Kommuner under angrep
Informasjonssikkerhet og internkontroll

Suhail Mushtaq
Fagsjef informasjonssikkerhet og personvern, KS
Leder av fagrådet for informasjonssikkerhet og personvern

Agenda

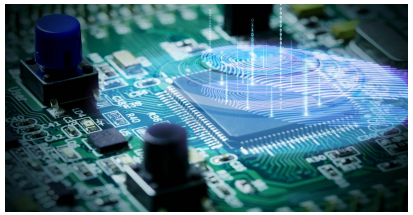
- Oppsummering
- Litt om det digitale rom
- Litt om påvirkningsoperasjoner
- Litt om dataangrep
- Litt om utredning innen sikkerhet, NPISK og hva gjør KS
- Noe råd på veien i forbindelse med revisjon

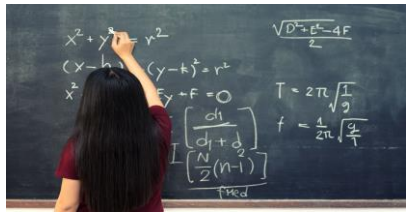
Oppsummering

Under arbeid!

Oppsummering

Hovedformålet med kommunene er å levere gode kommunale tjenester.





Kommunal sektor er helt avhengig av teknologi og kompetanse til å styre og forvalte teknologien for å kunne levere tjenester og ivareta kommunal funksjonsdyktighet.

Teknologi gir mulighetsrom, men samtidig sårbarhet.
For hver innretning som innfører, økes sårbarheten.
Riskohåndtering

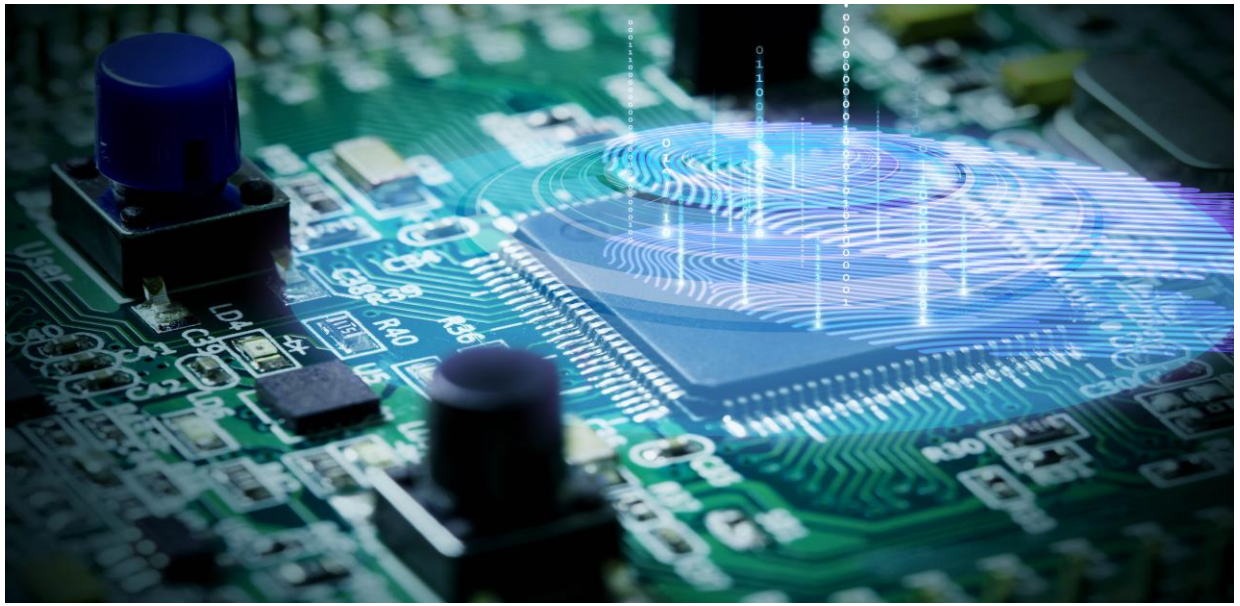
Sikkerhet i bred forstand er en forutsetning for trygg digitalisering, rettssikkerhet, demokratiutvikling og kommunens funksjonsevne.

Teknologiutnyttelse, kompetanse og digital sikkerhet dermed en nøkkelfaktor for vår samfunnsutvikling og velferd.

Oppsummering

Som et startpunkt still deg disse tre spørsmålene:

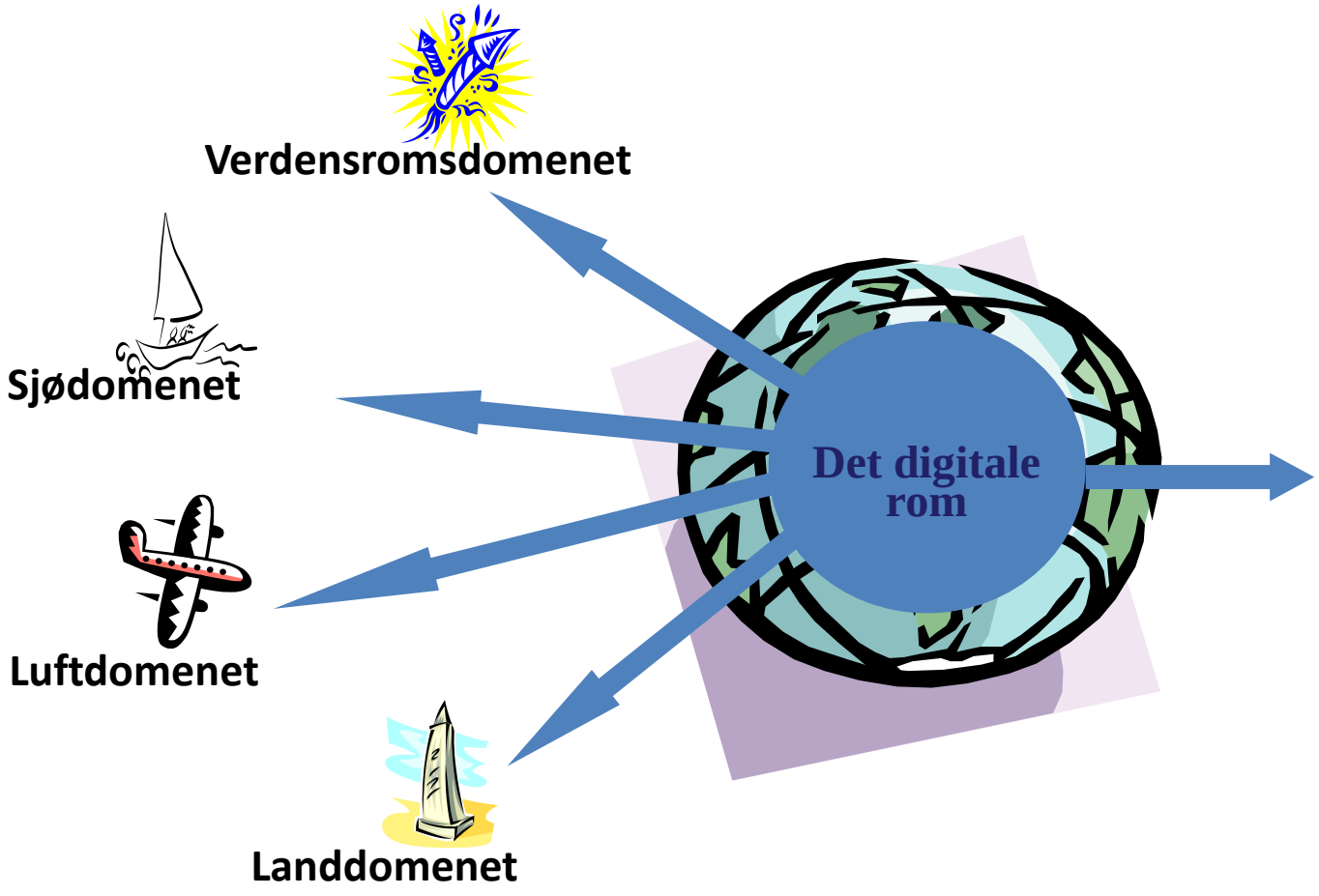
1) **Hva skjer med kommunen hvis systemene er helt utilgjengelige eller ikke er til å stole på?**
2) **Hvordan, hvor lenge og hvilken del i kommunen kan du operere på tross av at systemene er utilgjengelige eller ikke er til å stole på?**
3) **Hvor kan du søke ekstern hjelp hvis så skjer?**



Litt om det digitale rom

Under arbeid!

Litt om det digitale rom

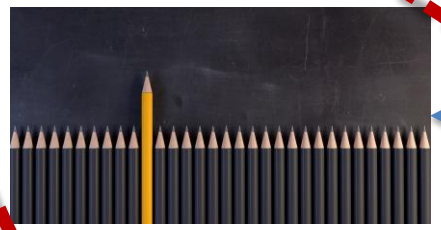


Aktører

- Deg og meg
- Kommersielle interesser
- X organisasjoner
- Kriminelle
- Befolkningsgrupper
- Informasjonskrigere
- Stater
- Hackere
- Med flere

Når aktørene påvirker hverandre
Informasjonsoperasjoner

Digital angrep i det digitale rom



Påvirke og endre

Mange virkemidler

Vinning

Påvirkningsoperasjoner

Digitale angrep

Målet er å påvirker styringsevne, rettssikkerhet, demokratiutvikling, samfunnsstyring, samfunnsutviklingen samt funksjonsevne.

Målet er først og frem vinning og funksjonsevne. Beskyttelse må ses på som en kost for å drive en virksomhet.

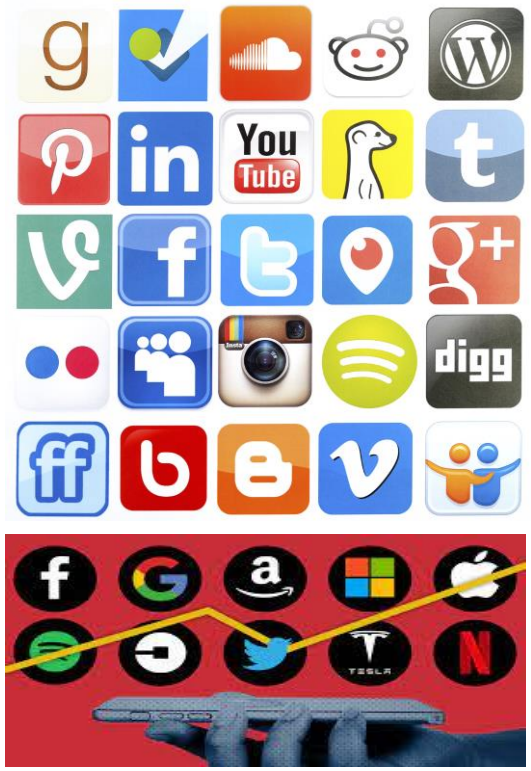
Litt om påvirkningsoperasjoner

Under arbeid!

Eksempel på en påvirkningsoperasjon – en start …

Eksempel på en påvirkningsoperasjoner

Påvirkning skjer i veldig stor grad, det foregår en «krig» om «heart and minds» i mange dimensjoner.



Eksempel på en påvirkningsoperasjoner

Fra ffi rapporten:

Siden 2014 har man sett en markant økning i staters koordinerte bruk av sosiale medier for å forsøke å påvirke andre staters befolkning.

De mest kjente påvirkningsforsøkene har funnet sted under anneksjonen av Krim i 2014, presidentvalget i USA i 2016 og covid-19-pandemien i 2020.

Mindre påvirkningsaktiviteter har blitt observert i forbindelse med terrorangrep i Storbritannia 2017 og valg i Tyskland og samt EU.

Gitt at slike påvirkningsoperasjoner har lave kostnader, er vanskelig å tilskrive en bestemt aktør og kan nå andre staters innbyggere direkte, er det rimelig å anta at slike operasjoner vil øke i omfang.

Det pågår mange påvirkningsoperasjoner nå, f.eks. betegnelsen av «terrorstat» om Russland og Ukraina eller vår oppfatning av Ukraina.

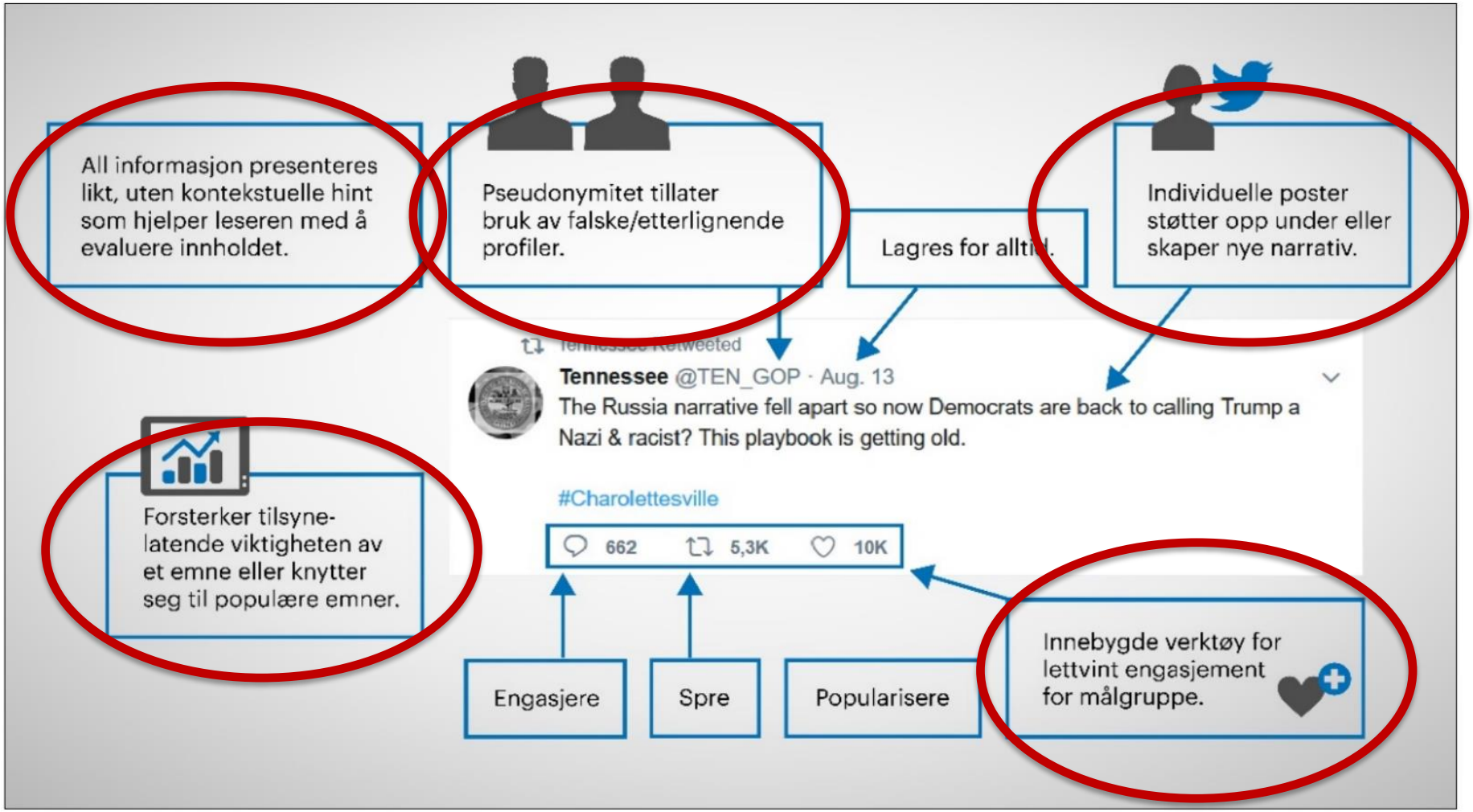
KRIGSHERRE: President Vladimir Putin besøker en russisk treningsleir 20. oktober. Foto: Mikhail Klimentyev / AP

Hevder at Ukraina bygger «skitten bombe»: – Absolutt ingen troverdighet

At ukrainerne skal slippe en bombe med radioaktive stoffer over sitt eget land, er ren propaganda fra Russland, mener tidligere forsvarssjef.

Av YASMIN SFRINTZERIS og LINE FAUSKO
For mindre enn 1 time siden

Eksempel på en påvirkningsoperasjon (fra ffi rapporten)



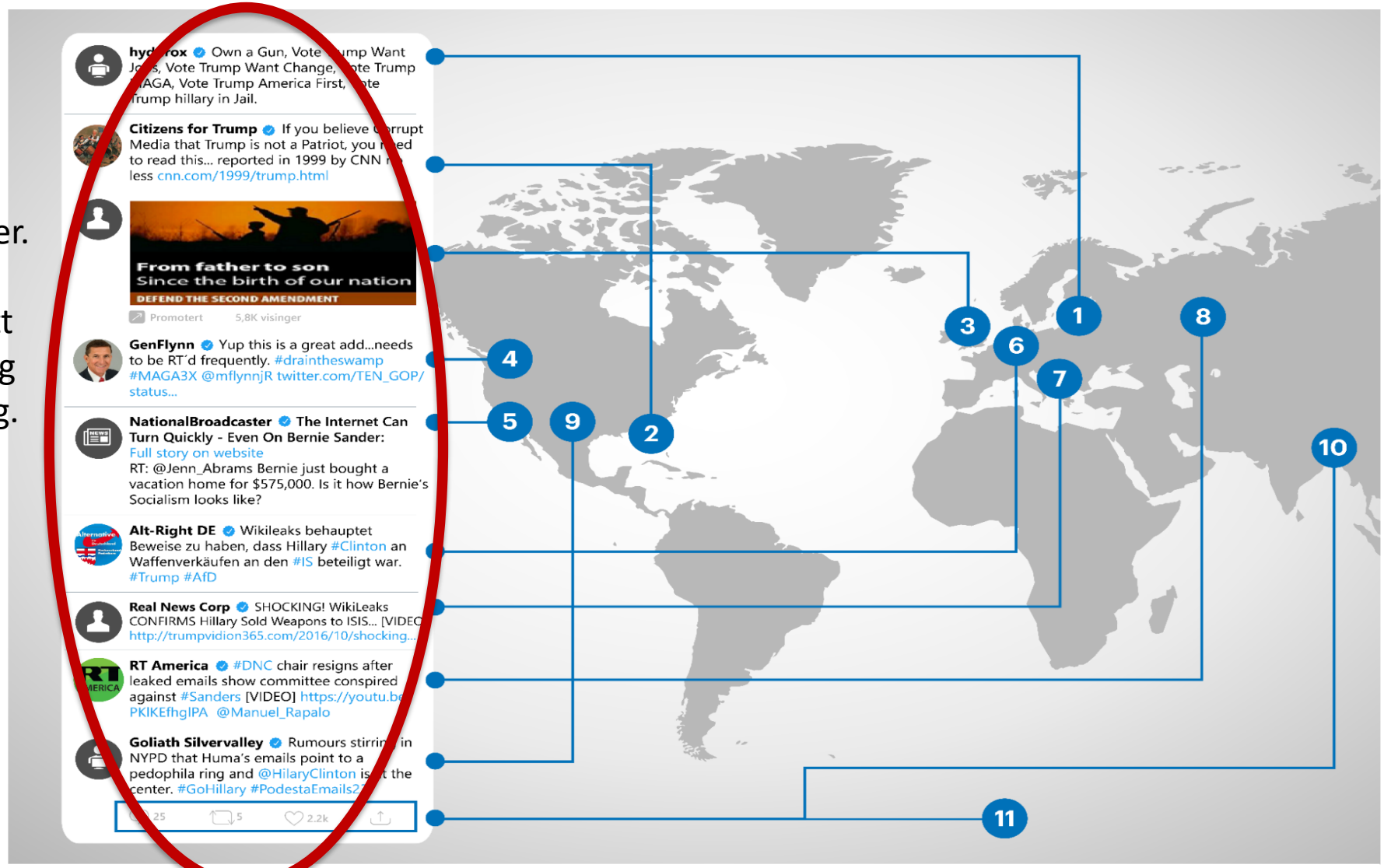
Figur 2.1 En tweet fra en IRA-kontrollert konto [15]. Kommentarene i boksene trekker fram aspekter som er nyttige for en påvirkningsoperasjon.

Eksempel på en påvirkningsoperasjon (fra ffi rapporten)

Feeden reflekterer dine interesser.

Forsterker ditt standpunkt og overbevisning.

F.eks. Pizzagate.



Figur 2.4 *Illustrasjon av forholdet mellom økosystemet rundt påvirkningsoperasjoner og nyhetsstrømmen. De forskjellige aktørene er 1: IRA (russisk troll fabrikk), 2: politisk aktiv pensjonist, 3: PR byrå, 4 & 5 - politisk støttespiller og nyhetsmedier retweeting IRA, 6: Alt-right supporter i Tyskland, 7: Fake news website, 8: State media outlet, 9: conspiracy theorist, 10 & 11: bots og klikkfarmer som øker synlighet.*

Eksempel på en påvirkningsoperasjon

#Pizzagate – konspirasjonsteorien som endte i restaurantskyting

WASHINGTON DC (NRK): Da en 28 år gammel tobarnsfar tok loven i egne hender og gikk inn på pizzarestauranten Comet i Washington og begynte å skyte med et automatvåpen var det den foreløpige toppen til konspirasjonsteorien som startet med et spørsmål på 4Chan.

Store politistryker rykket ut til pizzarestauranten Comet i Washington da en mann begynte å skyte på søndag.
FOTO: SARAH L. VOISIN / AP

Kristian Aanensen
@kaanensen
Journalist

Anders Tvegård
@anderstvegard
Journalist

Publisert 7. des. 2016 kl. 07:26

Artikkelen er flere år gammel.

Det kunne ha endt i en ny masseskyting, men 28 år gamle Edgar Maddison Welch ønsket ikke å drepe uskyldige, han ville bare finne ut om ryktene om Hillary Clinton og lederne i Demokratene var med i en pedofiliring og hadde seksuell omgang med mindreårige i kjelleren på restauranten Comet Ping Pong stemte.

Hemmelig kode

Historien startet uka før presidentvalget med at brukere på anonyme bildeforumet 4Chan lurte på om alle referansene til pizzafester i Clintons kampanjesjef, John Podesta sine hackede eposter egentlig var kodeord for bizzare sexfester og misbruk av mindreårige.

Trump i vitneboksen i

Eksempel på en påvirkningsoperasjon - oppsummering

Det er enkelt og skaffe seg narrativ, diskreditere, eller hevde i det digitale rom som vil påvirke vår demokrati og rettssikkerhet. Og i en forlengelse av dette vår funksjonsevne.

(Dagbladet 15.10.2022 - leder) Det er en systematisk elektronisk overvåking som griper inn i menneskers liv på ødeleggende og overveldende måter. Sensuren er betydelig skjerpet under Xi, og et styrket parti utfordrer enkelte steder privat eierskap i næringslivet. Alt for å tilfredsstille partiets og Xis behov for kontroll.

Norge?

Folkevalgte i kommuner og fylkeskommuner vil i de neste årene bli satt på prøve, og det må gjøres vanskelige prioriteringer.

Samtidig ser vi allerede nå at det offentlige ordskiftet er tøffere enn tidligere, noe som særlig går utover unge folkevalgte. Også fordekt valgpåvirkning, enten det er enkeltpersoner, organisasjoner eller stater som står bak, rykker nærmere den politiske hverdagen i Norge. Det dreier seg om falske, automatiserte kontoer på sosiale medier, falske nyhetsmedier som ikke er underlagt redaktøransvar, konspirasjonsteorier og trolling i kommentarfelt.

Når disse utfordringene kombineres med mer krevende arbeidsvilkår for folkevalgte, kan det føre til rekrutteringsutfordringer i lokalpolitikken. At vi klarer å rekruttere nye, engasjerte innbyggerne til lokalpolitikken, gjør at kommunestyret i større grad speiler befolkningen, som gir grunnlag for tillit.

Fortsatt rekruttering til lokaldemokratiet kan regnes som en del av den demokratiske beredskapen.

Litt om dataangrep

Under arbeid!

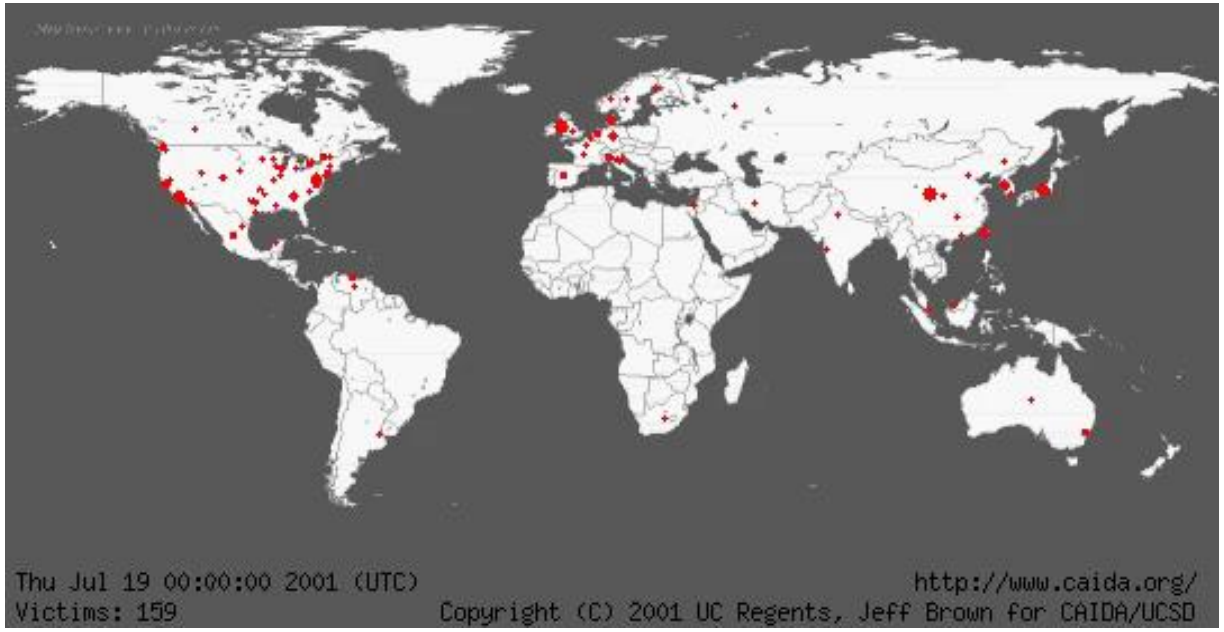
Digitale angrep

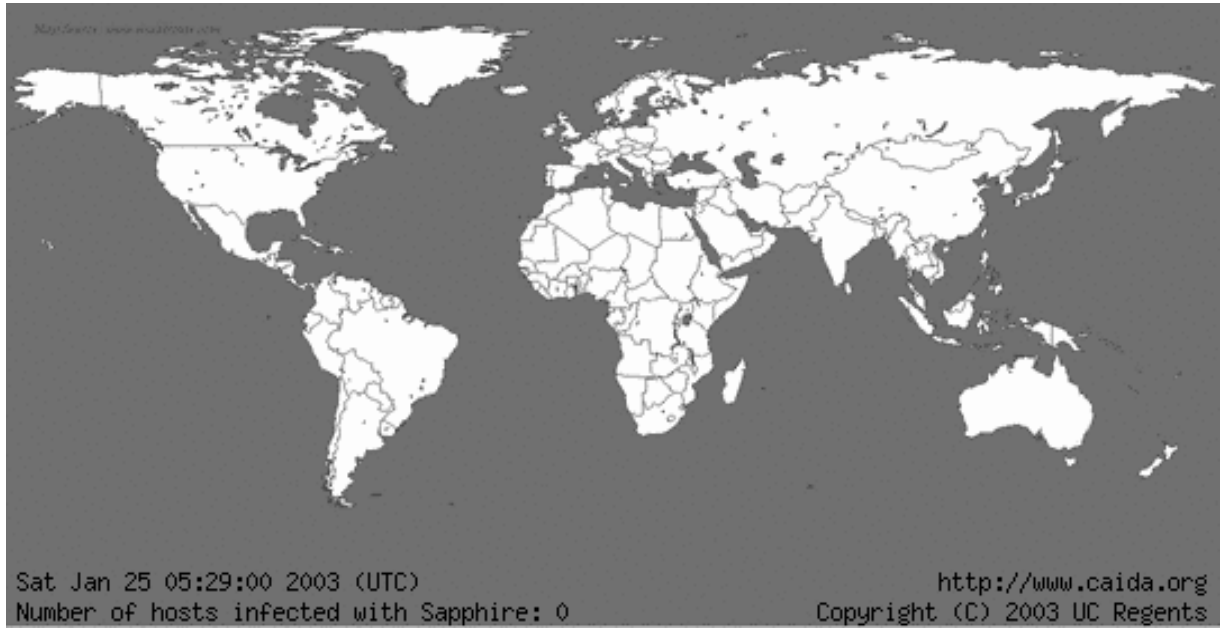
Mange digitale hendelser, og i nyere tid - enda hyppigere.

- Østre Toten kommune.
- Stortinget var utsatt for to dataangrep på et halvt år.
- Selskapet Volue ble offer for et løsepengevirus.
- Hackergruppe angrep ingeniørselskapet Inocean.
- Det kriminelle syndikatet Conti hacket Nordic Choice.
- Nortura ble utsatt for dataangrep – stanset mottak av dyr.
- Dataangrep på Norsk Hydro.
- Dataangrepet på Amedia.
- Dataangrepet på ….

- Det forgår flere tusen angrep mot Norge hver dag.

Operasjoner i digital rom

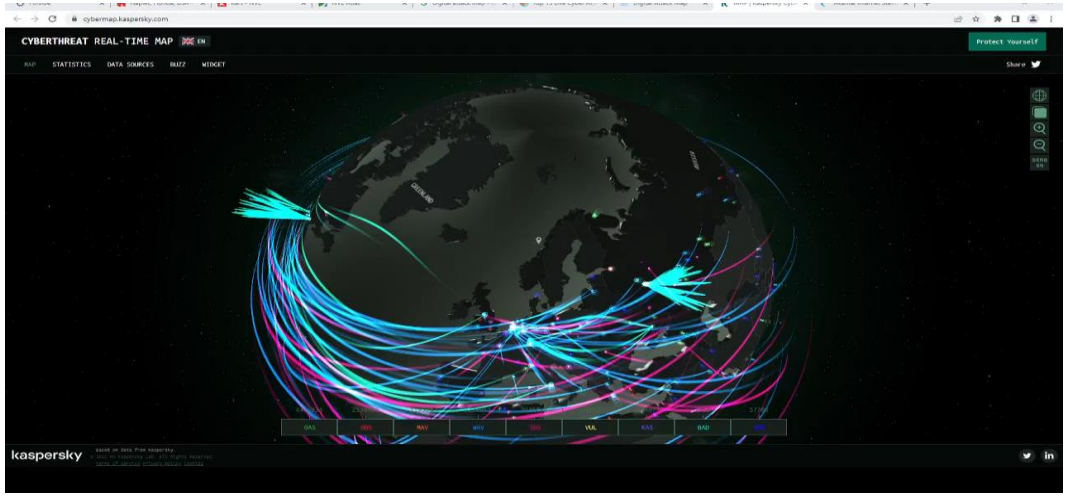


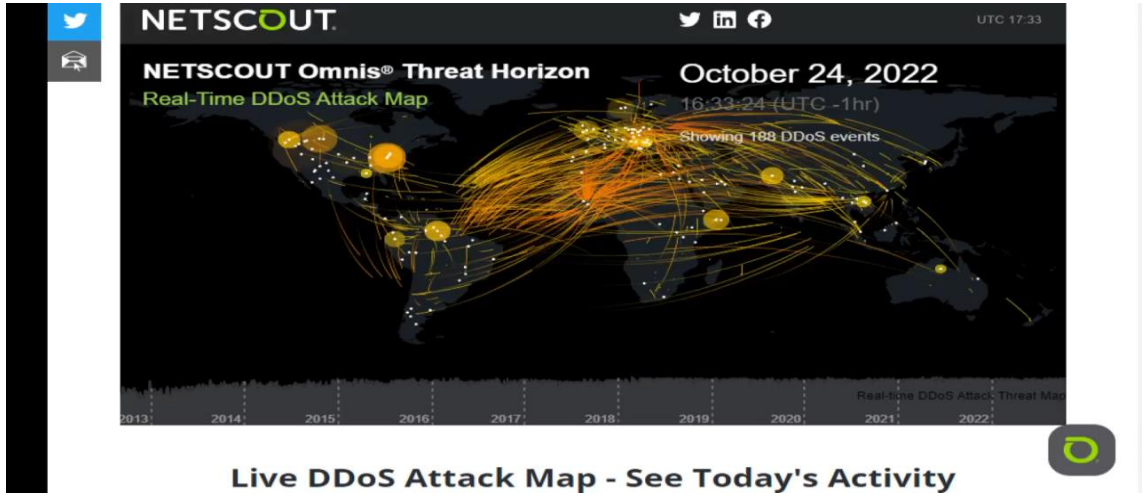


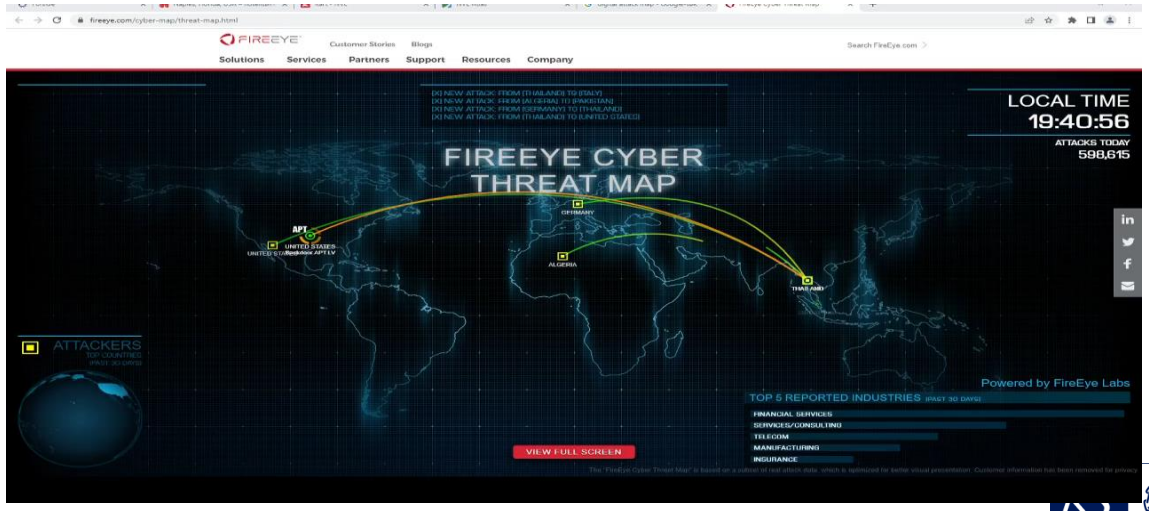
Det er som regel ikke slik at en angriper gjør ett «brekk» og at det blir synlig for deg, ofte har angriperen vært i systemene dine over lengere tid – gjerne flere måneder.

Du må derfor tenke at systemene dine er i utgangspunktet kompromittert, og hvordan du i en slik kontekst kan operere trygt i det digital rom.

Operasjoner i digital rom

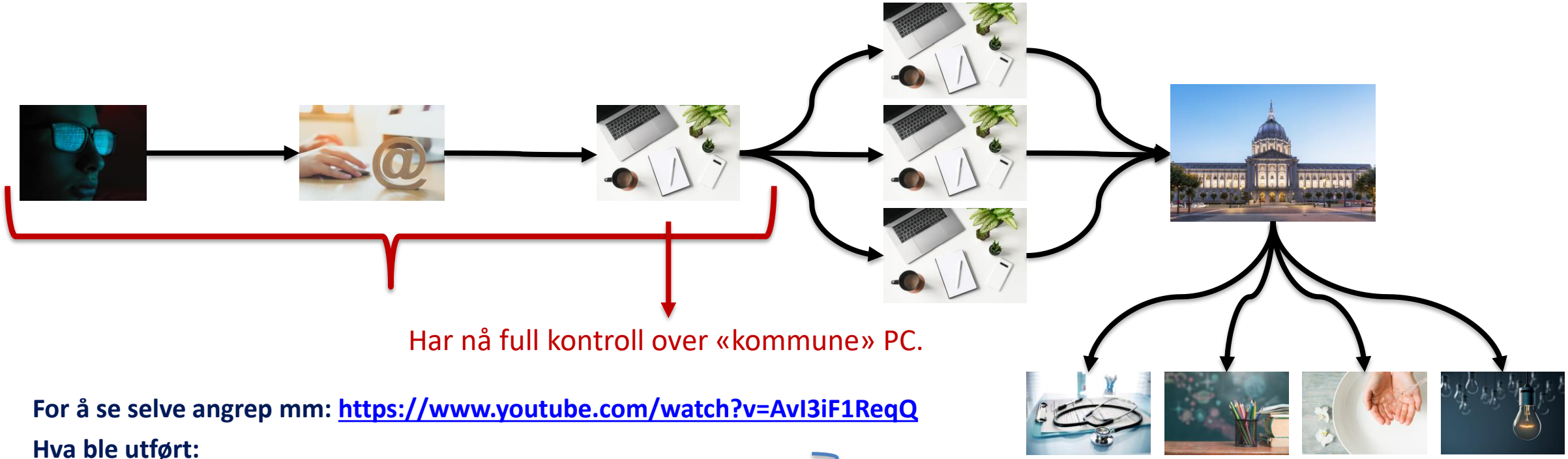






Digital angrep - oppsett

En «normal kommune».



Har nå full kontroll over «kommune» PC.

For å se selve angrep mm: https://www.youtube.com/watch?v=AvI3iF1ReqQ

Hva ble utført:

- Hente ut dokumenter og annen informasjon.
- Endring av dokumenter.
- Manipulering av data.
- Mulighet for å «slå» av/ut kommunenes systemer.
- Kontroll over kommunene arbeidsflyt/prosesser og informasjon.
- Avlytting.
- Overvåkning.

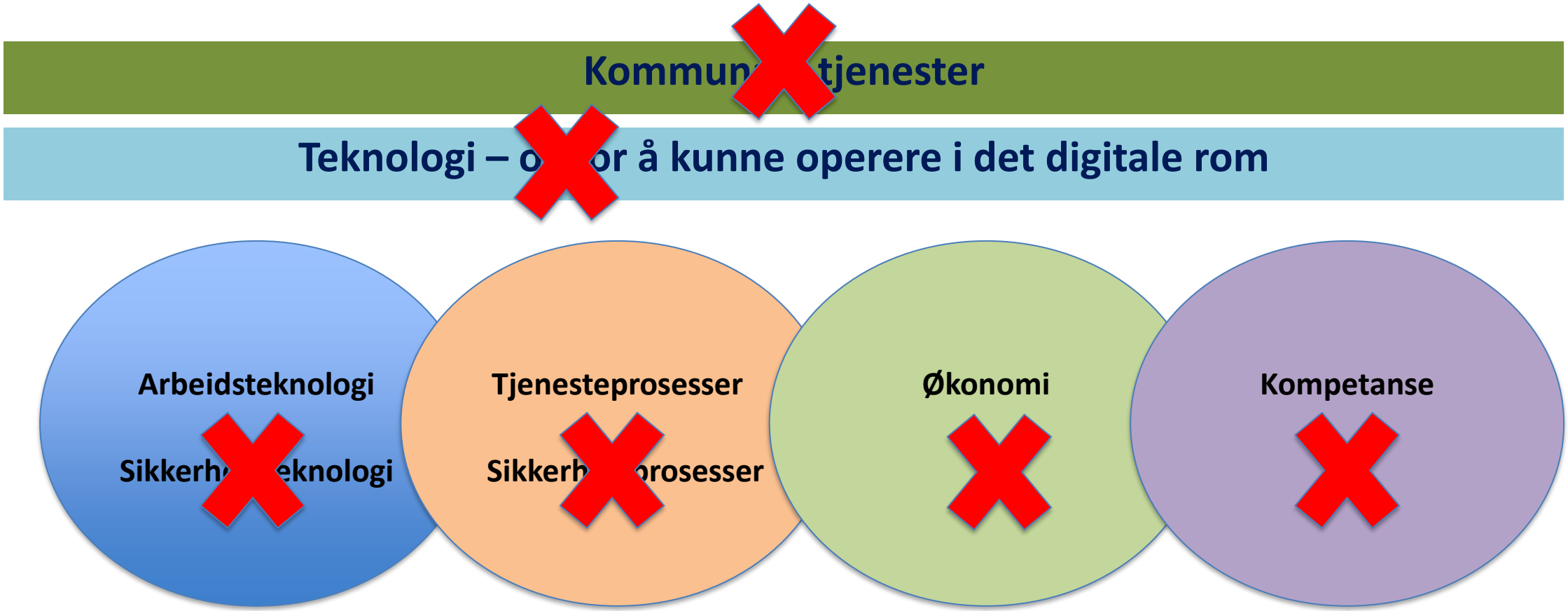
- «Styring» av kommunen.

Data på avveie

Styring og kontroll av virksomheten

For å kunne operere i det digital rom

Digitalisering gir store mulighetsrom – men har også en kost for å kunne muliggjøre handlingsrommet.



Det er ikke spørsmål om, men når du vil bli angrepet. Resultat av angrepet vil avhenge av din robusthet.

Hva slags kompetanse trengs for å kunne operere i det digital rom

- *Tjenestedesign-kompetanse:* Avgjørende for å sette brukeren/innbyggeren i sentrum – tenke nytt om hvordan prosesser bør være i fremtiden
- *Virksomhetsarkitektur-kompetanse* For å skape samspill mellom organisasjon og teknologi. Forstå hvordan data flyter/behandles i organisasjon
- *Bestillerkompetanse,* herunder innovative anskaffelser. For at organisasjonen får de teknologiske løsningene som understøtter behovene.
- *Krysskompetanse fag / teknologi* – For å oversette fagfolkenes behov til det løsninger må ivareta, herunder i forvaltningsfase.
- *Prosjektkompetanse* – prosjektlederkompetanse, prosjekt vs. forankring i linje, smidig vs tradisjonell prosjektmetodikk.
- *Teknologi-kompetanse* – forståelse av teknologi. I dette ligger kompetanse på kjerneteknologi, innføring, test, informasjonssikkerhet, arkitektur.
- *Prosess-kompetanse* samspillet mellom teknologi og organisasjon, i beskrivelse av ny arbeidsprosesser, som igjen er essensielt for opplæring.
- *Organisasjonsdesign-kompetanse*. Hvordan må organisasjonen settes opp? Hvilke roller må ivaretas i ny organisasjon?
- *Endringsledelse og opplæring* – hvordan motivere organisasjonen for endringene som skal til, gjennomføre effektiv opplæring av den enkelte.
- *Kompetanse på gevinstrealisering –* gevinstanalyse, omsetting i realiserbare gevinster, indikatorutvikling, analyse og dokumentasjon av effekter
- *Kompetanse-kompetanse* – Hva er gapet mellom kravene til kompetanse i ny organisasjon, og den som finnes i organisasjonen.
- *Omstilings/Arbeidsgiverkompetanse* – Hvordan skal menneskene ivaretas på en god måte i transformasjonsprosessen, samspill med tillitsvalgte, innplassering, endring av arbeidsavtaler, formelle forhold til hovedavtale etc.
- *Forvaltningskompetanse (herunder avtaler), revisjons og læringskompetanse*
- *Sikkerhets- og personvernkompetanse*
- *Juridisk kompetanse*
- *Kommunikasjons- og psykologisk kompetanse*

- *Drifts- og leveransekompetanse*

Litt om utredning innen sikkerhet, NPISK og hva gjør KS

Under arbeid!

Hva gjør KS?

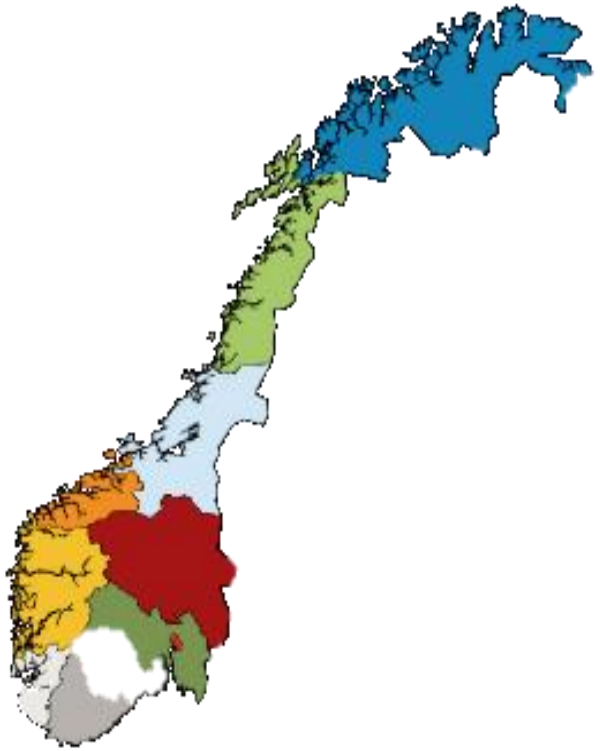
Situasjonen kan virke kompleks, uoversiktlig og krevende.

Dog ikke noe mer at den kan håndteres hvor nøkkelen er samarbeid og felles tilnærming.

Utfordringsbildet kommunal sektor

Ulik modenhetsgrad innen informasjonssikkerhet, digital beredskap og personvern.

- Ulik ressurstilgang (personell og økonomi).
- Ulik kompetansekapasitet.
- Ulik informasjonstilgang.
- Ulik konsumeringsevne.
- Ulike forvaltningsmodeller.
- Ulik strategisk styringskompetanse (politisk og ledelsesnivå).
- Mangel på felles krav og samstyring.
- Fagområdet er komplekst og i hurtig endring.
- Kommunikasjonsnettverk.



På tross av ulik utgangspunkt for kommunene er det vesentlig at man **når ut og løfter samtlige kommuner** for å gjøre dem mer robuste, og at de evner å forebygge, oppdage og håndtere digitale hendelser. Med dette som utgangspunkt, foreslås følgende struktur for å nå ut til samtlige kommuner.

Under arbeid!

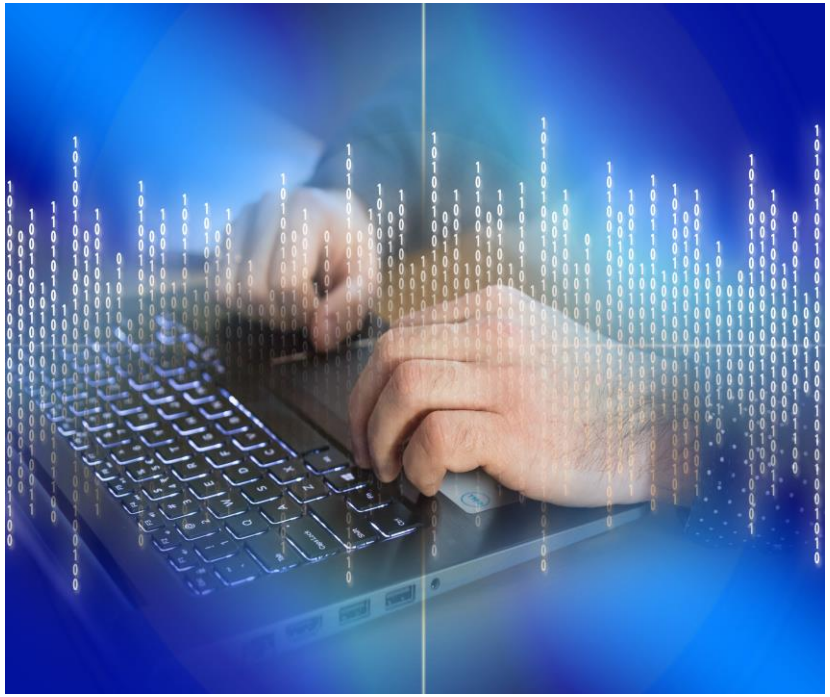
Aktiviteter fra KS / fagrådet

KS

- **Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet.**
- **FoU2 – informasjonssikkerhet i ansatt perspektiv.**
- **SkoleSec.**
- **Digitale fellestjenester**
- **Robushetsrapporten (tiltak 7 – anbefaling felles sikkerhetskrav)**

Fagrådet

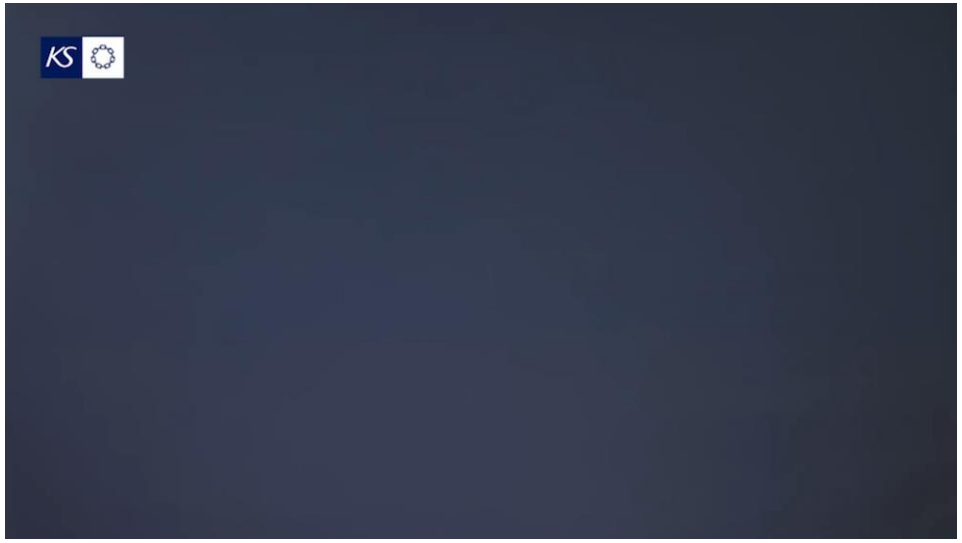
- **Veileder for bruk av sosiale media.**
- **Bidra til modning av kommunal sektor.**



FoU2 – adferdsendring i kommunal ansattes perpektiv

Oppmerksomhet

Fagvideo



10 adferdsendringer – over 10 måneder

Selv om det er 10 adferdsendringer – så er det fokus på totalsikkerhet

Noen råd på veien vedrørende revisjon

Under arbeid!

Oppdraget

Ansvar: Ansvaret for informasjonssikkerhet, digital beredskap, personvern og internkontroll i den enkelte kommune påhviler kommunedirektør og politisk ledelse.

Mål for oppdraget:

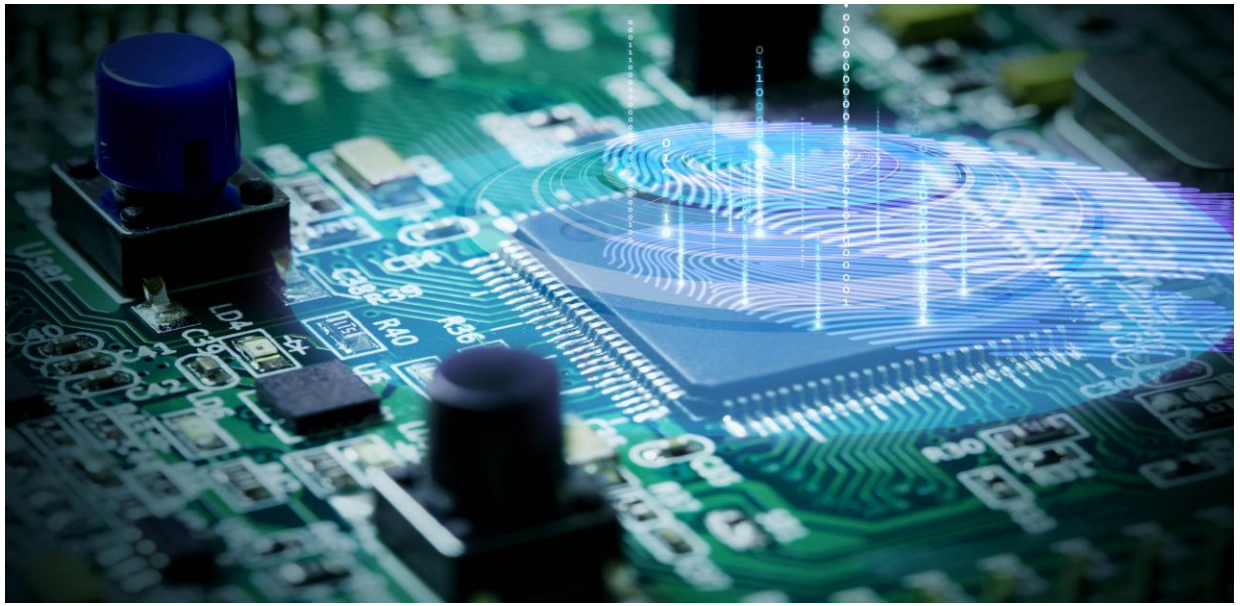
- Har kommunen tilstrekkelig evne til å forebygge, oppdage og håndtere digitale angrep?
- Er kommunen robusthet nok ved bortfall av teknologi?
- Har kommunen tilstrekkelig kontroll over persondata?
- Forvaltes teknologien på en god måte og understøtter den kommunale tjenester på kort og lang sikt?

Under arbeid!

Oppsummering

Som et startpunkt still deg disse tre spørsmålene:

1) **Hva skjer med kommunen hvis systemene er helt utilgjengelige eller ikke er til å stole på?**
2) **Hvordan, hvor lenge og hvilken del i kommunen kan du operere på tross av at systemene er utilgjengelige eller ikke er til å stole på?**
3) **Hvor kan du søke ekstern hjelp hvis så skjer?**

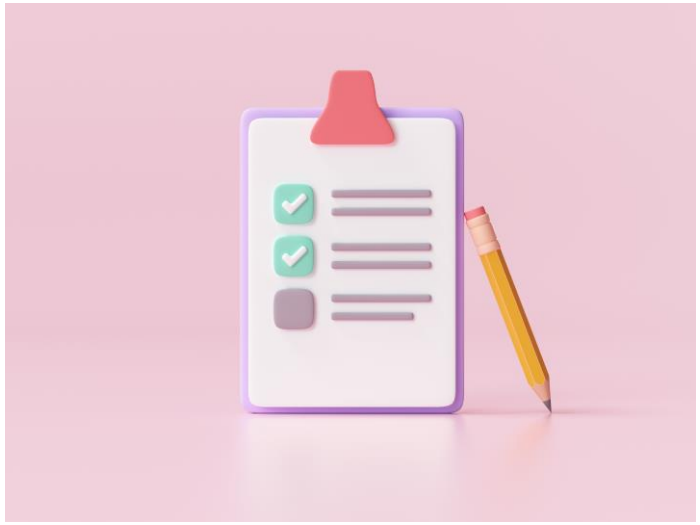


Noen råd på veien

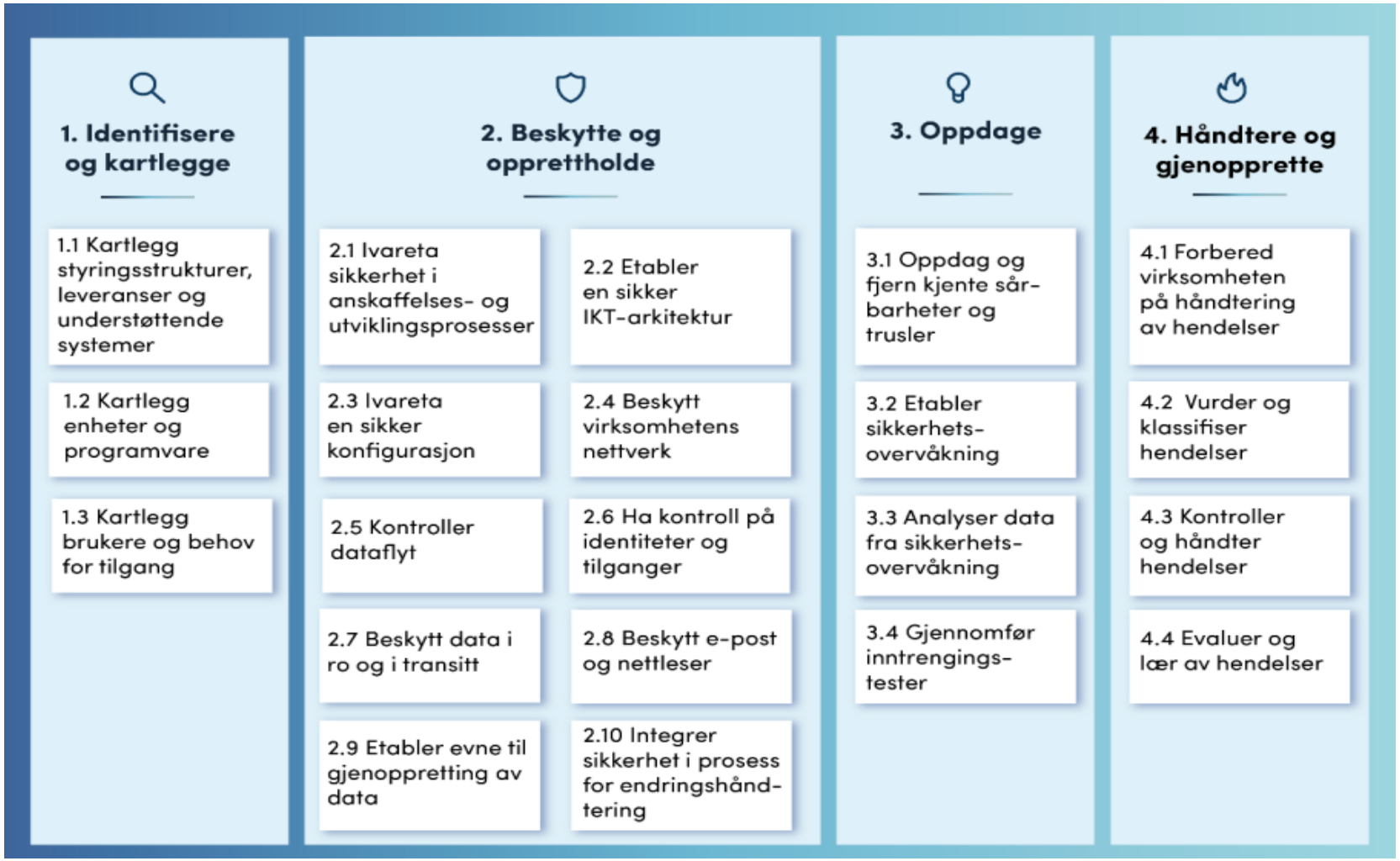
- **Innen IT-revisjon gir dokumentkontroll liten verdi – man må gå konkret til verks.**

- **Spør spesielt etter:**
  - Kontraktsforhold (manglende)
  - Eierskapskontroll
  - Hurtigdigitalisering

  - Skygge IT
  - Digital grunnmur
  - Kapasitetsstyring
  - Overvåkning og beredskap



Noen råd på veien – et utgangspunkt



Vær ute i virksomheten og spør hvordan de enkelte elementene faktisk gjøres eller gjennomføres.

Digital beredskap og informasjonssikkerhet «Kommuner under angrep»

Suhail Mushtaq
Fagsjef informasjonssikkerhet og personvern, KS
Leder av fagrådet for informasjonssikkerhet og personvern