Hva er trusselen og hvordan påvirker den oss?

Niklas Vilhelm
Forsker
Nasjonal Sikkerhetsmyndighet
Niklas.vilhelm@nsm.stat.no

Litt om meg

- Forsker i Nasjonal Sikkerhetsmyndighet
- IT utdannelse ved UiO
- Bakgrunn fra Seismikkindustrien
- FoU – Rammeverk for deteksjon og håndtering av skadevare i industrielle kontrollsystemer/ SCADA
- Bidra med økt kunnskap

14 åring fjernstyrer trikken

2008: Lodz i Polen. Tenåring modifiserer fjernkontroll for TV og tar kontroll over sporvekslere via IR protokoll. Fire trikker sporer av og 12 mennesker skades.

Brukte trikken som leke.

Saltsjøbanan krasjer inn i bolig

- 15. Jan 2013. Passasjertog starter på mystisk vis med bare en vaskehjelp om bord.
- Kjører i 80 km/t, sporer av og krasjer inn i bolighus.
- 22-årig kvinnelig vaskehjelp skades alvorlig. Hun blir først mistenkt for å ha startet toget, men blir senere klarert.
- Antatt årsak oppgitt å være uheldige omstendigheter og brudd på sikkerhetsrutiner.

Om Hacking

Kontroll. Informasjonstyveri. Hærverk.

- Valg av mål og rekognosering.
- Angrep for tilgang
- Øke privilegier
- Grave seg inn
- Tyveri, sabotasje
- Skjule sine spor

Metoder

- Phishing
- Vannhulls-angrep
- 0-days
- Gjette passord
- Minnepinner
- Sosial manipulasjon

Hacking 'Made Easy'

- Shodan
- Metasploit
- Salg av sårbarheter
- Hackerangrep på bestilling
- Cyberkrim er en gigantindustri

Kritisk infrastruktur

- Kraftproduksjon og overføring
- Tele, data og satellitt
- Samferdsel
- Olje og gass
- Finans
- Helse
- Militær
- Høyteknologiske bedrifter

Jernbanen: en kritisk infrastruktur

Stor utbredelse, distribuert kontroll

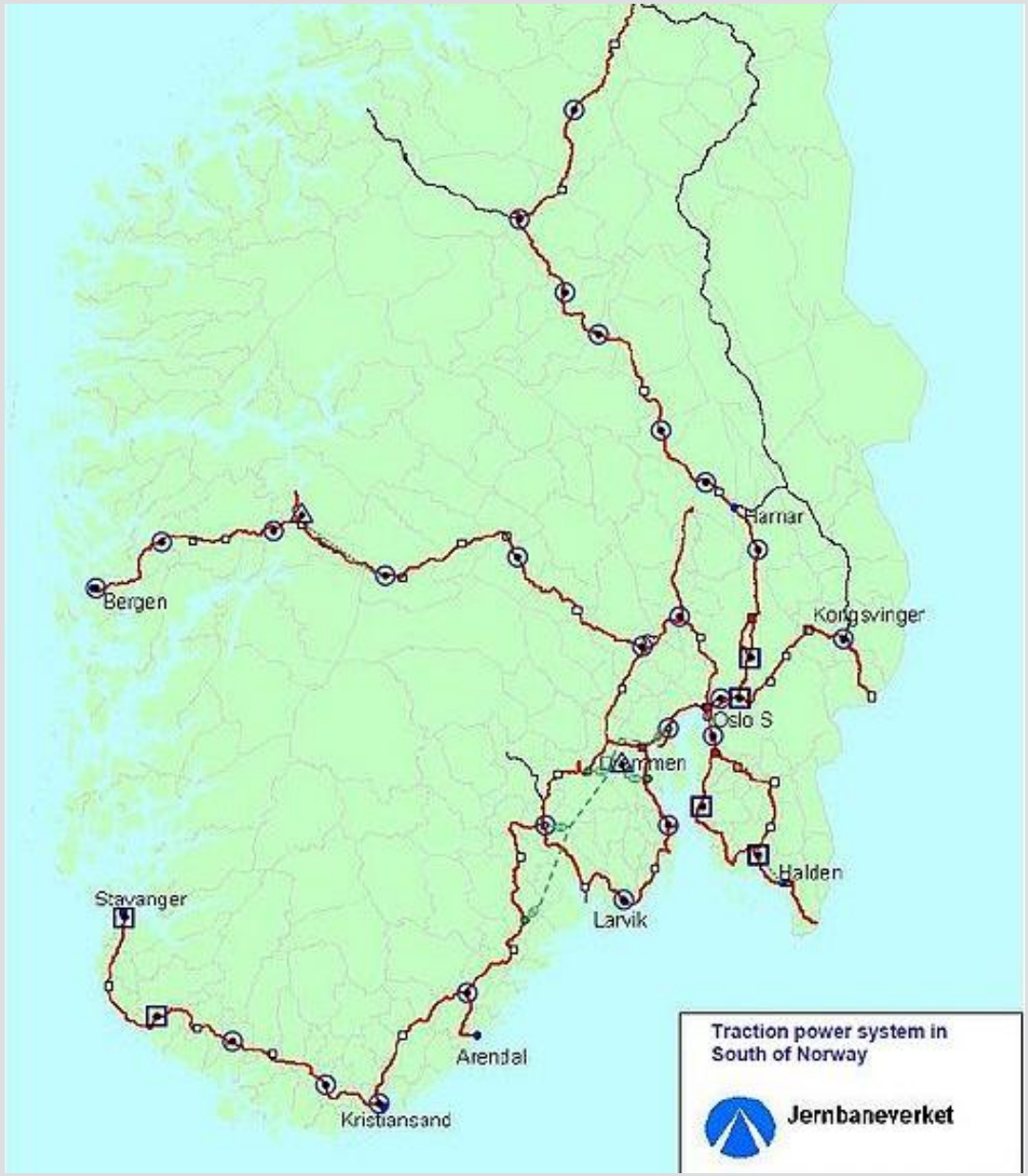
Vanskelig å sikre fysisk

Store konsekvenser ved bortfall

Tap av menneskeliv, farlig gods

Næringsliv kan rammes

Telecom



Valg av mål

- Cyberangrep er komplisert og ressurskrevende. Enklere med fysiske angrep.
- ’Lavt hengende frukt’.
- Hvordan ramme på systemnivå?
- Strategi

Test av cyberangrep på generator brukt i kraftforsyningen ved Idaho National Laboratory.

Fjernadgang. Resulterte i skader på generator.

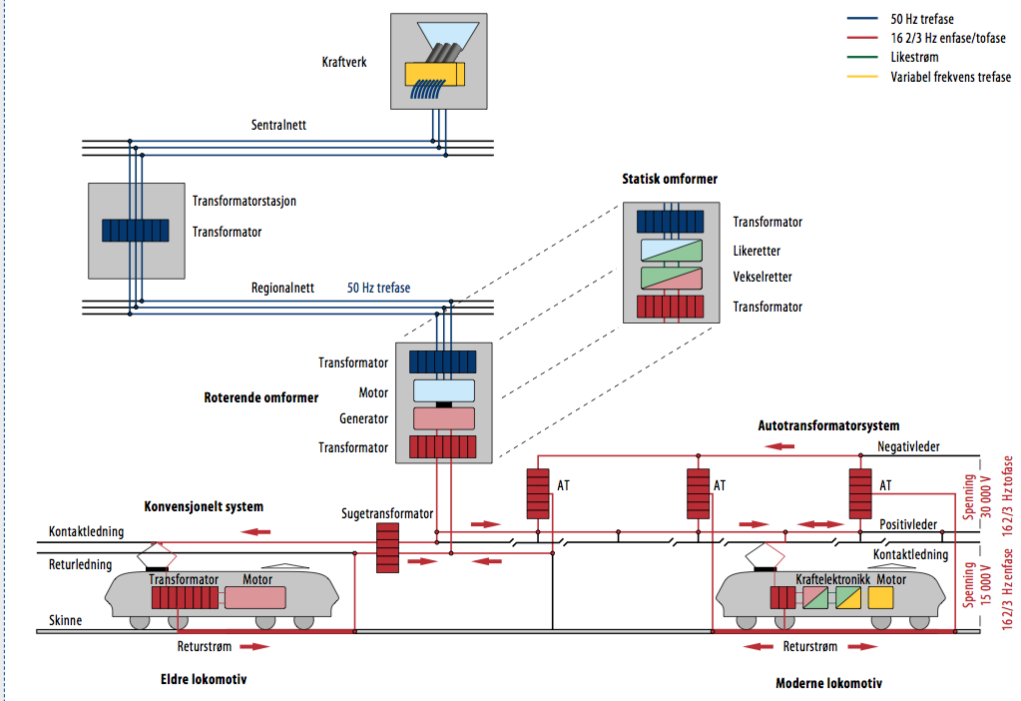
Strømforsyning

Matestasjoner og kontaktlednings-anlegg bruker mer avansert datautstyr

Fjernstyring fra elkraftsentraler

Fakta

Strømmens veg fra kraftverk til tog



Trafikkontroll

Fjernovervåkning av tog

Datastyrte lok

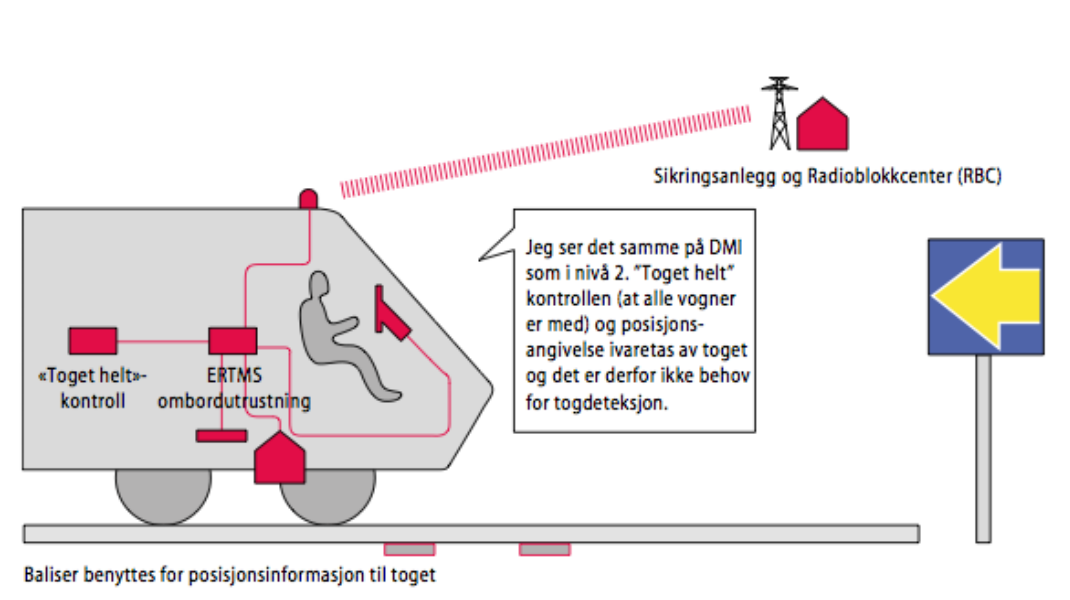
Blokkere nødbrems, øke hastighet?

Stasjonenes sikringsanlegg, fjernovervåkningssentral

Sporvekslere

Jamming, Spoofing av GSM-R

ERTMS 3



Narkosmuglere hacker havnen i Antwerpen

TRUSSELBILDET

- Økning i saker
- Spionasje mot norske interesser og næringsliv
- Avansert skadevare:

  Skade infrastruktur

  Samfunnsaktivitet

  Beslutningsprosesser

AKTØRENE

Statlige etterretnings- og sikkerhetstjenester

Militære motstandere

Globale næringsbedrifter

Terroristgrupper

Ekstremistgrupper

Organiserte hackergrupper

Enkeltpersoner

CIA virus sprenger gassledning

- Rørledning fra Sibir for å overføre 40 milliarder kubikkmeter gass til Europa
- Sovjetisk plan for å stjele teknologi fra Canadisk selskap
- CIA plantet virus i styringssystem for gassledning
- Pumper, Ventiler og turbiner slo seg av og på tilfeldig og økte trykket i rørledningen.
- ”Den største ikke-nukleære eksplosjon noensinne sett fra rommet”

Cyberkrig

- 2007. Massivt cyberangrep på Estland
- 2008. Krig i Sør-Ossetia
- 2010. Stuxnet rammer Natanz i Iran
- 2010. Pakistan og India
- 2013. Syria

- USA, Russland, Kina, Frankrike, UK, Israel, Iran, India, Nord-Korea.

Strategier for sikkerhet

- Luft-Skille
- DMZ, segmentert arkitektur
- IDS, network forensics
- Whitelisting
- Honey Pot. Trend Micro – Kyle Wilhoit
- Rutiner for å håndtere angrep

NorCert

- Gjennom forebyggende sikkerhetstiltak skal NorCERT redusere samfunnets sårbarhet
- Rask og riktig hendelseshåndtering (koordinering, respons og analyse)
- Innhente og dele informasjon
- Bistå beredskapsarbeid og hjelpe frem responsmiljøer
- Ha et oppdatert IKT-risikobilde

Oppsummert

- Flere og mer avanserte aktører
- Jernbane mulig mål for cyberangrep
- Trengs bedre overvåkning av nettverk
- Utvikle strategier basert på at angrep vil lykkes

- Spørsmål?