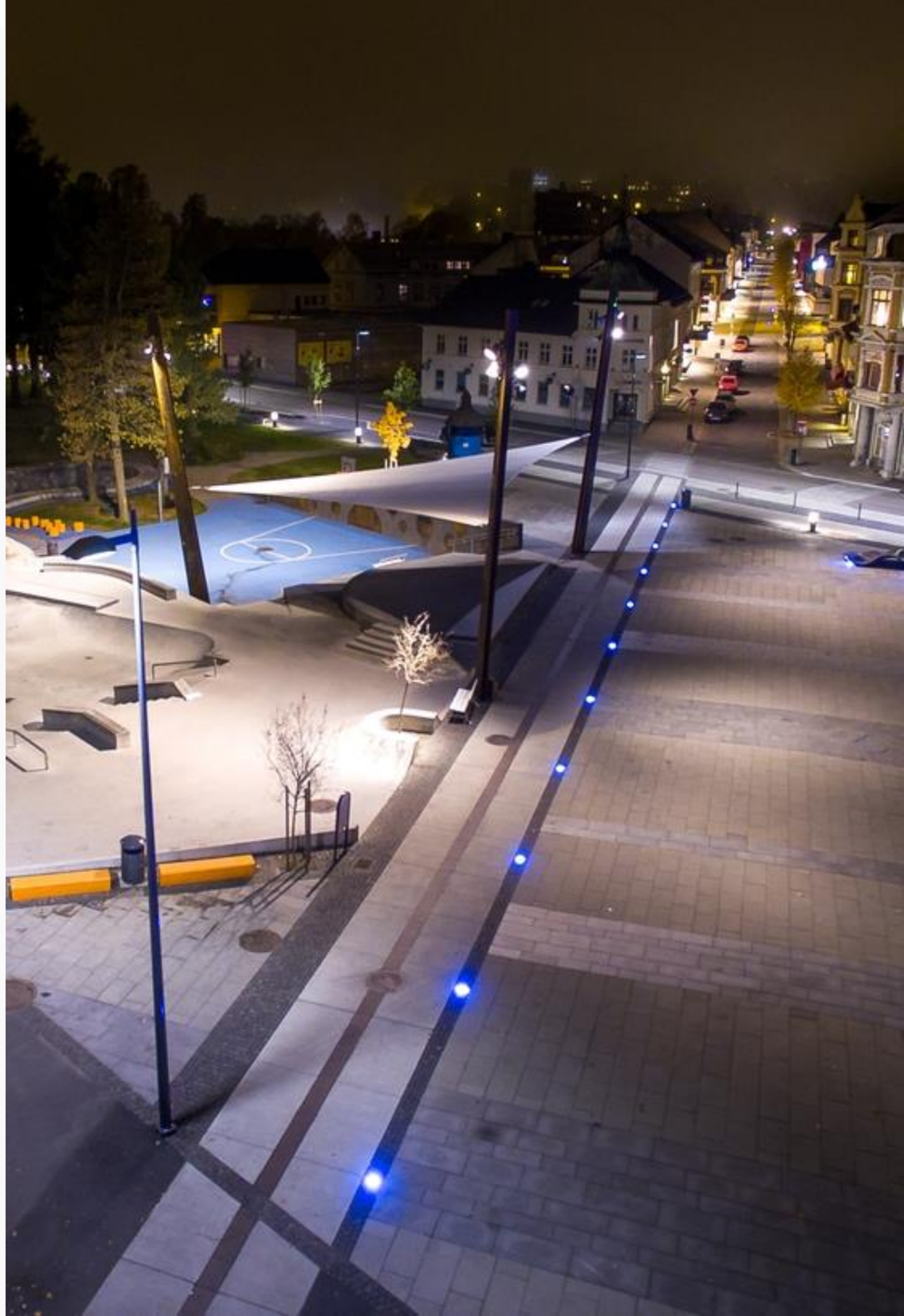
Hvordan kan kommuner øve på cyberangrep

Webinar for alle som jobber med IKT eller informasjonssikkerhet i kommunal sektor

31. mai 2024

Agenda

- Velkommen v/Digi Innlandet
- Hvorfor øve på cyberangrep? v/ prosjektleder Grethe Østby
- Organisering og gjennomføring av øvelsene v/ prosjektleder Grethe Østby
- Hva gikk bra og hva var vanskelig i prosjektet? v/programleder Pål Godard
- Hva lærte IKT-avdelingene av øvelsen? v/ IKT-ansvarlige i Gjøvik, Nordre Land, Søndre Land og Vestre Toten
- Presentasjon av maler og sjekklister for andre kommuner eller IKT-samarbeid, som ønsker å gjennomføre slike øvelser v/ prosjektleder Grethe Østby
- Tid til spørsmål og svar



Hvorfor øve på cyberangrep?

Grethe Østby

Rådgiver og prosjektleder for Styrmand AS https://www.styrmand.no/

Førsteamanuensis 2 ved Cyberingeniørskolen/Forsvarets høyskole

https://www.forsvaret.no/utdanning/utdanninger/ingeniorfag-studieretning-telematikk

Avsluttende fase/mindre oppgaver (frem til 1. mai 2025) som førsteamanuensis ved Institutt for Informasjonssikkerhet og kommunikasjons-teknologi på NTNU

https://www.ntnu.no/ansatte/grethe.ostby

Hvorfor øve på cyber-angrep?

-> Er det noe annerledes enn andre hendelser?

Kommuner i Norge i dag

Norske kommuner opererer i et stadig tøffere digitalt klima.

Den sikkerhetspolitiske situasjonen i Europa er i endring.

Cyberangrep har blitt hverdagskost også i Norge.

Ifølge Nasjonal Sikkerhetsmyndighet (NSM) sitt nasjonale digitale risikobilde 2022, er norske kommuner blant de som er spesielt utsatt for ulike typer cyberangrep.

Dette skjer samtidig som at norske kommunedirektører er mer bekymret for Informasjonsteknologi (IT)-sikkerhet i egne kommuner enn tidligere.

De siste årene har gitt oss mange eksempler på cyberangrep mot norske kommuner; Østre Toten kommune, Hedmark IKT, Nordland fylkeskommune, Drammen kommune og Skien kommune

https://nsm.no/getfile.php/1311995-1664550278/NSM/Filer/Dokumenter/Rapporter/NDIG%202022.pdf

https://www.kommunal-rapport.no/beredskap/toppledere-mer-bekymret-for-it-sikkerhet-enn-for/146621!/

https://www.nrk.no/nordland/dataangrep-rammer-nordland-fylkeskommune-1.15789412

https://www.kommunal-rapport.no/beredskap/russiske-hackere-angrep-vannsystemet-i-drammen/144235!/

https://www.nrk.no/innlandet/10.000-kommuneansatte-rammet-av-dataangrep-1.15143964

https://www.digi.no/artikler/skien-kommune-utsatt-for-stort-dataangrep/507274

Evner til å håndtere cyber-angrep – fra forskning

Evner til å håndtere cyber-angrep i offentlige beredskapsorganisasjoner blir av Riksrevisjonen blant annet beskrevet som ‘sterkt kritikkverdig’

Respons-kapabiliteter er ukjente

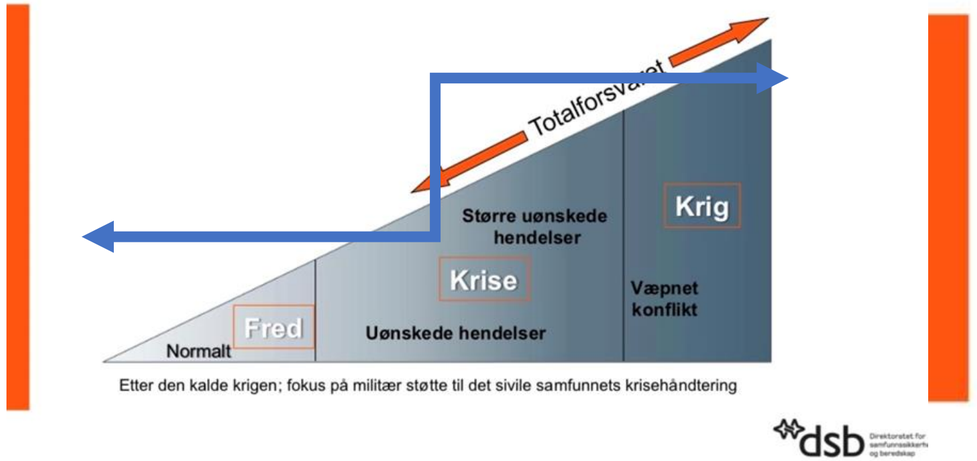
Personell med nødvendig informasjonssikkerhetskompetanse er mangelfull, og mangelen har økt i takt med utfordringene

Etter cyberangrepet mot Østre Toten fant man i tillegg til at ‘respons-kapabiliter’ er ukjente, og også at

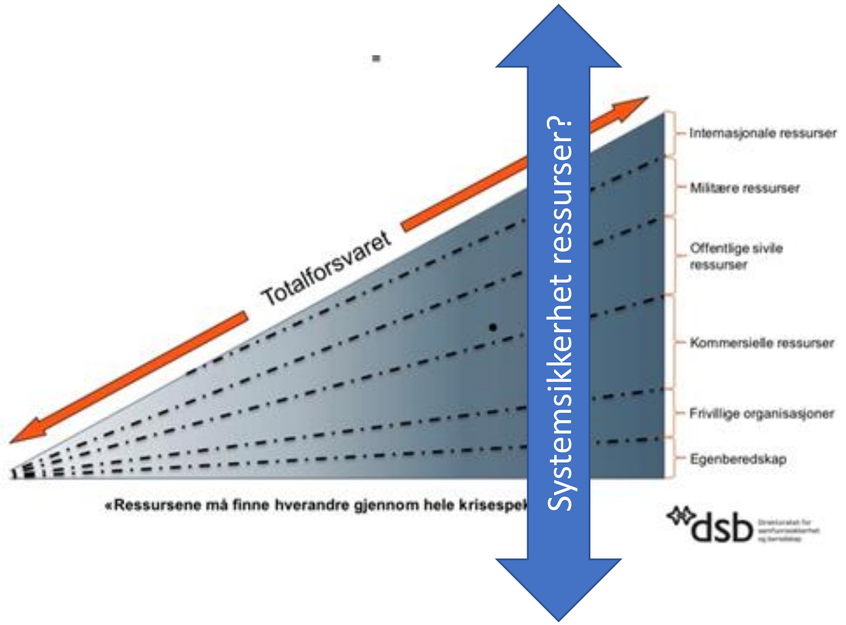
-> Kriseledelses-grupper og team trenger forståelse for og trening for å håndtere denne type hendelser

https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3062985

Krise nivå – hvem er involvert?

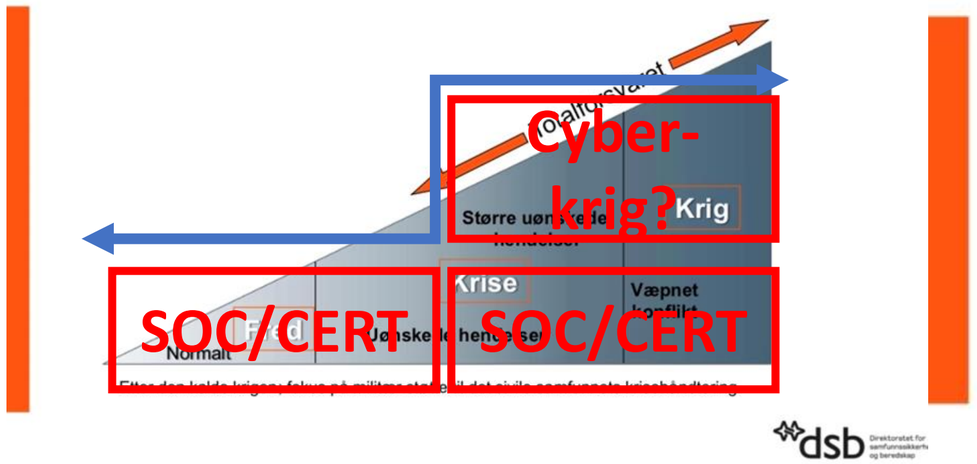


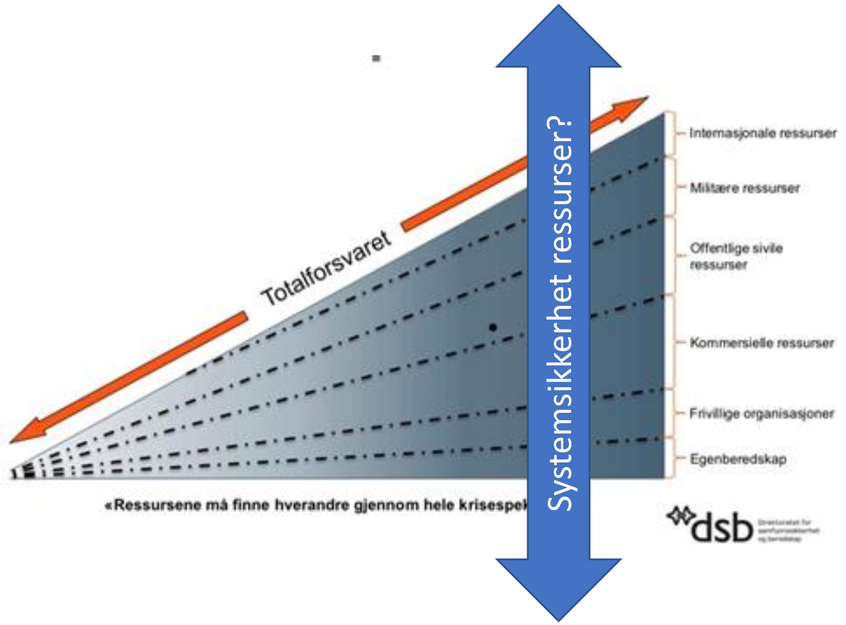
Etter den kalde krigen; fokus på militær støtte til det sivile samfunnets krisehåndtering



«Ressursene må finne hverandre gjennom hele krisespek

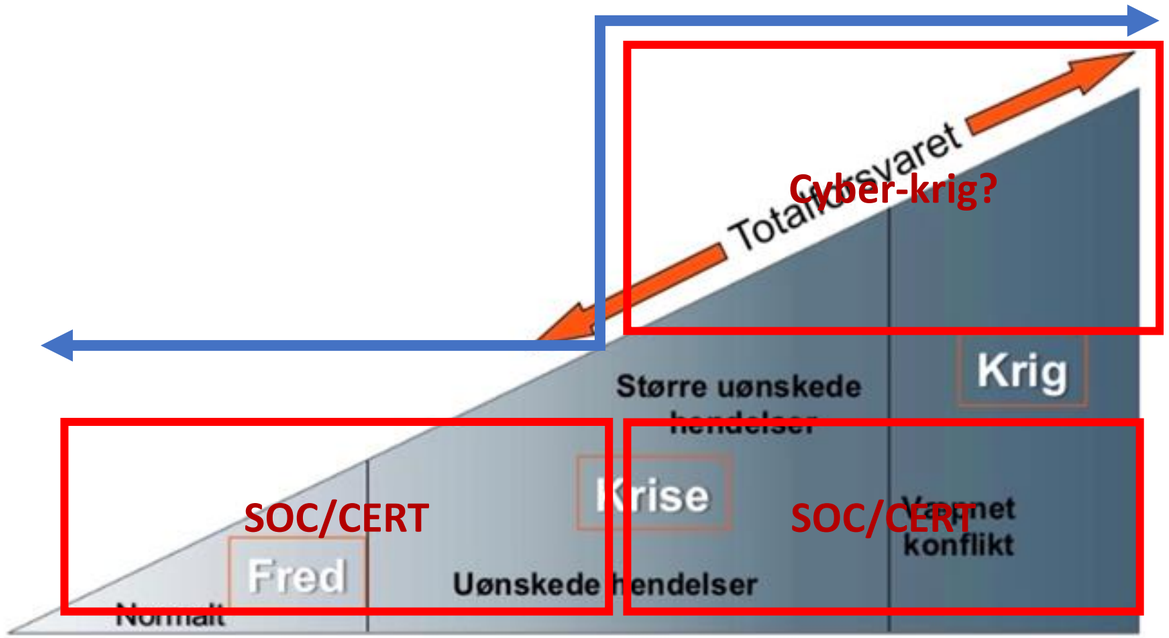
Krise nivå – hvem er involvert?



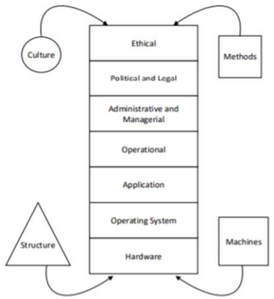


[Rammeverk for håndtering av IKT-sikkerhetshendelser]

Kriseledelse



Etter den kalde krigen; fokus på militær støtte til det sivile samfunnets krisehåndtering



dsb Direktoratet for samfunnssikkerhet og beredskap

Henleggelser av anmeldelser av cyber-angrep

PST: Henlegger dataangrep-saken mot depart-ementene

PST har gjennomført en omfattende etterforskning etter dataangrepet som ble avdekket i juli år. Tolv departement ble rammet. Nå henlegges saken.

Martin Gundersen
Journalist

Silje Haugen Myrseth
Journalist

Publisert 20. okt. 2023 kl. 13:24
Oppdatert 20. okt. 2023 kl. 16:30

Litt mer enn som så?

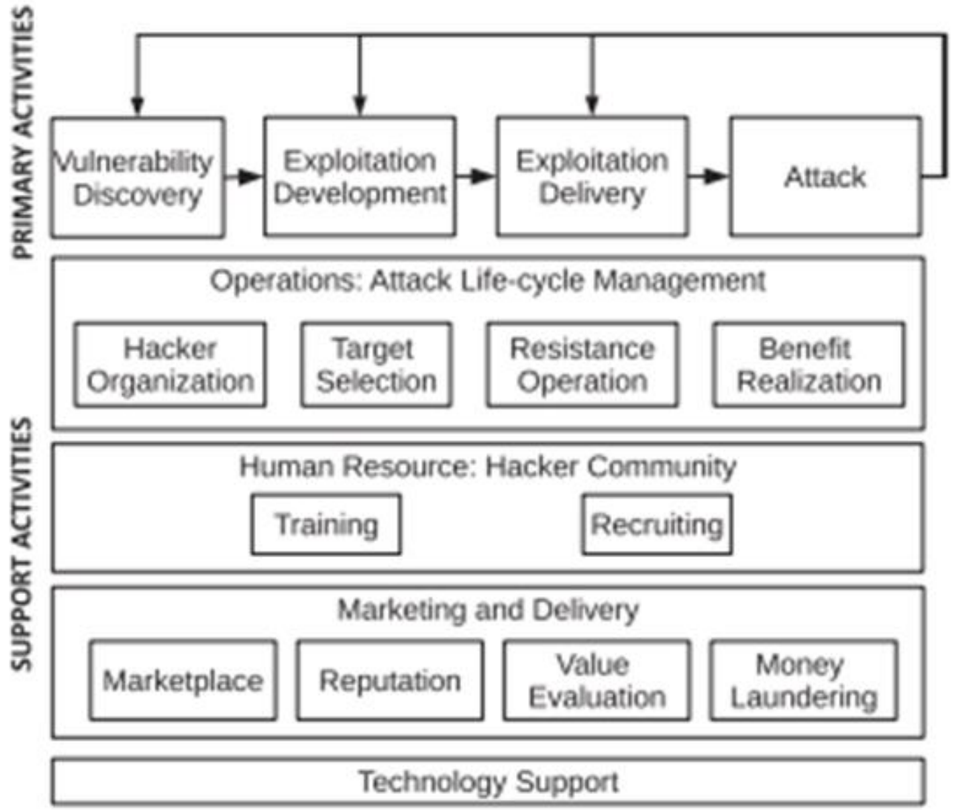


Fig. 1. Cybercriminal Value Chain Model.

https://dl.acm.org/doi/pdf/10.1145/3199674

Table 1. Status and Typical Pricing of Cybercrime Services

Service	Status	Pricing Model	Example Case	Estimated Price
EaaS	Existing	License	Exploit Trading [71]	up to more than $250,000
		Subscription	Up-to-date Zero-day Exploits [151]	$150,000 per month
PLaaS	Existing	Pay-per-install Commission	Payload Renting [10, 16]	$0.02–0.10 per install 40%
DaaS	Existing	Subscription	Phishing Service [145]	$85–$115 per month 40%
		Commission	Fake Anti-virus [97]	
OBaaS	Existing	Subscription	Obfuscation Platform [50]	$50–150 per month
SCaaS	Existing	Subscription	Scan4you [72]	$25 per month
TRaaS	Existing	Pay-per-click	Traffic Redirection [50]	$7–$15 per 1,000 visitors
BNaaS	Existing	Subscription	Botnet Shops [145]	$40 per month
BHaaS	Existing	Subscription	Cloud Bulletproof Servers [100]	$300 per month
TAaaS	Existing	Subscription	DDoS Attack Service [134]	$999 per month
REaaS	Existing	Pay-per-record	Reputation Escalation Markets [170]	$0.4–0.7 per record
MPaaS	Existing	License	Market Framework [35]	$4,500 per licence
		Commission	Marketplace [34]	2%–10%
MRaaS	Existing	License	Money Laundering Recruitment Package [99]	$1,700 per licence
MLaaS	Existing	Commission	Money Laundering Service [127]	2%–30%
HTaaS	Existing	License	Hacker Training Courses [138]	$250–$800 per person
PPaaS	Evolving	License	Personal Profile Investigator [59]	$4–$20 per record
TPaaS	Evolving	Subscription	"One-stop-shop" Platform [2, 73]	$4,000 per month
RaaS	Evolving	Subscription	Smart Contract [79]	/
HRaaS	Evolving	Subscription	Online Hacker Recruiting Market [105]	/
VDaaS	Emerging	Subscription	Bug Bounty Program [132]	$542.04–$1810.31 per vulnerability
TSaaS	Emerging	Subscription	Targets Ranking based on Value [101]	/
EPaaS,RPaaS	Emerging	Subscription	Repackaging Platform [143, 151]	$4,000 per month
DMaaS	Emerging	Subscription	"How-to" Knowledge Systems [27]	/
VEaaS	Emerging	Subscription	Comparison "Shopping" Service [57]	/

Services are defined and explained in the following sections. Examples for existing services are actual, emerging, and evolving services are based on offensive versions of actual legitimate services. Prices listed here are intended to be representative of current prices and are constantly evolving.

Statistikk og økonomi dark-web/deep-web

Ta en titt på trafikkmønstrene på The Onion Router (TOR):

TOR...

- Ca. 3 millioner aktive brukere daglig.
- Hadde ca. 1,5 millioner daglige aktive brukere i januar 2020
- Vert for anslagsvis 30 000 – dark-web-nettsteder

Det mørke nettet er satt til å være en betydelig bidragsyter til økningen i globale løsepengevirus-kostnadene, som er spådd å overstige 265 milliarder dollar årlig innen 2031

https://www.idagent.com/blog/the-thriving-dark-web-economy-is-bad-news-for-businesses/#:~:text=For%20a%20layman%2C%20it%20is,they%20were%20on%20the%20mark.

Blir det mulig å informere?

https://www.kommunal-rapport.no/nyheter/ble-hacket-av-russere-styrte-kommunen-via-snapchat/145874!/

Kommunedirektør Ole Magnus Stensrud og Østre Toten kommune har lært på den harde måten. Datainnbruddet de ble utsatt for i fjor hadde store konsekvenser.

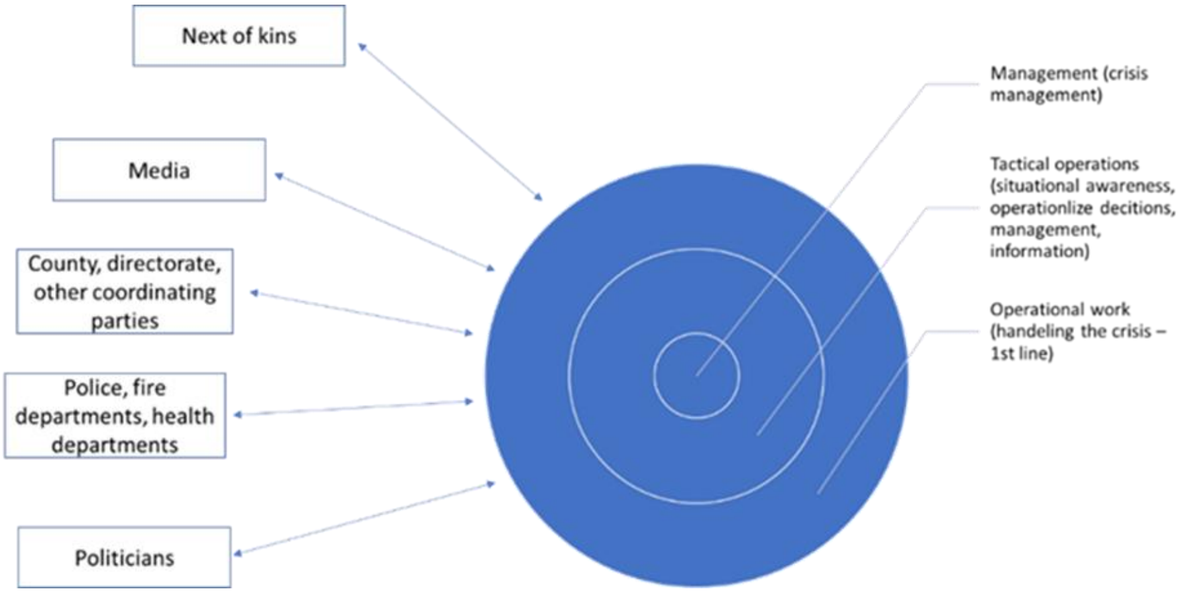
Foto: Nina Hansen/Dagbladet

› PUBLISERT 28.09.2022 09:51

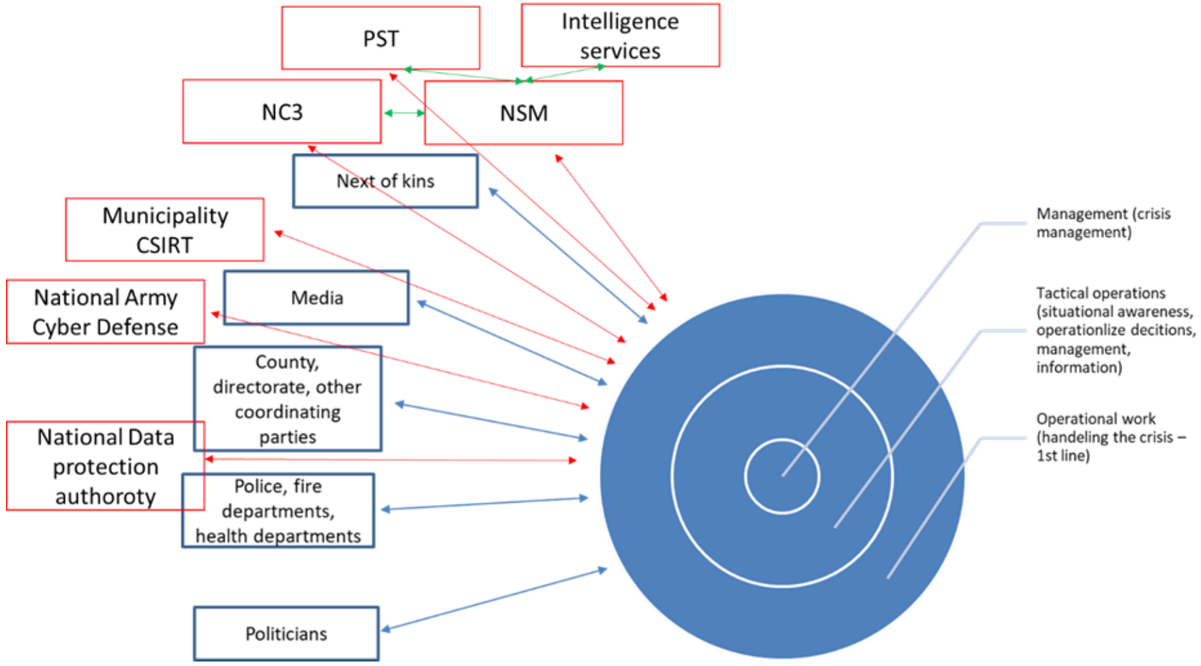
Ble hacket av russere: Styrte kommunen via Snapchat

Hva gjør du hvis hackere stenger ned hele

Informasjonslag kommunikasjon



Normal krisesituasjon



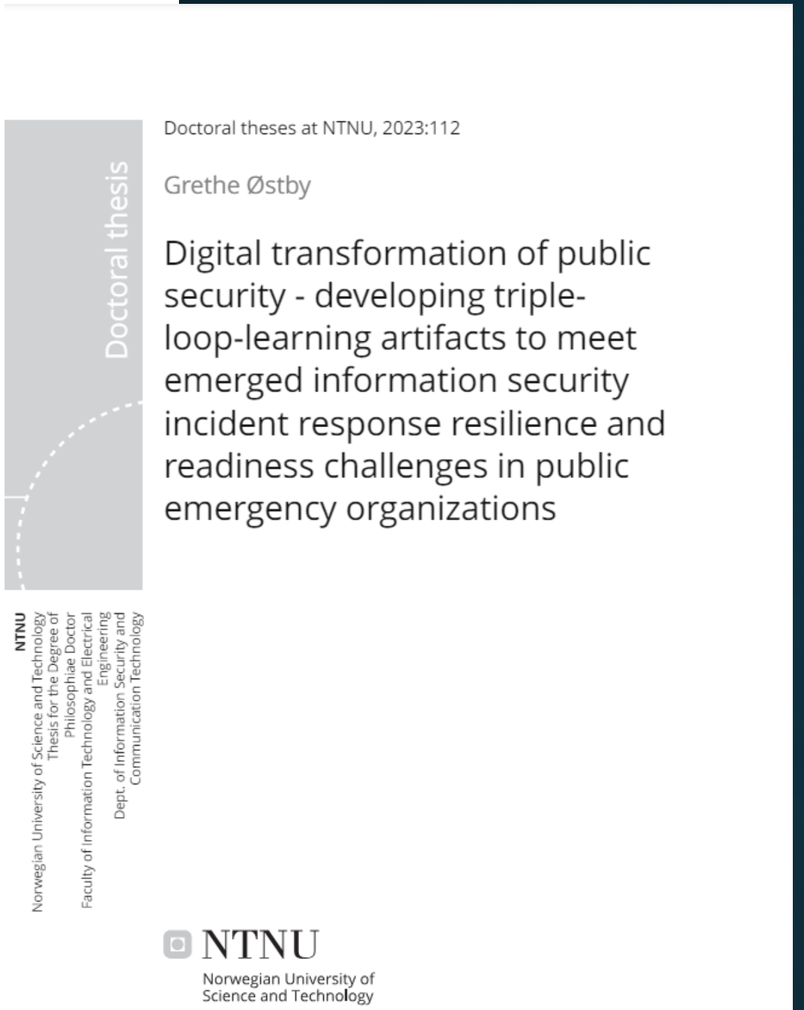
Østre Toten

https://www.ototen.no/aktuelt/rapport-etter-dataangrepet.15279.aspx

Organisering og gjennomføring av øvelsene

Øvelser for bedre informasjonssikkerhetsledelse

https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3062985



Fra forskningen (Østby, 2023)

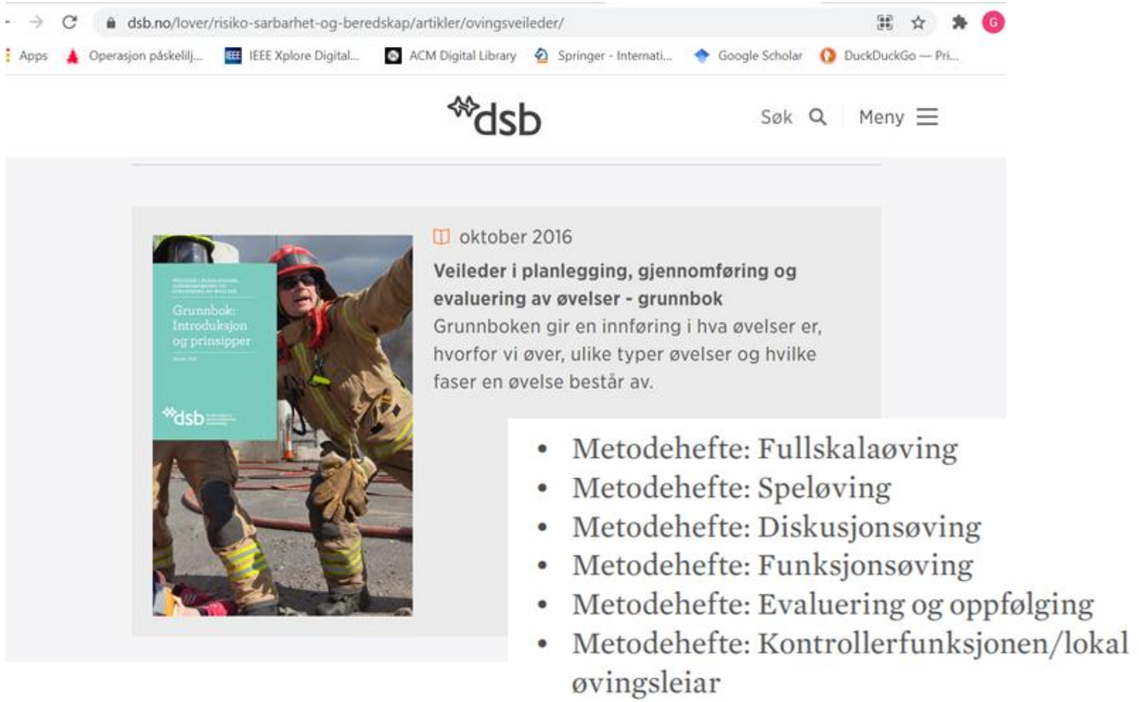
«De viktigste funnene fra forskningsarbeidet er **at forberedelse til øvelser** og hvordan **bygge spillstab-team** for fullskala informasjons- og cybersikkerhetsøvelser er **nytt i forsknings miljøet**, og også **nytt i forhold til samfunnsopplæring for beredskap og motstandsevne ved et cyberangrep**.

Forskningen tilsier også at 1) trippel-loop-learning og 2) utvikling av seriøse spill for informasjons- og cybersikkerhetshendelser, er både relevante og nye tilnærminger til ledelsesøvelser for informasjonssikkerhet. Finjusterte **koordinerte læringsaktiviteter for å møte tidslinjen til et scenario**, og **triple-looplæringsaktiviteter til bruk i øvelsene** er av stor betydning, og en brukersentrisk tilnærming er viktig for å kunne gjennomføre aktivitetene på riktig nivå i organisasjonen og for å tette gap ett trinn av gangen.

Et siste viktig funn er at sosiotekniske læringsaktiviteter har vist at 1) **målrettede treningsmål utviklet i scenarioene oppfylles under øvelsene**, 2) **sosiotekniske trinnvise forbedringer kan utvikles basert på nivået på eskaleringsmodenhet**, og 3) **organisasjoner kan lære fra trening og øvelser**.» (Østby, 2023)

https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3062985

Veiledere for å gjennomføre øvelser



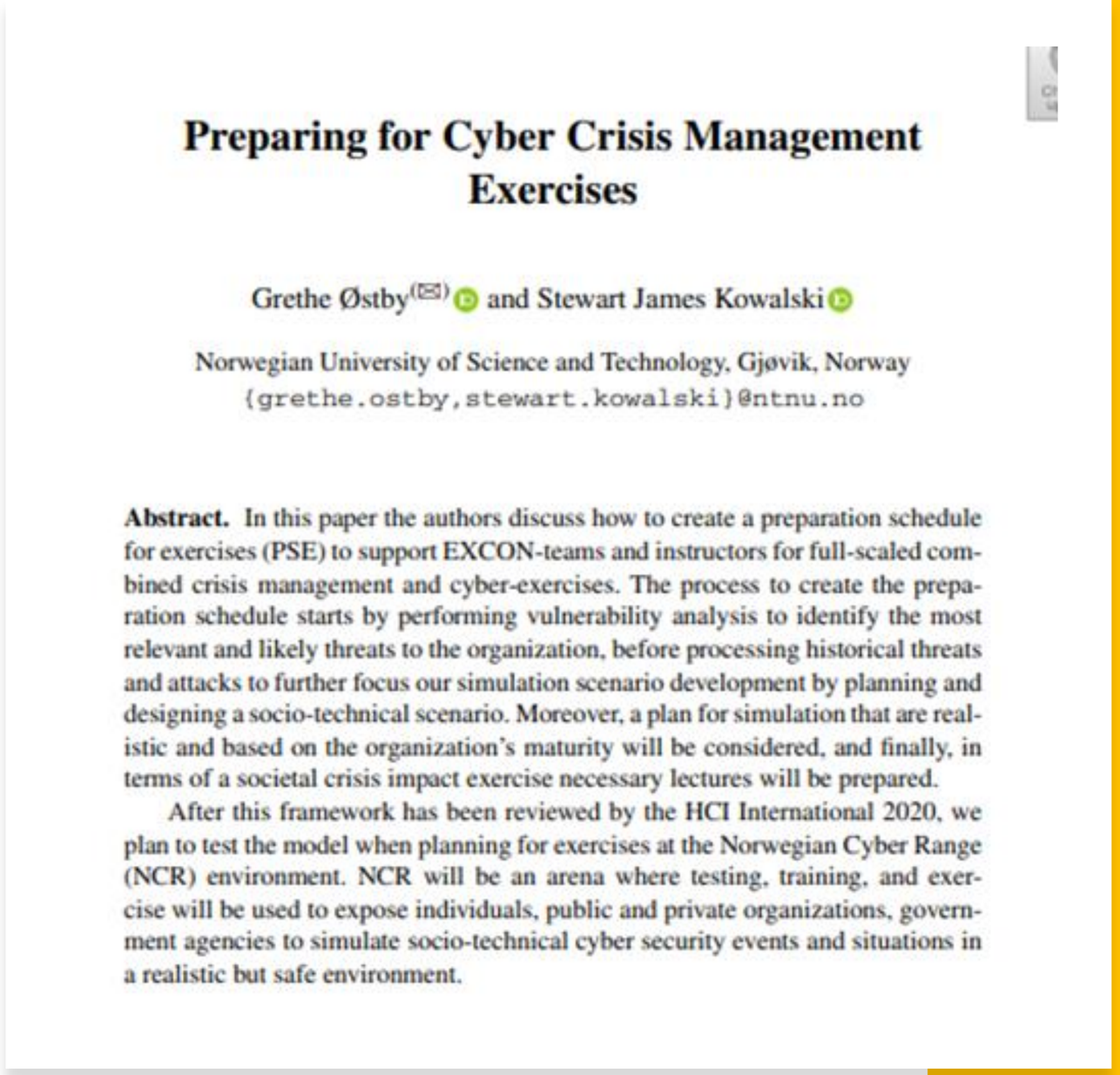
- https://www.dsb.no/lover/risiko-sarbarhet-og-beredskap/artikler/ovingsveileder/

https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

Forberedelser til øvelser

Forberedelser til informasjonssikkerhetsledelses-øvelser

- sårbarhetsanalyser for å identifisere de mest relevante og sannsynlige truslene mot organisasjonen, både fra et overordnet perspektiv og de som er spesifikke for organisasjonen,
- samarbeide med cybersikkerhetsteamene for å forstå historiske trusler og angrep for å tilpasse relevante scenarioer,
- planlegge og designe et sosioteknisk scenario for øvelsen,
- planlegge for simulering som er realistisk og basert på organisasjonens modenhet,
- og til slutt, i form av en krisehåndteringsøvelse; se på organisasjonens ansvar (lover og forskrifter), krisehåndteringsroller og -ansvar, og foreslåtte beredskapsplaner (inklusive kontinuitetsplaner), for å forberede forelesninger



Preparing for Cyber Crisis Management Exercises

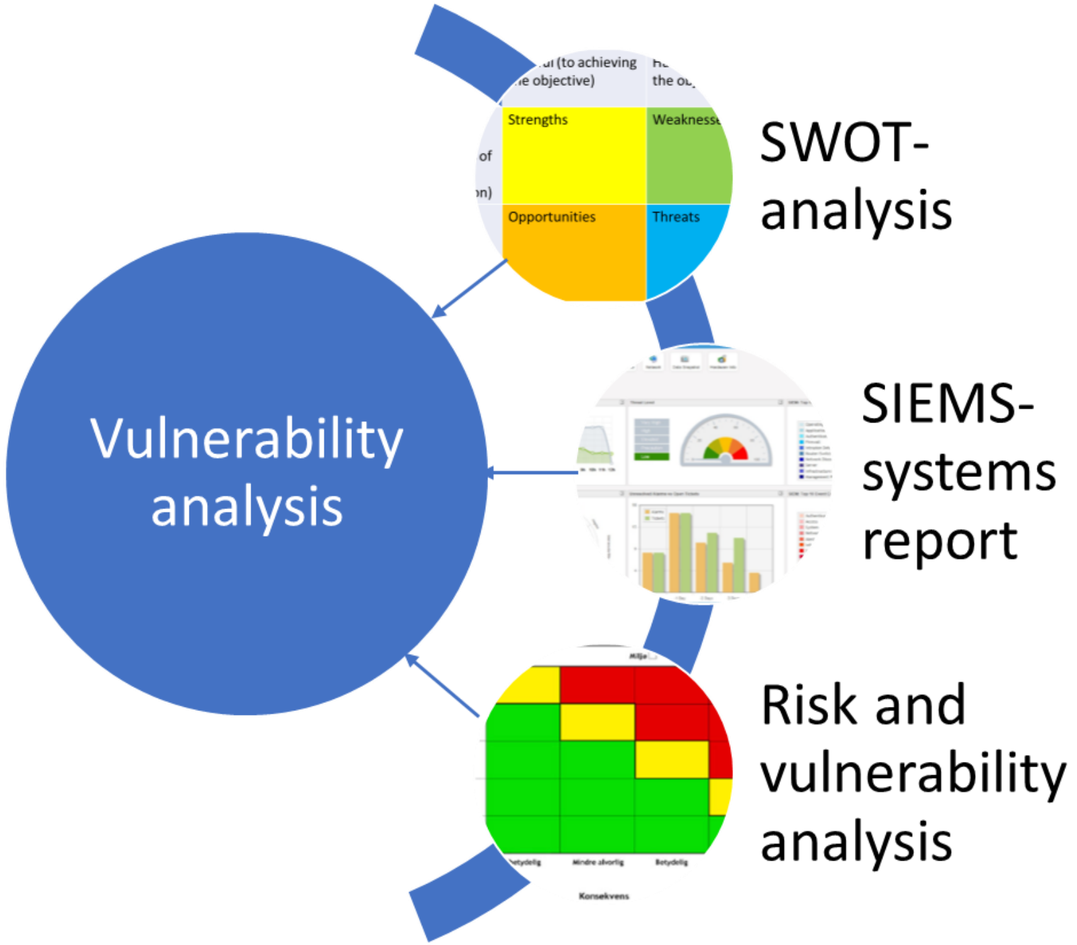
Grethe Østby(✉) and Stewart James Kowalski

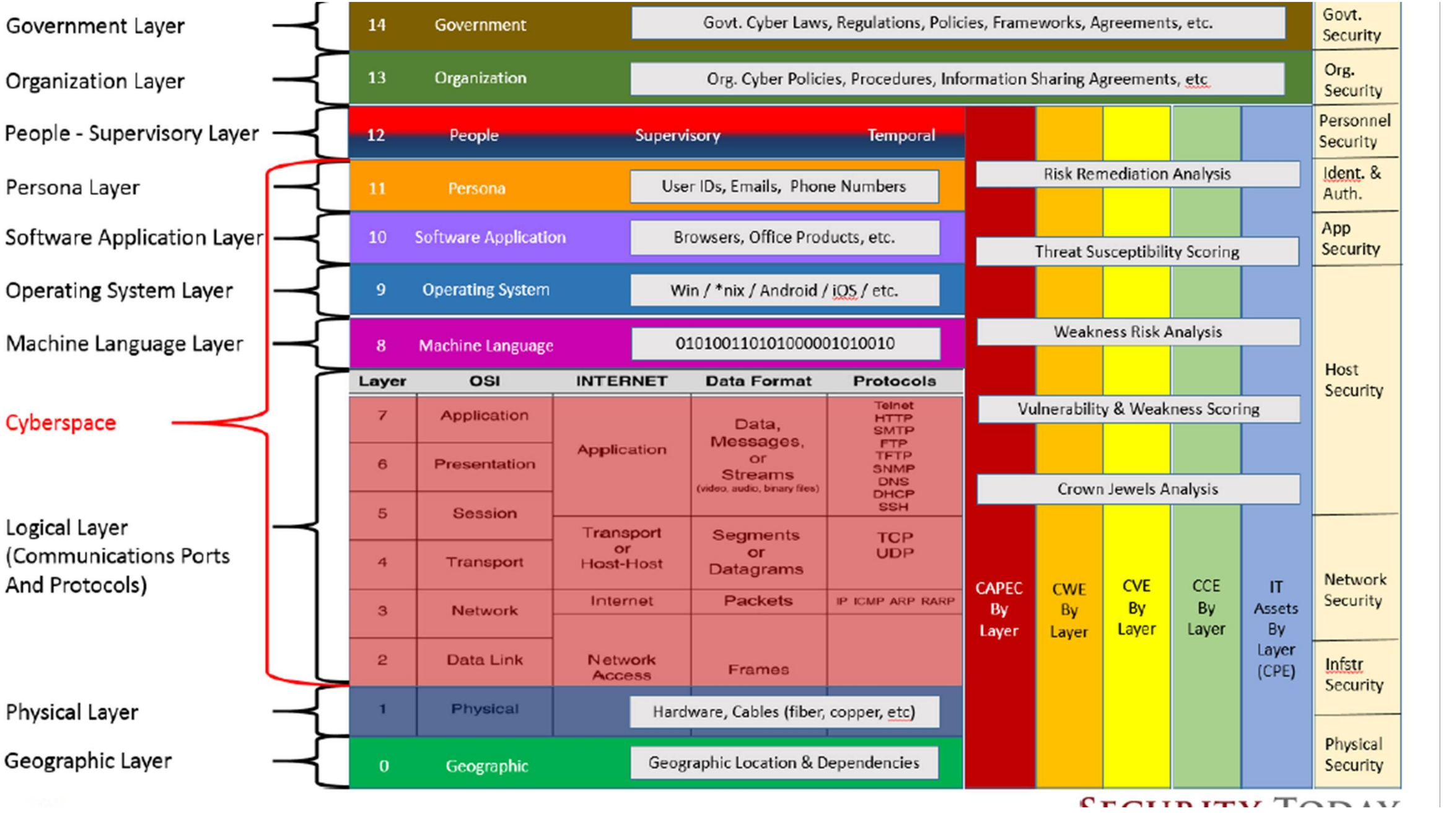
Norwegian University of Science and Technology, Gjøvik, Norway
{grethe.ostby,stewart.kowalski}@ntnu.no

Abstract. In this paper the authors discuss how to create a preparation schedule for exercises (PSE) to support EXCON-teams and instructors for full-scaled combined crisis management and cyber-exercises. The process to create the preparation schedule starts by performing vulnerability analysis to identify the most relevant and likely threats to the organization, before processing historical threats and attacks to further focus our simulation scenario development by planning and designing a socio-technical scenario. Moreover, a plan for simulation that are realistic and based on the organization's maturity will be considered, and finally, in terms of a societal crisis impact exercise necessary lectures will be prepared.

After this framework has been reviewed by the HCI International 2020, we plan to test the model when planning for exercises at the Norwegian Cyber Range (NCR) environment. NCR will be an arena where testing, training, and exercise will be used to expose individuals, public and private organizations, government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment.

Forberedelser til øvelser –> risiko- og sårbarhetsanalyser





https://www.researchgate.net/publication/280949461_Science_of_Cybersecurity_-_Developing_Scientific_Foundations_for_the_Operational_Cybersecurity_Ecosystem

Forberedelse til øvelser – Historiske trusler og cyberangrep

3600 dataangrep, i tillegg til utallige svindelforsøk. De leverte inn 47 anmeldelser.

Lunde mener Telenor blir utsatt for så mye datakriminalitet at de ikke har tid til å anmelde.

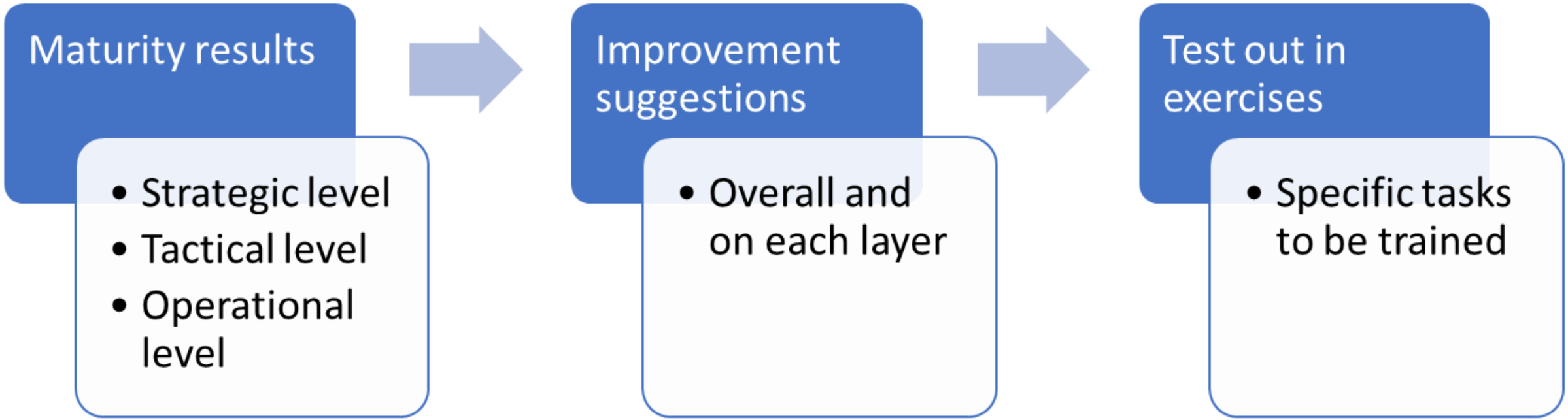
Dataangrep mot Visma

OPPSUMMERT
Hackere som skal jobbe for kinesisk etterretning, står bak et datainnbrudd hos det norske programvareselskapet Visma, ifølge nyhetsbyrået Reuters. Visma opplyser at kundedata ikke skal ha kommet på avveie.

8. februar 2019 kl. 07:29 **Tvil om hvem som står bak angrepet** - Sikkerhetskonsulentselskapet Recorded Future er åpne for at de kan ha tatt feil om Visma-hackingen. Visma og sikkerhetsselskapet har sagt at det er en kinesisk hackergruppe som står bak. Men analytikere fra Microsoft går direkte ut mot konklusjonene.

Tvil om hvem som står bak dataangrepet mot Visma

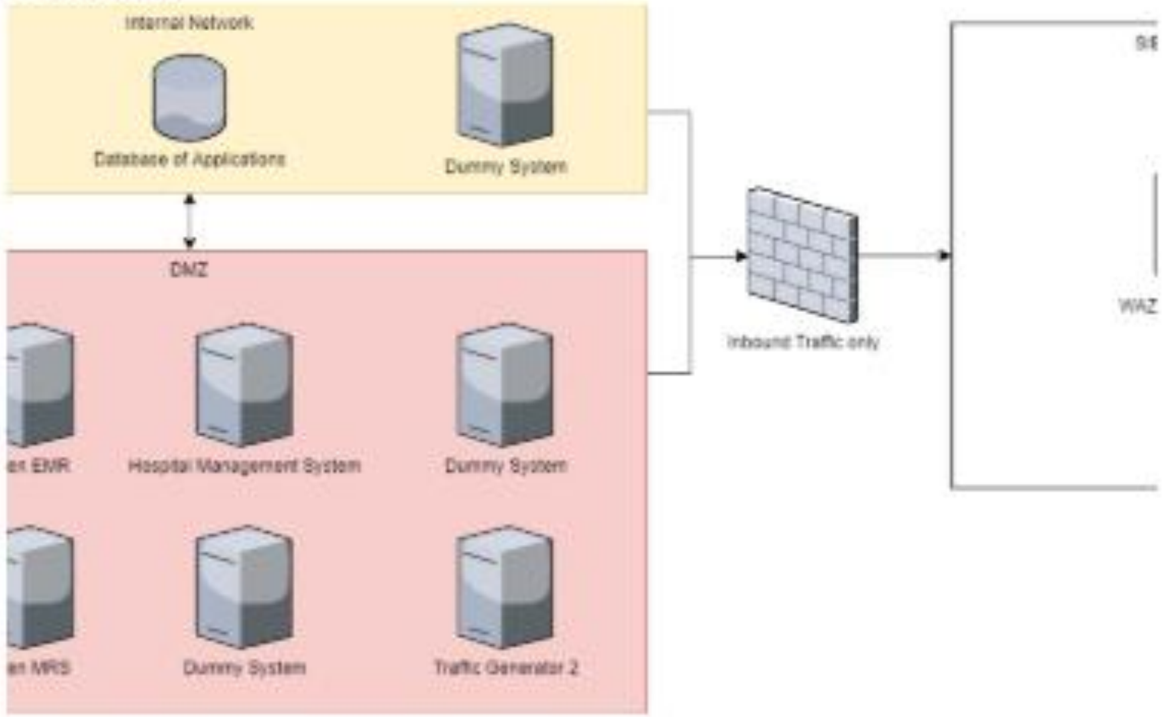
Forberedelse til øvelser – modenhetsanalyser og forslag til forbedringer



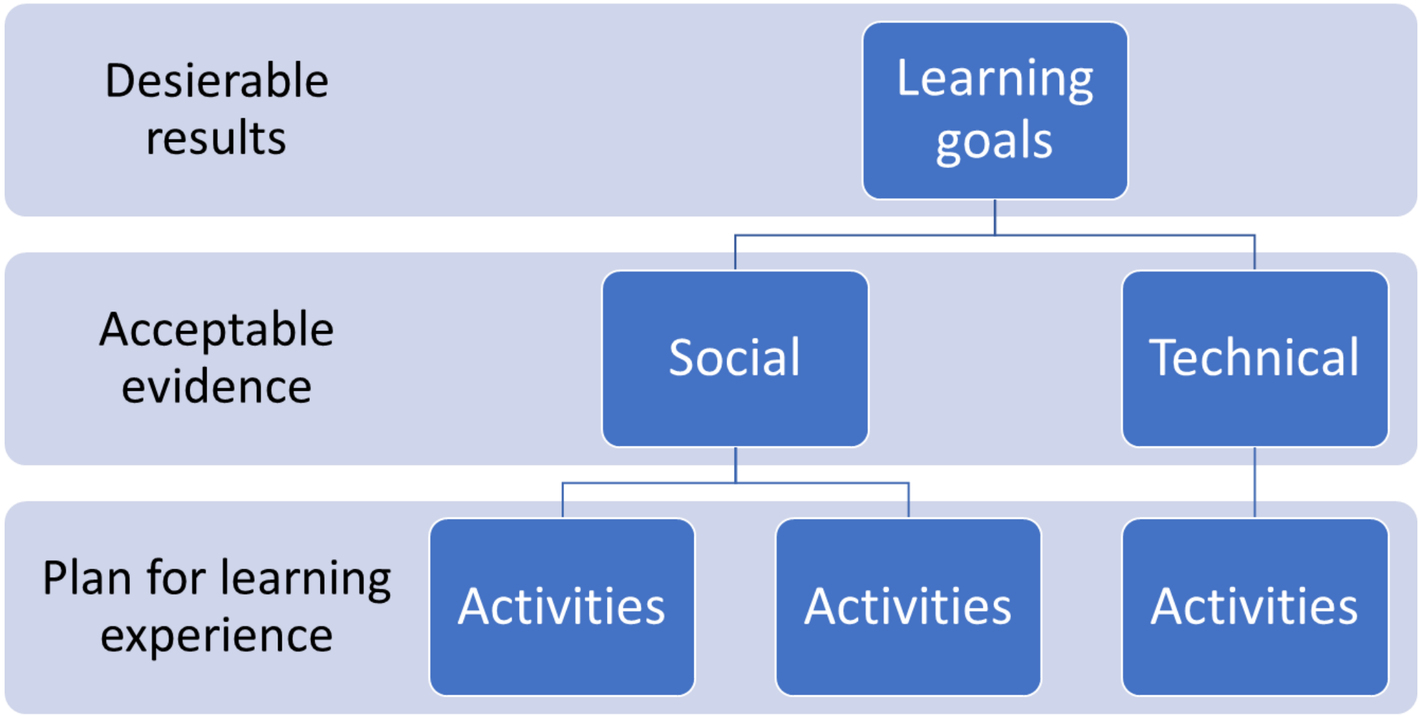
Forberedelser til øvelser – sosio-teknisk oppbyging av scenarioer

Socio

Technical



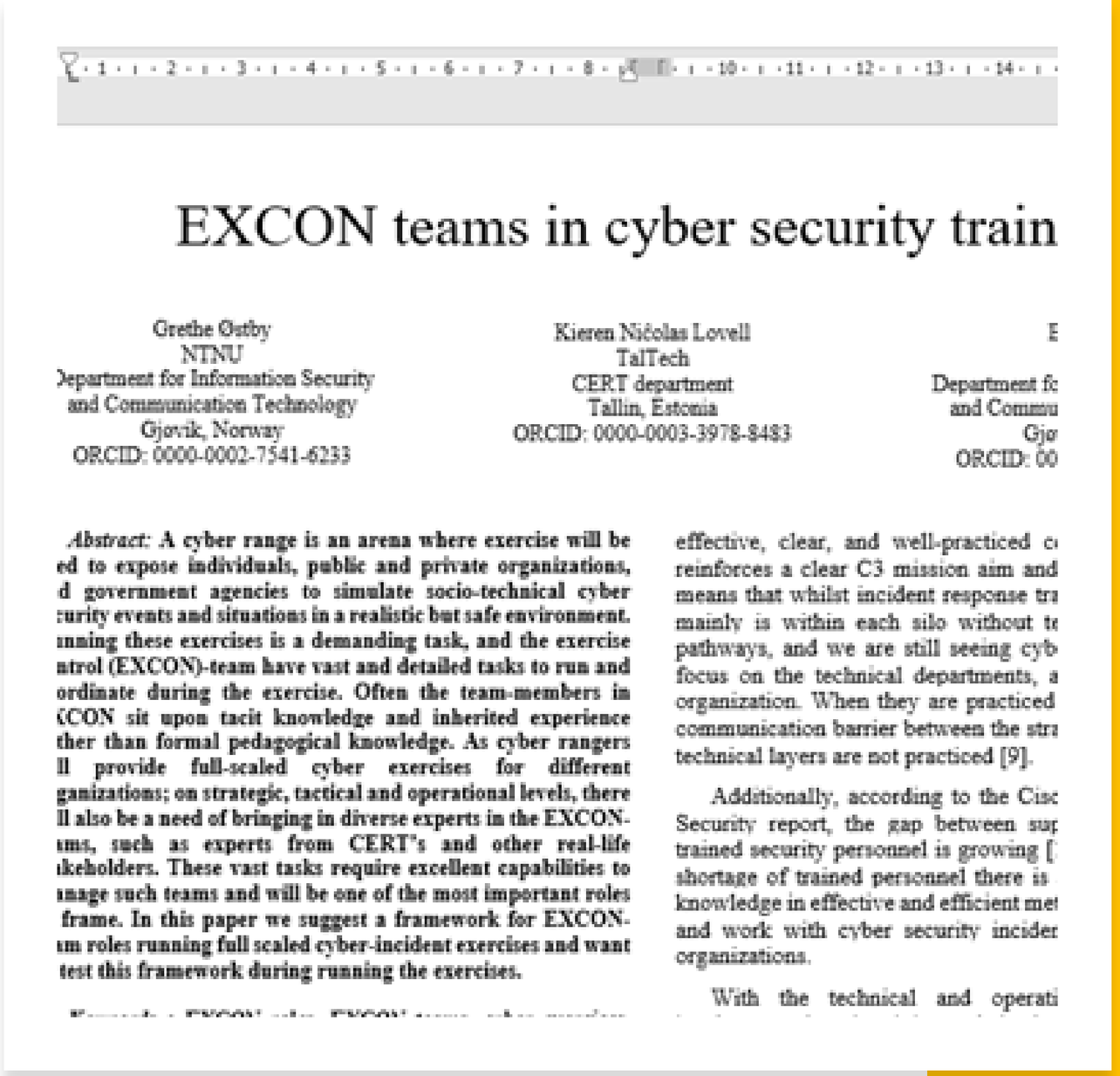
Forberedelse til øvelser - leksjoner



Spill-stab

Prosess i tre faser for å forberede relevante roller i spillstab

- Identifisere påvirkning i samfunnet av cyber-angrepet
- Identifisere ansvar og roller i håndtering av cyber-angrep
- Bygge relevant spillstab og roller i spillstab



EXCON teams in cyber security train

Grethe Østby
NTNU
Department for Information Security
and Communication Technology
Gjøvik, Norway
ORCID: 0000-0002-7541-6233

Kieren Nicolas Lovell
TalTech
CERT department
Tallin, Estonia
ORCID: 0000-0003-3978-8483

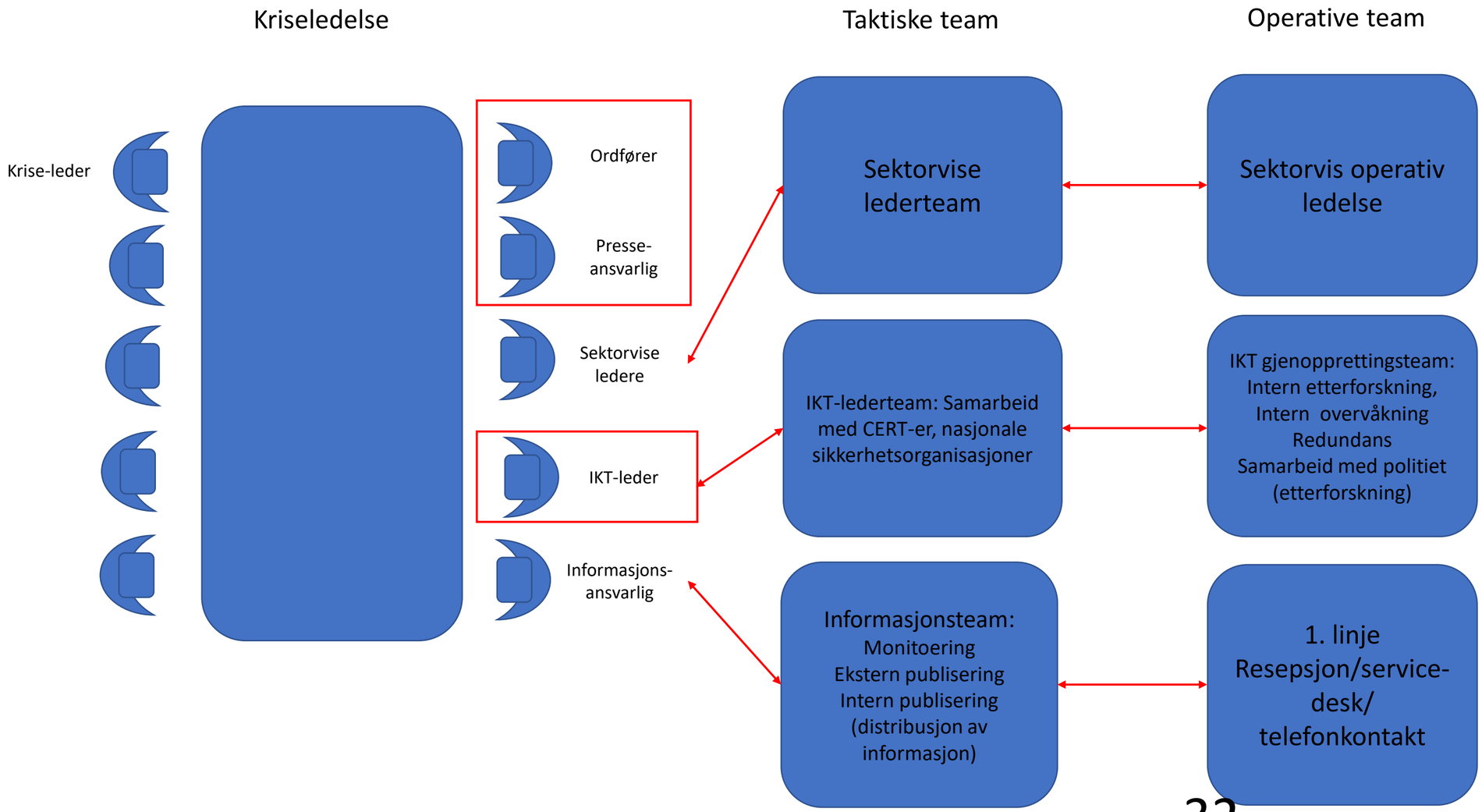
Abstract: **A cyber range is an arena where exercise will be ed to expose individuals, public and private organizations, d government agencies to simulate socio-technical cyber curity events and situations in a realistic but safe environment. nning these exercises is a demanding task, and the exercise ntrol (EXCON)-team have vast and detailed tasks to run and ordinate during the exercise. Often the team-members in CON sit upon tacit knowledge and inherited experience ther than formal pedagogical knowledge. As cyber rangers ll provide full-scaled cyber exercises for different ganizations; on strategic, tactical and operational levels, there ll also be a need of bringing in diverse experts in the EXCON-ms, such as experts from CERT's and other real-life keholders. These vast tasks require excellent capabilities to nage such teams and will be one of the most important roles frame. In this paper we suggest a framework for EXCON-m roles running full scaled cyber-incident exercises and want test this framework during running the exercises.**

effective, clear, and well-practiced c reinforces a clear C3 mission aim and means that whilst incident response tra mainly is within each silo without te pathways, and we are still seeing cyb focus on the technical departments, a organization. When they are practiced communication barrier between the stra technical layers are not practiced [9].

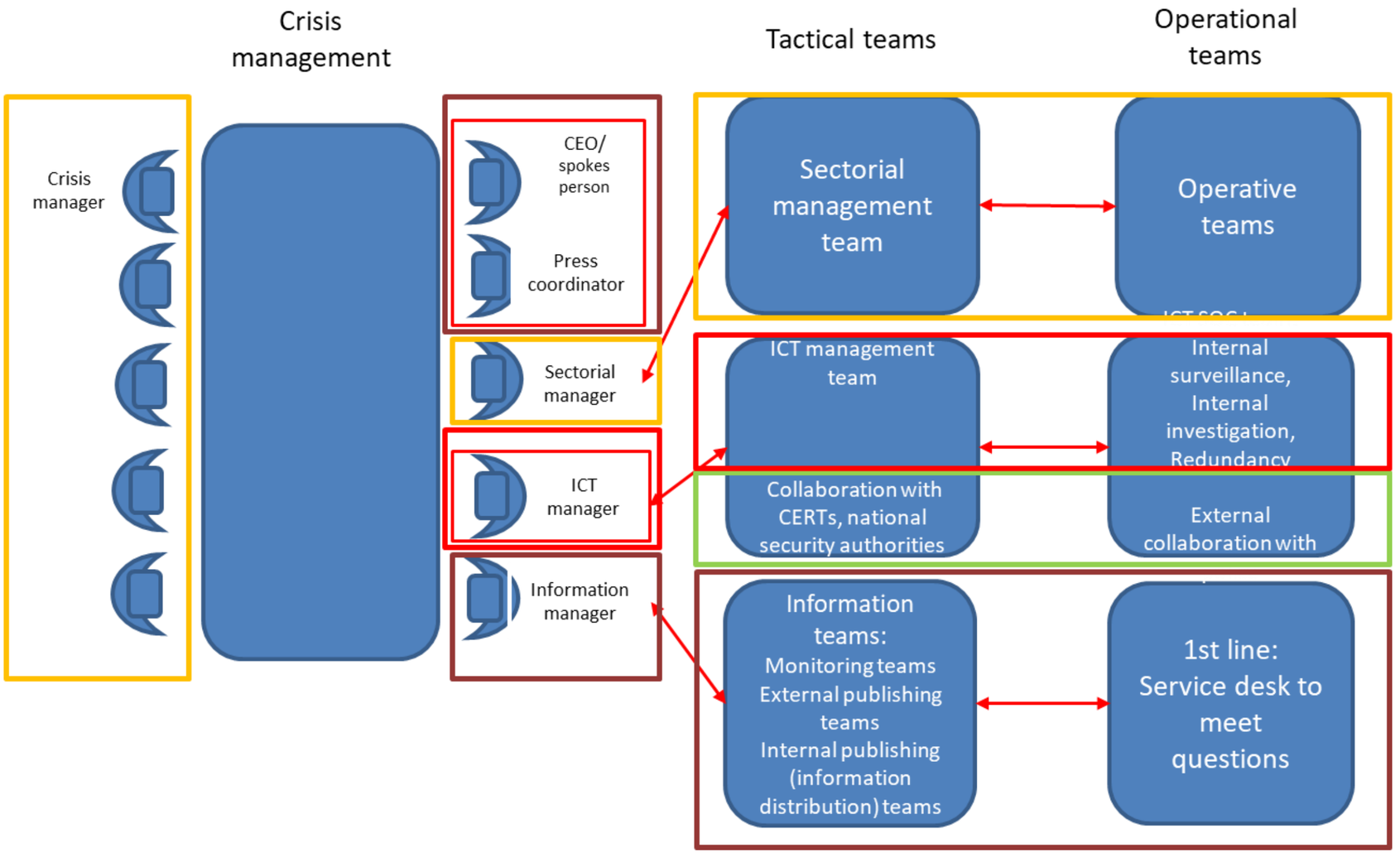
Additionally, according to the Cisc Security report, the gap between sup trained security personnel is growing [shortage of trained personnel there is knowledge in effective and efficient met and work with cyber security incider organizations.

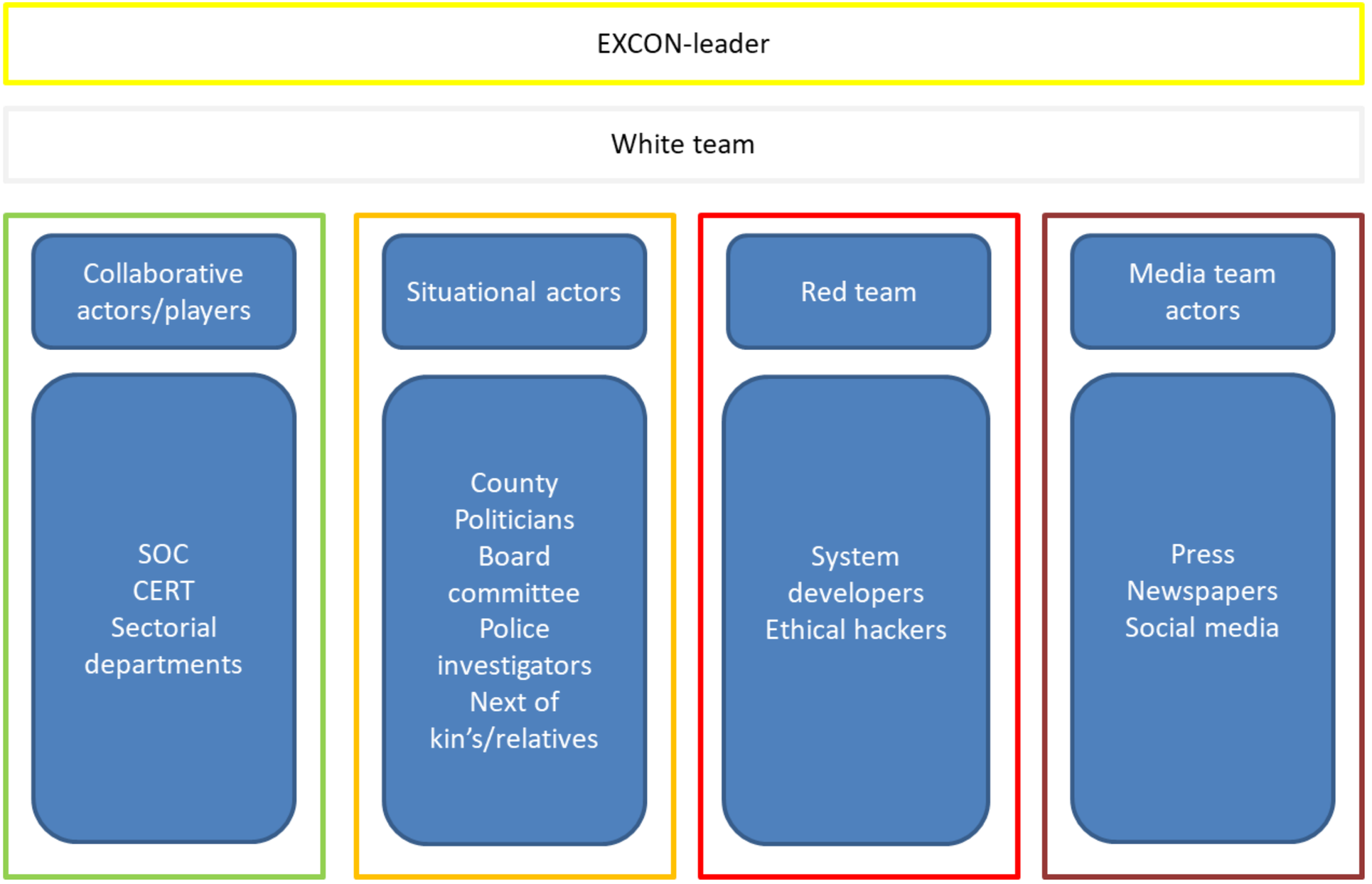
With the technical and operati

Kriseledelsesroller ved cyber-angrep



Hvordan kan vi trene rollene som deltar i øvelsene?

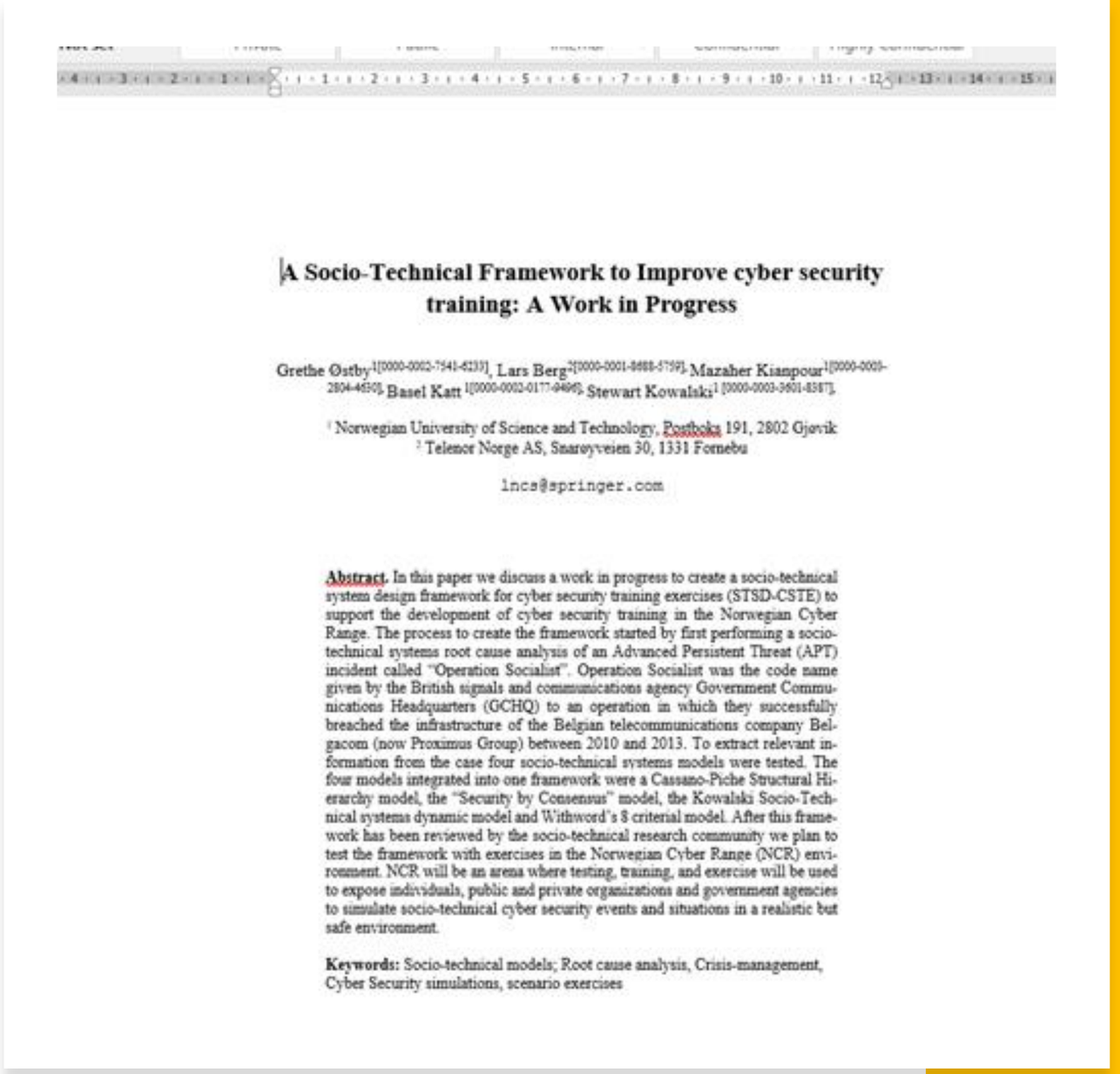



EXCON-leader
White team
Collaborative actors/players
SOC
CERT
Sectorial departments
Situational actors
County Politicians
Board committee
Police investigators
Next of kin's/relatives
Red team
System developers
Ethical hackers
Media team actors
Press
Newspapers
Social media

Scenarioer

En sosio-teknisk tilnærming for å forbedre trening innen håndtering av cyber-sikkerhetshendelser

“Social-technical models enables us to introduce more holistic and near-to-life elements needed to be factored in designing scenarios. We need to verify and validate the findings we already have made, and to enhance and improve the (STSD-CSTE) model proposed.” (Østby, et. Al. 2019)



A Socio-Technical Framework to Improve cyber security training: A Work in Progress

Grethe Østby[1][0000-0002-7541-6233], Lars Berg[2][0000-0001-8888-5759], Mazaher Kianpour[1][0000-0003-2804-4650], Basel Katt [1][0000-0002-0177-9496], Stewart Kowalski[1] [0000-0003-3601-8587]

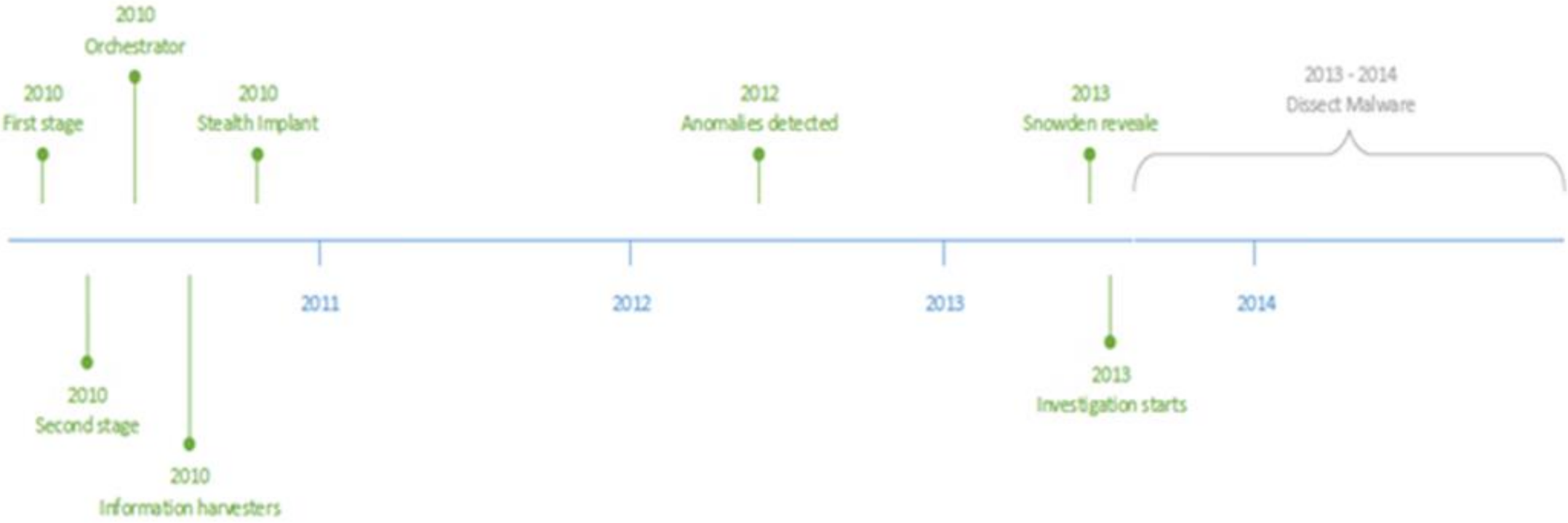
[1] Norwegian University of Science and Technology, Postboks 191, 2802 Gjøvik
[2] Telenor Norge AS, Snarøyveien 30, 1331 Fornebu

lncs@springer.com

Abstract. In this paper we discuss a work in progress to create a socio-technical system design framework for cyber security training exercises (STSD-CSTE) to support the development of cyber security training in the Norwegian Cyber Range. The process to create the framework started by first performing a socio-technical systems root cause analysis of an Advanced Persistent Threat (APT) incident called “Operation Socialist”. Operation Socialist was the code name given by the British signals and communications agency Government Communications Headquarters (GCHQ) to an operation in which they successfully breached the infrastructure of the Belgian telecommunications company Belgacom (now Proximus Group) between 2010 and 2013. To extract relevant information from the case four socio-technical systems models were tested. The four models integrated into one framework were a Cassano-Piche Structural Hierarchy model, the “Security by Consensus” model, the Kowalski Socio-Technical systems dynamic model and Withword’s 8 criterial model. After this framework has been reviewed by the socio-technical research community we plan to test the framework with exercises in the Norwegian Cyber Range (NCR) environment. NCR will be an arena where testing, training, and exercise will be used to expose individuals, public and private organizations and government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment.

Keywords: Socio-technical models; Root cause analysis, Crisis-management, Cyber Security simulations, scenario exercises

Operation Socialist – GCHQ infiltrering i Belgacom



Root årsaks analyser – modeler benyttet

Withford

Human level	Capability	Knowing about malware attacks in Belgium?
	Vulnerability	
	Reliance	Keeping their good jobs...
	Flexibility	Wants to be able to discover private activities at job (doing some job at home).
	Risk of use	Restriction in use of Internet might be considered as lack of trust to many.
	Security	Humans might want the company to take care of the security.
	Confidentiality	This might be the best argument for each employee within Belgacom. They want the same protections as any other.
	Reliability	Learn how to NOT rely on information/e-mails (eg. Bayanat).
Communal level	Synergy	Employees within Belgacom might be afraid of losing their jobs – therefore they are willingly to "shut down" the communication for that communal interest.
	Openness	In the case Belgacom was open about the incident, but not about possible consequences (Regin's case again).
	Transparency	Belgacom does not want transparency about the incident. This brings uncertainty to the customers.
	Freedom	Customers shift to other telecom companies.
	Morale	Have Belgacom really solved the issue? Are the Regin gone for sure?
	Identity	Taking care of the customers by privacy and handling the malware.
	Privacy	The communal "family" in the case are both large organizations and private persons. All are invested in keeping their Telecom information private.
	Color	

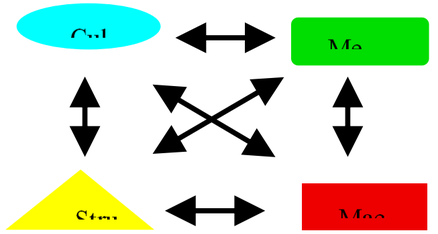
Criterias on the hardware requirements system level:

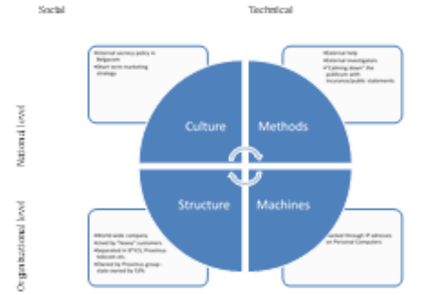
Human level	Power	
	Permeability	Permeability are high due to internet-private accounts such as Facebook, LinkedIN, Google accounts etc..
	Reciprocity	Pursuits – difficulty when malware is searching for specific IP-addresses among engineers
	Mobility	Might want refers to travel...
	Consumption	
	Armor	Ref. Private network design scenario pg. 20
	Stealth	Cyber Arm – attacker/defender. The attackers advance are (...)

SBC-model

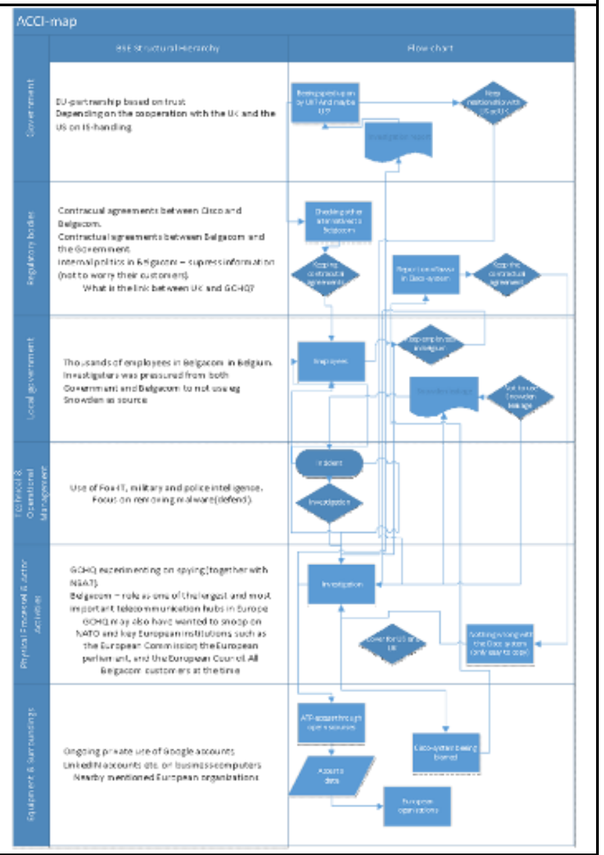
Social	Ethical-Cultural	Introverted marketing policy. Does not want any focus on what has happened. Marketing policy/long term strategy, eg. compare with Regin/Flame case. Public opinion?
	Legal-Contractual	Use the Fire-IT in the beginning, then the military intelligence analysis or military intervention. Is the Swedish trying to hide the information because they have contacts with the Government etc. to take care of? Only Cisco could handle the routers.
	Administrative-Managerial	Police can purge the spy bug. Public announce that their customers has nothing to worry about. Also announce that the case has been closed down when the investigation focus on the Regin's behavioral pattern and start all over again (instead of being humble). Is it the Government, Foreign Government or the Collaboration with the US and GB, that gave the attacker?
	Operational-Procedural	1) Hire Fire-IT 2) Hire the military intelligence 3) Hire the public intelligence 4) Focus on purging the spy bug. 5) Some employers at the Belgacom's were mad that the GCHQ is not fully removed
Technical	Mechanical-Electronic	Regin malware attacks as follows: **First stage.** Drivers which act as loaders for a re-cond stage. When started loading, loaded malware stage 2. **Second stage.** When launched it deletes traces of the initial loader, and then loads the next part and injects its own code into RAM. May disinfect by failure). **Orchestrator.** Is a modified stager working on Windows' kernel. Loads the next part of the malware. **Information harvesters.** Includes data collectors, self-defense engine, functionality for encrypted communications, network capture programs, and remote controllers of different kinds. **Stealth implant.** Plants itself as file-system specific locations in memory. Difficult to find, as it is very much like good working Kernel level memory (specific Windows).
	Application	+ Mechanical stage launched for particular engineers and system administrators by finding their IP-addresses. + E-mail servers at Belgacom had malfunctioned, but they did not find out why.
	Operating system	Belgacom operating systems worked out by Cisco. Some incidents happened at cross application (some applications implemented just NSA. Legacy-code makes vulnerable. UNIX computer systems was enforced.

Kowalski

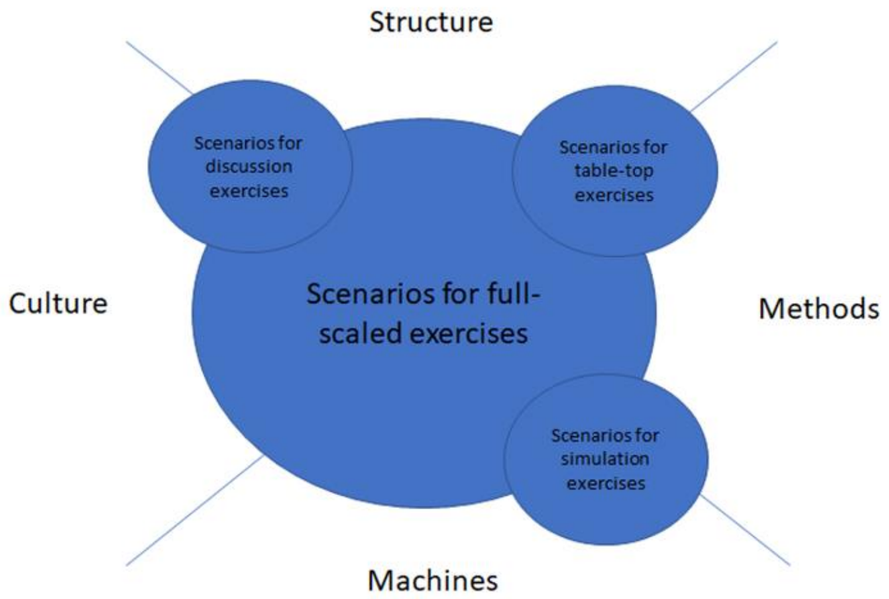


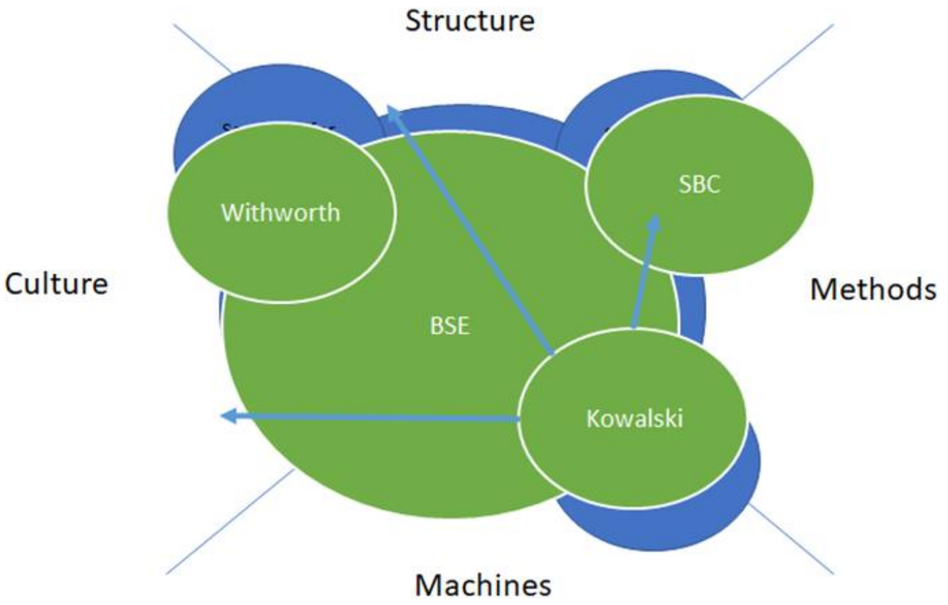


BSE-model

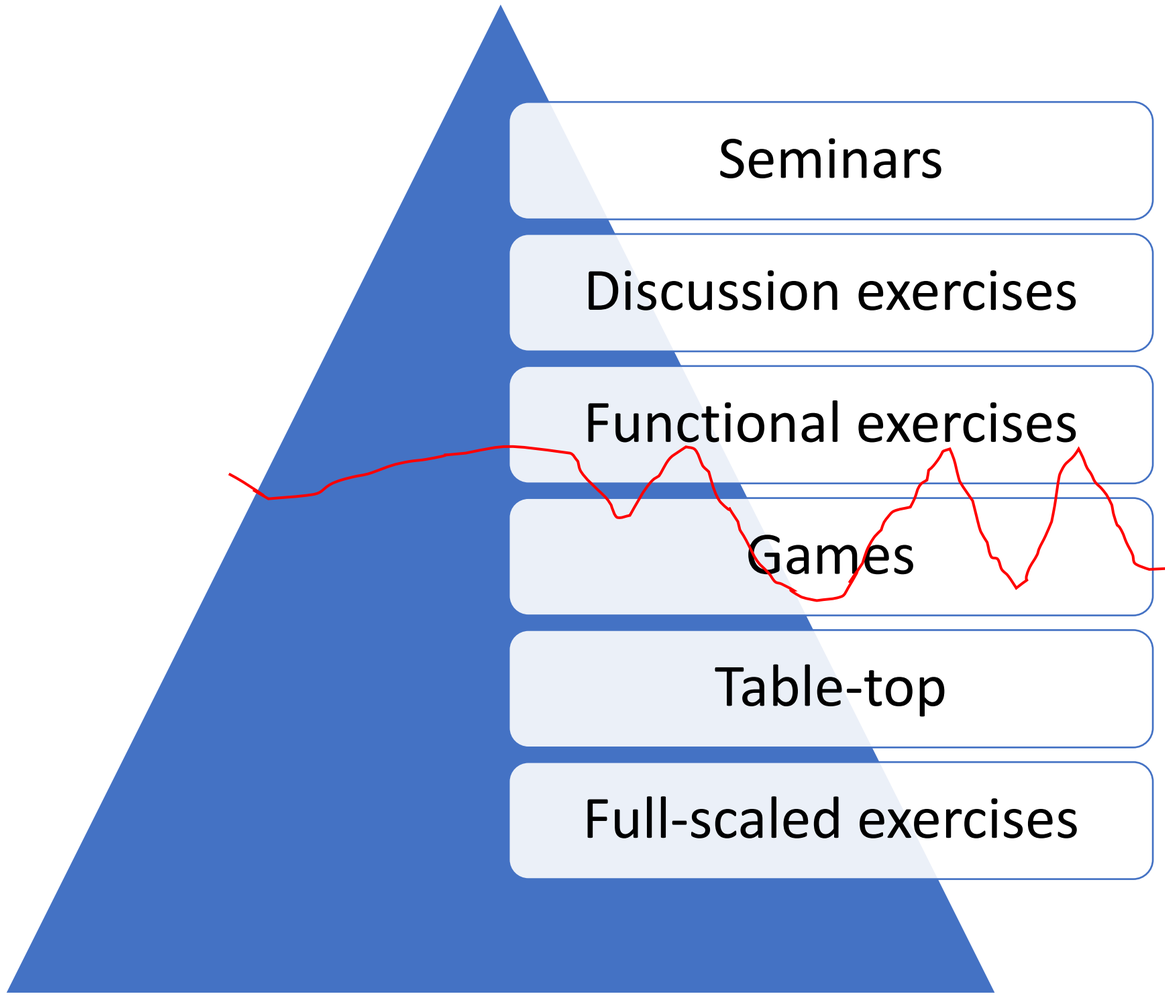


Sosio-teknisk modellering øvelser





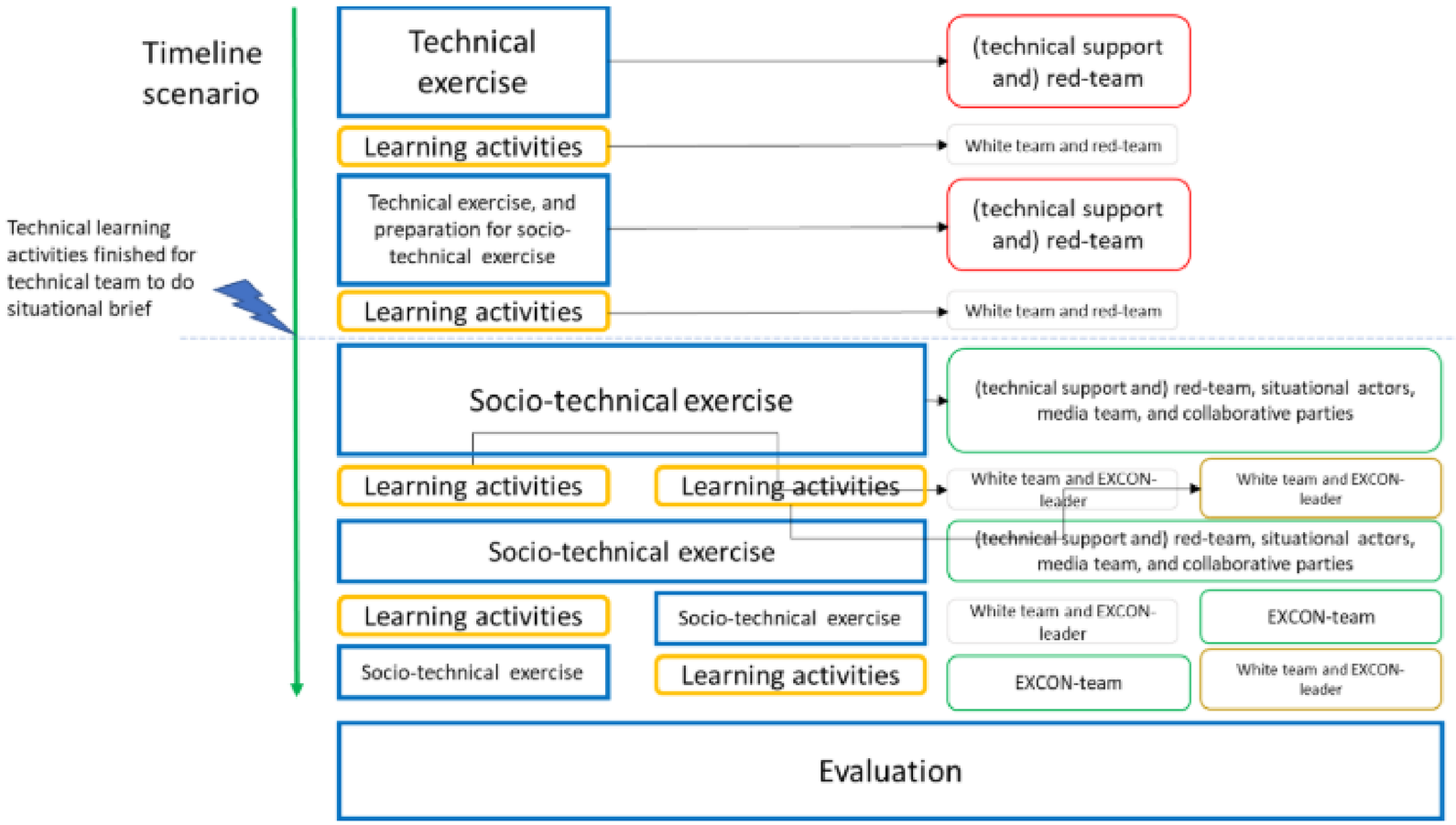
Statiske vs. dynamiske scenarioer



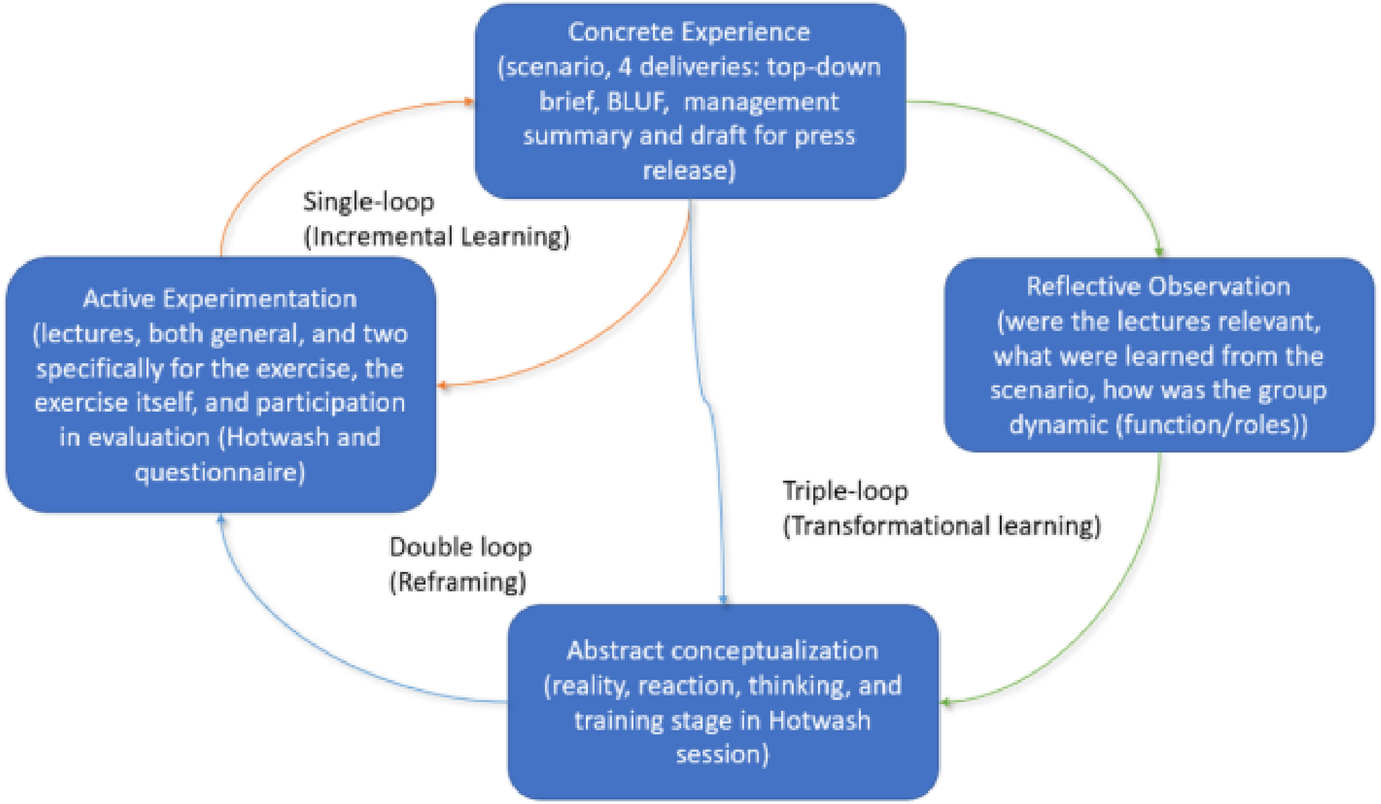
Static scenarios:
prewritten, no changes

Dynamic scenarios:
prewritten in playbooks, adapt from decisions

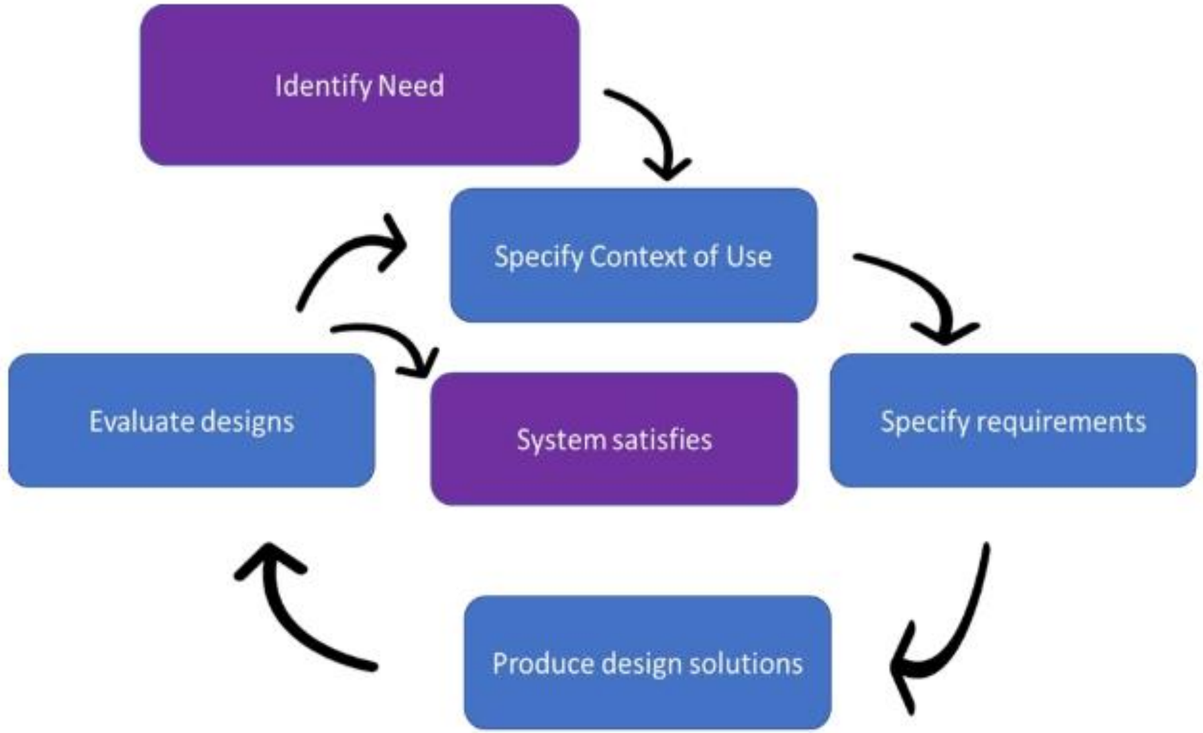
Lærings-aktiviteter i scenarioet



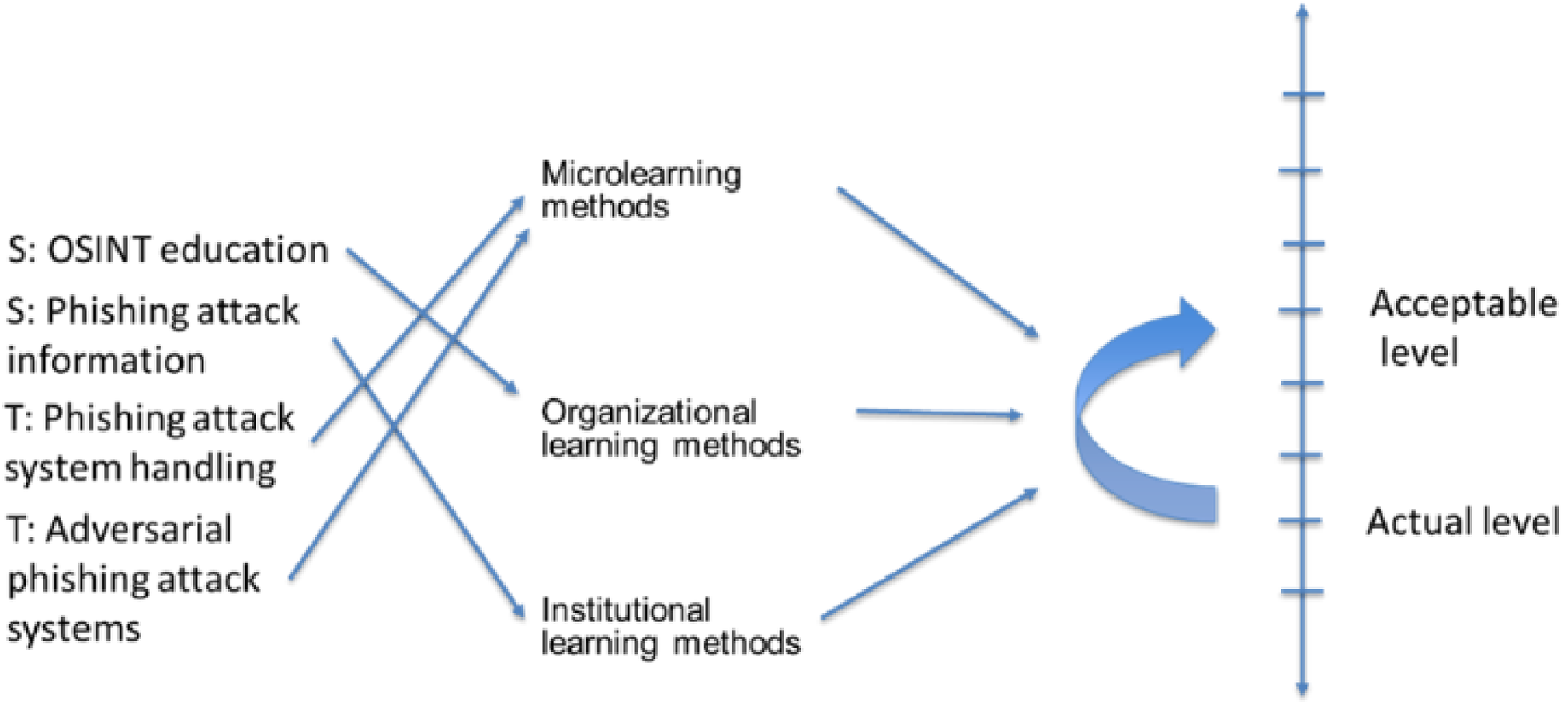
Læring i flere faser

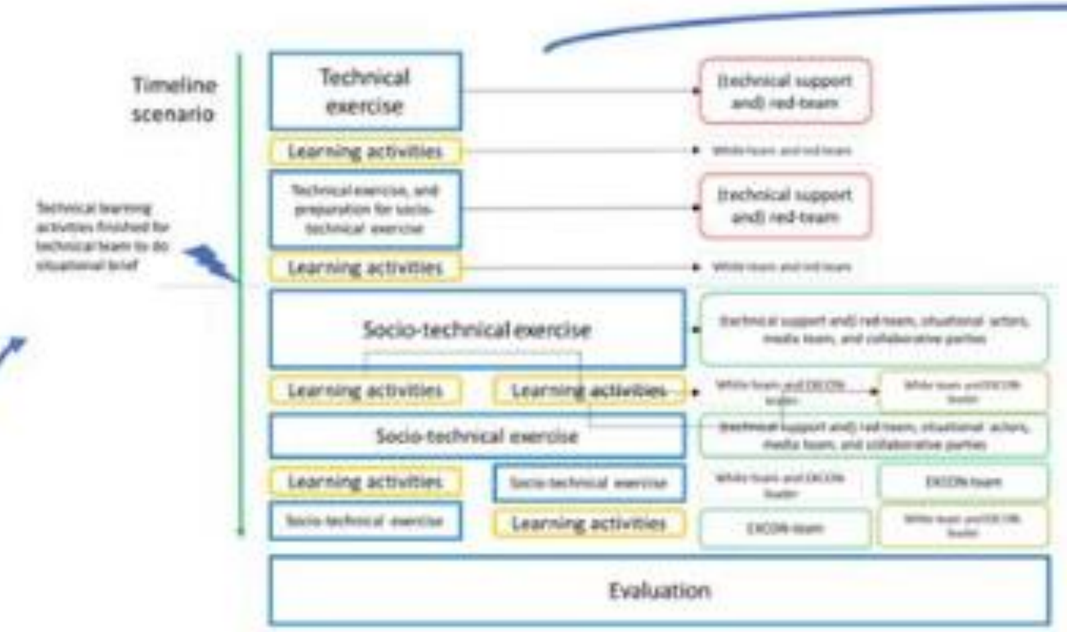


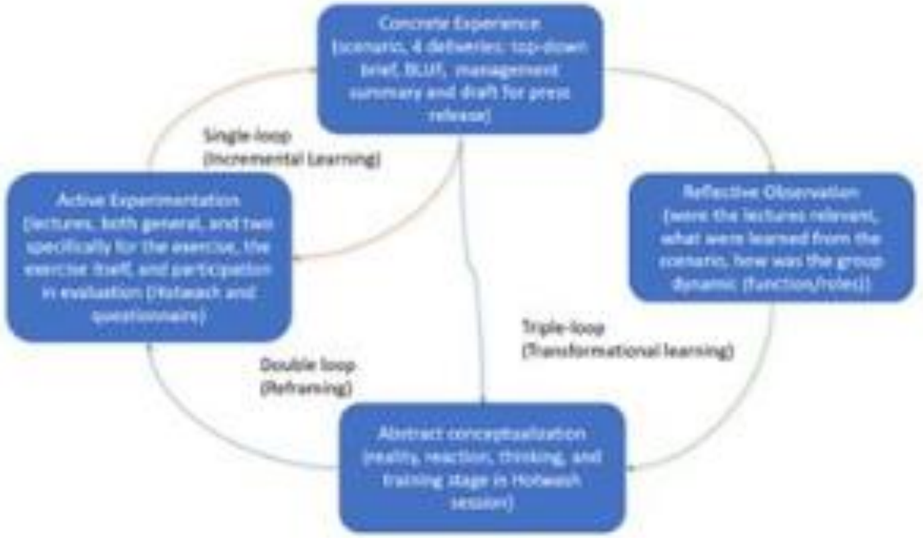
Behov i organisasjonene?

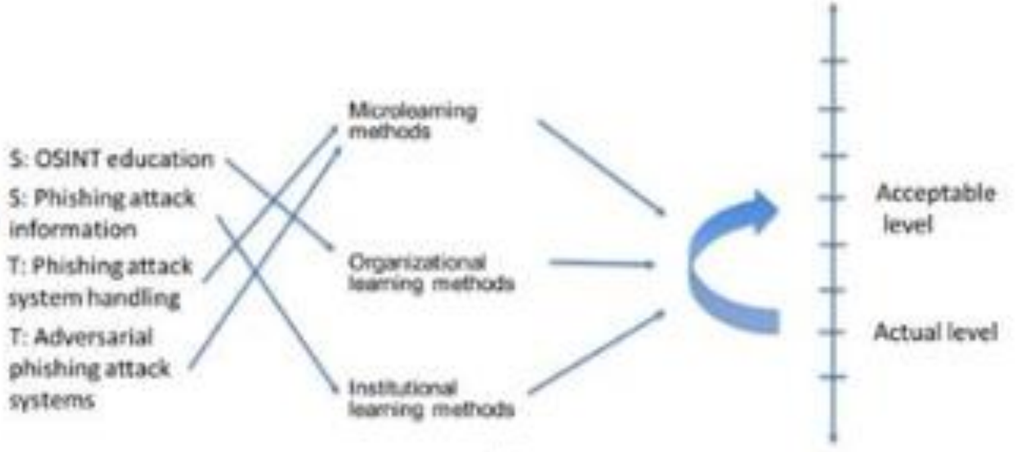


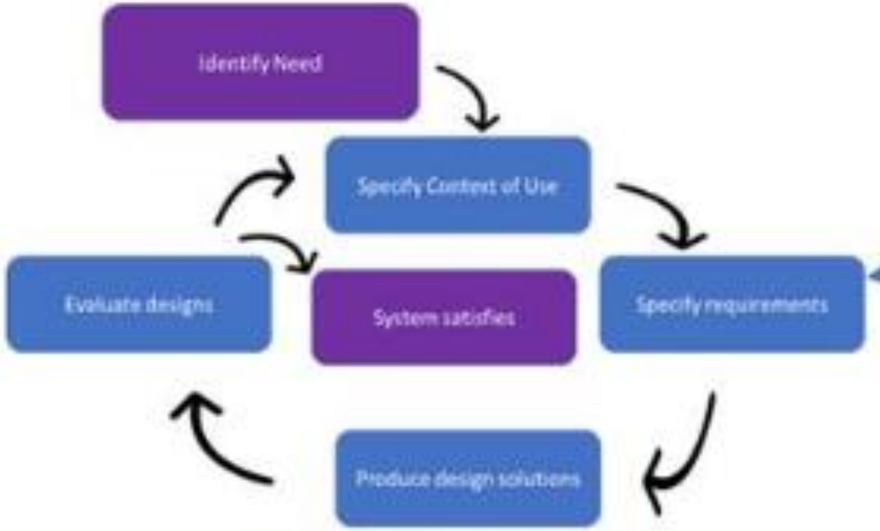
Ulike læringsmetoder -> hvordan komme til et akseptabelt nivå?




Timeline scenario
Technical exercise
(technical support and) red-team
Learning activities
White team and red team
Technical exercise, and preparation for socio-technical exercise
(technical support and) red-team
Technical learning activities finished for technical team to do situational brief
Learning activities
White team and red team
Socio-technical exercise
(technical support and) red team, situational actors, media team, and collaborative parties
Learning activities
Learning activities
White team and EXCON leader
White team and EXCON leader
Socio-technical exercise
(technical support and) red team, situational actors, media team, and collaborative parties
Learning activities
Socio-technical exercise
White team and EXCON leader
EXCON team
Socio-technical exercise
Learning activities
EXCON team
White team and EXCON leader
Evaluation


Concrete Experience (scenario, 4 deliveries: top-down brief, BLUF, management summary and draft for press release)
Single-loop (Incremental Learning)
Active Experimentation (lectures, both general, and two specifically for the exercise, the exercise itself, and participation in evaluation (Hotwash and questionnaire)
Reflective Observation (were the lectures relevant, what were learned from the scenario, how was the group dynamic (function/roles))
Triple-loop (Transformational learning)
Double loop (Reframing)
Abstract conceptualization (reality, reaction, thinking, and training stage in Hotwash session)


S: OSINT education
S: Phishing attack information
T: Phishing attack system handling
T: Adversarial phishing attack systems
Microlearning methods
Organizational learning methods
Institutional learning methods
Acceptable level
Actual level


Identify Need
Specify Context of Use
Specify requirements
System satisfies
Evaluate designs
Produce design solutions

Hva gikk bra og hva var vanskelig?

The good...

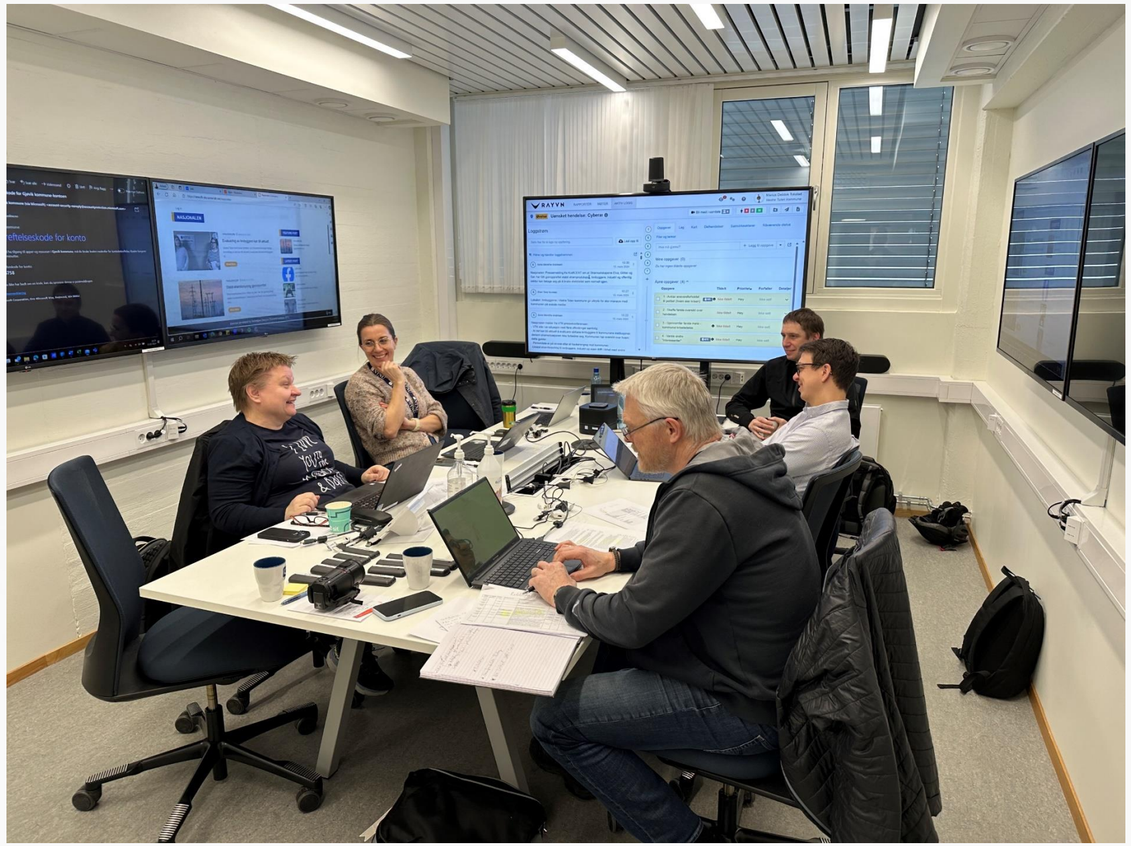
- Avgjørende med kompetanse både innen beredskap og cybersikkerhet i prosjektet
- Øvelser tilpasset hver kommune sitt behov/nivå
- Gjennomarbeidede scenarier og team
  - Øvelser med «trøkk»
  - Bruk av lokalkunnskap om kommunen
  - Bruk av personvernombud
- Gode øvingsfasiliteter (rom, utstyr)
- Følgeforskning på effekter

Spillstab for Gjøvik kommune.

Simulert mediebilde og RAYVN på veggskjerm.

Eiendomsavdelingen med i spillstaben.

...the bad, and...



Spillstab for Vestre Toten kommune.

På de to siste øvelsene hadde vi fått dreis på sakene.

- NTNU er ikke en kommersiell aktør
- Tilpassing av IKT-teknisk øvingsplattform til kommunenes hverdag/behov (både tid og kvalitet)
- Verktøy var «fremmede» for IKT-avdelingen
  - Verktøy for brannmurer
  - Systemovervåking
  - Loggverktøy
- En del barnesykdommer på første øvelse
  - Tekniske problemer (RAYVN + NTNU)
  - Mange i spillstab gjorde ting for første gang, tok oppmerksomhet bort fra hovedinstruktør

Hva lærte kommunene av øvelsene?

Hvilken verdi gir det for kommunen?

Gjøvik kommune avholder «pressekonferanse» med IKT-leder, personvernombud og varaordfører

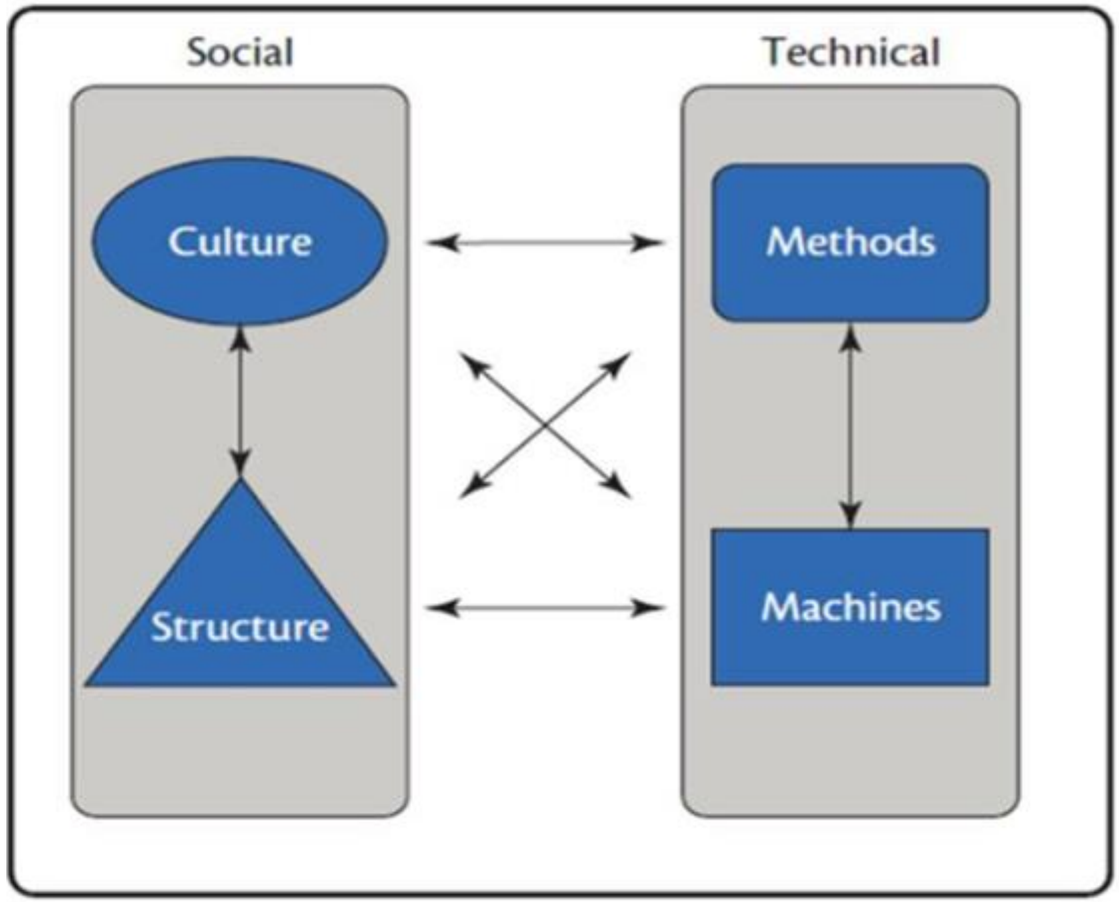
Nordre Land kommune sin pressekonferanse med ordfører, kommunikasjonssjef og personvernombud

Erfaringer Gjøvik kommune

- **Før øvelsen**
  - Mye planverk mangler/utdatert
  - Utarbeide nytt verktøy Rayvn
  - IRT (Responsteam internt)
  - Varslingslister/ terskler
- **Under øvelsen**
  - Roller/ ansvar - leder ut av rommet, hvem kan beslutte hva
  - Timeouts/status- oppdateringer
  - Beredskapsperm/papir i bruk
  - IRT- fungerte ok-
  - Oppgavelister
  - Eksterne aktører, avtaler mangler
- **Etter øvelsen**
  - Roller og ansvar
  - Beredskapslager av pc'er
  - Oppgaver i Rayvn
  - Øve regelmessig; Siste del av dag - natt - Første del av dag
  - Hvordan organisere over flere dager
- **Fremover**
  - Rolleavklaringer, internt, kriseledelsen
  - Revidering av planer, BIA, IRT (ikke teknisk ressurs)
  - Oppdatere, få på plass manglende minimums planverk
  - Formalisere samarbeid med nabokommuner
  - Anbud SOC- tjenester, planverk ++

Sjekklister for andre kommuner som ønsker å gjennomføre slike øvelser

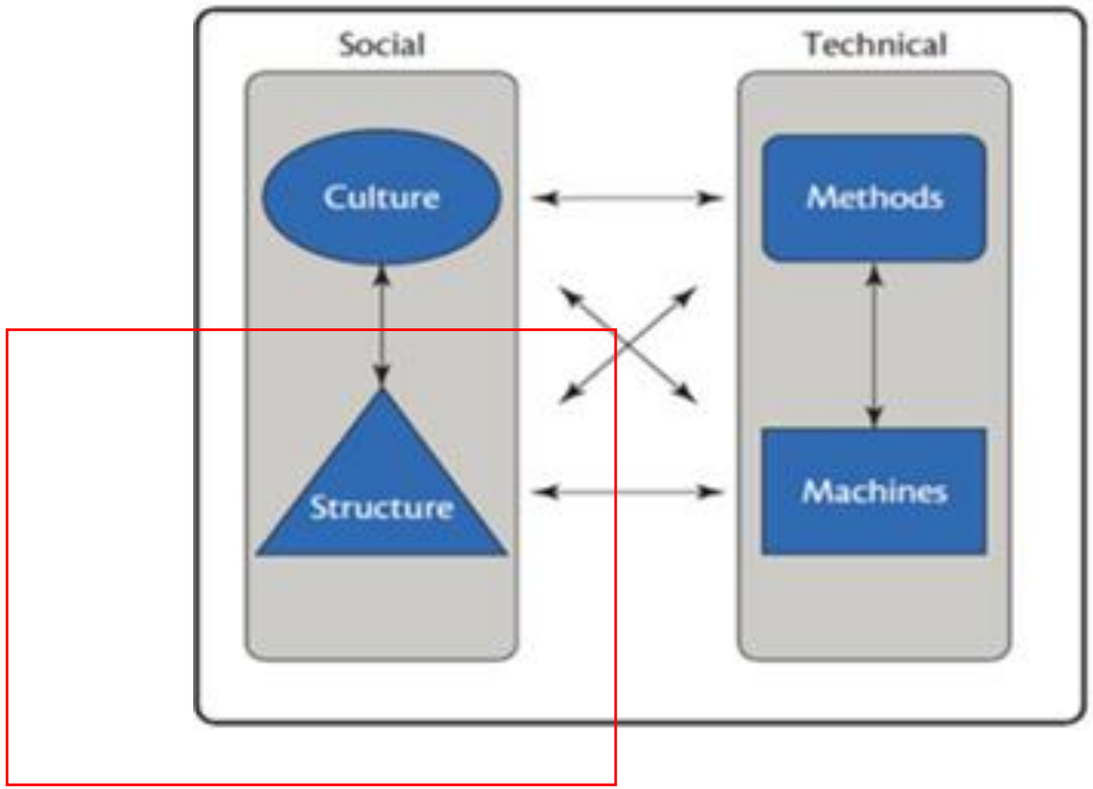
Sosio-teknisk tilnærming



- I øvingsdirektiv
- I leksjoner
- I scenario
- I forberedelser med instruktører (hvem gjør hva)
- I fordeling av oppgaver i spillstab
- Ved cyber-range
- Under evaluering

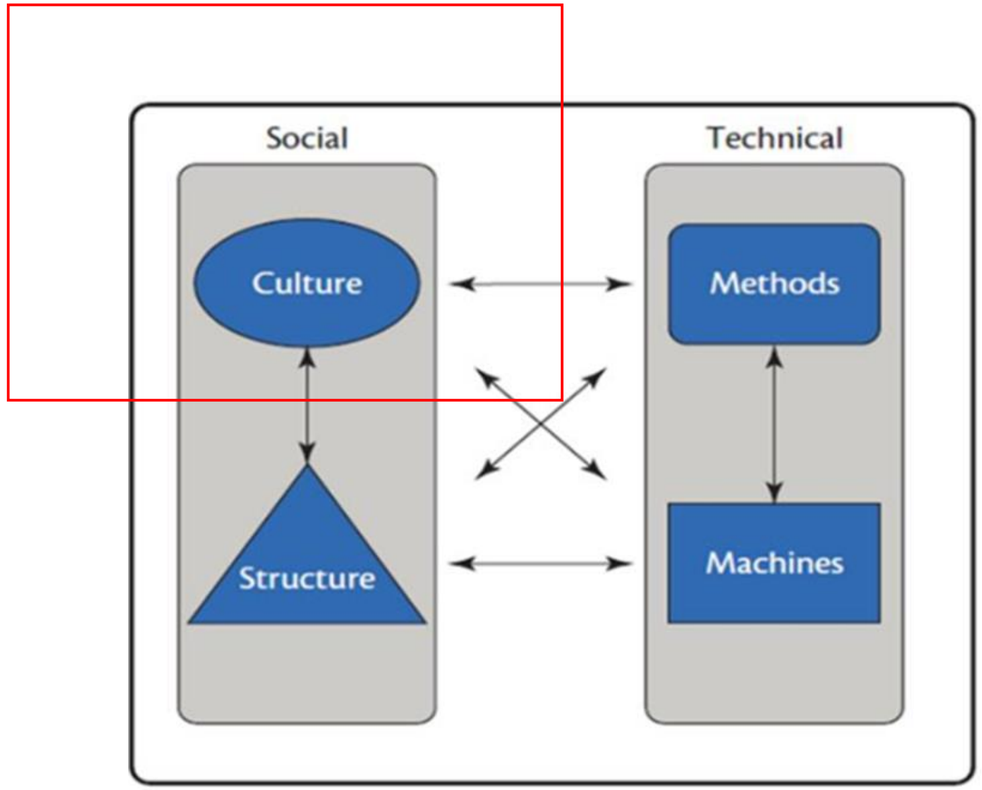
Struktur i øvelsene

- Øvingsdirektiv med utgangspunkt i DSB sine veiledere
- I tillegg i øvingsdirektivet (ut over 'vanlig'):
  - Kartlegging i organisasjonen i forkant (modenhetsvurdering?)
  - Leksjoner i forkant av øvelsene (basiskunnskap)
  - Hva er annerledes ved et cyber-angrep (hvordan bør beredskap ved slike hendelser struktureres)
  - Tekniske øvingsmål – i en 'passende' tidslinje
  - Evaluering (også tilrettelagt for triple-loop-learning)
  - Rapporter til kommunene



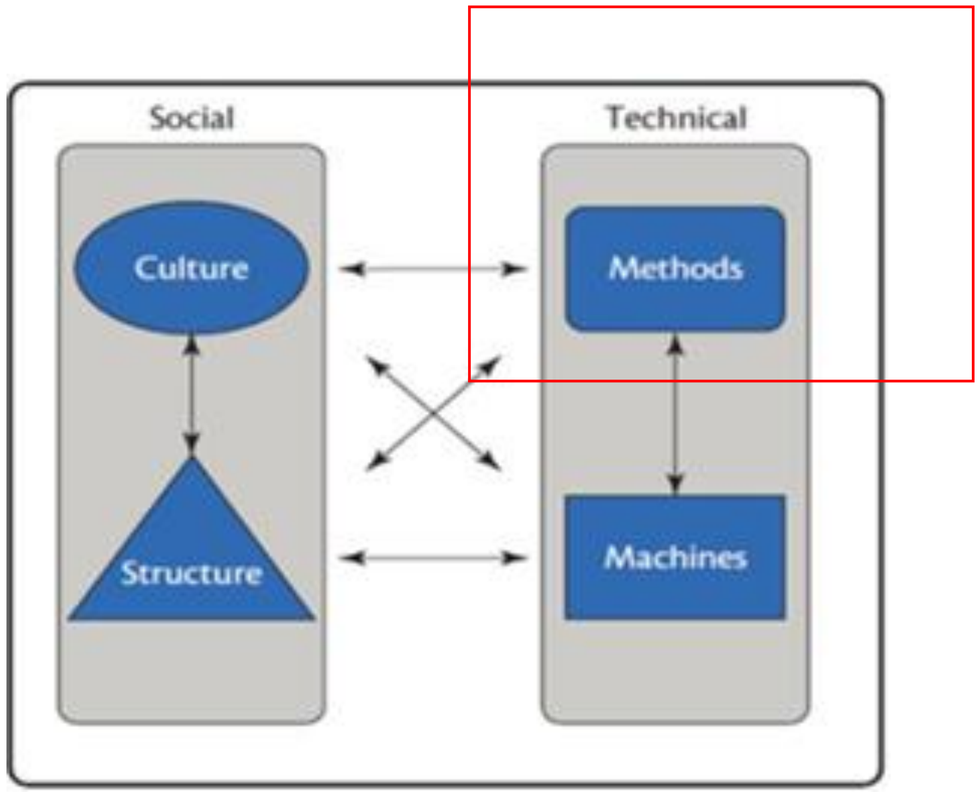
Kultur for øvelsene

- ‘Oppsett’ av informasjonssikkerhetsledelsesansvar i organisasjonene (hvem skal øves/få opplæring)
- Behov i organisasjonen basert på kunnskap (ikke bare kriseledelse og kommunens egne ønsker, men også kunnskap om informasjonssikkerhet)
- Trygge rammer for deltakere ved en cyber-range (vi tar oss tid til å prøve ut)
- Deri en leksjon som kanskje gjør ‘litt vondt’



Metoder for øvelsene

- Kundeorientert tilnærming
  - Dagens nivå på informasjonssikkerhetsledelse
  - Akseptabelt nivå (hvor skal vi i øvelsen?)
  - Hva ønsker kommunen selv å øve på?
- Tidslinje for øvelse og scenario
  - Læringsobjekter
- Oppbygging av spillstab
- Sosio-tekniske læringsartifakter
  - Krav til kommunene (lover, regler, forskrifter, veiledere, standarder)
  - Informasjonssikkerhetsledelse i ulike sektorer
  - Kriseledelse vs. 'incident response' -> beredskap innenfor informasjonssikkerhetsledelse
- Evaluering

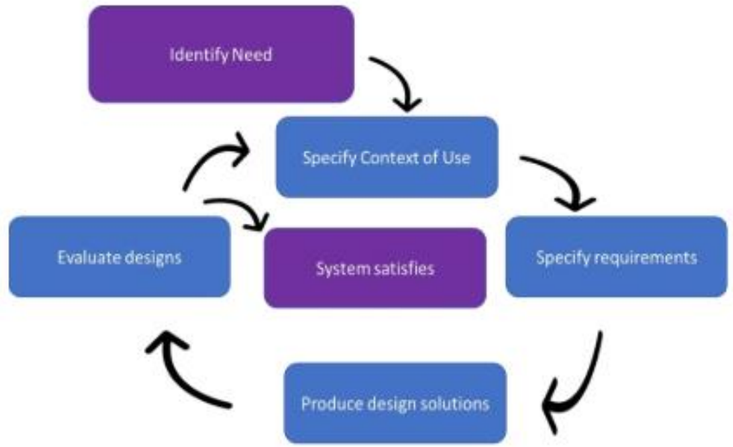


Kunde-orientert tilnærming

- ISO 27002?
- NIST?
- NSM sine grunnprinsipper?

- Whitman & Mattord?

1) Informasjonssikkerhetsstrategi
2) Informasjonssikkerhetspolicyer, deri instrukser, rutiner og oppfølging/avvikshåndtering av disse
3) GDPR/personvern
4) Risikostyring
   a. Teknisk
   b. Beredskap
   c. Modenhet
5) Program for informasjonssikkerhet
   a. Informasjon
   b. Opplæring
   c. Trening
   d. Øvelser
6) Vedlikehold IKT sikkerhet (vaktordning?)
   a. Ekstern sårbarhetsovervåkning (for patching)
   b. Ekstern trusselovervåkning
   c. Intern overvåkning
   d. SIEMS-verktøy etc.
   e. Maximum Tolerable Downtime - MTD (redundans, backup etc.)
7) Beredskap
   a. Business impact analysis
   b. Incident response planer IKT (continuity, etc.)
   c. Disaster recovery planer
   d. Business continuity plans
   e. Beredskapsplaner (krisehåndtering)



Tidslinje for øvelse og scenario

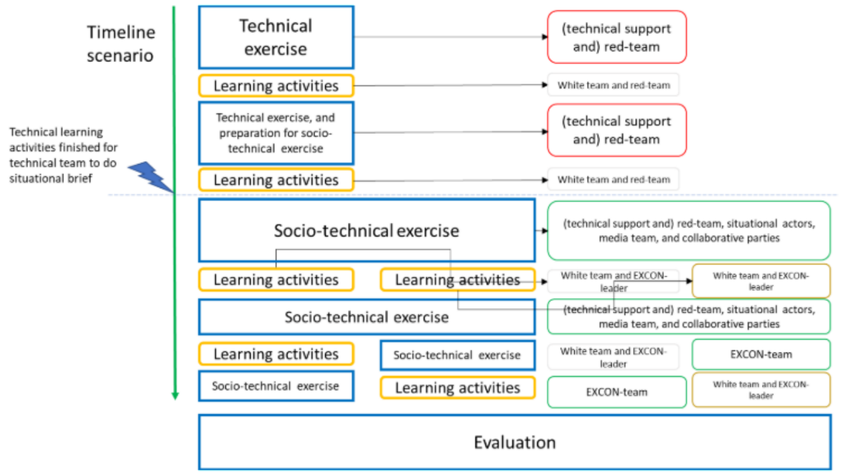
- Siste muligheter for middag er kl 1500…

14. mars 2024

09:45 – 10:00	Oppmøte og registrering H-bygget (1/3 auditorium) campus Gjøvik (kaffe og wienerbrød)	
10.00 - 11.00	Krav til samfunnssikkerhet og beredskap ved informasjonssikkerhets-hendelser (lover, forskrifter, veiledere og oppdragsbrev), og andre informasjonssikkerhets-oppgaver organisasjonen kan være forberedt på.	
11:00 - 11:10	Hente-kaffe-pause	
11:10 – 12:00	Kriseledelse og stabsarbeid: Situasjonsanalyse, ressursbehov (personell og materiell), rollefordeling og operativ oppfølging ved informasjonssikkerhetshendelser	Operativt team starter øvelse. Arbeid med utarbeidelse av situasjonsbrief i NCR-lokalene (kjeller A-bygget).
12:00 – 12:45	Lunsj kantina	
12:45 – 13:30	Informasjonsberedskap, leder-brief, krisekommunikasjon, RAVYN og SIEMS	
13:30 – 15:00	Status i dag, ROS-analyser, beredskapsplaner, tiltakskort roller	
15:00 – 15:15	Brief fra operativt team til ledelse (innledning til felles-øvelse – kjeller A-bygget)	
15:15 – 16:00	Middag (kantina)	
16:00 – 18:45	Felles øvelse starter (NCR-lokaler)	
18:45 – 19:00	Situasjonsanalyse fra instruktør (NCR-lokaler)	

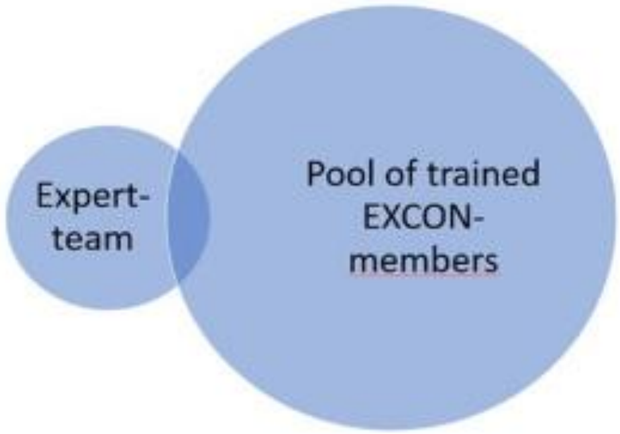
15. mars 2024

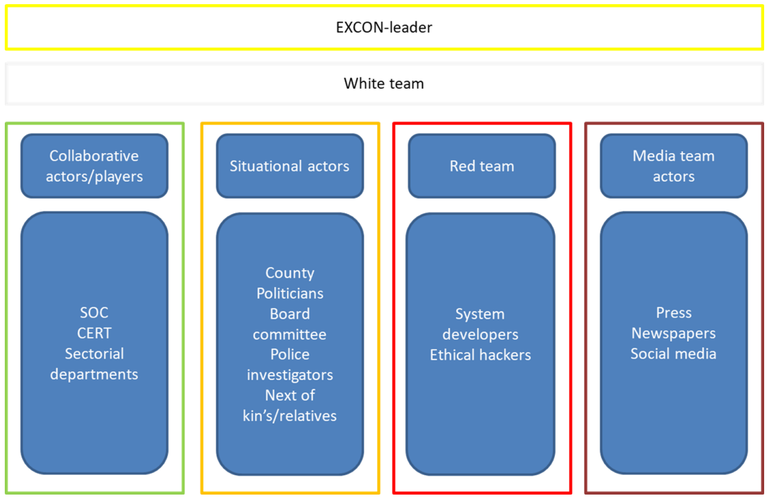
08:30	Registrering
08:30 – 11:00	Øvelse fortsetter ved NCR
11:00 – 11:45	Evaluering
11:45 – 12:30	Lunsj (kantina)
12:30 – 13:00	Hotwash sesjon (med en liten filmsnutt) og gjennomgang av evaluering
13:00	Takk for nå, og vel hjem!



Spillstab

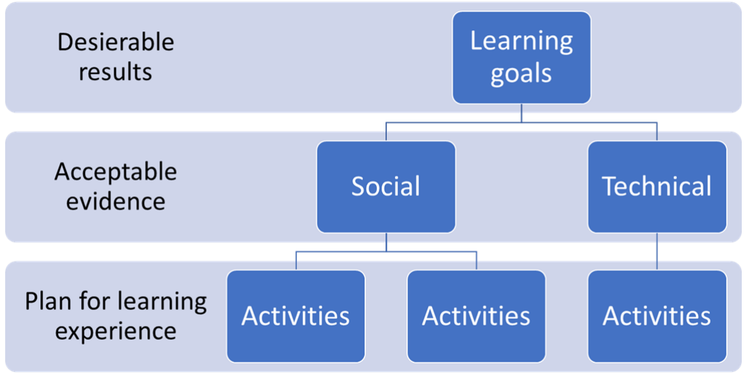
- Hovedinstruktør bør ha god kunnskap om krisehåndteringsansvar i en kommune, men også god kunnskap innenfor informasjonssikkerhetsledelse
- Instruktører for IKT-personellet må ha god kunnskap om hendelseshåndtering i systemer og eskalering av informasjon om hendelsen
- Spillstableder bør ha erfaring fra krisehåndtering, og planlegging og gjennomføring av øvelser. Det er alltid en fordel for hovedinstruktør å kjenne spillstableder godt.
- Det er også en fordel å ha med personell i spillstab som enten 'eier' sin egen rolle, eller har inngående kunnskap til den

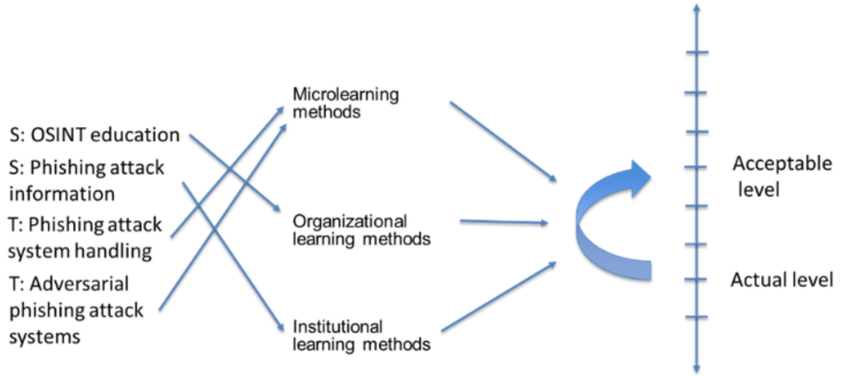




Læringsmål

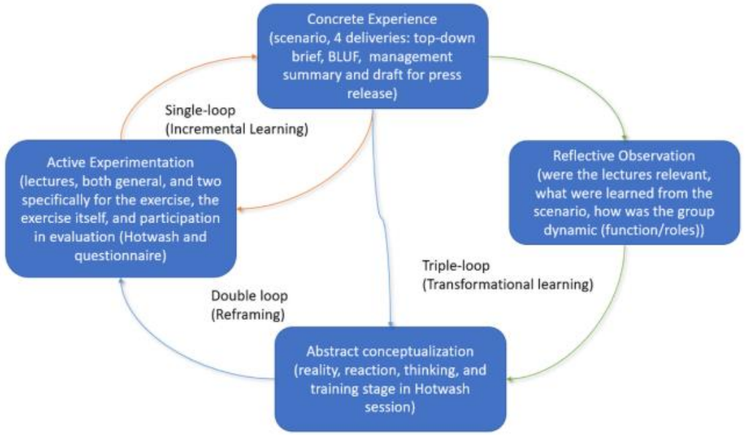
- Ulike metodikker (mikro-læring, organisasjonslæring, institusjonslæring etc.)
- Ulike aktiviteter (nå skal det gjennomføres en situasjonsbrief…en pressebrief…en isolering av systemer…)
- Ulik trening (eskalering fra IT-team… beslutninger fra kriseledelse…)
- Instruktører som KAN sin del av oppgavene





Tilrettelegge for triple-loop-learning (eksempel personvern)

- Inkrementell læring (forståelse for tema – leksjoner med case fra Østre Toten)
- Forandring basert på kunnskap (erfaring – eksempel med viktigheten av deltakelse av personvernombud i kriseledelse)
- Forandring i organisasjonen (i risikovurderinger, beredskapsplaner, i dette tilfelle opprette tiltakskort med personvernteam under ansvaret til personvernombud for å følge opp de som har fått personopplysninger på avveie)

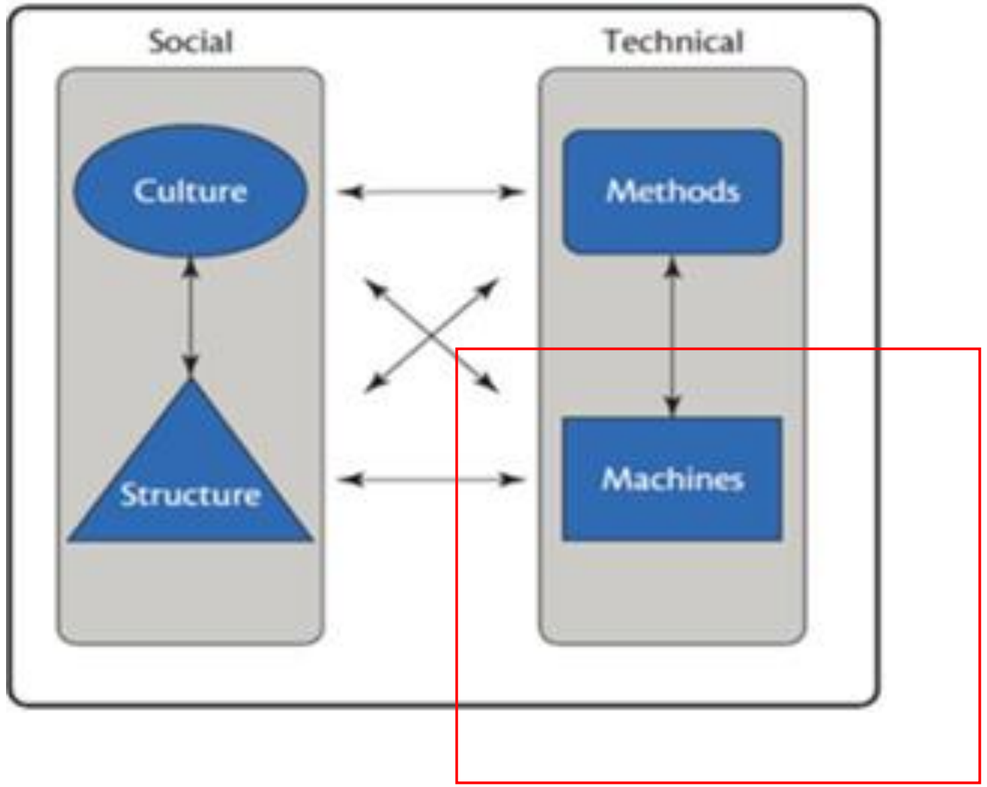


Evaluering

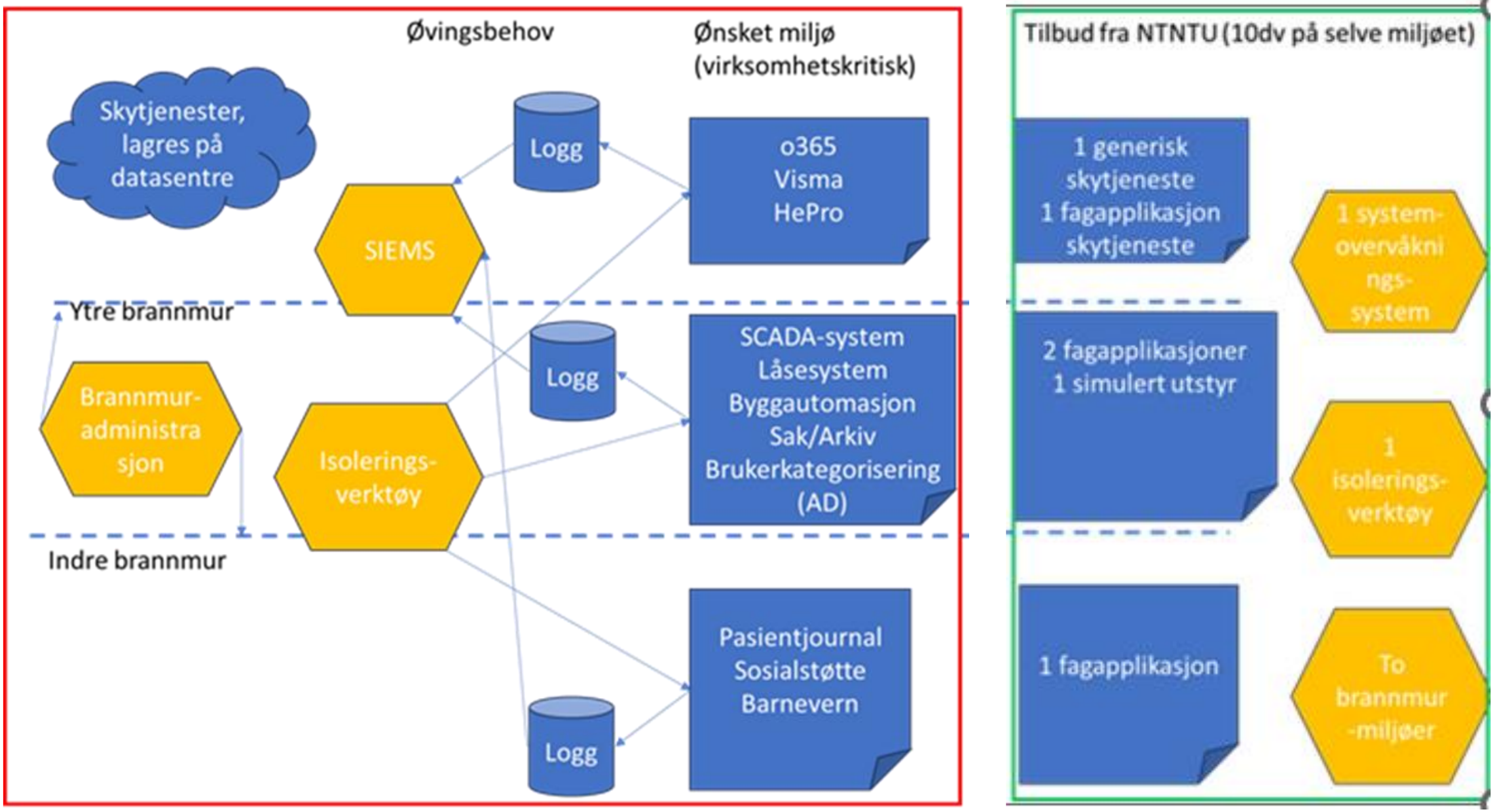
- Egen evaluering basert på øvingsmålene -> delt inn i team
  - IKT-personell
  - Kriseledelse (for større øvelser må også denne gruppen deles opp)
  - Spill-stab
- Hotwash!
  - Utvalg av spørsmål
- Evaluering fra øvingsledelse -> hva anbefales fulgt opp (rapport)

Maskiner (og systemer/verktøy) i øvelsene

- Varsel fra **SIEM**
- Søk i **logger**
- **Isolering** av systemer
- **Brannmuradministrasjon**
- (**Gjenoppretting**)



Hva er mulig å få til?



Spørsmål?

Takk for oss

Grethe Østby

Styrmand AS

go@styrmand.no

Pål Godard

Gjøvik kommune

pal.godard@gjovik.kommune.no

GJØVIK KOMMUNE