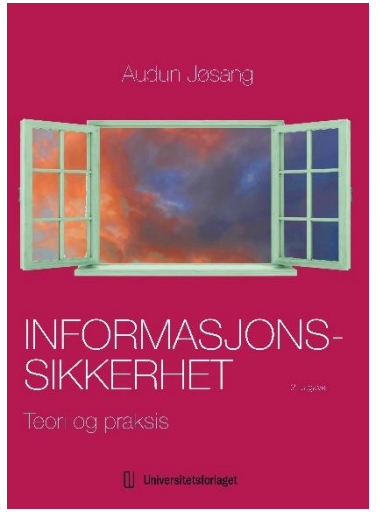
Kapittel 17
Cyberoperasjoner

Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utg. 2023

Universitetsforlaget



Oversikt

I denne forelesning vil du lære om

- Cyberoperasjoner
- Hva «cyber kill chain» er
- Avanserte trusselaktører / Advanced Persistent Threat (APT)
- MITRE ATT&CK rammeverket
- Digital trusseletterretning
- Cyberkrigføring

Hva er en cyberoperasjon?

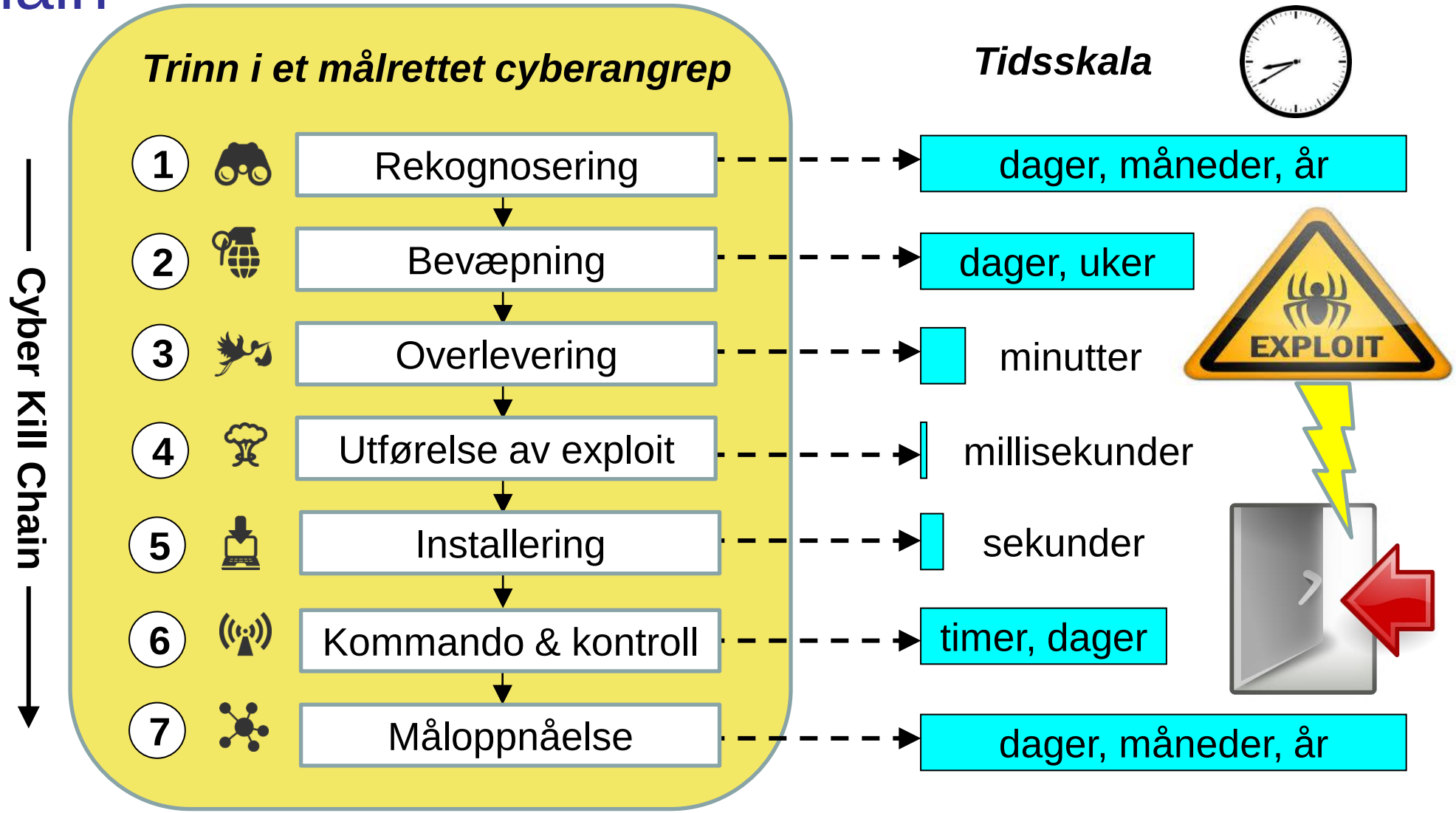
- «Cyberoperasjoner» er et ganske vagt begrep som ofte brukes om forsvar og angrep av digitale infrastrukturer
- I en militær setting snakker man ofte om *offensive* og *defensive* cyberoperasjoner
- *Offensive cyberoperasjoner* brukes om uautorisert tilgang til informasjon og data i IKT-systemer (datainnbrudd). For eksempel statlige aktører eller kriminelle som bryter seg inn i systemer for vinningskriminalitet eller sabotasje.
- *Defensive cyberoperasjoner* brukes om hvordan en cyberoperasjon brukes til å håndtere disse datainnbruddene, enten noen er rammet av dem eller de har mistanke om at målrettede datainnbrudd vil skje.

Avanserte angrep/cyberoperasjoner

- Cyberoperasjoner brukes ofte om aktiviteter i digitale infrastrukturer utført av statlige aktører.
- Vi har sett flere tilfeller av disse mot norske mål
  - Angrep mot Helse Sørøst (2018)
  - Angrep mot statsforvaltere (fylkesmenn) (2018)
  - Angrep mot Stortinget (2020,2021)
  - Angrep mot Østre Toten kommune (2021)
- Disse varer ofte over lengre tid
- … og over flere steg

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

CKC 1. Rekognosering

- Trusselaktøren velger ut det potensielle offeret
- Samler informasjon og «forsker» på det
- Forsøker å identifisere sårbarheter i nettverket som kan utnyttes
- Kan innebære skanning av infrastruktur, bruk av nyheter, sosiale medier, etc.
- Eksempel:
  - Et firma velges for å uthente spesifikk informasjon for bruk i vinningskriminalitet
  - Gjennom skanning av nettverket identifiser systemer som brukes og en gitt tjeneste har en kjent sårbarhet som kan utnyttes gjennom en makro i et PDF dokument
  - Gjennom annonser oppdages at firma her en jobb ute på anbud
  - Gjennom LinkedIn oppdages en aktuell kontaktperson for anbudet som trolig har god systemtilgang

CKC 2. Bevæpning

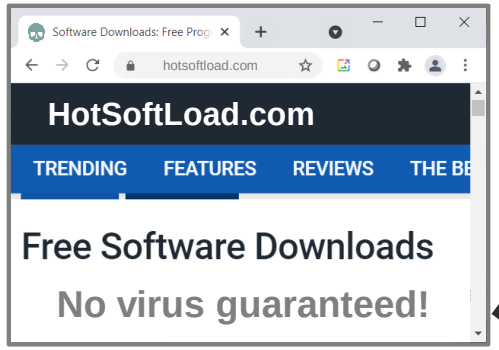
- Trusselaktøren konstruer exploit-skadevare i et egnet format som kan leveres til offeret
- Kan f.eks. utnytte en eller flere kjente sårbarheter eller nulldagssårbarheter

- Eksempel:
  - En exploit som utnytter den gitte sårbarheten lages og integreres i en PDF fil som skal imiterer et reelt anbud på jobben.

CKC 3. Overlevering

- Skadevare som ble utviklet overleveres til målet for angrepet
- Kan f.eks. være gjennom en USB, webtjener, phishing eller andre **angrepsvektorer**

CKC 3. Overlevering: Gjennom angrepsvektorer



7

Installering av skadelige programmer fra internett eller andre lagringsmedia.

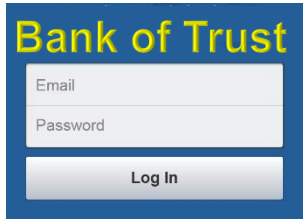
1

Drive-by-angrep fra kriminelle eller infiserte nettsider.

2

Phishing-e-post, SMS og meldinger

3



Falske nettsider som stjeler bruker-ID og passord.

6

Skadelige eksterne enheter.

5

Infisering og angrep gjennom leveransekjeden.

4

Direkte angrep gjennom internett.

CKC 3. Overlevering

- Skadvare som ble utviklet overleveres til målet for angrepet
- Kan f.eks. være gjennom en USB, webtjener, phishing eller andre **angrepsvektorer**

- Eksempel:
  - En spear-phishing epost som later som å være fra en tidligere brukt leverandør opprettes
  - Sendes til identifiserte kontaktperson med PDF som vedlegg

CKC 4. Utførelse av exploit/utnyttelseskode

- Kjøring av exploit som utnytter sårbarhet i system til målet.

- Eksempel:
  - Den identifiserte kontaktpersonen ser eposten
  - Den ser reell ut så PDF åpnes for å se tilbudet
  - Dette medfører at exploit kjøres

CKC 5. Installering

- Skadevare installeres på systemet
- En vanlig effekt av å kjøre exploit er å få åpnet en eller annen form for tilgangspunkt (f.eks. en bakdør) i form av en kommando og kontroll (K2, C2, C&C) kanal angriper kan bruke.
- Nå har angriper ekstern tilgang til det infiserte systemet.

- Eksempel:
  - Exploit kjøres og brukes til å installere seg på systemet og åpner en bakdør tilbake til angriperen
  - Angriper kan nå aksessere målets systemer gjennom K2-kanalen

CKC 6. Kommando og kontroll (K2)

- Angriper kan utforske nettverket rundt det infiserte systemet, forplante seg videre til andre systemer (lateral movement), skjule spor og identifisere ressurser som kan stjeles/saboteres/utnyttes.
- Kommunikasjon med angriper gjennom opprettet K2-kanal

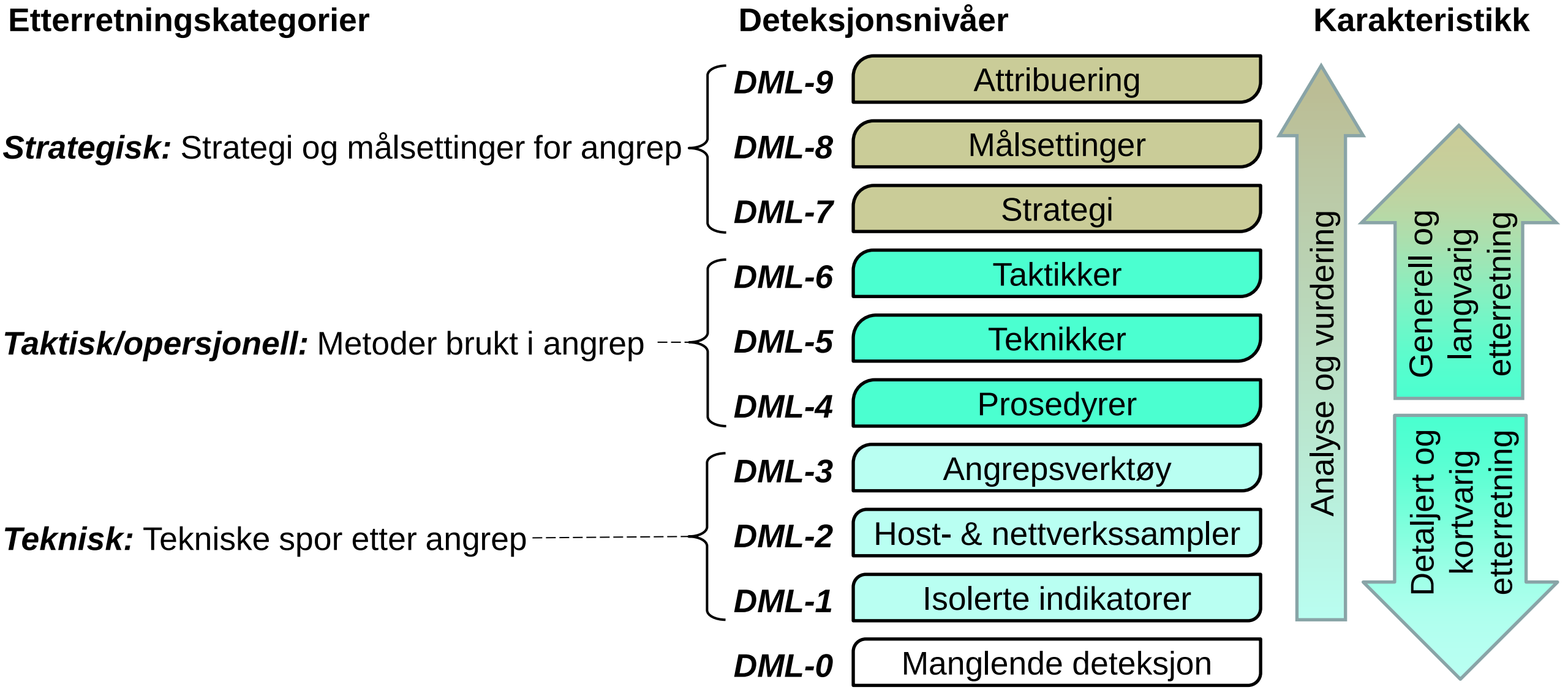
- Eksempel:
  - I dette eksempel var målet spesifikk informasjon
  - Angriper søker gjennom nettverket for å identifisere aktuell informasjon og skjuler sine spor på veien

CKC 7. Måloppnåelse

- Det faktiske målet med angrepet utføres
- Dette kan være uthenting av data som betyr at data samles inn, klargjøres og sendes ut av nettverket til servere som kontrolleres av angripere
- Det kan også være sabotasje, og i så fall blir ødeleggende aksjoner iverksatt.

- Eksempel
  - Angriper har nå funnet aktuelle documenter.
  - Det er såpass mange og de er store at disse overføres over lengre tid for å unngå at dette detekteres
  - Dette gjøres gjennom en skjult kanal mot Facebook
  - Etterpå slettes alle spor om uthentingen i systemet

Detection Maturity Leve (DML) modellen (Stillions)



Detection Maturity Level

- DML-modellen sier at det er relativt enkelt å detektere **tekniske spor** som IP-adresser, domener og filnavn på skadevare, fordi det kan leses direkte ut av loggene, det vil si at det kun krever lav modenhet i hendelsesrespons og digital trusseletterretning.
- Det kreves større modenhet av en virksomhet å kunne detektere hvilke **taktikker, teknikker og prosedyrer** en trusselaktør har benyttet i et angrep, fordi disse aspektene kan ikke leses direkte ut av loggene.
- Det kreves enda større modenhet for å kunne forstå angriperens bakenforliggende **strategier** og for å kunne **attribuere** et angrep til en spesifikk gruppering. Deteksjon av taktikker for uthenting av informasjon (MITRE ATT&CK Exfiltration) eller taktikker for sabotasje (MITRE ATT&CK Impact) vil indikere angriperens målsetting.

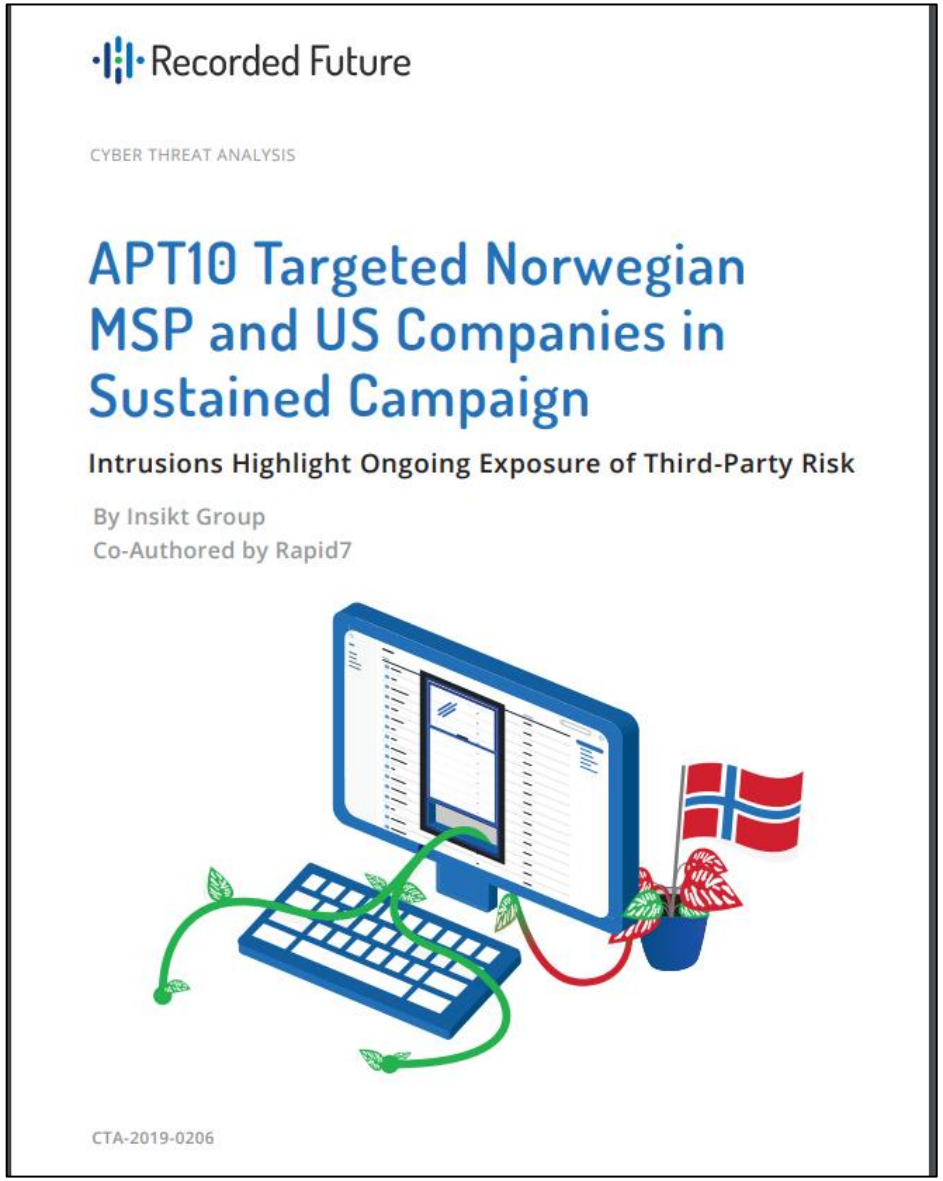
APT – Advanced Persistent Threat

- Et begrep som ofte brukes i tilknytning til det illustrerte eksempelet er APT.
- En APT (*Advanced Persistent Threat* eller *avansert vedvarende trussel*) er en trusselaktør eller gruppering.
- Tilhører ofte, eller er ofte sponset av, nasjonalstater.
- Finnes også kriminelle APT-er uten slik tilknytning til nasjonalstater.
- En APT må sees på som en gruppering med en *aktivitetsprofil.*
- Cyberoperasjoner fra APT-er er typisk målrettede mot land og sektorer (f.eks. forsvar, finans, industri, helse, energi, …).

APT – avansert og vedvarende trussel

- En APT er avansert (*Advanced*) fordi den har til rådighet rikelig med ressurser for etterretning, kompetanse og utvikling av expoits til å kontrollere infrastrukturer og utføre angrep.
- En APT er vedvarende (*Persistent*) fordi den har langsiktige målsetninger – ofte fastlagt av overordnede politiske eller strategiske enheter.
  - Betyr at den er utholdende og ikke lar seg stoppe av motstand
  - Har utholdenhet til å utføre angrep i sakte tempo
  - Går under radar og vanskeligere å oppdage
  - Cyberoperasjoner kan vare over flere år
- En APT er en trussel (*Threat*) da den har hensikt, mulighet og kapabilitet.

Beskrivelse av APTer - eksempler



- https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
- https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

MITRE ATT&CK

- MITRE er en amerikansk (non-profit) organisasjon. Gjennom forsknings- og utviklingsaktiviteter støtter de mange amerikanske organisasjoner på ulike nivåer, i både offentlig og privat sektor, inkludert akademia.
- MITRE ATT&CK er en kunnskapsbase som strukturer taktikker og teknikker brukt av angripere og ulike APT-grupper
- Inneholder mapping av ulike APT-grupper med teknikker observert av dem
  - *Merk: fokus er mot amerikanske/vestlige interesser og MITRE ATT&CK inneholder blant annet ikke amerikanske NSA, som er svært aktiv innenfor offensive cyberoperasjoner*
  - *De skyldes at de ikke anses som en trussel mot amerikanske interesser*
- Basert på observasjoner av faktiske hendelser
- En viktig del av rammeverket er ATT&CK-matrisen med flere tilhørende prosjekter. Kan blant annet brukes som basis for trusselmodellering

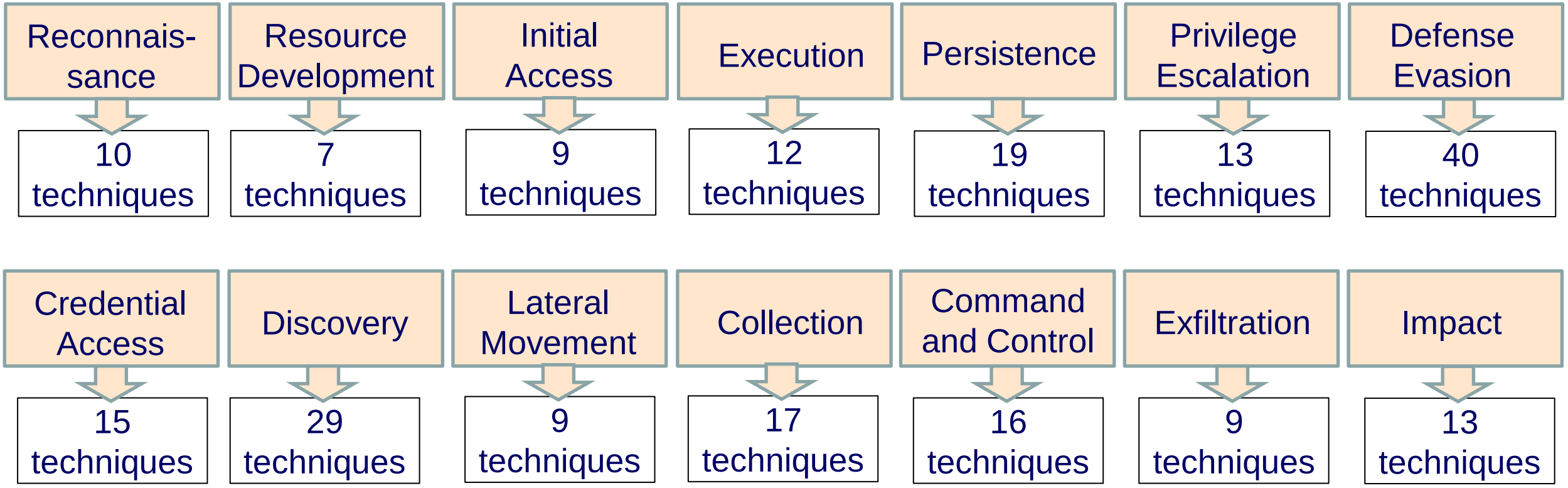
MITRE ATT&CK-matrisen

- ATT&CK matrisen er strukturert rundt teknikker og taktikker
- En *teknikk* representer *hvordan* en angriper oppnår et taktisk mål gjennom å utføre en handling.
  - Dette kan for eksempel være phishing for å få tilgang til et system.
  - En teknikk kan være deles opp i del/under-teknikker
- En *taktikk* representerer *hvorfor* en teknikk utføreres, med andre ord et (del)mål for angriperen.
  - For eksempel er «tilgang til system» en taktikk.
- I ATT&CK-matrisen er hver kolonne en taktikk med teknikker listet under dem.

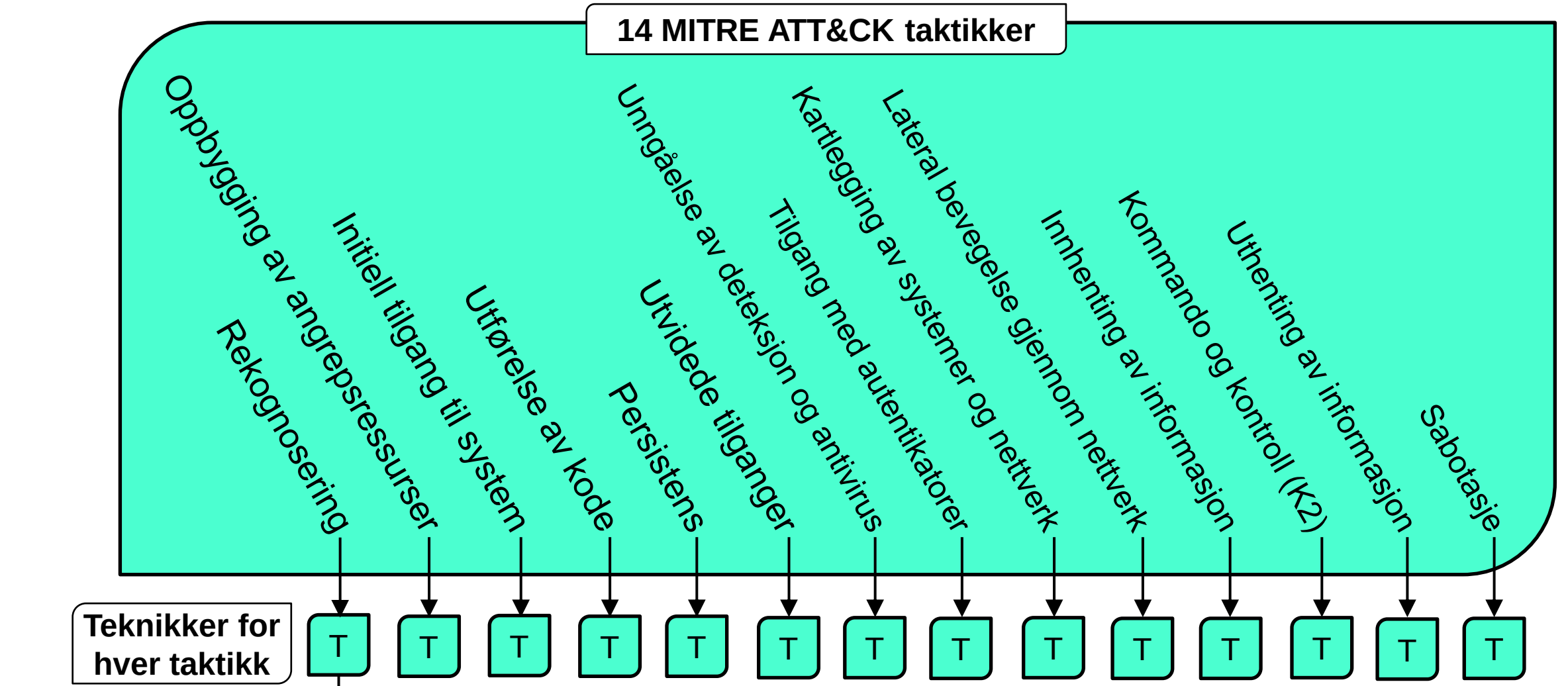
https://attack.mitre.org/

MITRE ATT&CK-matrisen

- For hver av de 14 taktikkene (delmål) er det spesifisert et antall teknikker som angripere typisk benytter for å oppnå (del)målet.



https://attack.mitre.org/


14 MITRE ATT&CK taktikker
Oppbygging av angrepsressurser
Initiell tilgang til system
Utførelse av kode
Unngåelse av deteksjon og antivirus
Kartlegging av systemer og nettverk
Lateral bevegelse gjennom nettverk
Innhenting av informasjon
Kommando og kontroll (K2)
Uthenting av informasjon
Sabotasje
Rekognosering
Persistens
Utvidede tilganger
Tilgang med autentikatorer
Teknikker for hver taktikk
T
Eksempel teknikker for rekognosering
• Aktiv skanning
• Kartlegg målnode
• Kartlegg målidentitet
• Kartlegg målnettverk
• Kartlegg målorganisasjon
• Phishing
• Søk lukkede kilder
• Søk åpne databaser
• Søk åpne nettsider
• Søk målorganisasjonens nettsider

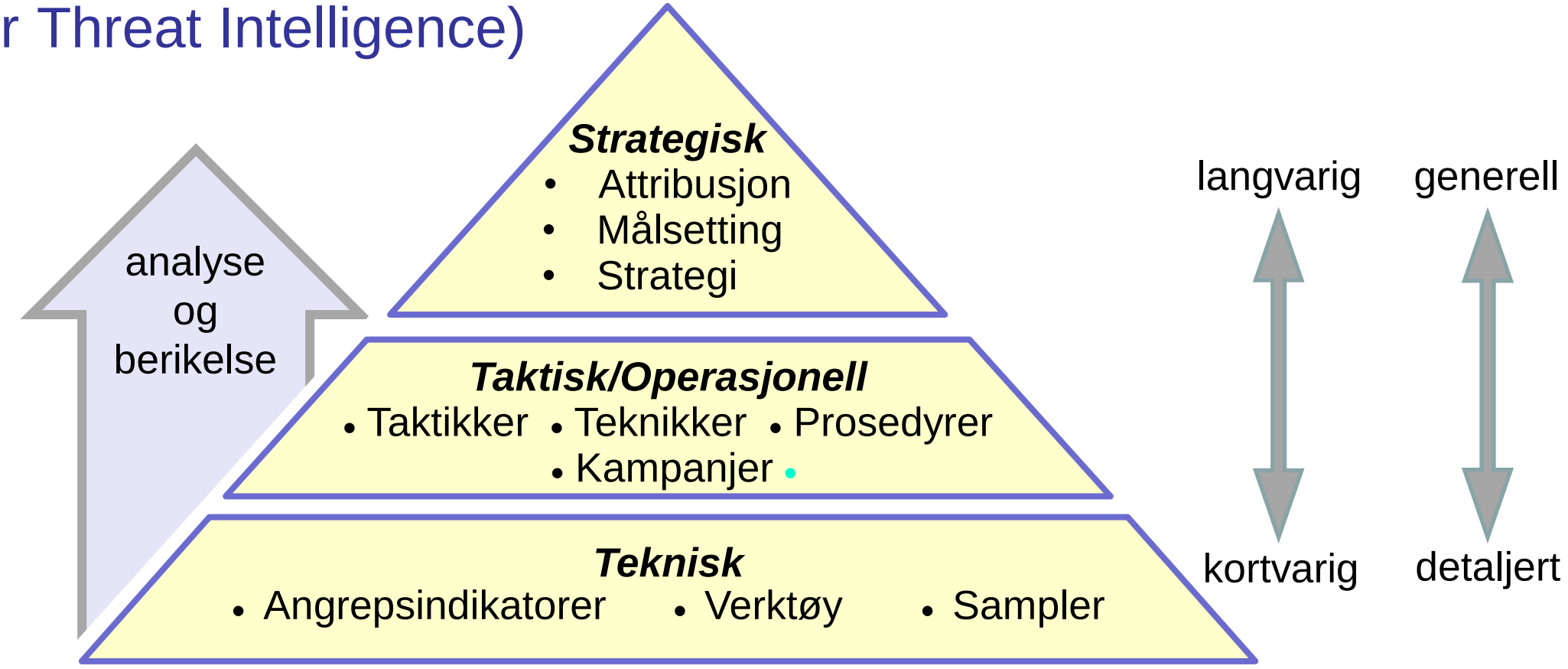
MITRE ATT&CK og APT-er

[https://attack.mitre.org/groups/]

- Oversikt over ulike grupper/APT-er, per dags dato info om 129 grupper
- Mapper hver APT til observerte teknikker i ATT&CK-matrisen

ID	Name	Associated Groups	Description
G0073	APT19	Codoso, C0d0so0, Codoso Team, Sunshop Group	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.
G0007	APT28	SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127	APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165. This group has been active since at least 2004. APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. In 2018, the US

Kategorier av digital trusseletterretning
(CTI: Cyber Threat Intelligence)

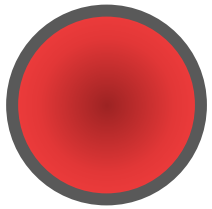


- CTI kan grovt sett deles inn i de tre hierarkiske kategoriene: teknisk, operasjonell og strategisk CTI.

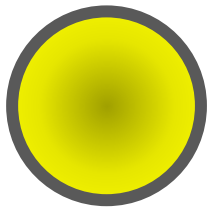
CTI-kategorier

- **Strategisk CTI:** Beskrivelse en trusselaktør/APT basert på observerte aktiviteter og annen etterretning, samt å forstå overordnede målsettinger og strategier hos trusselaktøren. Attribusjon betyr at en CTI-entitet er i stand til å identifisere hvilken gruppering som står bak et angrep. Strategisk CTI er viktig for bedre å posisjonere og prioritere ressurser i forsvar mot truslene.
- **Taktisk/operasjonell CTI:** Informasjon om hvilke verktøy og taktikker, teknikker og prosedyrer (TTP-er) som brukes i et angrep. Begrepet TTP kan tolkes som måten trusselaktøren utfører et angrep på, eller som en «angrepsoppskrift». En trusselaktør har som regel et begrenset utvalg av slike angrepsoppskrifter (TTP-er) som de mestrer og er vant til å bruke.
- **Tekniske CTI:** Indikatorer (eng.: indicators of compromise) om angrep, som typisk kommer fra monitorering og logging av aktiviteter i systemer og nettverk. Angrepsindikatorer består f.eks. av IP-adresser, domenenavn, signaturer (hash-verdier) av observert skadevare samt observert bruk av spesifikke verktøy.

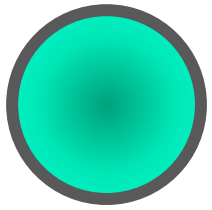
Trafikklysprotokollen for deling av CTI



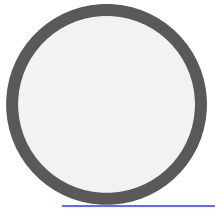
- **RØD (RED**): Personlig, kun for navngitte mottagere. Under møter mellom fagfolk er for eksempel RØD informasjon begrenset til de som er til stede. Distribusjonen av RØD informasjon går vanligvis til en fast liste, og under ekstreme omstendigheter kan den bare sendes muntlig eller personlig.



- **GUL (AMBER):** Begrenset distribusjon, mottageren kan dele AMBER-informasjon med andre i organisasjonen, men bare på «behov-for-å-vite»-basis (eng.: need-to-know). Avsenderen kan spesifisere de tiltenkte mottagerne på en detaljert måte.



- **GRØNN (GREEN):** Innen miljøet, kan sirkuleres bredt innenfor et bestemt miljø. Imidlertid kan ikke informasjonen publiseres eller legges ut offentlig på internett, og kan heller ikke videresendes utenfor miljøet.

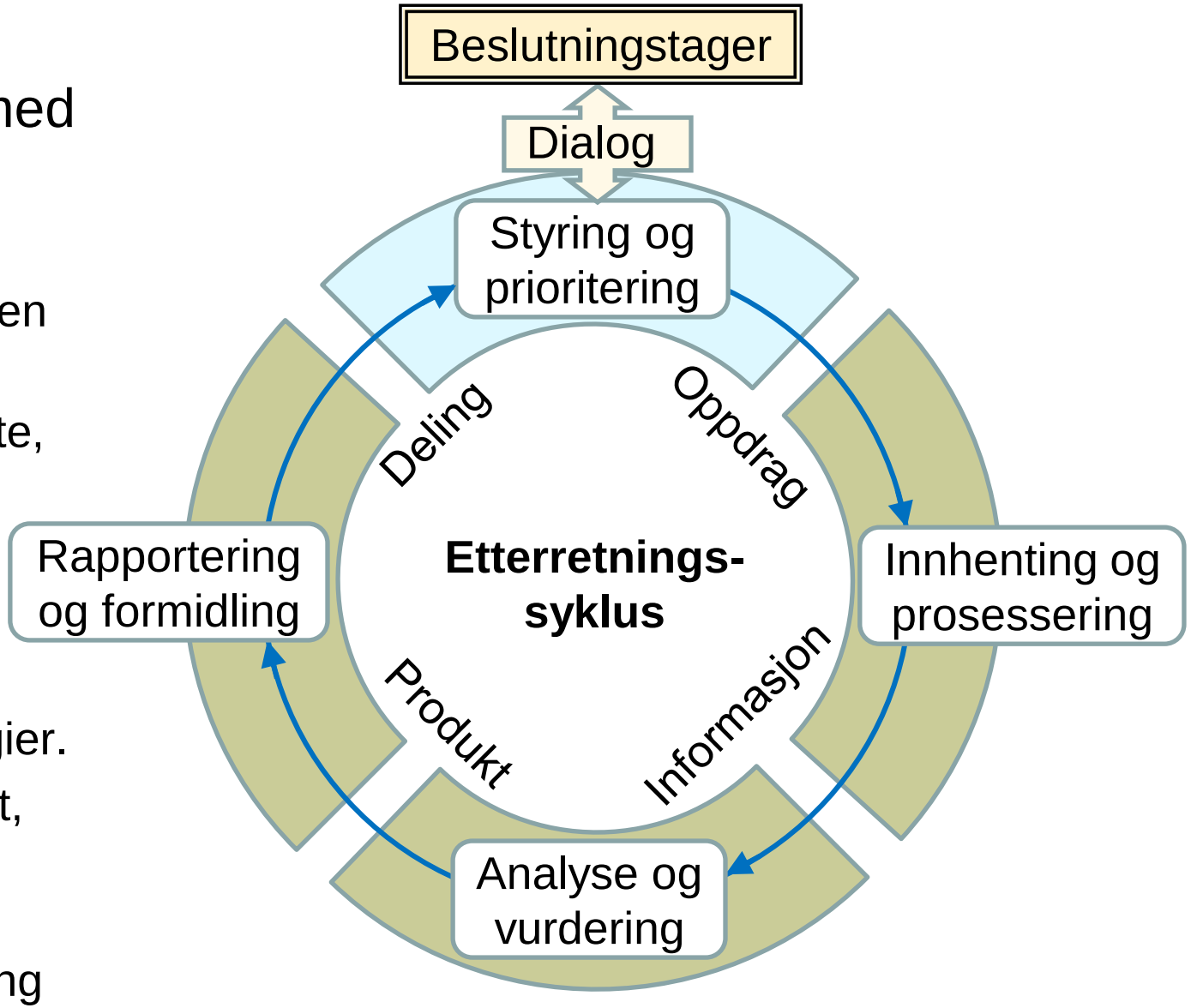


- **HVIT (WHITE):** ubegrenset, kan distribueres fritt, uten begrensning.

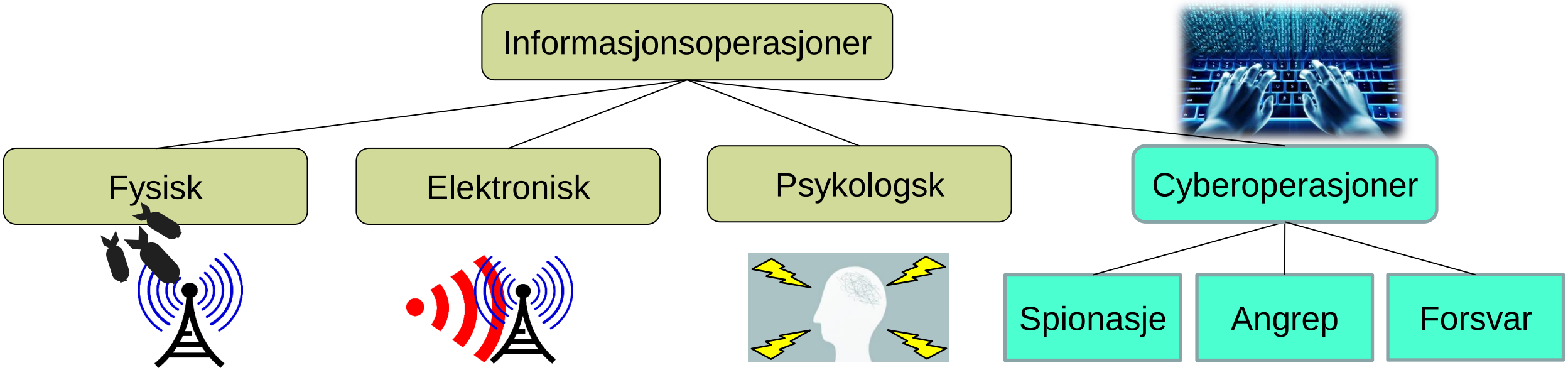
CTI-syklus

Etterretningssyklusen ble definert for med militær etterretning, men kan også benyttes for CTI.

- Trusler kan være rettet mot en virksomhet, en sektor eller en hel stat.
- Kilder kan være manuelle eller automatiserte, og kan være interne eller eksterne.
- Data som er innsamlet må kvalitetssikres.
- CTI som er nyttig for for å ta beslutninger.
- Analyse kan f.eks. gjøres med AI (kunstig intelligens) eller logisk-semantiske teknologier.
- Tradisjonelt artikuleres CTI som vanlig tekst, og deles som pdf-dokumenter med andre entiteter, men dette skalerer dårlig.
- Det utvikles platformer for automatisert deling basert på maskinlesbar CTI.



Informasjonskrigføring



Cyberoperasjoner, aka. Nettverksoperasjoner

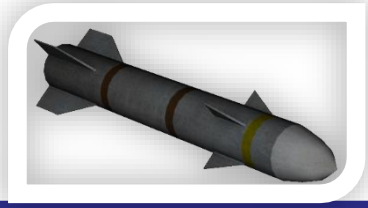
- Nettverksoperasjoner (Computer Network Operations)
  (NATO Allied Joint Publication)
  - Spionasje (Computer Network Espionage: CNE)
  - Angrep (Computer Network Attack: CNA)
  - Forsvar (Computer Network Defense: CND)

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

Attribusjon av cyberoperasjoner

- Ugjennomsiktig (the fog of) cyberkrigføring
  - Vanskelig å finne link til bakenforliggende makt og dens målsetting for en cyberoperasjon
  - Typisk flere hypoteser om identitet og intensjon for en cyberoperasjon.
  - Feil attribusjon av angrep kan forårsake utilsiktet (politisk) skade
- "Reversing" av cyberangrep
  - Basert på analyse av observerte indikatorer, og CTI (Cyber Threat Intelligence)
  - Attribusjon og forståelse av hensikten med angrep
  - Utfordrende fordi
    - Angrep kan kanaliseres gjennom flere kanaler og noder for å forvirre back-tracking
    - Bevisst feilrepresentasjon av angrepsindikatorer
    - Vanskelig å forstå intensjon basert på observert aktivitet

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

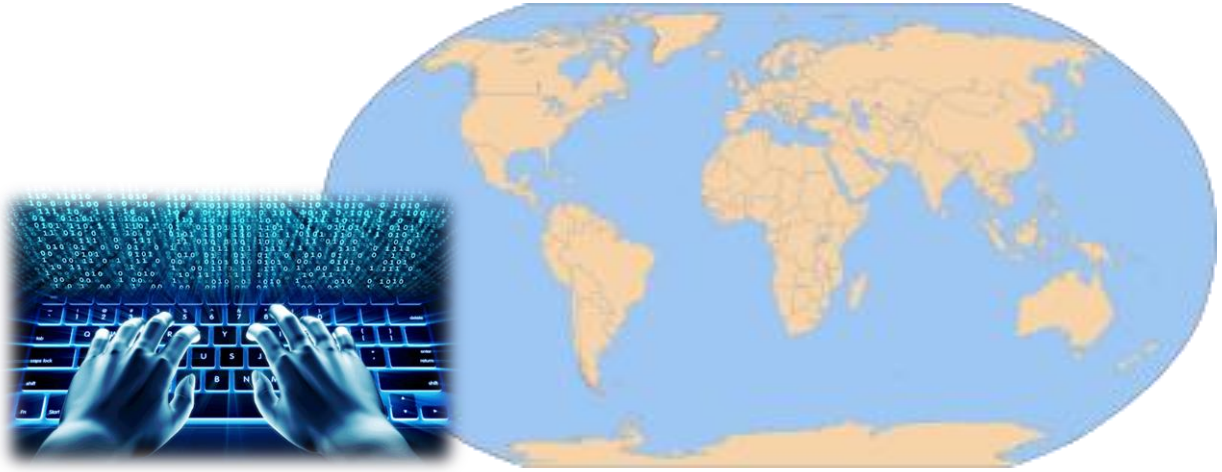
- Kan lamme digitale systemer og prosesser
- Angrep mot kritisk infrastruktur kan være spesielt skadelig
- Konsekvens kan reduseres ved god beredskap og hendelseshåndtering
- Angripere må ha betydelige ressurser for å oppnå betydelig effekt
- Ofte billigere å få tilsvarende effekt med fysiske angrep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

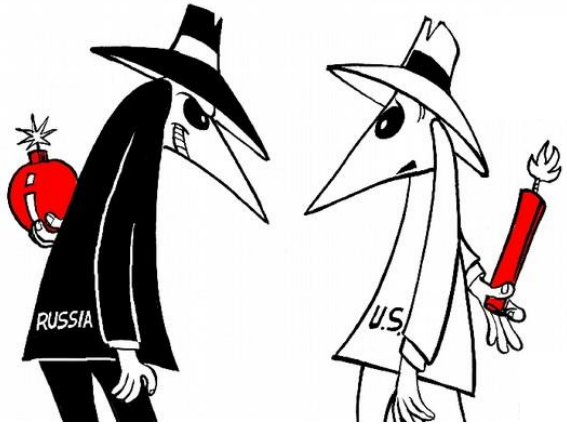
By DAVID E. SANGER APRIL 24, 2016

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, Maryland. 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.

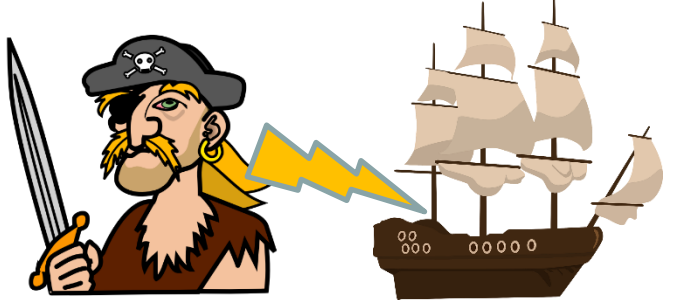
The New York Times

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

June 15 2019

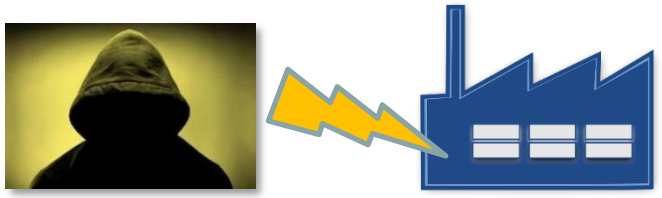
Cyberkaperfart



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

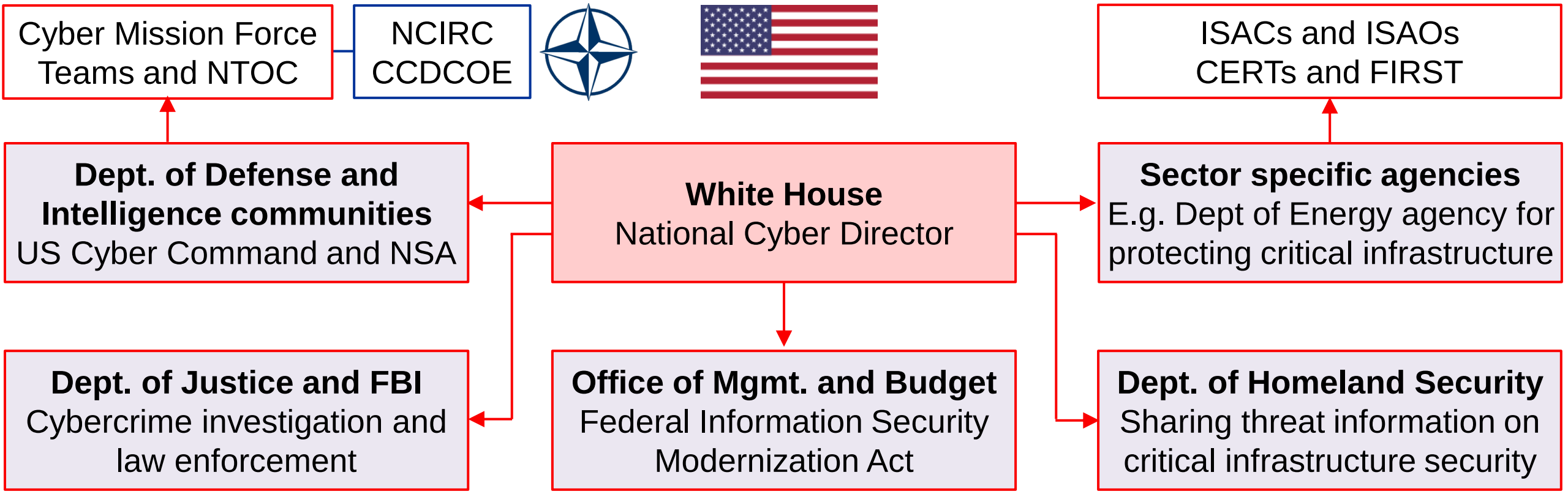
Computerprodusenter

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

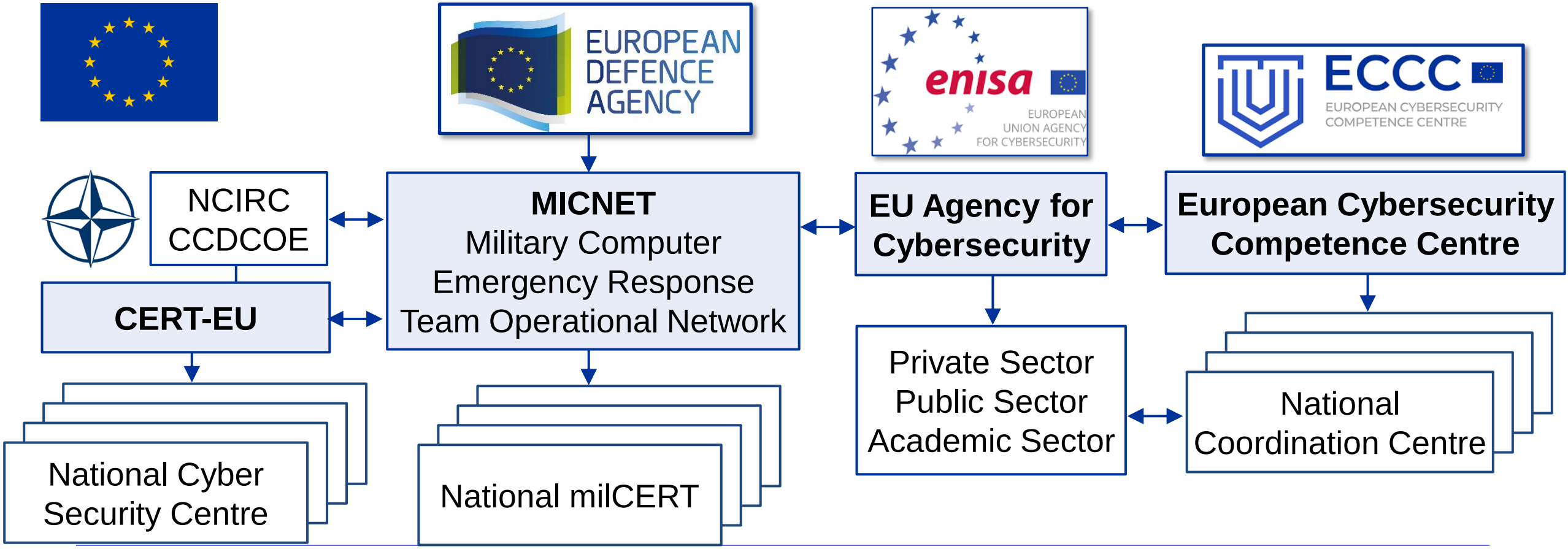
Skytjenester

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

Struktur av cyberorganisasjoner i USA



Struktur av cyberorganisasjoner i Europa



Struktur av cyberorganisasjoner i Russland

President of the Russian Federation

FSB (ФСБ)
Federal Security Service

SVR (СВР)
Foreign Intelligence Service

GRU (ГРУ)
Military Intelligence

Centre 16
of the collection of radio electronic Intelligence on communication facilities

Centre 18
for Information Security (TsIB)

Cosy Bear
(APT29)

85th
Special Service Main Center

GTsST
Main Center for Special Technologies

Berserk Bear
(APT)

Snake
(APT)

Star Blizzard
(APT)

Fancy Bear
(APT28)

Sandworm
(APT)

Struktur av cyberorganisasjoner i Kina

President of the People's Republic of China (PRC)
Chinese Communist Party (CCP)

State Council Information Office
(Central Propaganda Dpt of the CCP)

Cyberspace Administration of China
(Cyberspace Policy Enforcement)

State Council of the PRC
(Ministries)

People's Liberation Army (PLA)
(Chinese Army)

CNITSEC
Information Technology Evaluation Centre

Ministry of State Security

CNNVD
National Vulnerability Database

PLASSF
PLA Strategic Support Force

Magnese APT5	**Stone Panda** APT10	**Ke3Chang** APT15	**Lucky Mouse** APT27
Zirconium APT31	**Leviathan** APT40	**Winnti** APT41	**HoneyMyte** (APT)

Tonto Team (APT)	**Tick** (APT)
Putter Panda (APT)	**PLA Navy** APT18

Hvor går cyberkrigføring?

- Manglende internasjonale regler for cyberoperasjoner
- Cyberkrigføring rammer alle virksomheter
- Big Tech spiller en viktig rolle
- ?

Slutt på presentasjonen