IN5080
Sikkerhets- og risikostyring

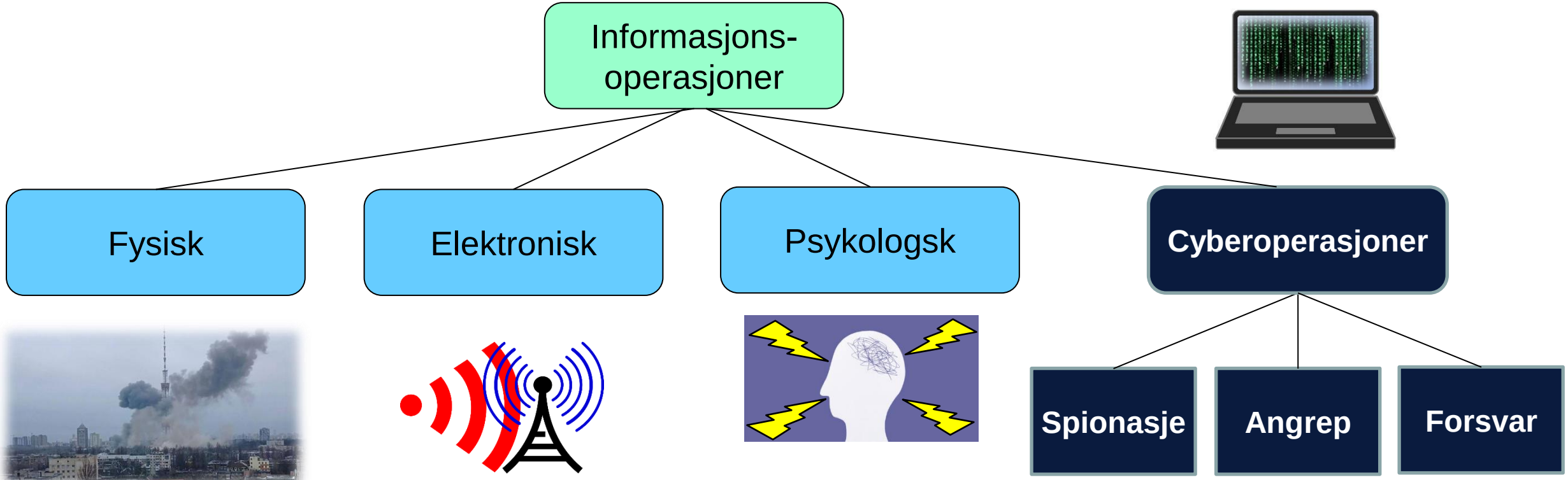
Del 12: Cyberkrigføring

Audun Jøsang
Universitetet i Oslo
Vår 2023

Oversikt: Cyberkrigføring

a. Begreper
b. Cybervåpen
c. Cyberavskrekking
d. Overvåkingsindustrien
e. Leveransekjeder
f. Cyberkaperfart
g. Big Tech sin rolle

Informasjonskrigføring



Cyberkrigføring er alle former for cyberoperasjoner mellom stater for å utføre spionasje, sabotasje, og forsvar mot disse.

Cyberoperasjoner, aka. Nettverksoperasjoner

- Nettverksoperasjoner (Computer Network Operations)
  (NATO Allied Joint Publication)
  - Spionasje (Computer Network Espionage: CNE)
  - Angrep (Computer Network Attack: CNA)
  - Forsvar (Computer Network Defense: CND)

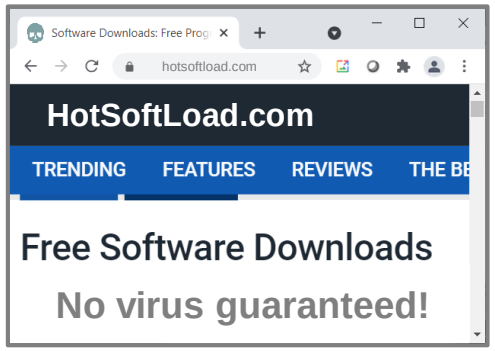
- Cyberoperasjoner (Cyber Operations)
  (US Cyber Operations Policy)
  - Cyber Collection
  - Offensive Cyber Effects Operations (OCEO)
  - Defensive Cyber Effects Operations (DCEO)

Cyber-angrepsvektorer

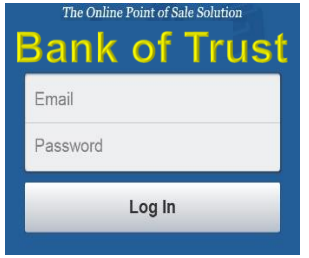
Innsideangrep fra utro tjenere i virksomheten.

Phishing e-post, SMS og meldinger med skadevare og lenker til skadige nettsider.

Drive-by-angrep fra kriminelle eller infiserte nettsider.



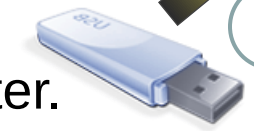
Installering av skadelige programmer fra internett eller andre lagringsmedia.



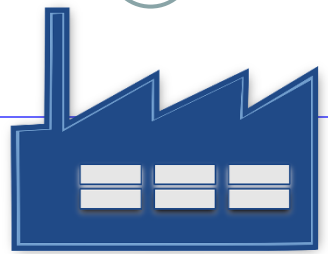
Falske nettsider som stjeler bruker-ID og passord.

Hacking av upatchede sårbare IoT-enheter.

Deepfake lyd og video for å spoofe identitet i online møter og samtaler.



Skadelige eksterne enheter.

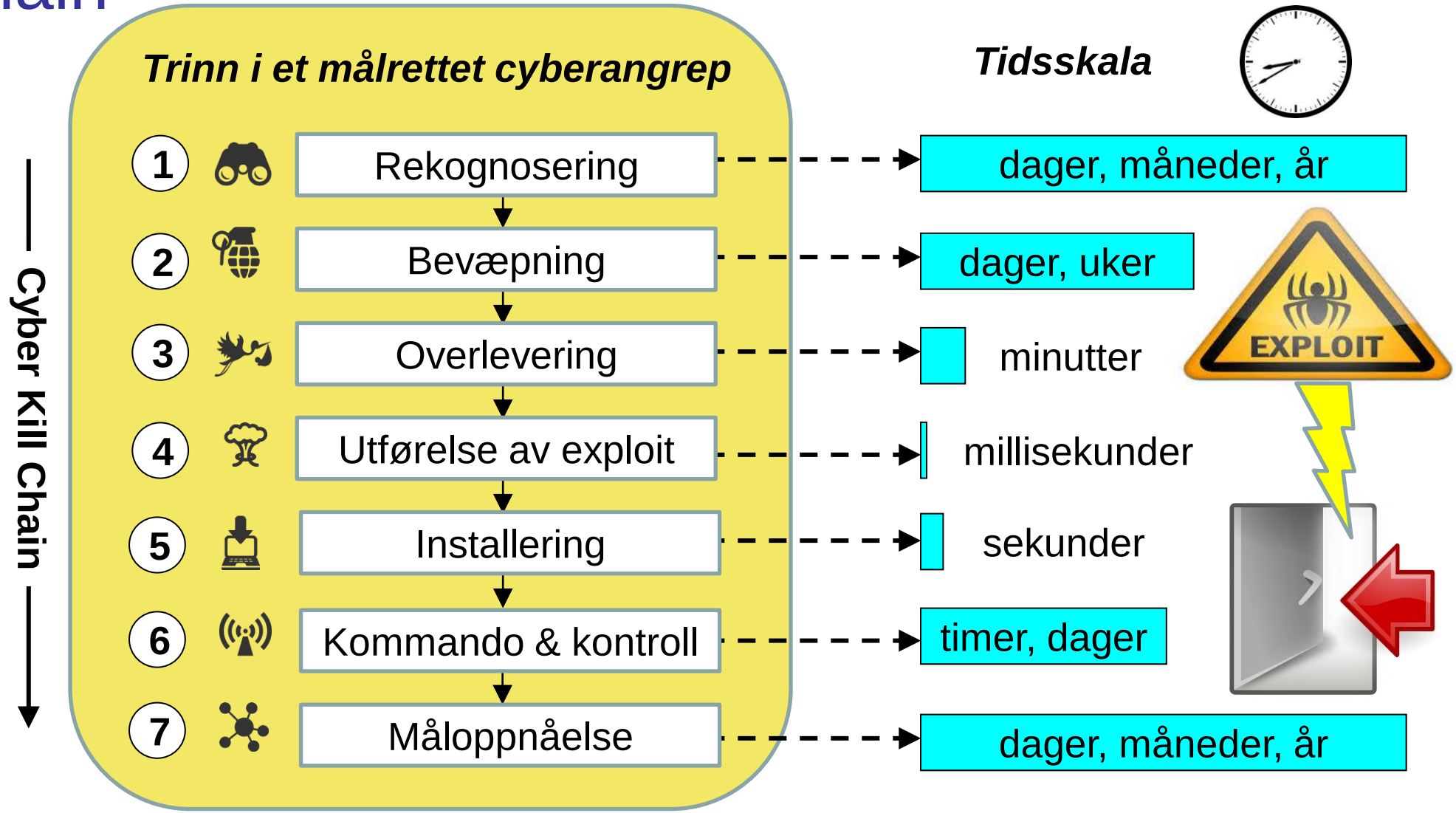


Infisering og angrep gjennom leveransekjeden.

Direkte angrep mot sårbare systemer og applikasjoner.

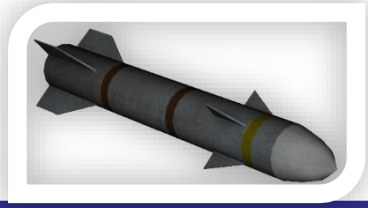
Cyber Kill Chain

- Cyber Kill Chain er utviklet av Lockheed Martin.
- Den beskriver trinnene i et målrettet «kill» cyberangrep.
- Angrepet kan bli stoppet på hvert av disse trinnene
  - Jo tidligere desto bedre



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cybervåpen og kinetiske våpen



	Cybervåpen	Kinetiske våpen
Skadeeffekt	Ingen direkte fysisk skade. Gjøre skade på IT-systemer og forretningsprosesser som støttes av IT.	Forårsaker direkte ødeleggende fysisk skade på infrastruktur. Rammer bare der våpenet treffer.
Gjenbruk	Kan gjenbrukes.	Kinetisk ammunisjon blir ødelagt i angrepet.
Åpenhet	Cybervåpen er immaterielle, og dermed lett å skjule.	Kinetiske våren er ofte store, og synlige fra fly og satellitter.
Attribusjon	Teknisk vanskelig å identifisere trusselaktør.	Vanligvis relativt lett å se hvor et kinetisk angrep kommer ifra.
Holdbarhet	Basert på nulldagssårbarheter med begrenset holdbarhet, ofte mindre enn ett år.	Lang holdbarhet, typisk flere tiår.

Nytten av cyberspionasje og offensive cyberoperasjoner

Cyberspionasje

- Gir store fordeler for innhenting av etterretning
- Billigere og mindre risikabelt enn tradisjonell fysisk spionasje

Offensive cyberoperasjoner

- Kan lamme digitale systemer og prosesser
- Angrep mot kritisk infrastruktur kan være spesielt skadelig
- Konsekvens kan reduseres ved god beredskap og hendelseshåndtering
- Angripere må ha betydelige ressurser for å oppnå betydelig effekt
- Ofte billigere å få tilsvarende effekt med fysiske angrep
- Angriper har fordelen av vanskelig attribusjon

Offensive cyberoperasjoner kombinert med fysiske angrep

- Observert bruk av cyberoperasjoner i nåværende konflikter (Ukraina)
- Ansett for å være svært nyttig sammen med fysiske militæroperasjoner.
- Forvirrer og forstyrrer fienden når kommunikasjon og koordinering er mest kritisk

Land med offisiell strategi for cyberoperasjoner

- Militære forsvarsstrategier i det 21. århundre må nødvendigvis inkluderer en strategi for cyberoperasjoner.
- USA har en klart uttrykt offisiell policy for cyberoperasjoner.
- Andre land resonnerer kanskje med at cybervåpen er usynlige, og at det er en fordel å ikke publisere strategi for cyberoperasjoner.

The New York Times

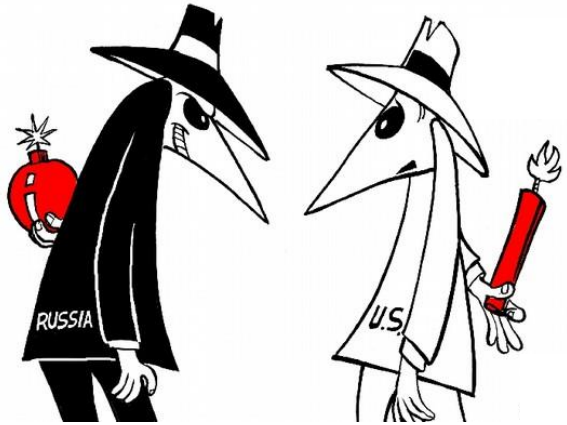
By DAVID E. SANGER APRIL 24, 2016

ISIS Targeted by Cyberattacks in a New U.S. Line of Combat

https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html

The National Security Agency headquarters in Fort Meade, Md. The agency has for years listened to Islamic State militants, but its military counterpart, Cyber Command, will now direct operations against the militant group.

Cyberavskrekking



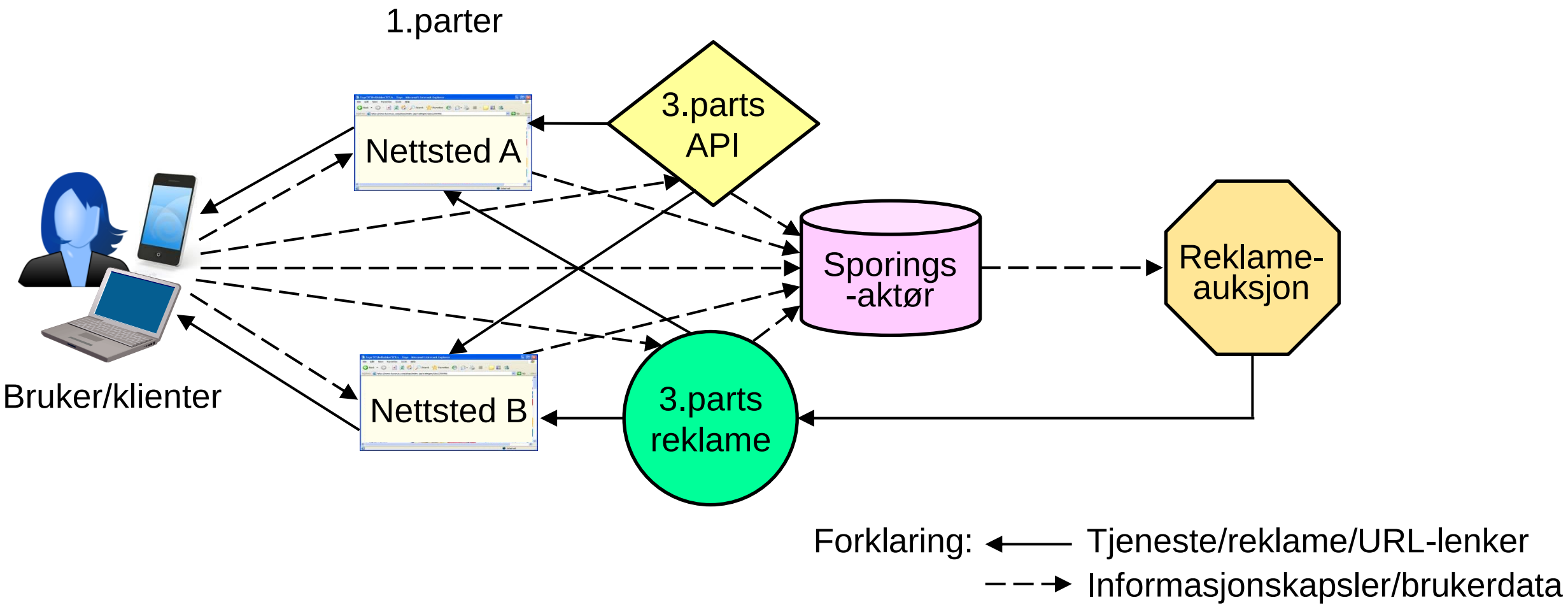
- Russland har kompromittert kraftnett i vestlige land siden 2014
  - Rapporter om kompromittering og spionering mot kraftnett i USA
  - Sabotasje mot Ukraina i desember 2015
- USA har kompromittere kraftnett i Russland siden 2018
  - Hvordan vet vi det? Artikkel i New York Times:
    https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
  - Hvorfor? For å avskrekke.

The New York Times

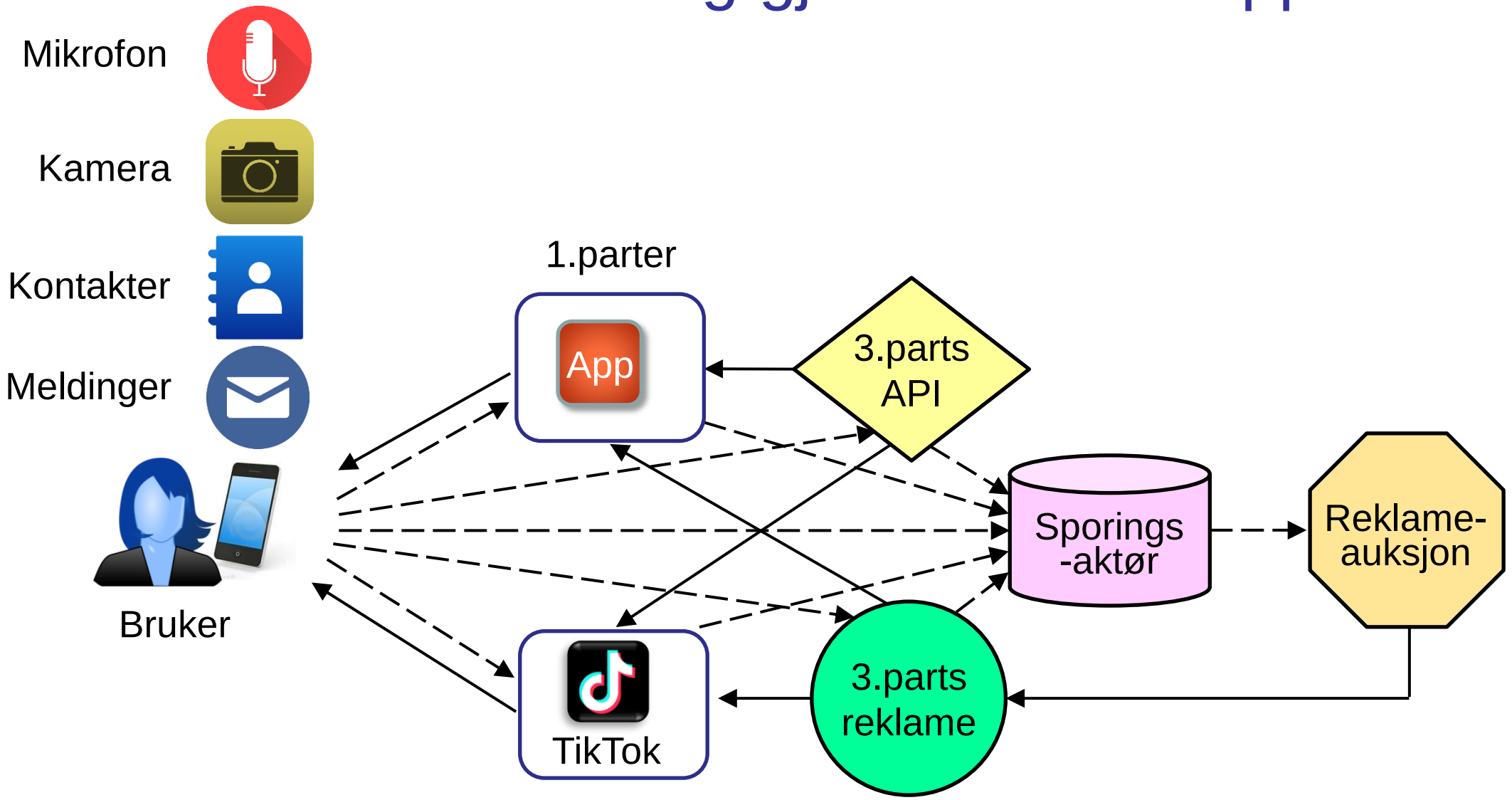
U.S. Escalates Online Attacks on Russia's Power Grid

A heating power plant in Moscow. Officials described the move into Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections. Maxim Shemetov/Reuters

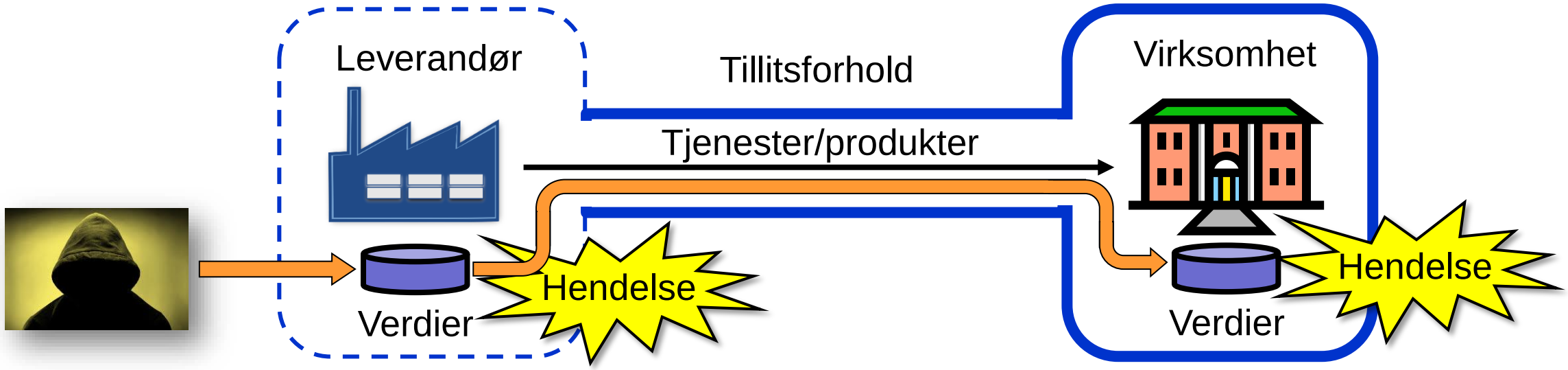
Overvåking på nett



Overvåking gjennom mobilapper

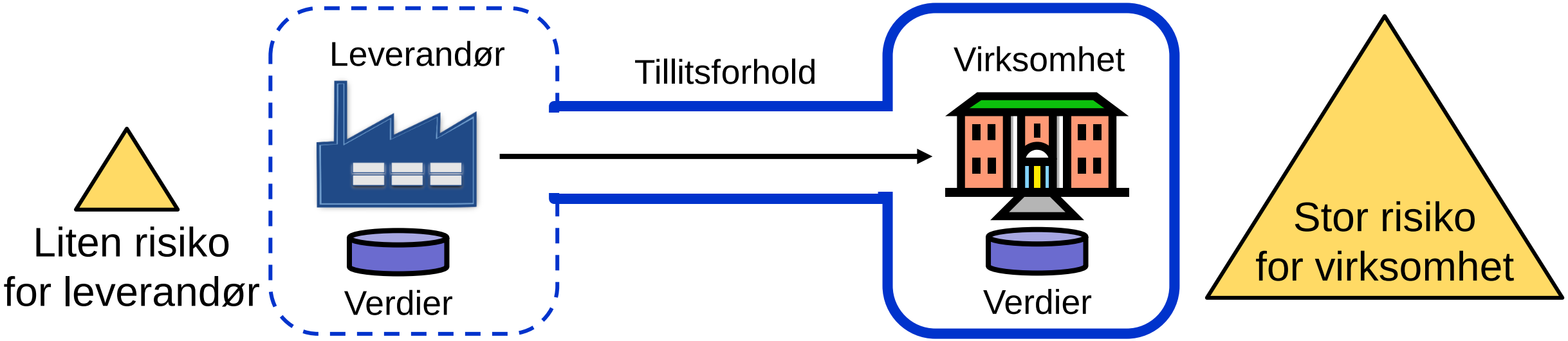


Leveransekjedeangrep



- Leveransekjedeangrep er at trusselaktøren først angriper og kompromitterer produkter og tjenester hos en leverandør, noe som deretter gjør det mulig å angripe leverandørens kunder (virksomheter). Det er et 2-trinnsangrep.
- Det er altså intet leveransekjedeangrep at en trusselaktør angriper en virksomhet ved å utnytte en **utilsiktet** sårbarhet i et produkt eller en tjeneste fra en leverandør.
- Trusselaktører følger det svakeste ledd, som kan være å angripe en virksomhet gjennom først å angripe en leverandør.

Markedssvikt gjennom leveransekjeder

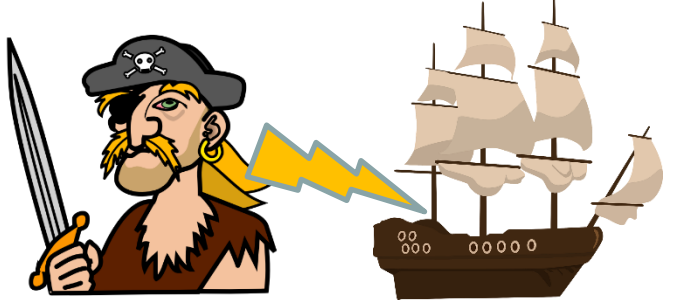


- Leverandører med liten risiko har lite insentiv til å implementere sterke (og dyre) sikkerhetstiltak.
- Virksomheter med høy risiko ønsker sterke sikkerhetstiltak, men har få muligheter til å implementere sikkerhetstiltak i leveransekjeden.

Risikostyring for leveransekjeder

- Elementer som bør inkluderes i kontrakter og avtaler
  - Rapportering og varslingsplikt om sikkerhetsrelaterte ting som sikkerhetshendelser sikkerhetspolicyer og endringer av eierstruktur
  - Tilsyn og revisjonsrapporter om sikkerhet
  - Nivå for risikoaksept hos underleverandør
  - Forventet oppetid av tjenester, og underleverandørens risikoaksept for overholdelse av denne
  - Endrings- og exit-klausuler, f.eks. basert på avvik eller endring i eierstruktur
- Virksomheten bør kartlegge og overvåke underleverandørens eierstruktur. En mulig trussel er at en underleverandør kjøpes opp av et selskap lokalisert i et land Norge ikke har sikkerhetspolitisk samarbeid med. Da er det plausibelt at myndighetene i det landet kan utnytte den nye eierens styringsrett til å angripe virksomheten via leveranse av produkter og tjenester.

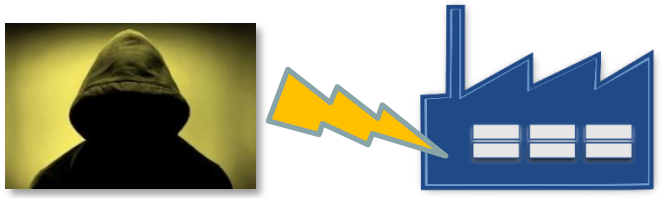
Cyberkaperfart



Kaperfart 1600 - 1850

- Kaperfart i perioden 1600 – 1850 var legalisert sjørøveri.
  - Piratene fikk utdelt kaperbrev

- Russlands president Putin har uttalt at russiske grupperinger som utfører cyberangrep mot andre land ikke anses å være kriminelle, *«fordi de ikke bryter russisk lov».*
  - Russiske hackergrupperinger har dermed fått kaperbrev.



Cyberkaperfart 2020→

- Paris Call for Trust and Security in Cyberspace (2018) feilet fordi stormaktene ønsker å kunne utføre cyberoperasjoner, og fordi overholdelse av en traktat ville være vanskelig å håndheve.

Cyberkrigføring og Big Tech

- Onsdag 23. februar, noen timer før russiske stridsvogner begynte å rulle inn i Ukraina, fant Microsofts Threat Intelligence Center indikatorer på en aldri tidligere sett «Wiper“-skadevare som ble brukt i angrep mot Ukrainas regjeringsdepartementer og finansinstitusjoner.
- Microsoft Threat Intelligence Center plukket raskt fra hverandre skadevaren, kalte den "FoxBlade" og varslet Ukrainas øverste cyberforsvarsmyndighet.
- FoxBlade-skadevaren er programmert til å slette - “wipe" - alle data på computer som er tilgjengelige i et datanett.
- I løpet av tre timer hadde Microsofts virusdeteksjonssystemer på Windows-servere blitt oppdatert for å blokkere FoxBlade.

Yanukovych and Putin

Petro Poroshenko

Volodymyr Zelenskyy

Potensiale for samarbeid med Big Tech

OS-tilbydere (Operativsystemer)

- Programvareoppdateringer og regelmessig patching
- Potensiell total kontroll over alle systemer som er online

CPU- og microchip-produsenter

- Spesielle triggere kan åpne bakdører
- Fjernkontroll av systemplattformer

Computerprodusenter

- Konfigurerer oppstart, kan bygge inn spionvare under produksjon
- Overvåking og styring av computerplattformer under drift

Skytjenester

- Passiv eller aktiv tilgang til IaaS, PaaS og SaaS
- Overvåking og styring i skyen

Hvor går cyberkrigføring?

- Manglende internasjonale avtaler, alt er lov
- Økende kompleksiteten i leveransekjeder fører til større angrepsflater
- Big Tech spiller en viktig rolle