Cyber threat intelligence and management decision-making behavior: Gathering data through agent-based simulations, cyber exercises and serious games

Erjon Zoto & Grethe Østby,

Information Security Management group

19-Nov-2025

Main goal of this presentation

- Get your attention
- Contact us

erjon.zoto@ntnu.no

grethe.ostby@ntnu.no

Cyberspace

Actors in cyberspace

Defense

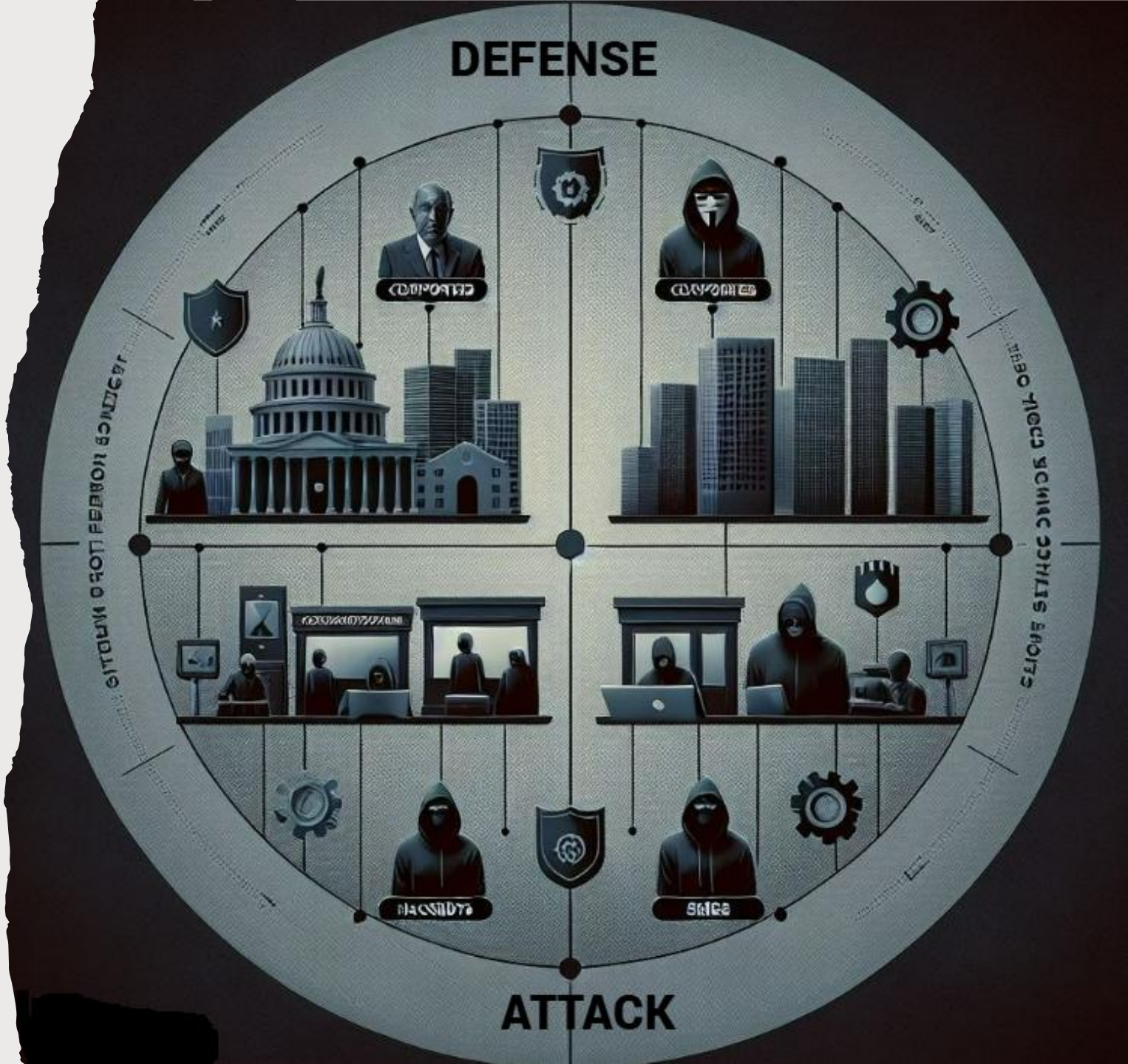
- State actors
- Coorporates
- SME-s

Attack

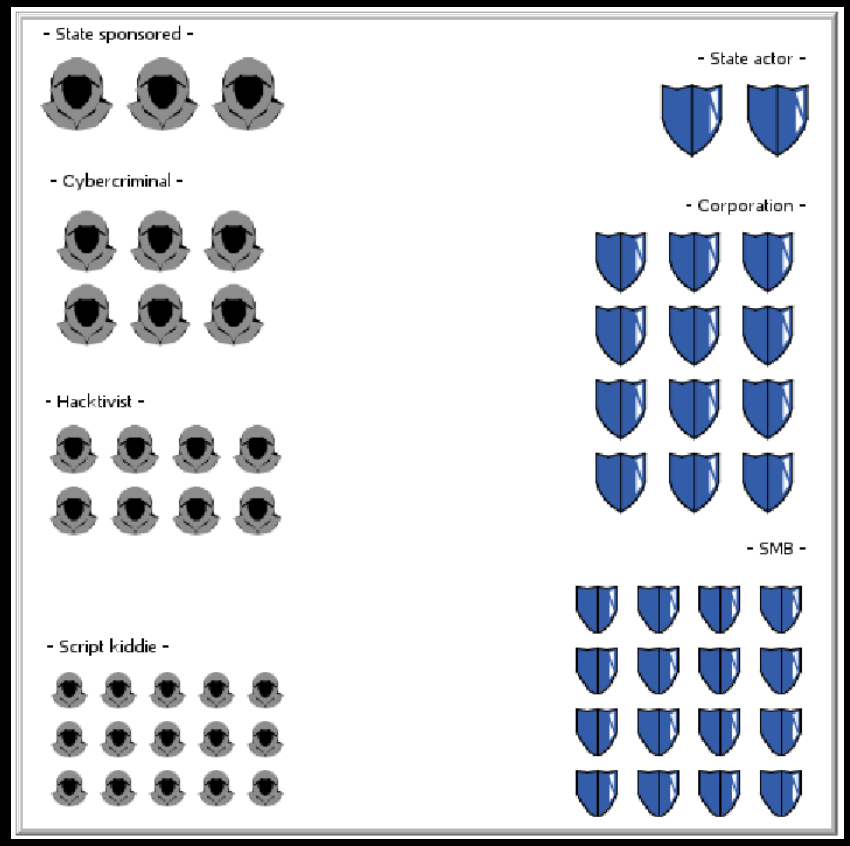
- State-sponsored
- Cybercriminals
- Hacktivists
- Script kiddies

Result

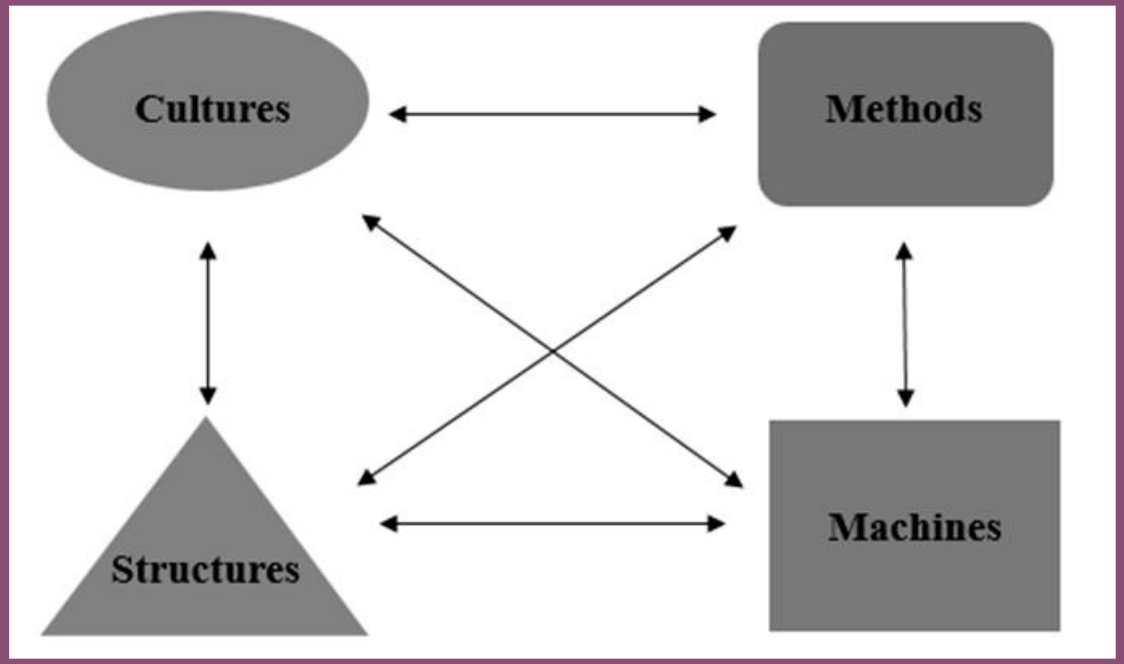
- Copilot



Cyberspace in CyberAIMs



Socio-technical approach



- "Adversarial thinking, as a process that considers the potential actions of the opposing force working against the desired result.
- "Systems thinking, as a process that considers the interplay between social and technical constraints to enable assured operations."

Agents and Attributes

Attributes

- Resources
  - Budget for activities in cyberspace
- Skills
  - Knowledge, tools and techniques
- Motivation

Levels

- Low to High
- Default

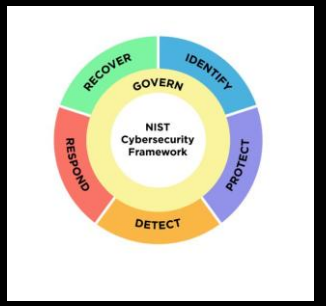
Agent count

- More agents from lower tiers

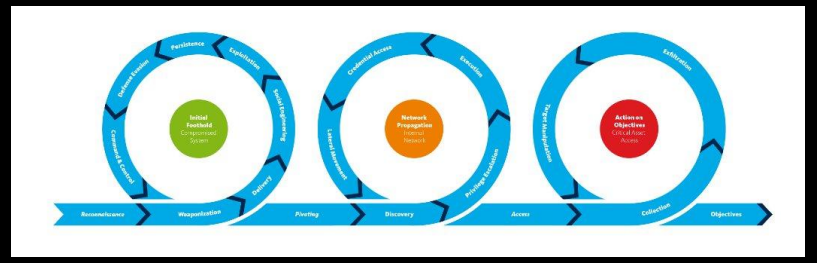
Strategies

Techniques and activities that an agent can allocate resources to

- Defense: *NIST CSF [7]*
  - IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER, GOVERN

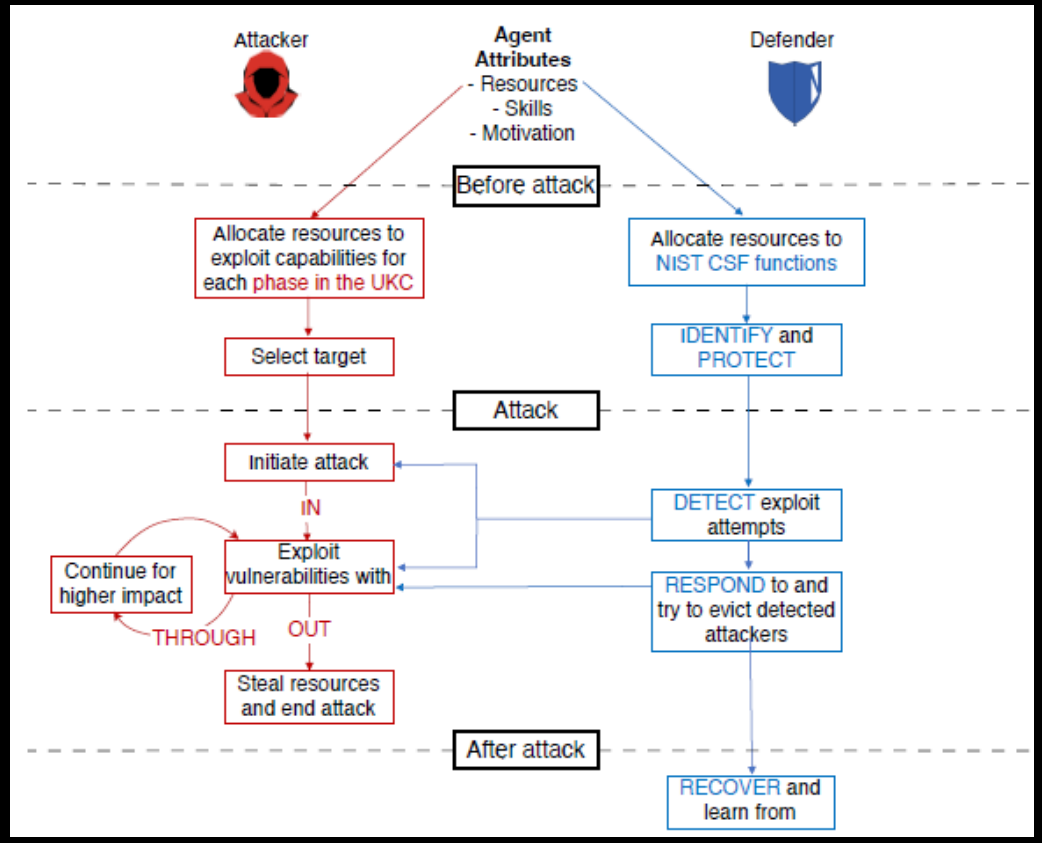


- Attack: *Unified Kill Chain [8]*
  - In, Through, Out



- Measuring costs: *The importance of Essential Security [9]*

Designing the tool

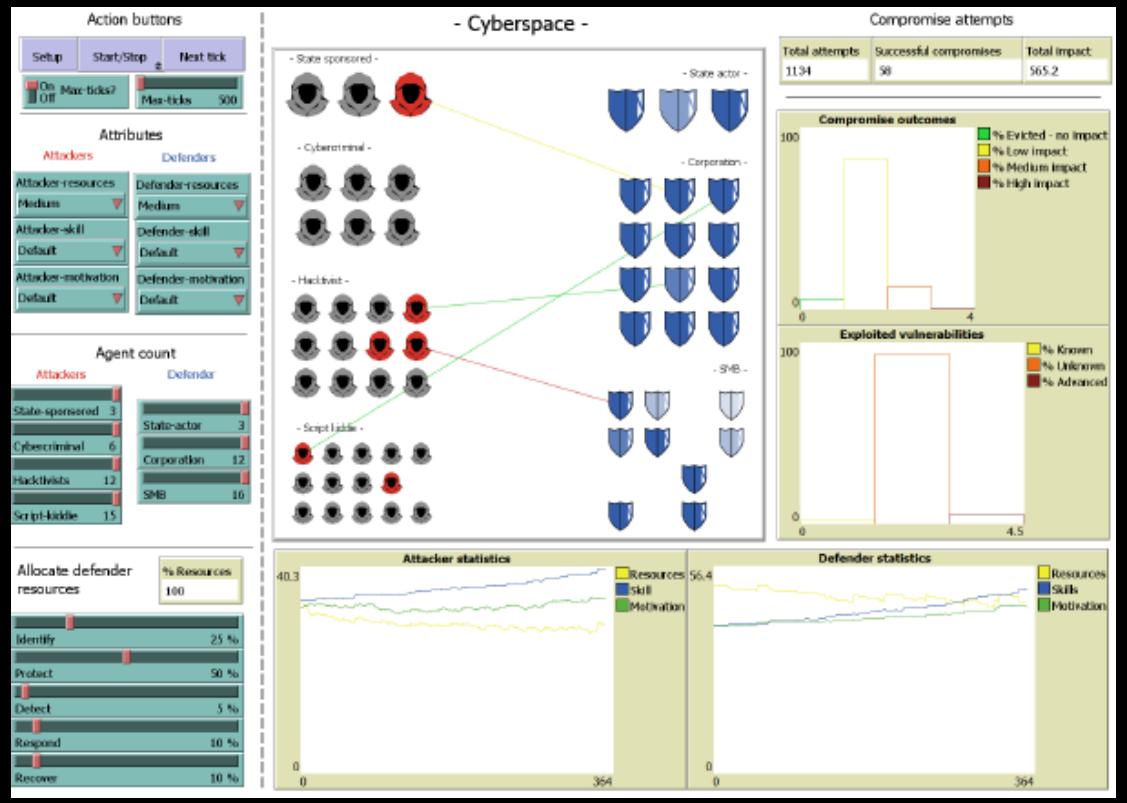


Interface

Adding monitors and charts

- Statistics
- Compromises
- Vulnerabilities exploited

Forming the puzzle



CyberAIMs 2025

Addressing Motivation

- Adding theoretical insights to Motivation
  - PMT
  - SDT
  - Schwartz theory (Theory of Basic Human Values)
  - …

Scenarios

attempt-count	18
compromise-count	1
low-impact-count	1
medium-impact-count	0
high-impact-count	0
total impact	5
known-vuln-count	0
unknown-vuln-count	2
advanced-vuln-count	0

Script kiddie vs Talk talk

attempt-count	5
compromise-count	3
low-impact-count	0
medium-impact-count	1
high-impact-count	2
total impact	87
known-vuln-count	0
unknown-vuln-count	5
advanced-vuln-count	5

Stuxnet

attempt-count	350
compromise-count	11
low-impact-count	10
medium-impact-count	0
high-impact-count	0
total impact	58
known-vuln-count	0
unknown-vuln-count	15
advanced-vuln-count	0

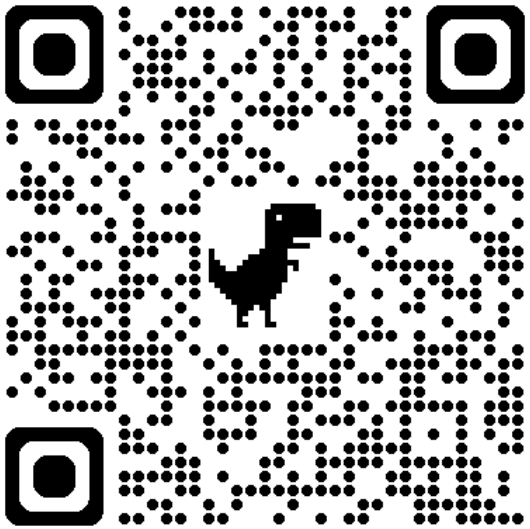
Playstation

Scenarios*

Østre Toten, 2021

		Østre Totens allocation	Optimal allocation
Input	Identify	5	20
	Protect	80	55
	Detect	5	5
	Respond	5	10
	Recover	5	10
Output	low-impact	0.03	0.79
	medium-impact	0.72	0.19
	high-impact	0.25	0
	total-impact	21.98	11
	eviction	0	0.02
	detection-attempt	4.55	5.92
	detection	0.26	0.35
	exploit-attempt	9.2	13.59
	exploit	2.88	2.54
	known-vuln	1.47	0
	unknown-vuln	1.41	2.45
	advanced-vuln	0	0

Student assignments: Risk management (DCSG2005)



Hva egner seg som oppgave?

I kurset begynner vi å få en ganske bred portefølje av oppgaver innen risikovurdering og sikkerhetsrevisjoner vi har løst. I de fleste tilfeller ender vi opp med gode resultater som kan benyttes senere. For eksempel:

- IKT systemer av ulike størrelser: Webapplikasjoner, SCCM/CFEngine, printløsninger, IAM, databus, samhandlingstjenester, skylagring, og klientsikkerhet, med mer.
- Digital sikkerhet i SMBer, eller seksjoner og avdelinger i større bedrifter
- Revisjoner mot eksisterende beste praksis og risiko (ISO27001/2, Normen for informasjonssikkerhet, etc.) for bedrifter
- Problemstillinger, som sikker håndtering av adminkontoer og livsløpet på brukere
- Diverse oppgaver innen fysisk sikkerhet og adgangskontroll
- (Ulike prosesser som forskningsprosessen og kvalitetsprosesser)

Det er et ganske bredt spekter av oppgaver vi kan gjennomføre og vi er alltid åpne for nye utfordringer. For at oppgaven skal være aktuell må den ha en tydelig IT komponent og en relasjon til digital sikkerhet. Vi i DCSG2005 er godt digitaliserte og geografi er stortsett ingen hindring for godt samarbeid i prosjektet. Alle forslag er velkomne.

Oppgave 8 – Risikovurdering av Public Cloud sammenlignet med egendriftet Server Rom / Senter

I en verden som blir stadig mer digitalisert, er det av største viktighet å forstå de forskjellige risikoene som er forbundet med ulike teknologiske løsninger. Dette forslaget til forskningsoppgave tar sikte på å vurdere risikoene forbundet med bruk av offentlige skytjenester sammenlignet med egendriftede serverrom eller datasentre.

Bakgrunn

- Data er en verdifull ressurs.
- Avgjørende å beskytte data effektivt og sikkert.

Forskningens Fokus

- Vurdering av sikkerhetsmekanismer i offentlige skytjenester og egendriftede løsninger.
- Inkluderer digitale, fysiske og geopolitiske aspekter.

Sikkerhetsstrategi

- Omfattende tilnærming som adresserer alle trusler og risikoer.
- Cyberangrep og sofistikerte datainnbrudd øker.

Mål

- Inspirere diskusjoner og forskning.
- Forståelse av sikkerhet for en tryggere digital fremtid.

Oppgave 9 – Risikovurdering av Github.com

I en verden som blir stadig mer digitalisert, er det av største viktighet å forstå de forskjellige risikoene som er forbundet med ulike teknologiske løsninger. Dette forslaget til forskningsoppgave tar sikte på å vurdere risikoene ved å benytte åpen kildekode tjenesten Github.com

Bakgrunn

•Deling og håndtering av utviklingsdata og kode er viktig

Forskningens Fokus

a) Hvordan vurderer dere risikobildet knyttet til bruk av Github
   a. Teknisk
   b. Organisatorisk
   c. Geopolitisk

b) Studenene kan gjerne ta utgangspunkt i Altinn sine åpne repositories på Github, men her ønskes det en objektiv vurdering rundt bruk av tjenesten. I tillegg til observasjon, og testing kan det være nyttig å se til de hemmelige tjenester sine åpne trusselvurderinger for å finne aktuell informasjon

Sikkerhetsstrategi

•Omfattende tilnærming som adresserer alle trusler og risikoer.

Mål

•Inspirere diskusjoner og forskning.
•Forståelse av sikkerhet for en tryggere digital fremtid.

Education, training and exercises

how to be cyber-literate, and more specific information security cyber-literate

Grethe Østby

- Exercises at the Norwegian Cyber Range/NTNU in Gjøvik
- Student studies in the Introduction to information management course

Combined crisis management and incident response exercises

NYHETER 17

SAMLET: *Hele ledelsen i Gjøvik kommune møtte inn i rollene når det ble simulert et stort og omfangsrikt dataangrep mot kommunens tjenester.* FOTO: HENRIK HOVI

Krisen er inntruffet: – Denne type øvelse har aldri blitt gjennomført

Denne uken gjennomfører Gjøvik kommune en fullskala cyberangrep øvelse.

HENRIK HOVI
henrik.hovi@oya.no

Aldri før har det blitt gjennomført i vårt langstrakte land: Nå skjer det i kjelleren til et av de mange byggene ved NTNU i Gjøvik.

Bak en lukket dør sitter hackerne. Omtalt som «red teams». Krisestaben og IKT-avdelingen til Gjøvik kommune jobber for å respondere best mulig på det simulerte cyberangrepet. I et annet rom sitter «spillstaben» – de som setter opp scenarioet som fort kunne vært realitet.

Akkurat nå er det øvelse.

– Denne type øvelse er verken forsøkt på eller gjennomført noe steder så vidt vi det. Dette er helt nytt. Det er en ny måte å øve på, forteller Grethe Østby, som er prosjektleder og ansatt i Styrmand AS.

Haugtun er rammet

Varmen på Haugtun er borte. Barnehagene er stengt, for de mangler fjernvarme. Personopplysninger er også på avveie.

Den tilhenkte krisen har inntruffet, og nå jobber kriseledelsen og IKT-avdelingen sammen for å minske konsekvensene av dataangrepet. Gjøvik kommune må løse dette så raskt som mulig.

– Vi som kommune øver nå på å håndtere kriser som kan oppstå. Det her er veldig viktig. De siste årene har vi fått øvd oss på kriser med sværer Hans og pandemien. Men hver krise er unik, og det er variert fra gang til gang hva som oppstår i den enkelte tjeneste, forteller varaordfører Torvild Sveen, som var til stede under øvelsen.

Torvild Sveen har akkurat gjennomført en pressekonferanse i øvelsen. Der har han informert Gjøviks innbyggere om hvilken situasjon byen står i. Det som foregår på NTNU i disse dager, blir tatt på alvor.

FORNØYDE: *Grethe Østby og Pål Godard er fornøyde med øvelsen så langt.* FOTO: HENRIK HOVI

– Det er som å være med på «gamming». Det blir reelt når du står i det. Når vi sitter der, går alle inn i de rollene man har og det blir alvor. Vi ser at alle er om bord og tar oppgavene sine alvorlig. Det er slik at når krisen er der må vi opptre og være ute, forteller Sveen.

Her hva Torvild Sveen sier om øvelsen i videoen under.

Veldig viktig

De siste årene har vi sett flere eksempler på cyberangrep mot norske kommuner. Lokalt er det nærliggende å tenke på da Østre Toten ble rammet i 2021.

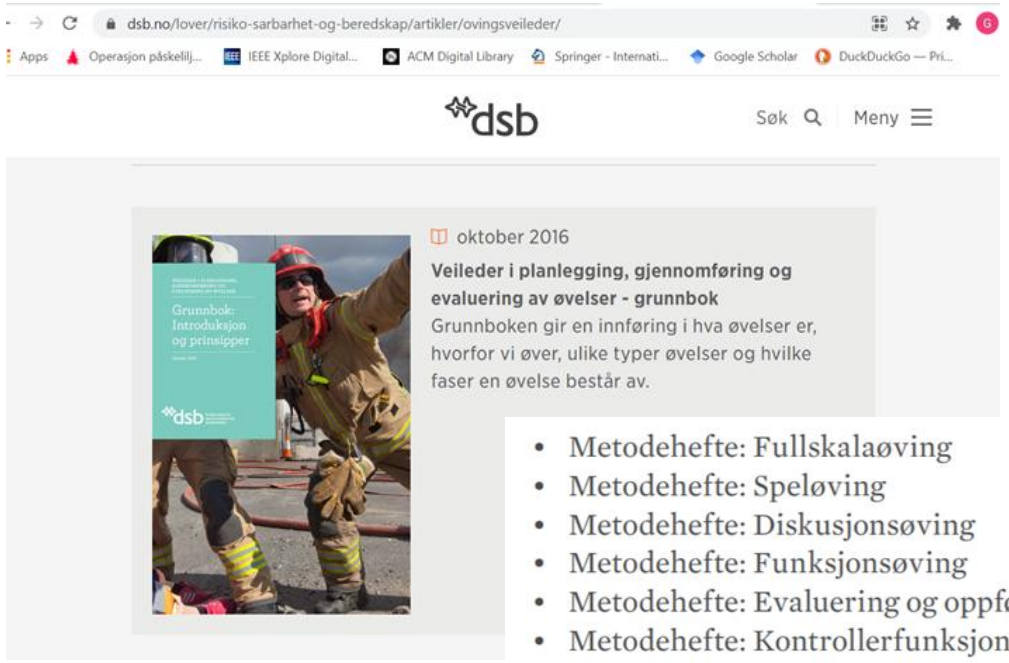
– Hvis vi ser på rapportene fra da Østre Toten ble rammet, var det jo slik at de ikke hadde noen oversikt over hverandre i det hele tatt. Det vi søker, og ønsker å oppnå, er å få den følelsen av virkelighet på kroppen. Såsn at man er forberedt når det skjer, forteller Østby.

Angrep på kommuner og bedrifter kommer til å skje i framtida.

– Det er ikke såsn at man kan forhindre alle hackerangrep i framtiden. Det kommer til å skje, men når det skjer handler det om å være klare, legger rådgiver Pål Godard i Gjøvik kommune til.

– Det vi bygger her er jo noe andre kommuner kan komme å få øve på senere. Vi håper at flere kommuner i Innlandet ønsker å teste det her i framtiden, sier Godard.

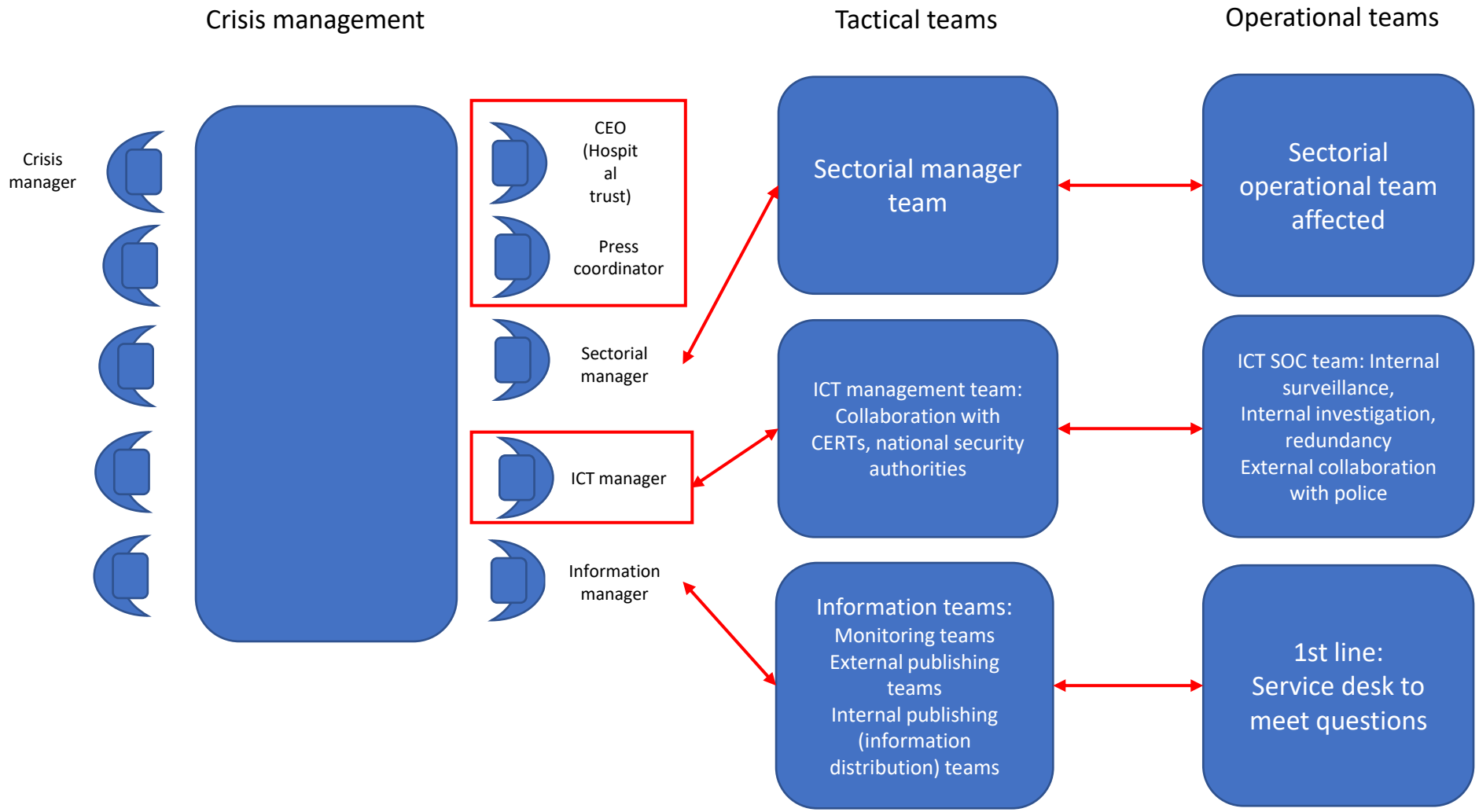
Guidance's for executing exercises



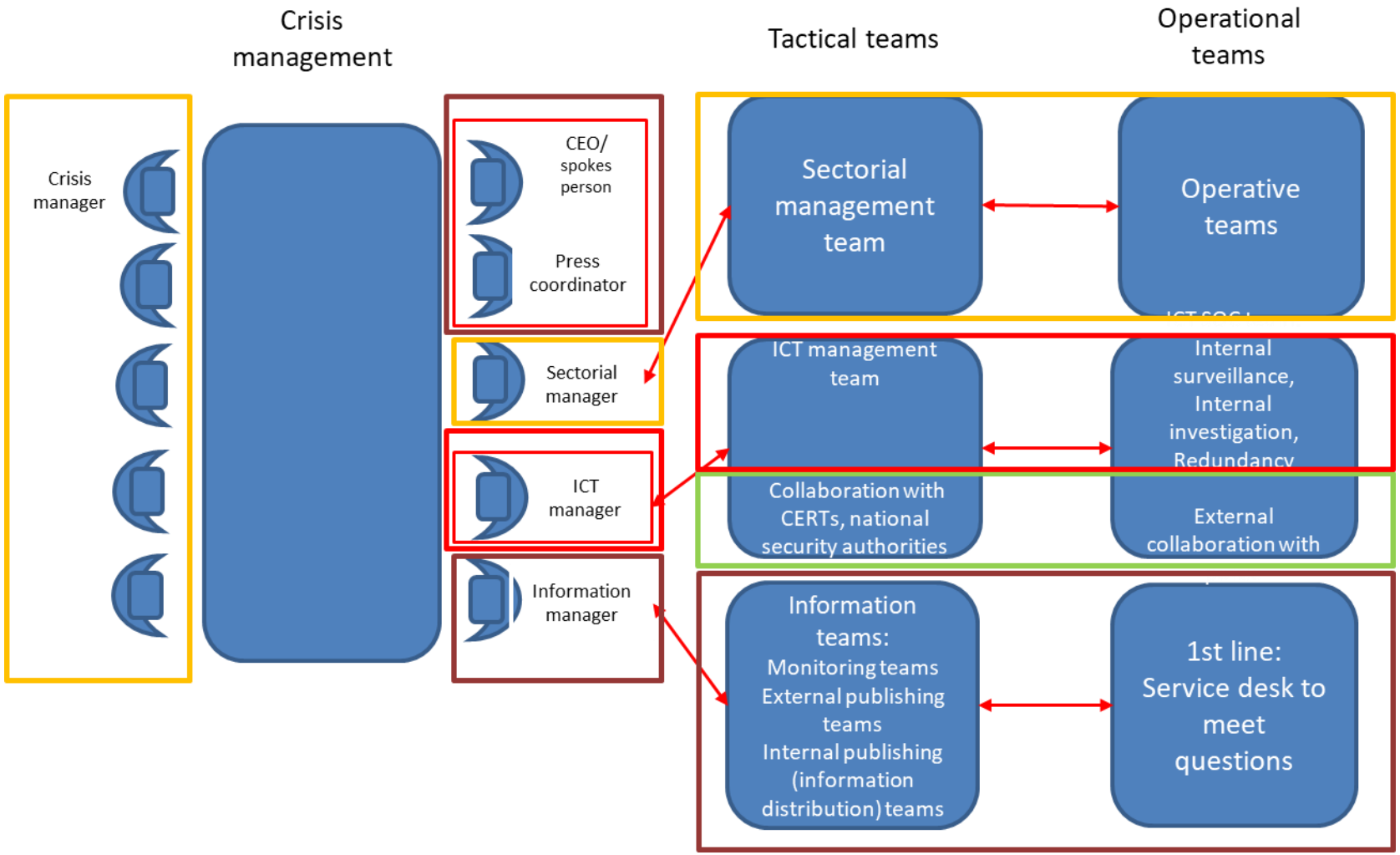
- https://www.dsb.no/lover/risiko-sarbarhet-og-beredskap/artikler/ovingsveileder/
- https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

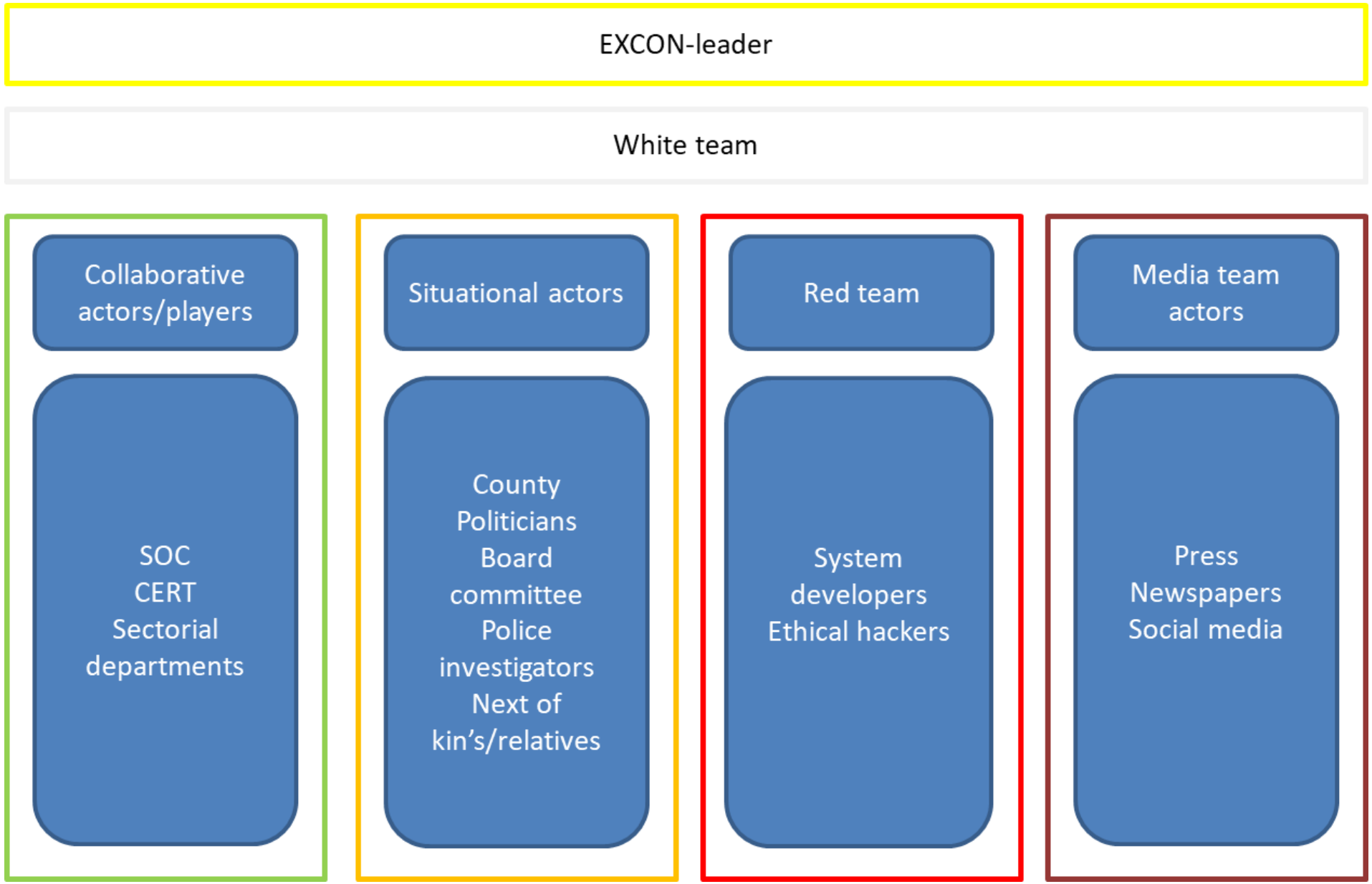
Socio-technical improvement process

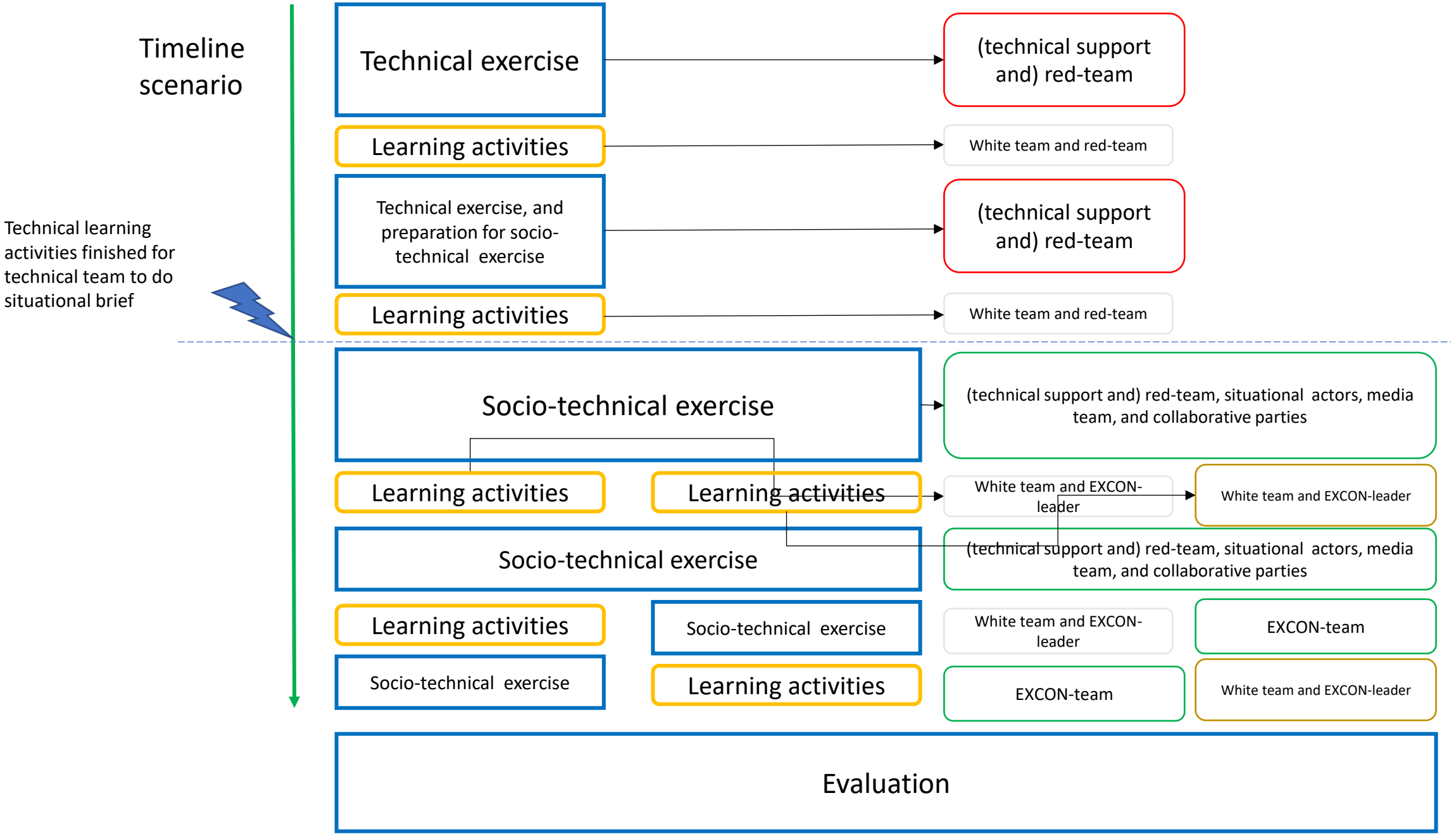
Cyber crisis management roles



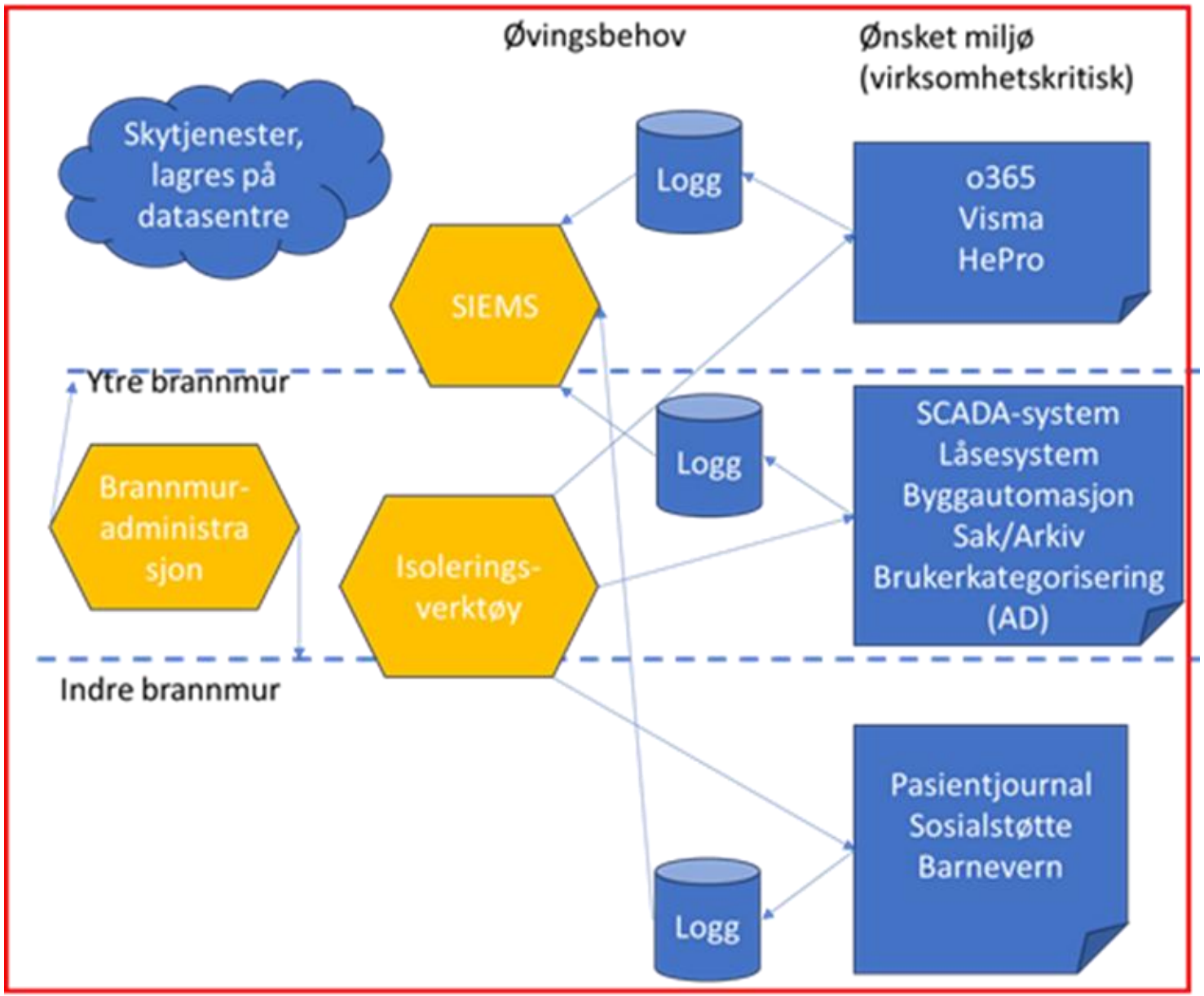
How can we train the roles attending the exercise?



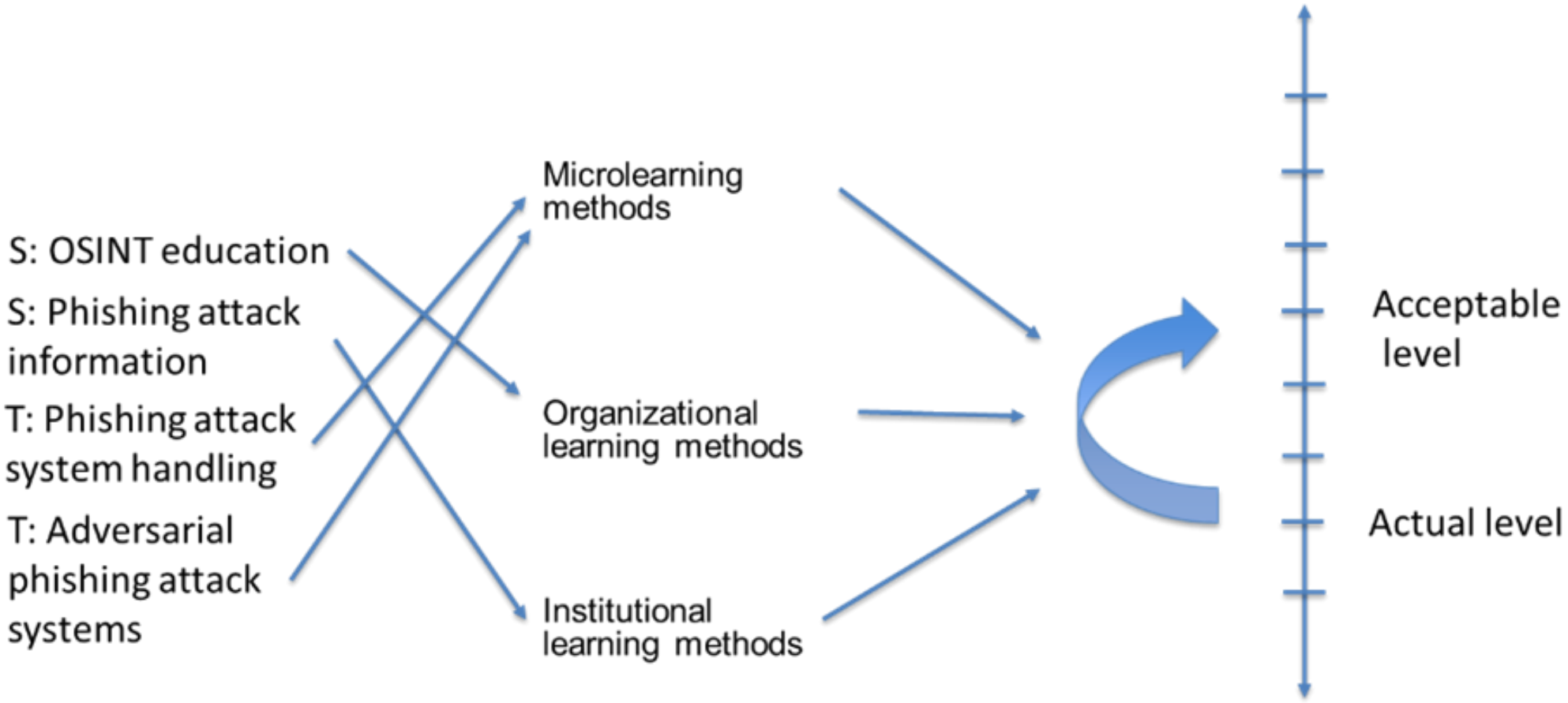

EXCON-leader
White team
Collaborative actors/players
SOC
CERT
Sectorial departments
Situational actors
County Politicians
Board committee
Police investigators
Next of kin's/relatives
Red team
System developers
Ethical hackers
Media team actors
Press
Newspapers
Social media


Timeline scenario
Technical learning activities finished for technical team to do situational brief
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
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

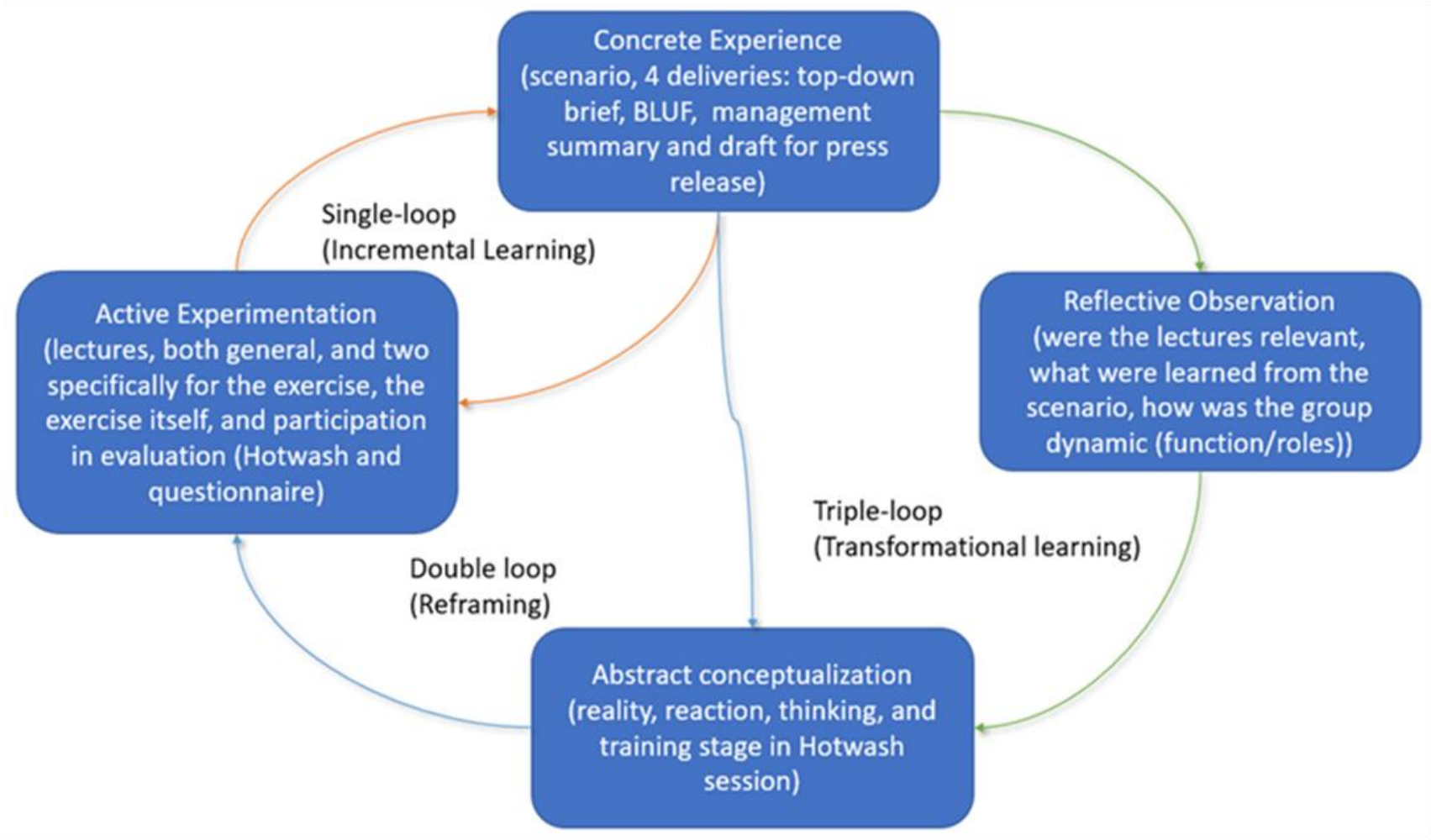
What could we possibly execute?



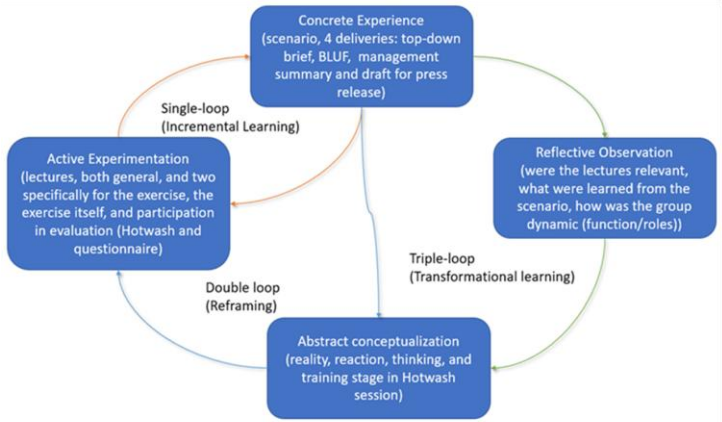
Towards a maturity improvement process



Learning loops – recent studies



Exercises and research – Guro B. Olsborg



Socio-technical study (questionaire) before the exercise.
Socio-technical action research (as instructors) during the exercise.
Evaluation on exercise-goals.
What has happened 1 year after the exercise? What types of learning do we see? Single, double or triple-loop?
Socio-technical study (same questionaire) one year after.
Interviews 1 year after.

Pressekonferanse sto også på agendaen da det skulle øves på alle aspekter ved en reell krisesituasjon.

Varaordfører Torvild Sveen mener at det er kun én måte å stå i dette på på stikk, og det er nettopp ved å øve.

Pål Godard og Grethe Østby var med på banebrytende øvelse.

Her satt hele kriseledelsen til kommunen og trente på en potensiell fare.

Forsker ved NTNU, Guro Bråten Olsborg, reagerer på at en slik øvelse ikke har blitt gjennomført tidligere.

Gjøvik første ute med *unik* øvelse

Som de første kommunene i landet, gjennomfører Gjøvik, Nordre Land, Søndre Land og Vestre Toten fullskala øvelser på cyberangrep mot hver av kommunene.

Nora Klöppe Brennhagen
nora@gjovik-blad.no

Rådgiver i Gjøvik kommune, Pål Godard, forteller at målet med beredskapsøvelsene er at kommunene i distriktet skal være forberedt på den dagen et reelt dataangrep kommer.

Det som er spesielt med denne øvelsen er at de forbereder seg på det tekniske ved et angrep, samtidig som de øver på å håndtere angrepet for kommunen.

– Det er veldig sjeldent at en kommune øver med mer enn bare kriseledelsen. Her øver IT-folka samtidig som vi har bygget opp en liksom-kommune i IT-systemet, hvor vi angriper og forsvarer den, sier Godard.

Øvingsarenaen for beredskapsøvelsen er Norwegian Cyber Range ved NTNU Gjøvik, som i dette prosjektet har utviklet det tekniske øvingsmiljøet til å simulere IT-miljøet i en typisk norsk kommune.

Krever øvelse

Øvelsen, som kun var basert på en oppdiktet hendelse, startet med en brist i fjernvarmetilførselen til et par bygg på Gjøvik, samtidig som det kom opplysninger om at det hadde skjedd noe med datasystemene i kommunen.

I dette scenarioet som, i reelle kriser, handler det alltid om å skaffe overblikk og finne ut hvor man skal sette inn støtet, forteller Gjøviks varaordfører Torild Sveen.

– Det er dette vi trener på å håndtere, sier han og legger til at de på Gjøvik har gjort seg noen gode erfaringer de siste par årene både med pandemi og ekstremværet Hans, hvor de har sittet nye sammen i krisestab, noe han forteller er gull verdt også i en slik situasjon.

– Denne øvelsen viser også at enhver situasjon og hendelse er nytt i seg selv. Selv om vi vet om ulike mekanismer, så må vi handle annerledes fra gang til gang. Det er kun én måte å kunne stå i dette på slikt, og det er nettopp ved å øve, sier Sveen.

Spesielt utsatt

Ifølge Nasjonal sikkerhetsmyndighets (NSM) «Nasjonalt digitalt risikobilde for 2022», er norske kommuner blant de som er spesielt utsatt for ulike typer cyberangrep. Kommunene i Gjøvikregionen er ekstra interessante mål med sin nærhet til forsvarsindustrien. Cyberforsvaret og informasjonssikkerhetsmiljøet ved NTNU.

De siste årene har gitt oss mange eksempler på cyberangrep mot norske kommuner, deriv Østre Toten.

Torvild Sveen forteller at de har denne hendelsen friskt i minne når de nå øver på et potensielt dataangrep.

– De erfaringene og det arbeidet som ble lagt til grunn i Østre Toten er erfaringer som vi tar med oss videre. Selv om Østre Toten ble rammet, så man at deres viktigste ressurs var folk på jobb, sier Sveen som har stor tro på at Gjøvik kommune har den kunnskapen som trengs for å håndtere en potensiell fare.

– Systemer kan falle sammen og data kan bli borte, men vi har fortsatt 2.300 ansatte i Gjøvik med kunnskap og kompetanse som er istand til å gjøre en forskjell. Den kunnskapen forsvinner ikke selv om et datasystem skulle bli borte, sier han.

På spørsmålet om han er bekymret for at kommunen skal bli rammet av et dataangrep, svarer Sveen følgende:

– Det er klart at teusselbildet raudt oss viser at dette kan ramme oss hver dag, og det er klart at det hver dag er noen som prøver å komme seg inn i systemene våre, men vi har en oppegående IKT-avdeling. Likevel er det klart at alt er sårbart og derfor er denne øvelsen viktig, sier han.

Banebrytende

Grethe Østby er prosjektleder for å etablere denne typen øvelser, noe som baserer seg på hennes tidligere doktorgrad i temaet.

Hun forteller at en slik øvelse aldri før har blitt gjennomført i Norge.

– Dette er banebrytende og helt nytt. Det er en ny form å øve på. Vi er opptatt av at dem som kommer hit skal lære noen læringsobjekter i løpet av hendelsen og hvordan man håndterer ulike systemer som brannmurer og isolering og nedstengning av systemer. Kriseledelsen vil være tilstede og ta beslutninger som følge av at systemer har blitt stengt ned, sier Østby.

Realistisk

Sveen forteller at selv om de under øvelsen er godt klar over at øvesituasjonen kun er et spill, er de godt innforstått med at det likeså godt kunne ha vært en realistisk situasjon.

– Enhver beslutning vi tar om å for eksempel stenge en barnehage, får konsekvenser ikke bare for ansatte i barnehagen, men også foreldre og bestefriedre som er i jobb. Enhver krise påvirker liv, sier han og legger til:

– Det samme gjelder sånn som nå, hvor vi blant annet ser på hva som skjer dersom det skulle skje noe med strømforsyningen og det skulle bli kaldt på Haugtun. Da må vi tenke på hva vi skal gjøre dersom vi må evakuere samtlige beboere på Haugtun, sier han.

Skal dele erfaringer

I tillegg til kommunenes egne ansatte, deltar også personell fra NTNU, Statsforvalteren i Innlandet og Tienoléwy med på øvelsen. Forskere fra NTNU bruker øvelsene til å forske på læringseffekten av slike øvelser.

Andre kommuner som ønsker å gjennomføre tilsvarende øvelser, kan gjenbruke metoder og maler fra disse øvelsene, samt simulasonsmiljøet ved NTNU.

Først ut til å trene på krisesituasjonen var Gjøvik kommune, før de andre kommunene står for tur i nær fremtid.

Forsker ved NTNU, Guro Bråten Olsborg har vært med på øvelsen som en del av spillstaben til de som arbeider teknisk, hvor hun har fulgt øvelsen både som forsker og som en reell aktør.

Olsborg reagerer på at en slik øvelse ikke har blitt gjennomført tidligere.

– Jeg synes det er overraskende. Forskningsmessig tror jeg det er viktig at vi går inn i dette med åpne spørsmål siden vi vet så lite om det fra før av. Det er viktig å se på om en slik øvelse gir læring, hva slags læring det gir og i hvilken sammenheng denne læringen blir satt i, sier hun.

Kommunen har fått 1,2 millioner kroner fra Statsforvalteren i Innlandet og til å gjennomføre beredskapsøvelsene, i tillegg til at kommunen selv har gått inn med egne midler i prosjektet.

Master in Information Security

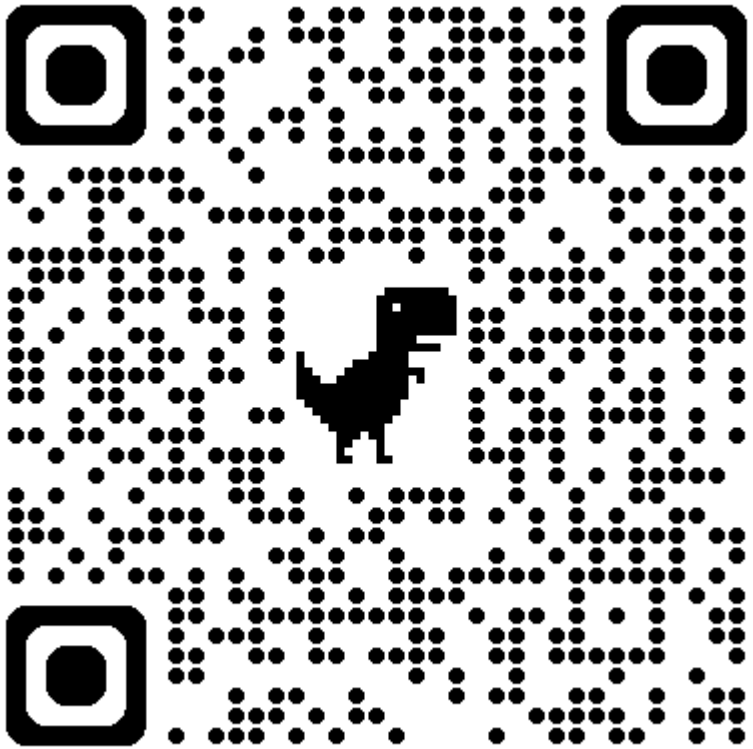
Introduction to information security management - 4115

Student studies: Book-projects

Management and responsibiliy aspects

Are they relevant?

Collaboration?



Geoffrey Hinton shared an important message about potential risks with artificial intelligence

AI adversarial thinking

Book 7 – Adversarial thinking, AI – how does threat actors apply AI to hack information security components

"Intelligent Intrusion Detection Systems (IDS), automated cyber defense, network monitoring and surveillance as well as secure software development and orchestration are all examples of assets that are reliant on machine learning (ML) and automation. These applications are (however) of considerable interest to malicious actors due to their importance to society." (Hartman & Steup, 2020) In addition, adversarial thinking about the AI-system themselves, if such could be a threat, learning from "a world where AIs can be hackers" (Schneier, 2021), would be of interest in terms of 'when should we just pull out the plug'? Please also see video of God Father of AI below (first in the line of references).

Thereby, 3 research questions are suggested:

Research question 1: What scientific literature provides relevant suggestions to raise knowledge (digital literacy) on hacking adversaries against AI-models, and from AI-models themselves?

Research question 2: How would AI-models, and what state-of-the-art AI-models would be able to develop malicious hacking today?

Research question 3: How can 'adversarial thinking' be used to understand the possible development of malicious AI-models to exploit today's system-security?

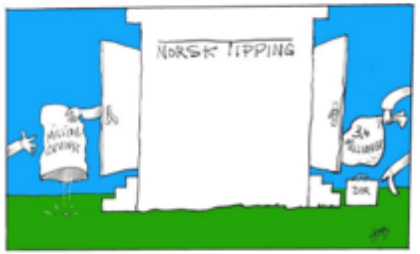
Input validation

Book 3 – Manage 'input validation' and system-vulnerabilities that may cause unrepairable damage

Input validation is one of the most common vulnerabilities when web-applications are developed, as web-applications also are frequently targeted by attackers (Scholte et. al., 2012). Thereby, both specification-based tests and code-based tests are suggested to meet the challenges, and thereby "extract path partition and input conditions from code for testing input validation" (Liu & Tan, 2008)

> "The path partition can be used to design white-box test cases for testing input validation. It can also be used to measure the coverage of input validation testing. The valid and invalid input conditions recovered can be used to check against the specifications and aid the test suite design in blackbox testing." (Liu & Tan, 2008)

Those tests may not, however, be able to manage insider threats and human failures. Friday 23. of June, Norsk Tipping failed to code the input from Eurojackpot correctly and coded the input multiplied with 100 instead of divided by 100. That is, the code itself had not been tested.



OWASP top 10 (OWASP, 2021) and SANS 25 software errors (SANS, 2025) management systems are suggested to meet input validation vulnerabilities (Fadlalla & Elshoush, 2023), but possibly, those may overlook insider threats and insider human failures.

To meet the following challenges, 3 research questions are suggested:

Research question 1: What relevant socio-technical (not just technical) scientific literature (proven results) may meet the challenges presented?

Research question 2: What state-of-the-art frameworks (like OWASP and SANS) may provide information security management support, and how may the frameworks specifically support the insider threats and insider human failures?

Research question 3: What methods can be developed to avoid insider threats and insider human failures to input validation?

1. september kl. 10:43

Lotteritilsynet utreder nytt regelverk

Lotteritilsynet opplyser i en pressemelding at de har fått i oppgave å utrede et nytt regelverk.

Regelverket skal stille krav til bruk av uavhengige testinstitutter, for å teste at spillene er gode nok.

– Det er for å forebygge flere feil, og vi ser det er helt nødvendig å få på plass, sier direktør Atle Hamar i Lotteritilsynet.

Exit strategies

- What happens in
  - The USA
  - The Ukraine
  - Israel

...all tech-countries

Book 5 – Exit strategies in uncertain times

The invalidation of the EU-US privacy shield in 2020 (Cory et. al., 2020) and recent uncertainty of the Data Policy Framework in 2025 (Henthorn-Iwane, 2025) have challenged data privacy protection between Europe and USA.

It is not always transparent how the data is shared across borders, especially for services targeted at private individuals. Institutions and organizations have some degree of control, dependent on services used and subscription models, but they may not have the ability to protect citizens and employees, and exit-strategies are considered. Therefore, e.g., 'the right to be forgotten' and other legislations to protect data would require extra attention in the transition period. Exit strategies must be developed to support such transitions, and a huge number of risks must be considered.

To meet these challenges 3 research questions are suggested:

Research question 1: What risks must be considered to prepare for privacy protection exit strategies?

Research question 2: What relevant scientific literature about exit strategies is relevant to understand the necessary steps in such transitions?

Research question 3: What methods can be developed to support privacy protection exit strategies?

And what about

Book 1 – Diia, a Ukrainian public friendly service - accessibility and vulnerabilities in times of war

Book 2 – Information security responsibility in and management of system-security in AI-models

Book 4 - ISO-certification (and other types of certifications) requirements to start-up companies

Book 6 – Information security training narratives – what can we learn from narratives, and how can we induce triple-loop-learning to make actual changes to the level of security in critical infrastructures?

Book 8 – Attacks on water-supply-systems – are we tested? How to understand govern threat actor organizations

Book 9 - Misinformation and manipulation, wanted or unwanted – how to manage information security in relevant media channels

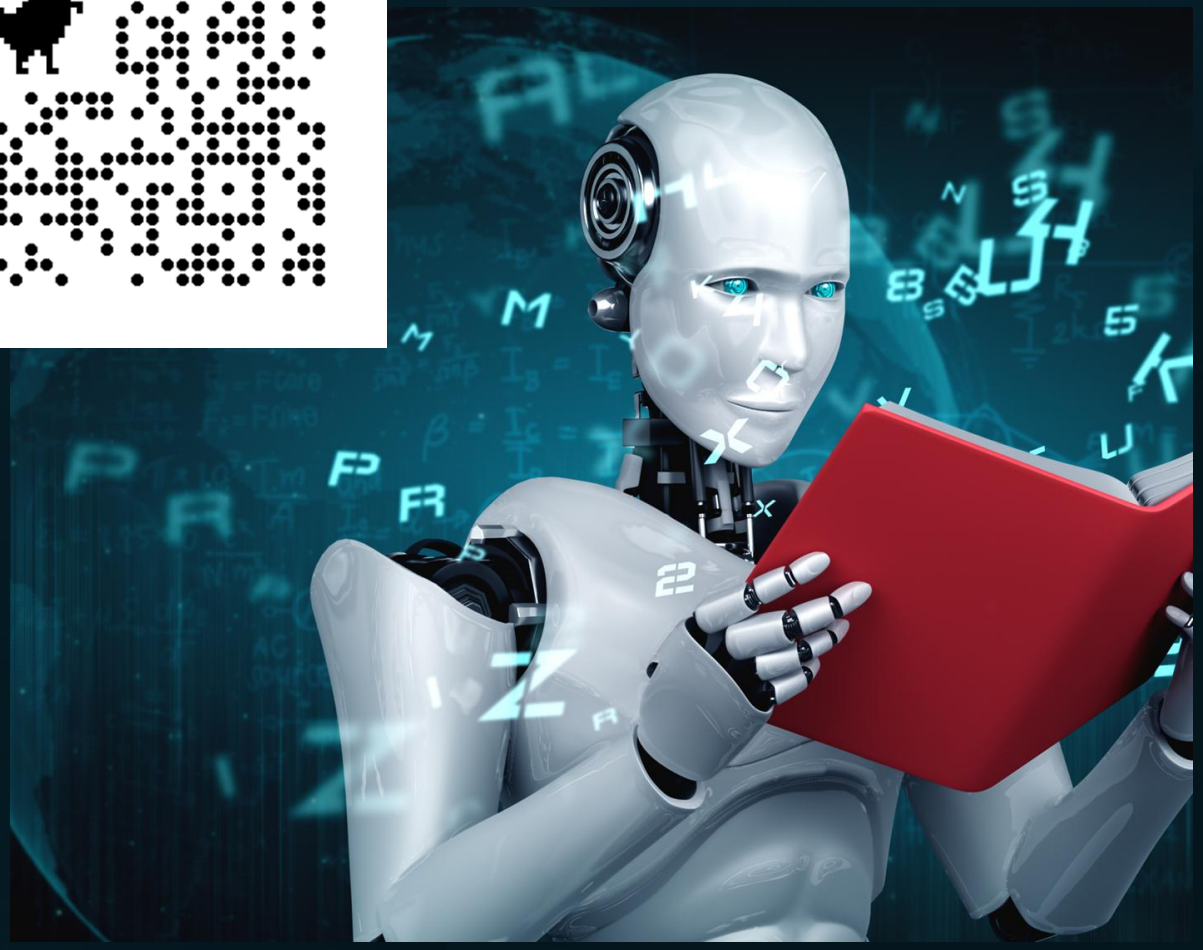
Book 10 – Espionage – research, health- and personal information, and political decisions and emergency- and crisis management abilities

Book 11 – Vulnerabilities in food-supply chains – how may societies be affected?

Book 12 – Value chain attacks, how to prepare for and manage value chain risks

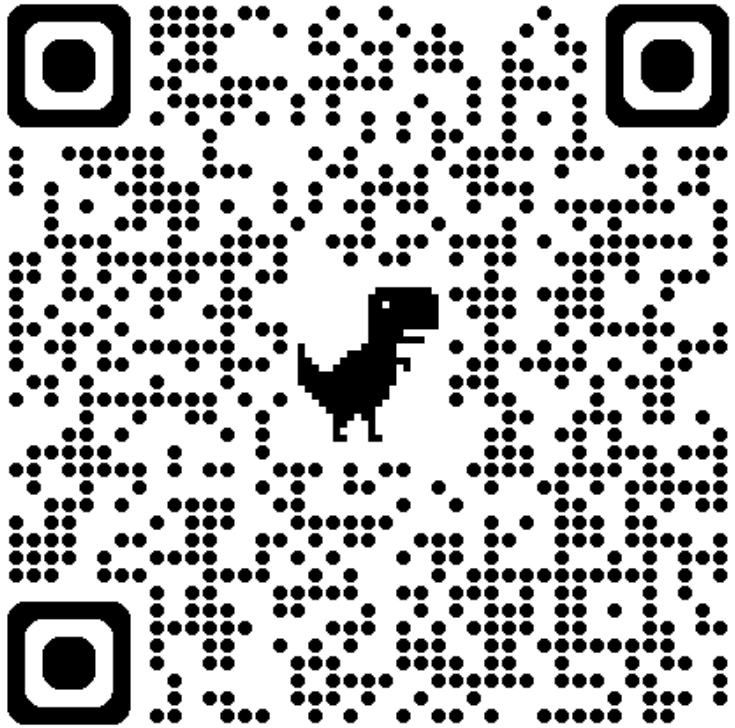
Book 13 - Cyber security to space technology – how to manage and collaborate with rocket and space communities within the content of secure testing and launch of new space technologies

Do you have an idea?

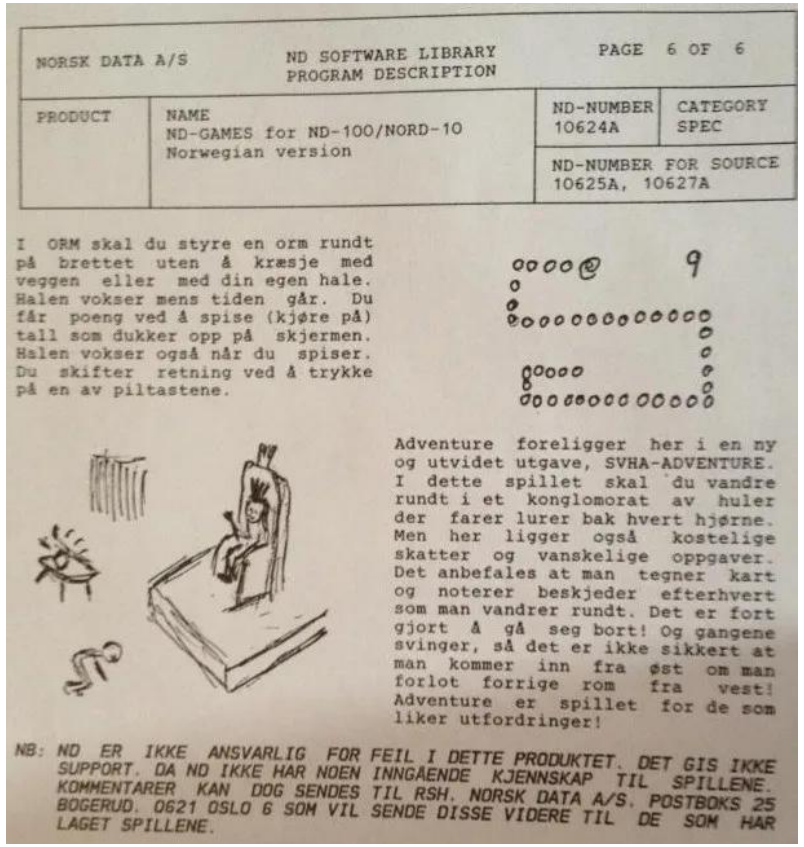


Questions

- Which of the topics presented would be relevant to explore further with your organization?
- What management topics (book projects) do you find relevant to be involved in?
- Suggestions on additional topics (book projects) do you suggest we should explore?
- Suggestions on risk assessment cases related to your organization/partners…?



Thank you for your attention!



NORSK DATA A/S — ND SOFTWARE LIBRARY PROGRAM DESCRIPTION — PAGE 6 OF 6

PRODUCT	NAME	ND-NUMBER	CATEGORY
	ND-GAMES for ND-100/NORD-10 Norwegian version	10624A	SPEC
		ND-NUMBER FOR SOURCE 10625A, 10627A	

I ORM skal du styre en orm rundt på brettet uten å kræsje med veggen eller med din egen hale. Halen vokser mens tiden går. Du får poeng ved å spise (kjøre på) tall som dukker opp på skjermen. Halen vokser også når du spiser. Du skifter retning ved å trykke på en av piltastene.

Adventure foreligger her i en ny og utvidet utgave, SVHA-ADVENTURE. I dette spillet skal du vandre rundt i et konglomorat av huler der farer lurer bak hvert hjørne. Men her ligger også kostelige skatter og vanskelige oppgaver. Det anbefales at man tegner kart og noterer beskjeder efterhvert som man vandrer rundt. Det er fort gjort å gå seg bort! Og gangene svinger, så det er ikke sikkert at man kommer inn fra øst om man forlot forrige rom fra vest! Adventure er spillet for de som liker utfordringer!

NB: ND ER IKKE ANSVARLIG FOR FEIL I DETTE PRODUKTET. DET GIS IKKE SUPPORT. DA ND IKKE HAR NOEN INNGÅENDE KJENNSKAP TIL SPILLENE. KOMMENTARER KAN DOG SENDES TIL RSH, NORSK DATA A/S, POSTBOKS 25 BOGERUD, 0621 OSLO 6 SOM VIL SENDE DISSE VIDERE TIL DE SOM HAR LAGET SPILLENE.

Norway’s first adventure game

You are all welcome to the ISM Partner Christmas Lunch: 12th Dec, 11:00-14:00, Oslo

*The **Information Security Management** research group will be holding a Christmas Lunch for all Partners at the CityBox Hotel.*
***Goal:** Discuss Information Security Management Education and Research for Norway for the coming year!*

*Also a chance to meet the **Norwegian Cyber Rangers** 2026 team preparing for next year's Cyber 9/12 Challenge*

Find out who has been naught and nice

What's New
What's Old
What's Next

11:00-14:00
Prinsens gate 6, 0152 Oslo

Contact: stewart.kowalski@ntnu.no; erjon.zoto@ntnu.no;

Atlantic Council

INSIGHT EVENTS ACTV ISSUES REGIONS EXPERTS ABOUT DONATE

Cyber Statecraft Initiative

Cyber 9/12 Strategy Challenge

The Cyber 9/12 Strategy Challenge is an annual cyber policy and strategy competition where students from across the globe compete in developing policy recommendations tackling a fictional cyber catastrophe.

https://www.linkedin.com/pulse/på-innsiden-av-en-cyber-challenge-ntnuigjovik-mokxf/

Search

Home My Network Jobs Messaging Notifications Me For Business Try Premium for SEK0

Studenter ved NTNU deltok denne våren i Geneva Cyber Strategy Challenge.

På innsiden av en cyber challenge

NTNU in Gjøvik (Norwegian University of Science and Technology)
1,593 followers

July 8, 2025

Kritiske satellitter sender ut feilsignaler som truer nødkommunikasjon, landbruk og energiproduksjon. En intern ansatt står bak, og USA vurderer militær respons for å stanse angrepet.

Hva gjør dere? Dere har 15 minutter.

Comments

47 · 2 comments · 3 reposts

Like Comment Share

Add a comment...

Most recent

Freddy Murre • 1st
Helping Orgs Apply Intelligence Tradecraft...
3mo

Det var utrolig gøy å være medveileder for denne kjempeflinke gjengen. At de havnet på 2. plass er helt klart fortjent

Show translation

Like · 1 | Reply

Christoffer J. Falchenberg • 2nd
Cybersecurity Analyst | Digital Forensics (G...
4mo

Jeg ringer alltid Tinius Presterud når kritisk rominfrastruktur er under angrep.

Show translation

Like · 2 | Reply

Messaging

[(19) På innsiden av en cyber challenge | LinkedIn]

digi.no

Ledige stillinger Nyhetsbrev Nyhetsstudio Tips oss Innlogget Meny

NTNU-lag gjorde det skarpt i internasjonal cybersikkerhetskonkurranse

Skulle løse en situasjon hvor kommunikasjonssatellitter var blitt kapret av hacktivister.

Lytt til artikkelen 2m

References - CyberAIMs

[1] Engesvik, S. L. Lindstøl, A. Meinich, A. H.: Addressing Agents' Strategies in a Cyberwar Simulation, *NTNU Open*, 2024

[2] N. Ben-Asher and C. Gonzalez, "Cyberwar game: A paradigm for understanding new challenges of cyber war," in Cyber Warfare: Building the Scientific Foundation, S. Jajodia, P. Shakarian, V. Subrahmanian, V. Swarup, and C. Wang, Eds. Cham: Springer International Publishing, 2015.

[3] Kowalski, S. IT Insecurity: A Multi-disciplinary Inquiry. Stockholm University

[4] Flipping the economics of attacks, Webinar, Traverse City, 2016. [Online]. Available: https://www.paloaltonetworks.com/research/apac-ondemandwebinar-2016-ponemon-flipping-the-economics-of-attacks (visited on 01/23/2024).

[5] Lillian Ablon, Martin C Libicki, and Andrea A Golay. Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation, 2014.

References - CyberAIMs

[6] U.Wilensky, Netlogo, Evanston, Illinois, 1997. [Online]. Available: https://ccl.northwestern.edu/netlogo/ (visited on 03/15/2024).

[7] C. Pascoe, S. Quinn, and K. Scarfone, “The nist cybersecurity framework (csf) 2.0,” 2024.

[8] P. Pols, “The unified kill chain,” Tech. Rep., 2023. [Online]. Available: https :/ /www . unifiedkillchain. com/ assets /The-Unified-Kill-Chain.pdf (visited on 0 4/15/2024).

[9] “Cis critical security controls v8,” 2023, This work is licensed under Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License.

[10] M. Andresen, M. Johannesen, K. Larsen, Motivasjon i en cyberkrig, NTNU Open, 2025

[11] G. Østby and S. J. Kowalski, “Hendelseshåndtering ved cyberangrepet mot Østre Toten kommune,” NTNU, Tech. Rep., version 1.0, 2022.