

Udvidelse af cyberværnepligten til IT-byen Katrinebjerg i Aarhus

I erkendelsen af de voksende digitale trusler mod national og global sikkerhed, foreslås en udvidelse af den eksisterende cyberværnepligt i Fredericia, en ny civil cyberværnepligt samt etableringen af en overbygning til cyberværnepligten, som foregår i IT-innovationsmiljøet på Katrinebjerg i Aarhus. Initiativet vil drage fordel af de eksisterende uddannelsesfaciliteter og synergieffekter med IT-ingeniør- og datalogiuddannelserne på Aarhus Universitet samt IT-sikkerhedsuddannelserne på Erhvervsakademi Aarhus. Målet er at forme fremtidens cyberforsvarere gennem en dybdegående og hands-on tilgang til cybersikkerhed.






FORMÅL

Uddannelserne sigter mod at forberede de værnepligtige på at beskytte Danmarks digitale infrastruktur mod cyberangreb og andre cybertrusler. Det vil omfatte udvikling af færdigheder inden for cyberforsvar, etisk hacking, digital efterretning og sikkerhedsanalyse, som er afgørende for at håndtere det skiftende trusselsbillede i cyberspace.

INDHOLD I CIVIL CYBERVÆRNEPLIGT OG OVERBYGNINGEN




Ny civil cyberværnepligt

En ny civil cyberværnepligt på Katrinebjerg struktureres som en intensiv uddannelse, der varer 10 måneder, og som er opdelt i moduler. Hvert modul fokuserer på specifikke kompetenceområder inden for cybersikkerhed og er designet til at bygge videre på de færdigheder, der er opnået i de foregående moduler:

-  **Indledende modul:** Introduktion til cybersikkerhed, herunder grundlæggende IT-færdigheder, netværkssikkerhed og programmering.
-  **Efterretningsanalyse:** Fokus på dataindsamling, trusselsanalyse og efterretningsmetoder.
-  **Offensiv sikkerhed:** Læring af avancerede teknikker inden for penetrationstesting og etisk hacking.
-  **Defensiv sikkerhed:** Kurser i oprettelse og vedligeholdelse af sikre netværk, beredskabsplaner, incident response og katastrofeberedskab.
-  **Digital forensics og lovgivning:** Indføring i teknikker for digital forensics samt en gennemgang af relevante lovgivningsmæssige og etiske overvejelser.

Ny meritgivende overbygning på cyberværnepligten

En ny meritgivende uddannelse, som overbygning på cyberværnepligten skal være med til at fastholde de unges tilknytning til forsvaret. Uddannelsen opbygges med følgende overordnede moduler:

-  **Praktik i forsvaret:** I løbet af uddannelsen, tilbringer den studerende flere år i forsvaret
-  **Faglig overbygning af de moduler der indgår i cyberværnepligten:** De 5 moduler fra civilværnepligten udbygges yderligere.
-  **Ikke militære fagmoduler:** Fagmoduler der sikrer at den studerende opnår de fornødne kompetencer og ECTS point i forhold til at opnå en meritgivende uddannelse.

Udvidelse af cyberværnepligten til IT-byen Katrinebjerg i Aarhus

Metoder i uddannelsen

Uddannelsen benytter sig af en række forskelligartede undervisningsmetoder for at sikre, at de værnepligtige ikke kun tilegner sig den nødvendige teoretiske viden, men også den praktiske erfaring, som er vital for at operere effektivt i cybersikkerhedsdomænet:



Forelæsninger og seminarer: Tilbyder en solid teoretisk forståelse af cybersikkerhedskoncepter, teknologier og politikker med udgangspunkt i nogle af verdens førende forskningsmiljøer.



Laboratoriearbejde og praktiske øvelser: Gennemføres i state-of-the-art faciliteter, hvor de værnepligtige kan anvende deres viden i praksis gennem simulationer af cybersikkerhedsangreb og forsvarsstrategier.



Casebaseret læring og projektarbejde: Fokuserer på analyse af reelle cyberangreb og udvikling af løsningsstrategier i gruppesamarbejde, hvilket fremmer teamwork og problemløsningsfærdigheder.



Krigsspil og simuleringer: Simulerede cyberangrebsscenerier, hvor de værnepligtige kan opleve presset fra realtidsbeslutningstagning og responsstrategier.



Gæsteforelæsninger og workshops: Brancheførende eksperter og gæsteundervisere deler deres viden og erfaringer, hvilket giver indsigt i de nyeste trends og trusler inden for cybersikkerhed.

TILKNYTNING TIL FORSVARET EFTER UDDANNELSEN

Efter afslutningen af cyberværnepligtsuddannelsen vil de værnepligtige have mulighed for at fortsætte deres karriere inden for forsvaret på flere måder:



Ansættelse i forsvaret: De mest fremtrædende kandidater kan blive tilbudt fastansættelse i forsvarets cyberforsvarsenheder.



Reservist: Andre kan vælge at indgå i forsvarets reserve som reservist, hvor de kan blive kaldt ind til tjeneste eller deltage i regelmæssige øvelser.



Videreuddannelse: Muligheder for yderligere specialisering gennem ny meritgivende overbygning i forsvarsregi der placeres på Aarhus Universitet, forsvarets egne kurser eller ved at tage en civil uddannelse inden for cybersikkerhed.

Denne tilgang sikrer, at Danmark kontinuerligt udvikler sit forsvar mod cybertrusler ved at investere i uddannelse af talentfulde individer og ved at tilbyde dem veje til at fortsætte deres karriere inden for national sikkerhed.

NY MÅLGRUPPE

Den civile værnepligt åbner op for en ny målgruppe til forsvaret, som eksempelvis neurodivergente, overvægtige, fysisk handicappede mv., som har stærke IT-kundskaber, men som vil have svært ved at passe ind i en traditionel militæruddannelse.

FYSISKE FACILITETER

Uddannelsen stiller krav om at være placeret i et stærkt fagligt miljø. Sådant et miljø findes i IT-byen Katrinebjerg i Aarhus, og man har allerede nu faciliteterne klar, så man vil kunne starte uddannelsen af civile cyberværnepligtige op primo 2025.

Udvidelse af cyberværnepligten til IT-byen Katrinebjerg i Aarhus



Undervisningslokaler i beskyttet område på INCUBA (60 % ejet af FEAS Aarhus Universitets forskningsfonds ejendomsselskab)



Allokerede overnatningsfaciliteter på kollegie i umiddelbar tilknytning til INCUBA

AFSLUTNING

Den foreslåede civile cyberværnepligtsuddannelse på Katrinebjerg og overbygningen er en ambitiøs tilgang til at styrke Danmarks cybersikkerhedsforsvar. Ved at integrere den med de eksisterende akademiske ressourcer og benytte en bred vifte af undervisningsmetoder bl.a. i samarbejde med erhvervslivet, vil uddannelsen forberede de værnepligtige til at møde fremtidens cybertrusler med kompetence, selvsikkerhed og innovation.

3 handlinger skal iværksættes for at skabe flere cyberværnepligtige

1. Udvidelse af antallet af cyberværnepligtige i Fredericia. Pt. uddannes 32 om året. Undervisere er den største forhindring for at udvide antallet. Aarhus kan levere dette til Fredericia fra vores uddannelsesinstitutioner og virksomheder. På kort sigt skal antallet fordobles til 64 om året og på lang sigt til 128 eller flere om året.
2. Etablering af en civil cyberværnepligt i Aarhus, kapacitet på kort sigt 50 værnepligtige på længere sigt 200 værnepligtige om året.
3. Etablering af en flerårig overbygning på værnepligten. Hvor 50 % af tiden anvendes i forsvaret og 50 % af tiden anvendes til undervisning. Overbygningen skal give en civil titel svarende til Diplomingeniør. Kapacitet 25-50 personer om året.

Hvorfor Aarhus?

1

Verdensførende forsknings- og uddannelse: Aarhus Universitet har gennem 20 år været placeret blandt de 3 bedste i verden indenfor kryptografi og er blandt verdens bedste på en række it-sikkerhedsteknologier. Miljøet har i den seneste år skabt en række innovative virksomheder.

2

Teknologisk hub: Byens stærke IT-miljø med startups og etablerede virksomheder inden for cyberteknologi og sikkerhedsløsninger tilbyder et solidt grundlag for innovation og samarbejde mellem den militære og private sektor.

3

Erfaring med forsvarsindustri: 90% af Danmarks forsvarsindustri er i dag placeret i Aarhus.

4

Økonomiske og strategiske fordele: Oprettelsen af cyberværnepligtige i Aarhus vil medføre økonomiske fordele for Østjylland, genoplive militære arbejdspladser, og styrke Danmarks forsvar mod cybertrusler.

5

Styrkelse af Danmarks cyberberedskab og samfundet: Ved at uddanne flere cyberværnepligtige og dygtiggøre dem med eksisterende ressourcer kan der skabes større kapacitet og beredskab hurtigt. Samtidigt ved vi, at cyberkompetencer er stærkt efterspurgte i erhvervslivet, hvorfor det også vil være en investering i vækst og udvikling i erhvervslivet.