

# IN5080

## Sikkerhets- og risikostyring

---

### Del 11b: Cyberkrigføring



Audun Jøsang

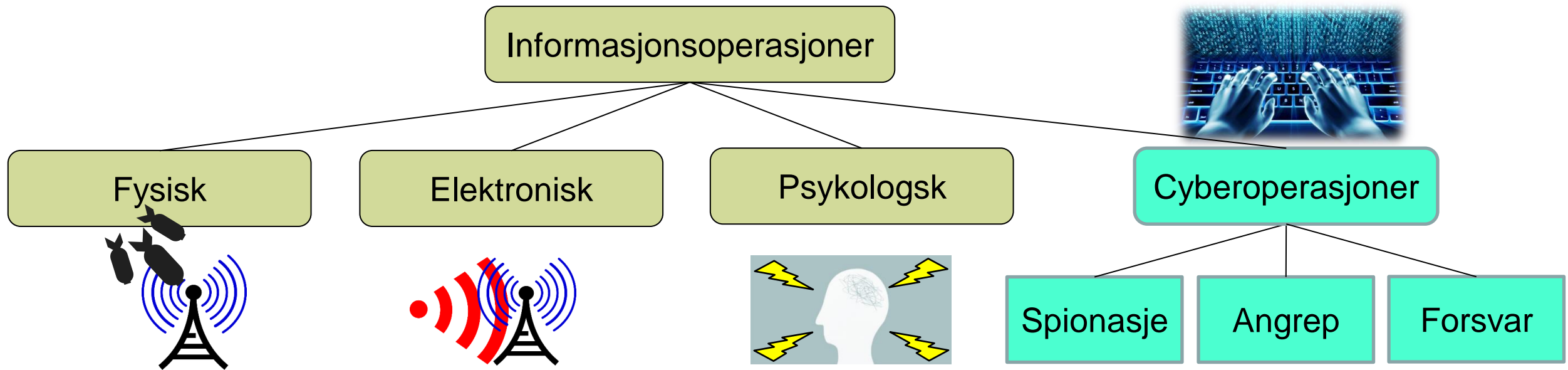
Universitetet i Oslo

Vår 2024

# Oversikt: Cyberkrigføring

- a. Begreper
- b. Cybervåpen
- c. Cyberavskrekking
- d. Cyberkaperfart
- e. Big Tech sin rolle
- f. Cyberorganisasjoner

# Informasjonskrigføring



# Cyberoperasjoner, aka. Nettverksoperasjoner

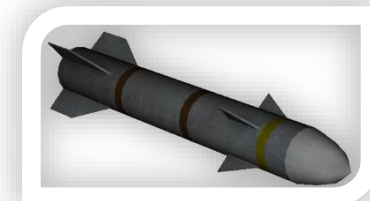


- Nettverksoperasjoner (Computer Network Operations)  
(NATO Allied Joint Publication)
  - Spionasje (Computer Network Espionage: CNE)
  - Angrep (Computer Network Attack: CNA)
  - Forsvar (Computer Network Defense: CND)



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

# 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 våpen 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 inkludere 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.



# 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.



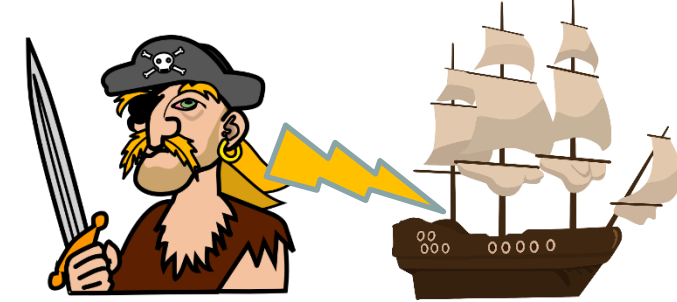
## *U.S. Escalates Online Attacks on Russia's Power Grid*



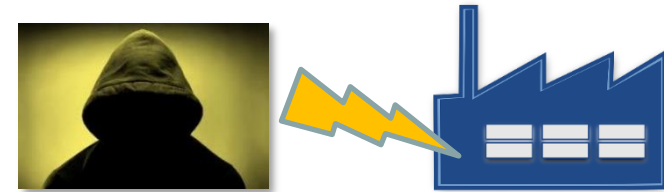
A heating power plant in Moscow. Officials described the move into Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections. *Maxim Shemetov/Reuters*

# Cyberkaperfart

- 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.
- 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.



Kaperfart 1600 - 1850



Cyberkaperfart 2020→



# 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



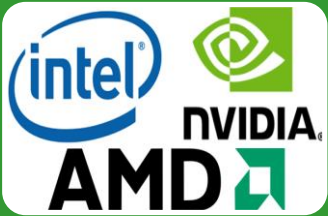


# Potensiale for samarbeid med Big Tech



## 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

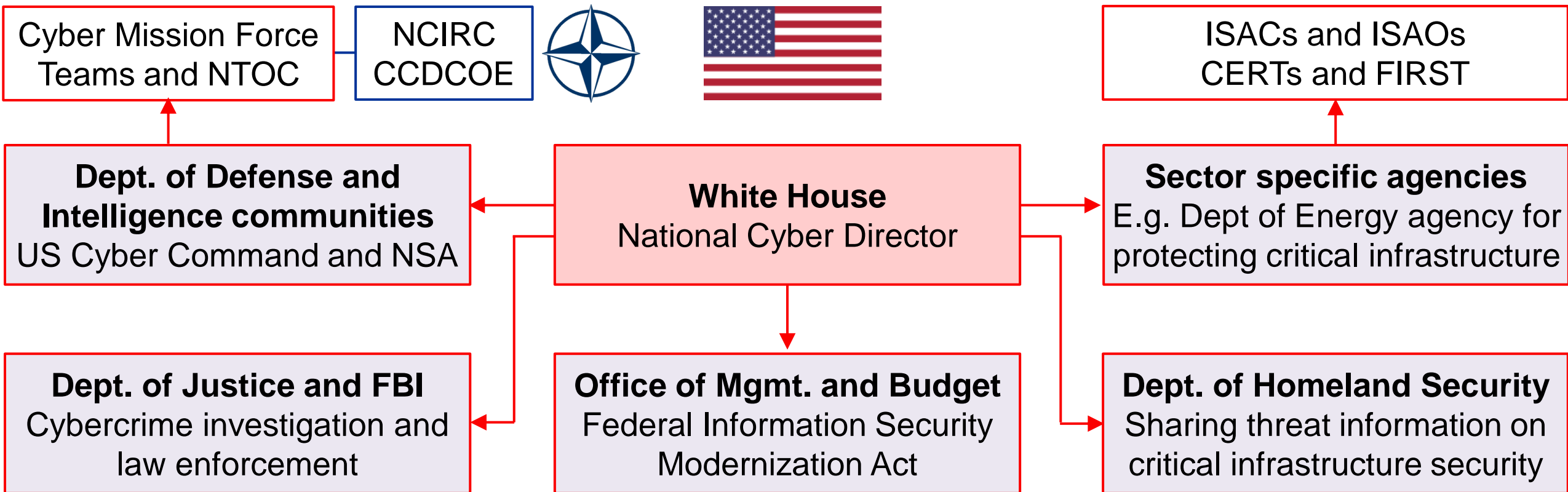
- Konfigurerer oppstart, kan bygge inn spionvare under produksjon
- Overvåking og styring av computerplattformer under drift



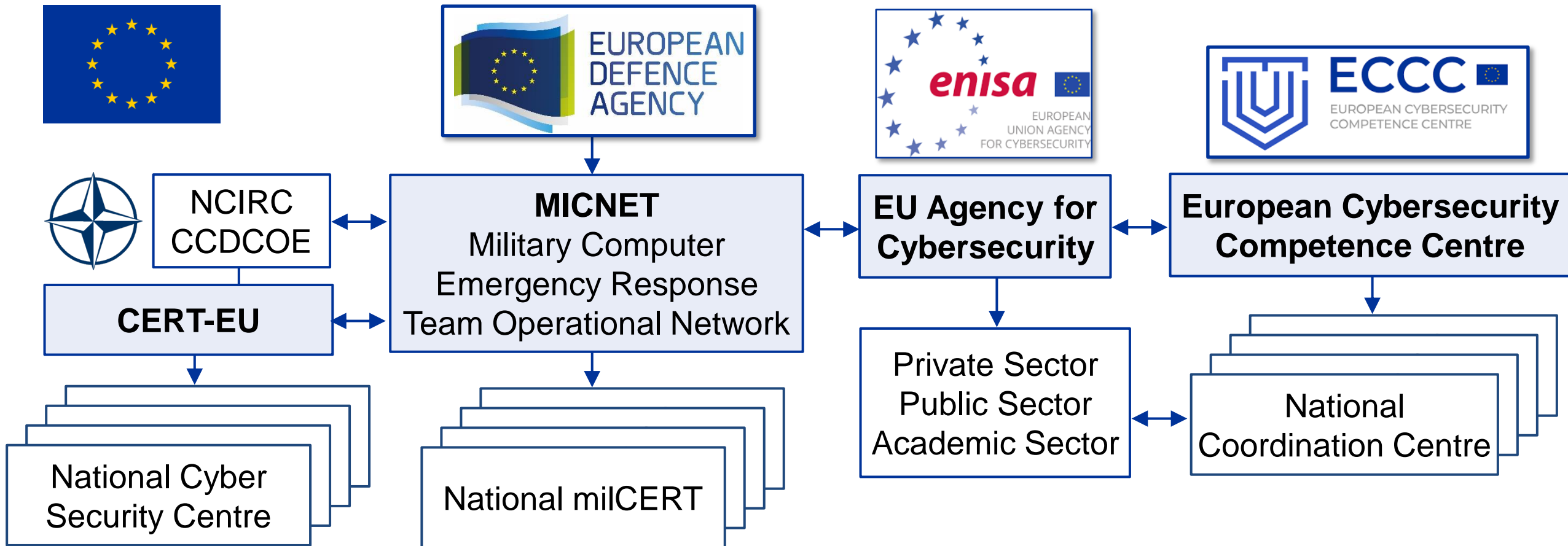
## Skytjenester

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

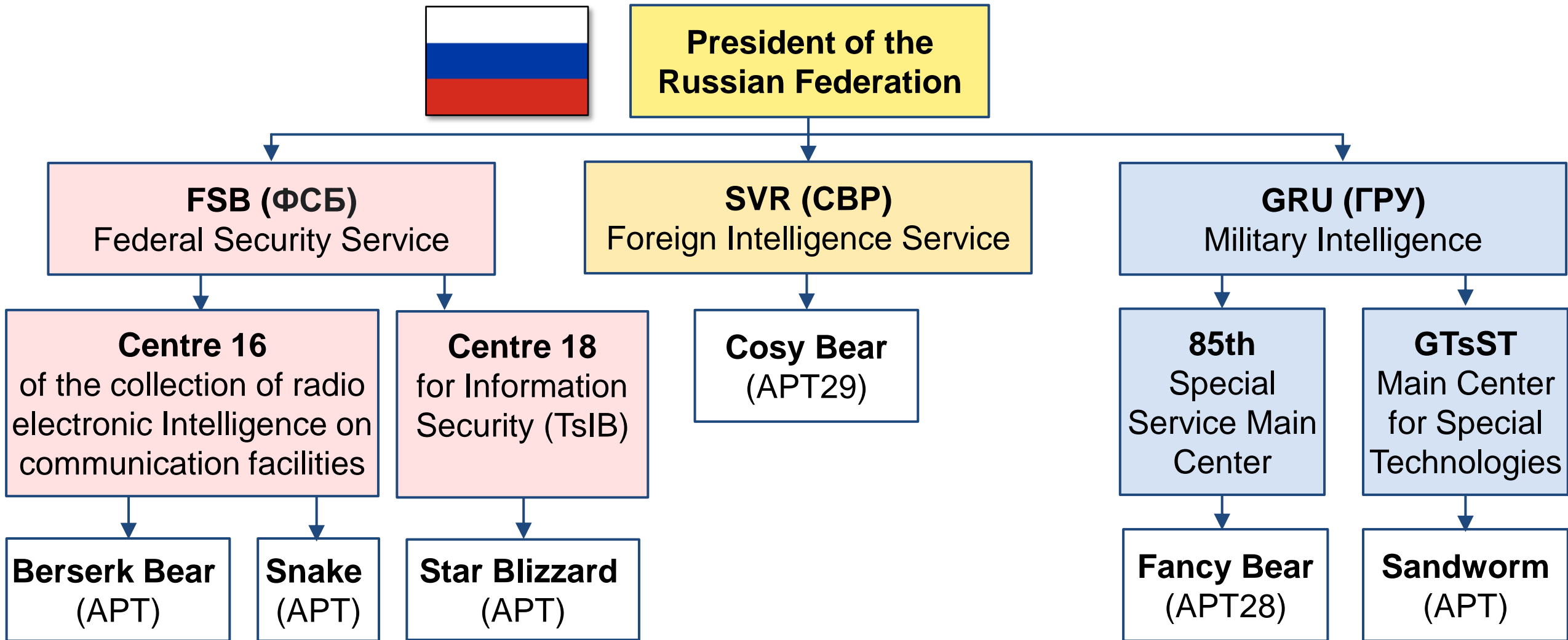
# Struktur av cyberorganisasjoner i USA



# Struktur av cyberorganisasjoner i Europa



# Struktur av cyberorganisasjoner i Russland







# Hvor går cyberkrigføring?

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

