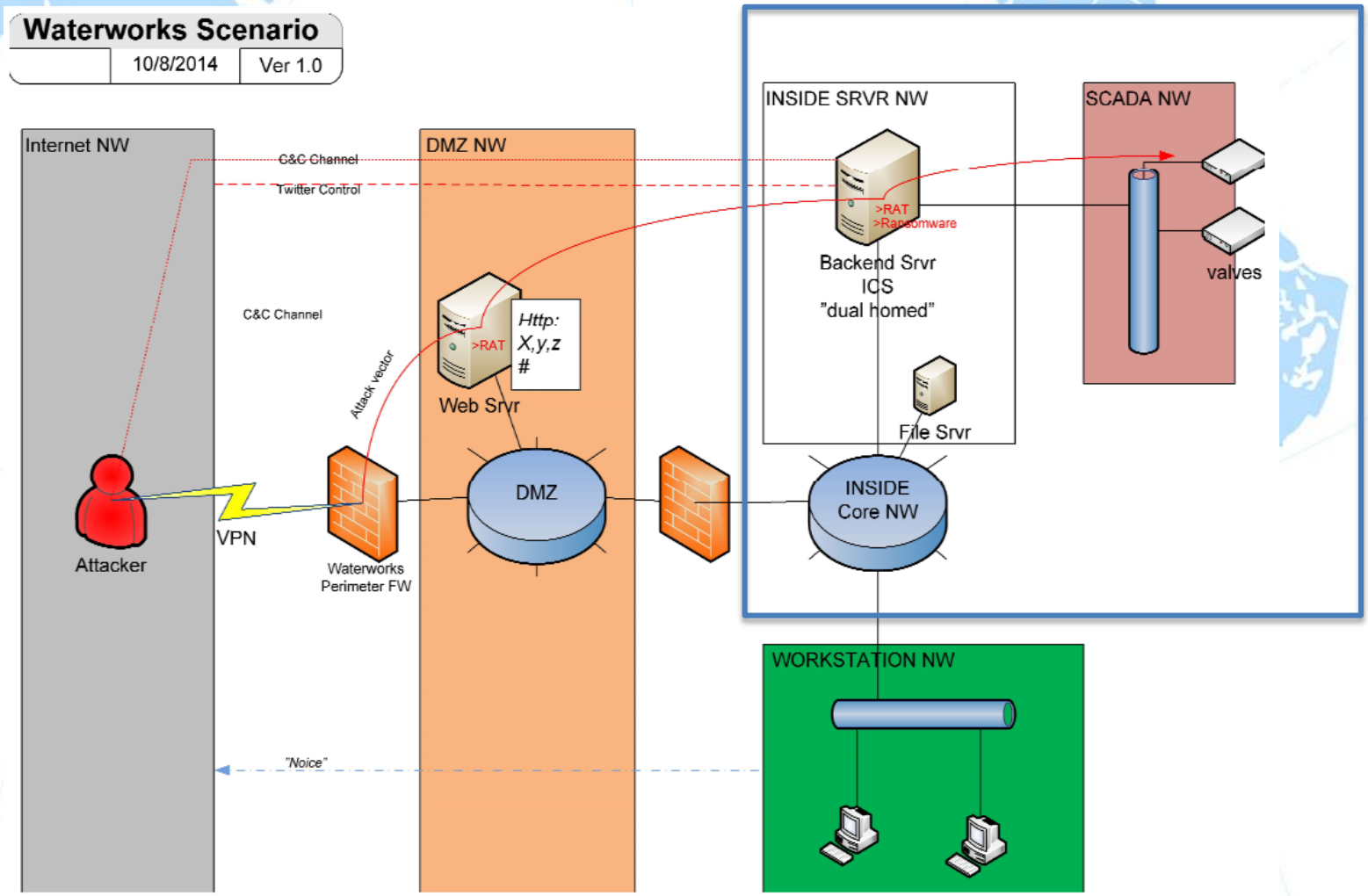
- 2 days simulation exercise
- A simulated society created in the cyber range
- Advanced technical and operational callanges

Trust aspects

- Demi-distributed
- Social gatherings in evening



Example: Waterworks



Digital and physical IT challanges

```
0125FEA8  010424B6 ╢$♦0 ┌CALL to CreateMutexW from KERNEL_1.010424B0
0125FEAC  0108AAFC ⁿ¬◘0 │pSecurity = KERNEL_1.0108AAFC
0125FEB0  00000000 .... │InitialOwner = FALSE
0125FEB4  0107D8C0 └┬·0 └MutexName = "Global\{5EC171BB-F130-4a19-B782-B6E655E091B2}"
0125FEB8  0125FF84 ä %0
0125FEBC  0125FF84 ä %0
0125FEC0  009733C8 ╚3ù.
0125FEC4  0125FEDC ▄■%0
0125FEC8  010626FC ⁿ&♣0 RETURN to KERNEL_1.010626FC from KERNEL_1.01063259
0125FECC ┌0125FF2C , %0
0125FED0  01042449 I$♦0 RETURN to KERNEL_1.01042449 from KERNEL_1.0104249C
0125FED4  0107D8C0 └┬·0 UNICODE "Global\{5EC171BB-F130-4a19-B782-B6E655E091B2}"
0125FED8  00000008 ◘...
0125FEDC  01051DEE ∈#♣0 RETURN to KERNEL_1.01051DEE from KERNEL_1.0104243B
0125FEE0  00973B70 p;ù.
0125FEE4  0107D8C0 └┬·0 UNICODE "Global\{5EC171BB-F130-4a19-B782-B6E655E091B2}"
0125FEE8  0125FF84 ä %0
0125FEEC  00000000 ....
0125FEF0  01052619 ↓&♣0 RETURN to KERNEL_1.0105261
0125FEF4  7C90DA0C .┌É¦ RETURN to ntdll.7C90DA0C
0125FEF8  7C8024C7 ╠$Ç¦ RETURN to kernel32.7C8024C7
0125FEFC  000004C0 └♦..
0125FF00  00000000 ....
0125FF04  0125FF30 0 %0
0125FF08  010525D2 π%♣0 RETURN to KERNEL_1.010525D2
0125FF0C  000004C0 └♦..
0125FF10  0125FF84 ä %0
0125FF14  0106C8ED φ╒♣0 KERNEL_1.0106C8ED
0125FF18  009733C8 ╚3ù.
0125FF1C  00973B70 p;ù.
```

Framtiden

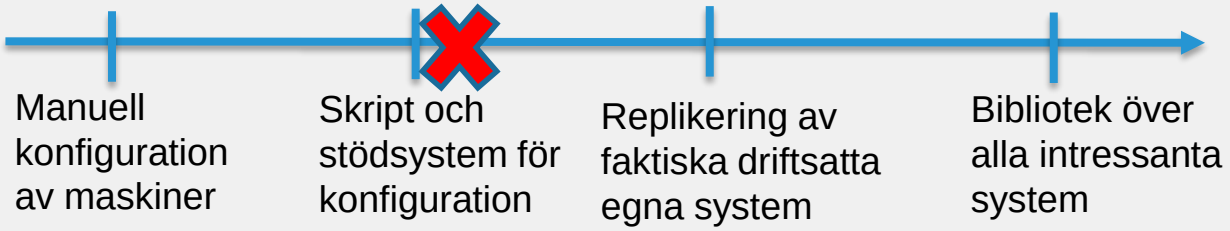
Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

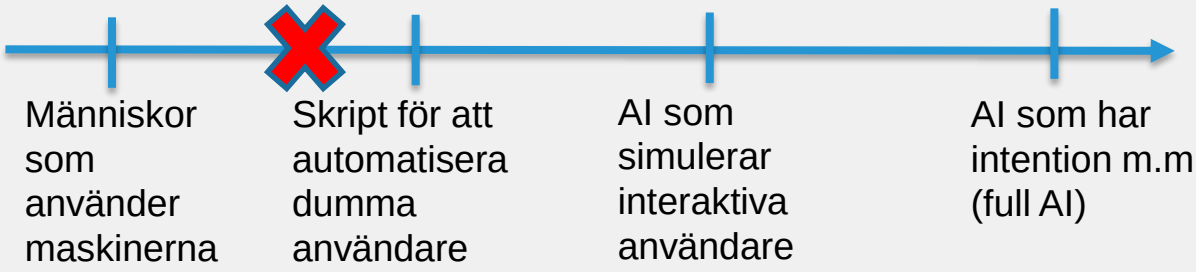
FOI

Nuläget i CRATE

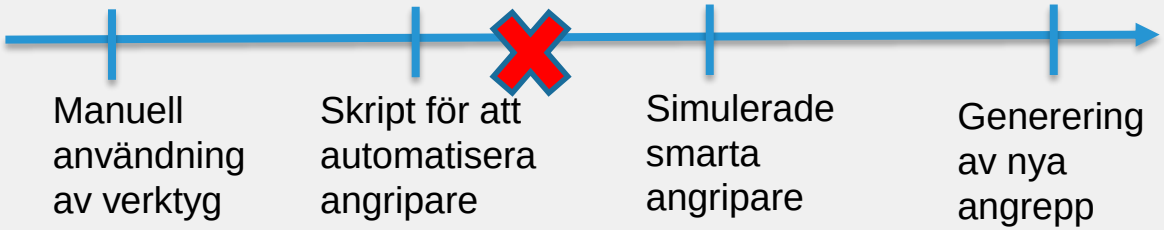
Verktyg för att skapa cybermiljöer
(t.ex. för realistiska tester och övningar på system/nätverksnivå)



Verktyg för att simulera användare
(t.ex. för test och övning av intrångsdetektion eller UND-tillämpningar)



Verktyg för att simulera angrepp
(t.ex. för sårbarhetstester och storskalig övning)



MSB Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

FOI

Pågående arbete

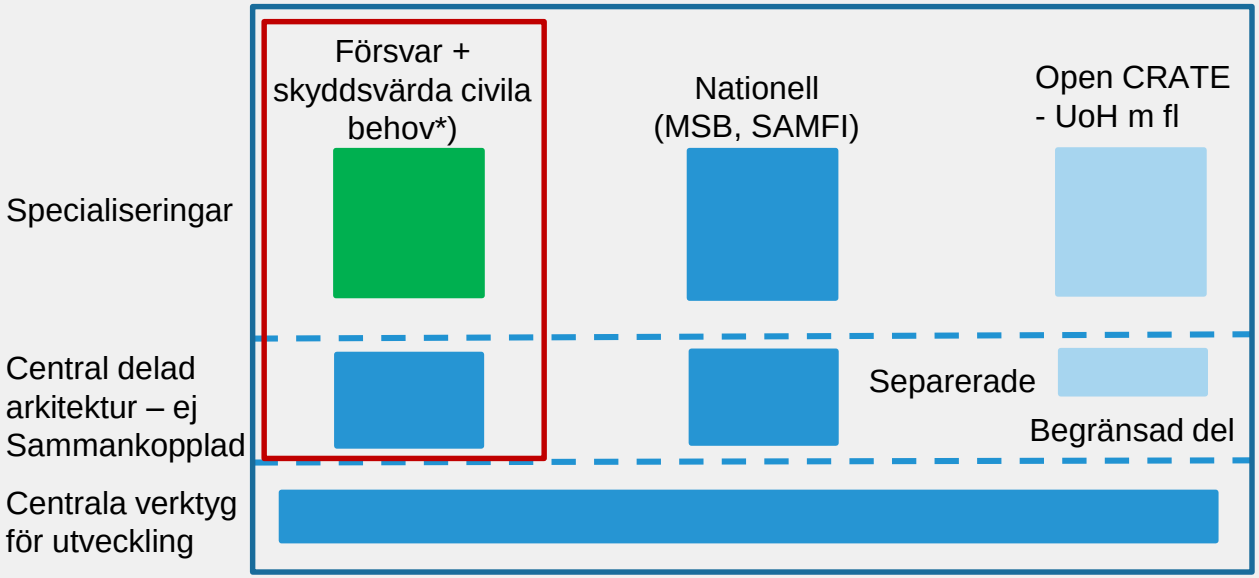
Pågående projekt:

- Förstudie: Metodik Nationell Cyber range
- Administration & styrning Nationell Cyber range; -> 2018
- Vidareutveckling CRATE 2.0 -> 2018

- Forskning inom NCS3
- Studier
- Samarbete Nationellt och internationellt

Nationell cyber range (CRATE 2.0)

- Myndighetsgemensam anläggning för forskningsbaserad kunskap
- Utbildning/träning inom incidenthantering
- Instanser och modulär



Pågående arbete

Samordnande & styrande aktörer i dagsläget:

- MSB
- Försvarsmakten
- FOI

Visionen om IoT och “The Networked Society”

Peter Stenumgaard
Enhetschef Informationssäkerhet & IT-arkitektur
Totalförsvarets forskningsinstitut

FOI

Introduktion

- IoT – “Sakernas internet”
  - Föremål som försetts med inbyggda elektroniska delar, såsom sensorer, datorer och internetuppkoppling, vilket gör att föremålen kan spara och utbyta data.

- Begreppet IoT myntades 1999 av Kevin Ashton, executive director Auto-ID Center.

- 5G ses idag som möjliggöraren för IoT i full skala

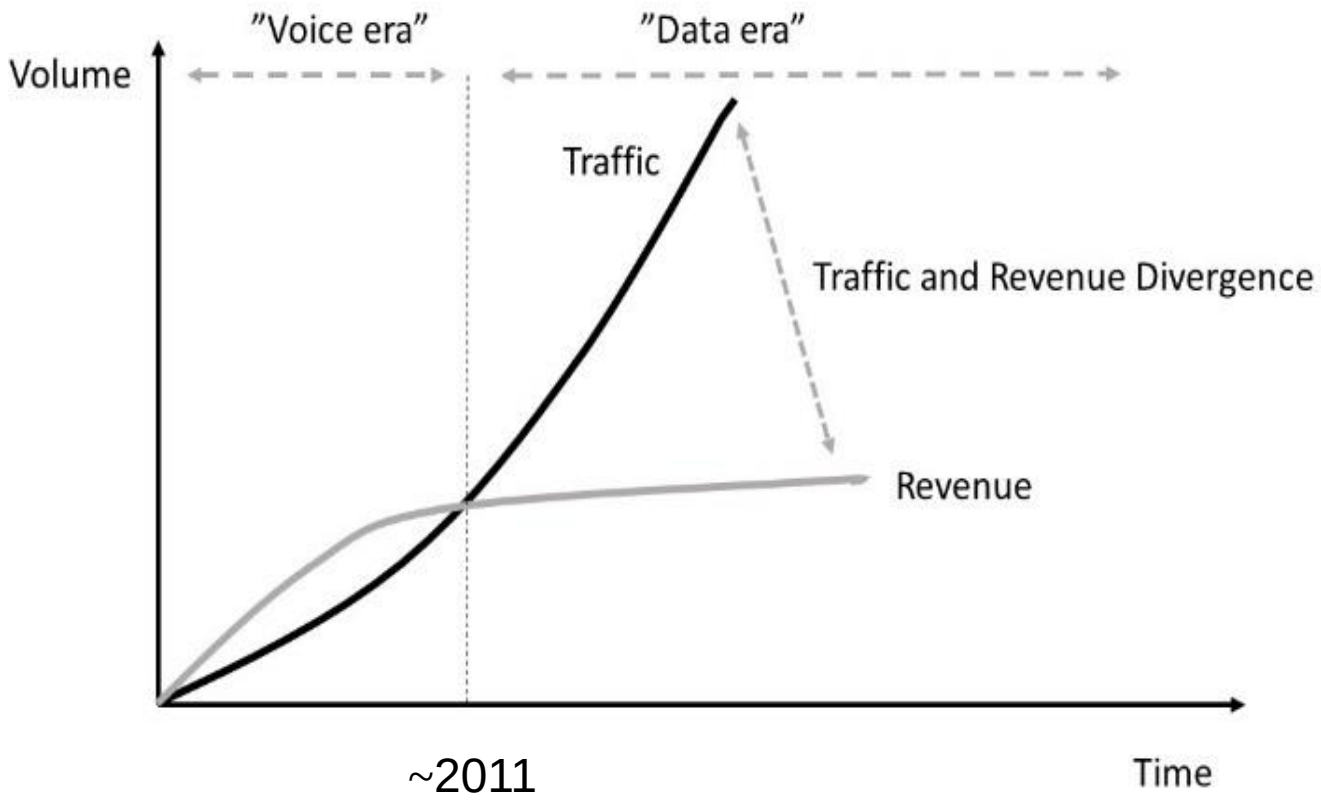
- IoT i full skala via 5G => “The Networked Society”

- “The Networked Society”
  - nytt globalt uppkopplat “ekosystem” för att “förändra världen” inom flera sektorer
  - molntjänster, “smarta” tjänster, delning av kommunikationskapacitet mm

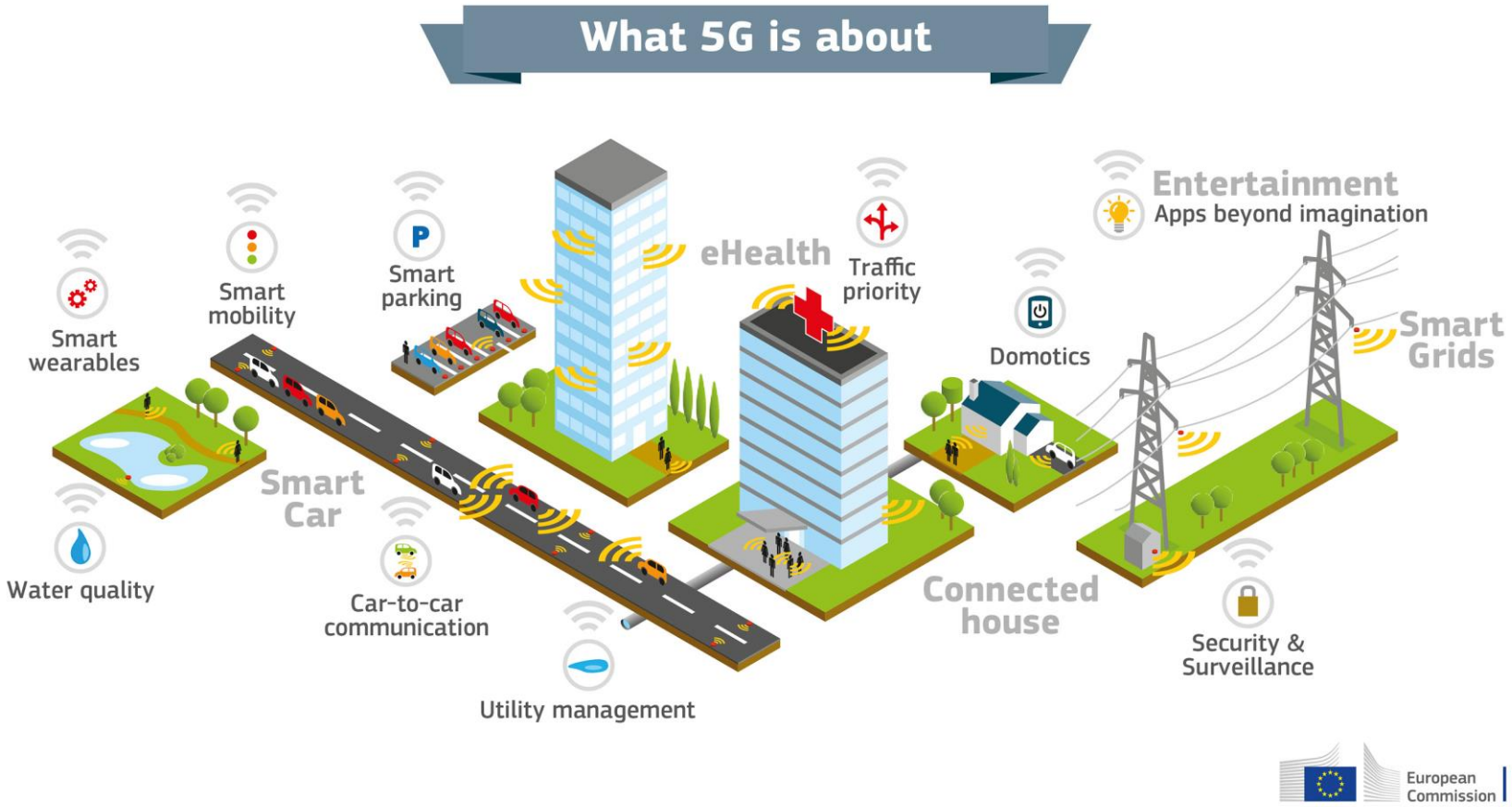
Bakgrund 5G

- Idag ungefär lika många mobilabonnemang som antalet människor på jorden
- Krav på högre datatakter för mobilt bredband kräver ständig uppgradering och ut byggnad av de trådlösa näten.
- Affärsmöjligheterna inom IoT bedöms som så stora att ingående aktörer talar om en ny “guldrusch” runt hörnet.
- För att visionen om IoT skall bli verklighet i full skala så krävs att den trådlösa delen i internetinfrastrukturen byggs ut väsentligt
- Den trådlösa andelen av global Internet-trafik är idag ca 50% och förväntas växa till runt 75% år 2020.

The ”revenue gap”

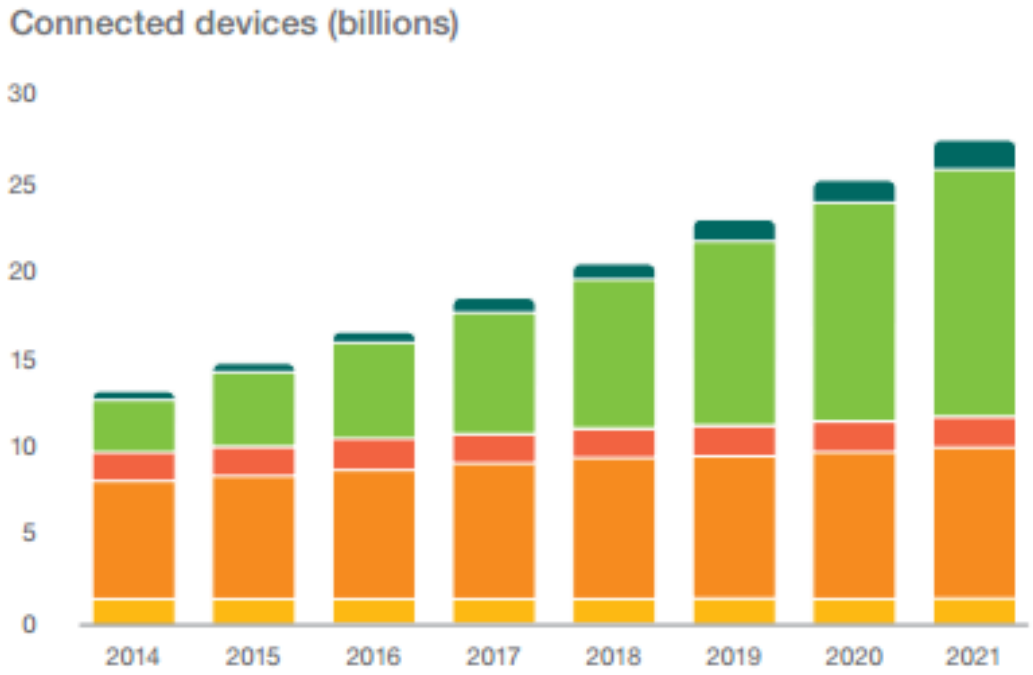


5G – the Networked Society



”Internet of everything”

Ex på prognos för antal uppkopplade enheter globalt*)



	15 billion	28 billion	CAGR 2015–2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	2015	2021	

*) Bild: *Ericsson Mobility Report, June 2016*

"Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated", Amy Nordrum, *IEEE Spectrum, 8 Aug 2016*

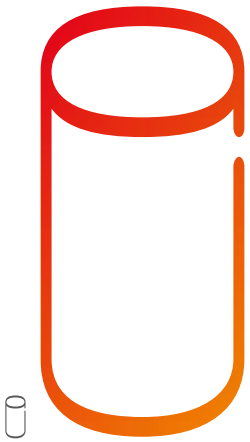
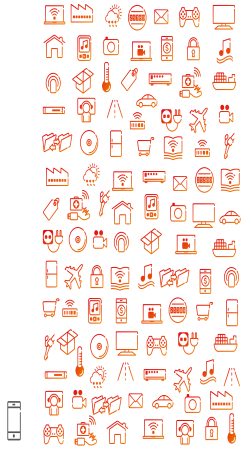
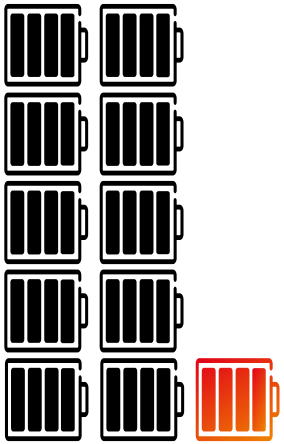
1000x data volume	50/500 B devices	Up to 10Gbps	Few ms E2E	10 years
				
1000x higher mobile data volumes	10-100x higher number of connected devices	10-100x typical end-user data rates	5x lower latency	10x longer battery life for low-power devices

Bild: METIS

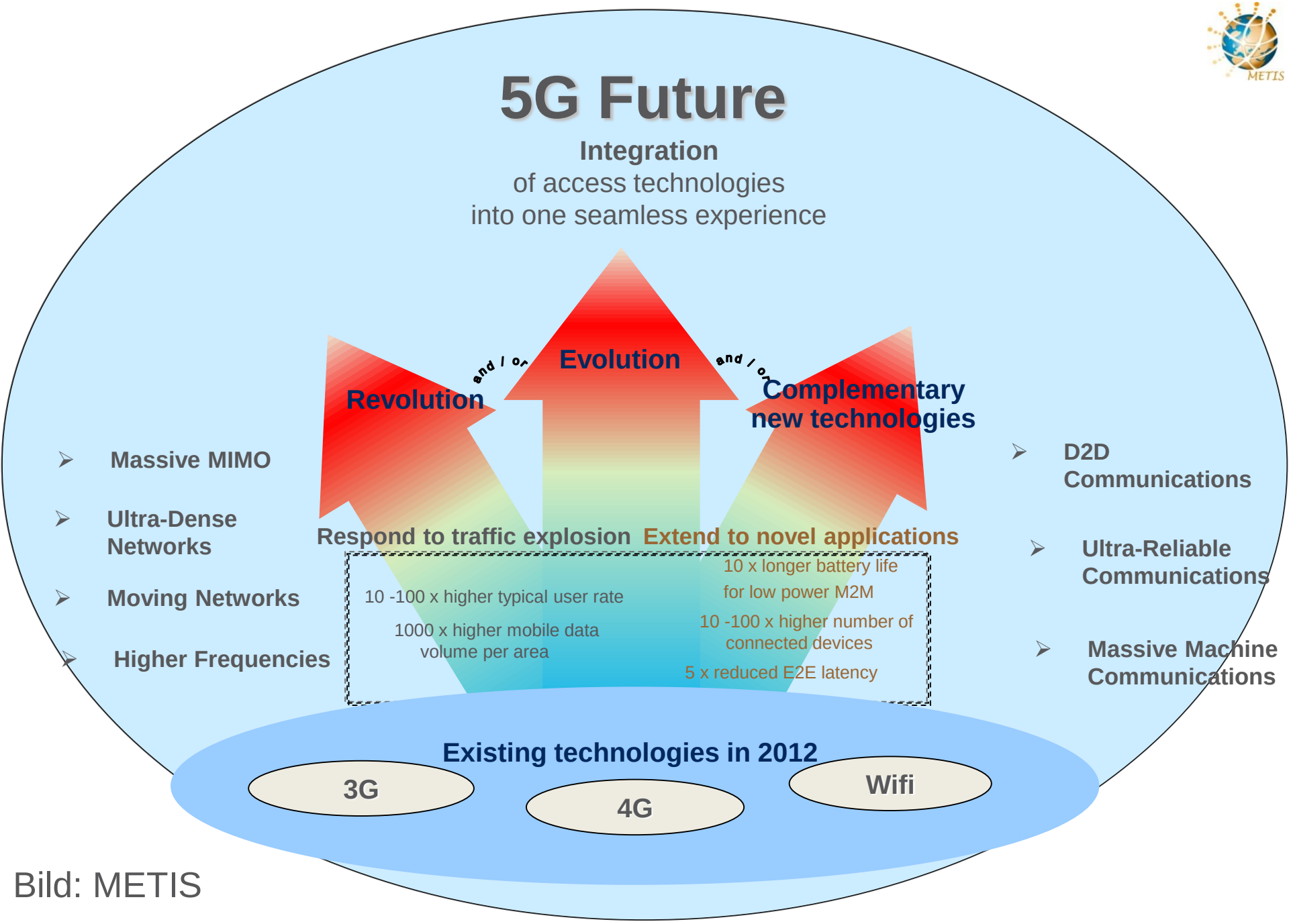

5G Future
Integration
of access technologies
into one seamless experience
Revolution
and / or
Evolution
and / or
Complementary
new technologies
Massive MIMO
Ultra-Dense Networks
Moving Networks
Higher Frequencies
D2D Communications
Ultra-Reliable Communications
Massive Machine Communications
Respond to traffic explosion
Extend to novel applications
10 -100 x higher typical user rate
1000 x higher mobile data volume per area
10 x longer battery life for low power M2M
10 -100 x higher number of connected devices
5 x reduced E2E latency
Existing technologies in 2012
3G
4G
Wifi

Bild: METIS

Konsekvenser för FM inom spektrumfrågor

- 5G-utvecklingen leder till krav på mer frekvensspektrum
  - Största 5G optimisterna:
    Utomhustäckning < 30 GHz
    Inomhustäckning < 90 GHz

- Konsekvens:
  - Tryck från civil telekom på att få tillgång till militära frekvensband

Ex på utmaningar för IoT

- IT-säkerhet
  - antal angreppspunkter mot system med låg IT-säkerhet ökar
  - trådlös teknik => möjligt med cyberattacker via luftgränssnittet

- Personlig integritet
  - massiv ökning av datamängder => risker för oönskad användning av data

- Trådlös teknik => ”Klassiska” radiostörningsaspekter – oavsiktlig/avsiktlig störning

HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack

HP News, July 29, 2014

Ökad trådlöshet ger nya angreppsytor

Bloomberg Business July 31, 2015
Hacked Jeep Cherokee Exposes Weak Underbelly of High-Tech Cars

Wired, 07.29.15
Hackers Can Disable a Sniper Rifle—Or Change Its Target

Drone Hacked By University Of Texas At Austin Research Group
The World Post 06/29/2012

Wi-Fi on planes opens door to in-flight hacking, warns US watchdog (The Guardian 2015-04-15)

FBI claims security researcher took control of plane (CNET 2015-05-17)

FOI

EX utnyttja ”IoT-enheter” till cyberangrepp

Cyber attack: hackers 'weaponised' everyday devices with malware to mount assault

Hundreds of thousands of devices such as webcams and DVRs were infected with malicious code to create a so-called ‘botnet’ to target leading sites

Sam Thielman and Elle Hunt
The Guardian, 22 Oct 2016

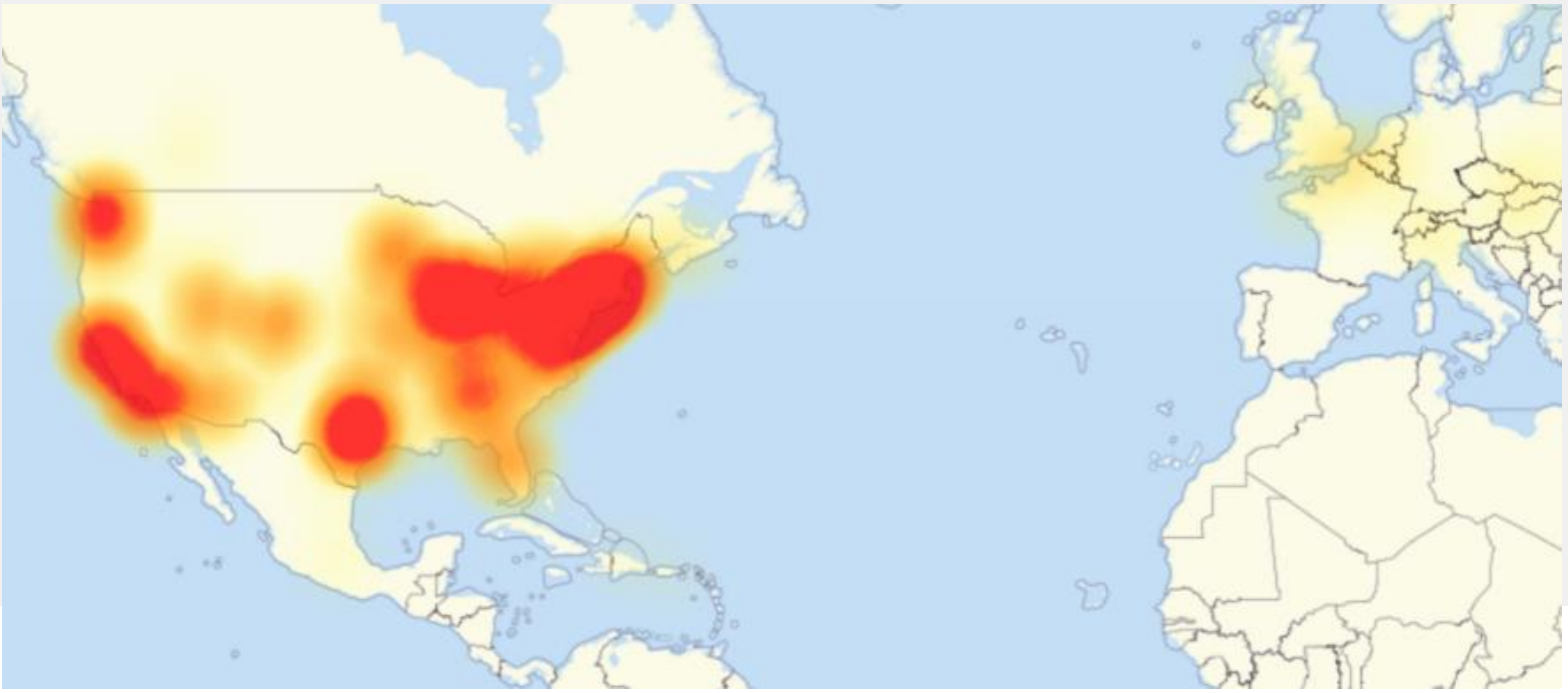


Bild: Wikipedia

Sammanfattning

- Visionen om IoT förväntas realiseras i full skala via en massiv ökning av trådlös teknik i form av 5G => The Networked Society
- Affärsmöjligheterna med IoT bedöms vara så stora att en ny ”guldrush” förutspås.
- Kombinationen av trådlös teknik och enheter med låg nivå på IT-säkerhet öppnar för sårbarheter som innebär stora utmaningar inom IT-säkerhet.
- Den massiva ökningen av data innebär stora utmaningar beträffande integritetsfrågor.

Cyberforensiska utmaningar och möjligheter

Cyberforensikens historia

Utmaningar

- Forensik
  - Våra ögon och öron
  - Djup kunskap om antagonist
  - Informationsövertag

Utmaningar

- Ökande datamängder
  - Big data vs large data
  - Större höstackar, lika många nålar
  - Trend mot att ALLT sparas

Utmaningar

- Molnabstraktion
  - Var finns data?
  - Vem äger data?
  - Vem manipulerar data?

Utmaningar

- Kritisk infrastruktur
  - Skydd ej i paritet med exponering
  - Hur göra forensisk undersökning?
  - Totalförsvarskritiskt!

Utmaningar

- Sakernas internet
  - ALLT ska vara uppkopplat
  - Intrångsskydd övergår till konsument
  - Hur göra forensisk undersökning?

Utmaningar

- Ökande antagonistkompetens
  - X as a Service
  - Ökad användning av krypto och skydd
  - Vi blir reaktiva

Utmaningar

- Vi ligger efter!
  - Ärendeinflödet högre än personalökning
  - Ej resurser till proaktivitet (FoU)
  - Isolerade kompetenskluster

Vad behöver göras?

- Ökad (svensk) kunskap och FoU
- FOI:s bidrag
  - Visa (forskning)
  - Instruera (kurser och rapporter)
  - Öva (CRATE)
- Vi behöver …

Nationellt cyberforensiskt forskningscentrum (NCF2C)

- Agera som totalförsvar!
- Koppla samman isolerade kompetenser
- FOI Linköping
  - Nära FM:s relevanta delar
  - Nära NFC
  - Nära UoH

Slut! Frågor?

Martin Karresand, FOI

martin.karresand@foi.se

013-378543 eller 013-378081