Security
Tech Space
NATIONAL TRYGHED - MED SIKKERHED

Danmark kan udvikle NATO's og EU's Cyberskjold

I fremtidens hybridkrige er det nødvendigt med et cyberskjold, der er lige så effektivt som et moderne missilskjold i den fysiske verden. Et sådant cyberskjold vil beskytte både kritiske militære installationer og civile infrastrukturer mod cyberangreb. Cyber Campus Denmark bygger på Danmarks stærke position inden for cybersikkerhed og sigter mod at udvikle et robust cyberskjold, der kan beskytte Danmark, NATO og EU's infrastrukturer.

FORSVARSMÆSSIGE EFFEKTER I AT INVESTERE I CYBER CAMPUS DENMARK

Hvis Danmark investerer i Cyber Campus Denmark, vil vi kunne bidrage til at løse følgende udfordringer for Forsvaret og allierede i NATO og EU:

- **National Sikkerhed:** National og international sikkerhed med et effektivt cyberskjold, der beskytter kritisk infrastruktur, offentlig administration, medier m.m.
- **Cybertrusler:** Effektivt cyberskjold med kompetencer og værktøjer til at forsvare os mod stadigt mere sofistikerede cyberangreb.
- **Personelmangel:** Rekruttering, uddannelse og fastholdelse af cyberpersonel på alle niveauer.
- **Teknologisk niveau:** Modernisering af Forsvarets kommunikations- og datasystemer for at holde trit med udviklingen i cyberangreb og spionage.
- **Vækst i forsvarsindustri:** Erhvervsudvikling og innovation indenfor forsvarsindustrien, der kan styrke Danmarks position i EU og NATO.

ET CYBERSKJOLD KRÆVER INVESTERING I KAPACITET OG KOMPETENCER

For at opnå de nævnte effekter på både kort og langt sigt skal der investeres på fire centrale områder: Uddannelse, forskning, innovation og udvikling af forsvarsindustrien.

1 UDDANNELSE ER NØDVENDIG FOR AT KUNNE SKALERE CYBERFORSVARET

Etablering af en cyberbrigade med op til 4000 cyber-soldater.

- **Cyberværnepligtige:** I første omgang udvides cyberværnepligten i Fredericia, dernæst etableres en ny cyberværnepligt i Aarhus. Med mulighed for en kompetencegivende universitetsoverbygning (tid fordelt mellem universitet og Forsvar efter forsvarets behov).
- **Cyberofficerer og cyberforsvarsforskere:** Med basis i cybersikkerheds-universitetsuddannelser på alle niveauer uddannes forsvarsledere op til de højest rangerende officerer samt forskere med fokus på cyberforsvar til Forsvarsakademiet.
- **Efteruddannelse:** Basale cyberkompetencer bør være en del af alle videregående IT-uddannelser. Der vil ydermere være behov for kontinuerlig opkvalificering i cybersikkerhed for fastansatte, reservister og frivillige i Forsvaret mange år fremover.

2 FORSKNING ER NØDVENDIG FOR AT VÆRE FORAN FJENDEN

- **Kryptografisk fundament:** Udvikling af stadigt mere effektiv og sikker kryptering til kommunikation, distribution og datadeling, herunder kryptering, der kan køre på små enheder og kryptering, der kan forsvare os mod fremtidens kvantecomputere. Metoderne kan potentielt spille ind fremtidens NATO-standarder,
- **Kunstig Intelligens:** Implementering af AI-baserede screeningssystemer, der kan detektere og respondere på cyberangreb i realtid og finde fejl i programkode.
- **Sikker systemudvikling:** Metoder til at sikre verificeret fejlfri og robust software og hardware systemarkitekturer uden sikkerhedshuller til både militære og civile anvendelser. Herunder udnyttelse af særlig "trusted" hardware, der er sikkerhedsverificeret.
- **Kriseledelse:** Forskning i krisehåndtering på strategisk, operationelt og taktisk niveau
- **Menneskelige faktorer:** Forskning i menneskers håndtering af cybersikkerhed og krisehåndtering.
- **Sikkerhedslaboratorium:** Etablering af et sikkerhedslaboratorium (Security LAB) for fortrolig forskning i cybersikkerhed, hvilket vil bidrage til innovative og sikre løsninger.

3 INNOVATION ER NØDVENDIG FOR AT OMSÆTTE FORSKNING OG VIDEN TIL CYBERLØSNINGER

- **Innovation med Forsvaret:** Udvikling af et tæt samarbejde mellem universiteter, forsvarsindustrien og Forsvaret for at fremme innovation, der leverer konkrete løsninger.
- **Rapid Prototyping:** Oprettelse og vedligeholdelse af nyeste software-, hardware- og netværksplatforme for hurtig udvikling og test af nye cybersikkerhedsløsninger under virkelige angrebsscenarier.
- **Entrepreneurship:** Rådgivning og investering til etablering af virksomheder inden for cybersikkerhed gennem inkubatorer og acceleratorprogrammer.

4 FORSVARSINDUSTRIEN SKAL UDVIDES MED EN STÆRK CYBERINDUSTRI

- **Styrkelse af virksomhedsøkosystemet:** Udvikling af et stærkt økosystem af nye og etablerede cybervirksomheder, der kan levere cybersikkerhedsløsninger til både det nationale forsvar, EU og NATO.
- **Investeringsfond:** Ud over de ovenstående aktiviteter skal der mobiliseres risikovillig kapital fra NATO's innovationsfond til støtte for nye cybersikkerhedsvirksomheder.
- **Internationale standarder:** Forskningen kan i samarbejde med Forsvaret bidrage til udviklingen af internationale standarder og politikker for cybersikkerhed.

FAKTA: CYBER CAMPUS DENMARK

Flere lande etablerer nationale Cyber Campus'er - f.eks. har Sverige gjort det med udgangspunkt i KTH i Stockholm – Sveriges største universitet. Cyber Campus Denmark er en tilsvarende organisation under etablering med:

Security Tech Space: Et videns- og innovationscenter stiftet i et samarbejde mellem Aarhus Kommune, Alexandra Instituttet, INCUBA og Aarhus Universitet, med et konsortium af +65 medlemmer, f.eks.: Dansk Erhverv, Dansk Industri, KL, TERMA, Systematic, Vestas, Bankdata, Nordea, Microsoft og Cisco samt højtspecialiserede startups som Kvantify og Partisia.

Aarhus Universitets fyrtårn i cybersecurity: Med en international og national førerposition indenfor centrale cybersecurity discipliner (f.eks. top-3 i verden indenfor kryptografi) etableres tværfaglig forskning og uddannelse med involvering af de relevante enheder på universitetet, der dækker områder som datalogi, ingeniørdiscipliner, kriseledelse, organisation, menneskelige faktorer og entrepreneurship.

Bredt nationalt samarbejde: Forskning og uddannelse vil foregå i tæt samarbejde med relevante enheder på alle danske universiteter og GTS-institutter. Samarbejdet faciliteres gennem Nationalt Forsvarsteknologisk Center (NFC), Digital Research Centre Denmark (DIREC), klyngerne Center for Defence, Space & Security (CenSec) og Danmark's nationale klynge for digitale teknologier (DigitalLead). CCD er også i løbende dialog med Forsvaret, FE, og Center for Cybersikkerhed m.fl.

Et behov for en investering på 1,5 – 2 mia. kr. over en 10-årig periode. Investeringen vil skulle dække udvidet cyberværnepligt, et cybersikkerhedslab samt uddannelse, forskning og innovation.