JUSTITSMINISTERIET

Dato: 22. juni 2023
Kontor: Sikkerhedskontor II
Sagsbeh: Simon Bundegaard Eriksen
Sagsnr.: 2023-0035-0341
Dok.: 2870216

UDKAST TIL TALE

Til brug for besvarelsen af samrådsspørgsmål N-P fra Folketingets Retsudvalg om kinesisk producerede overvågningskameraer

Samrådsspørgsmål N:

Hvordan forholder ministrene sig til, at Forsvaret, Politiet og Vejdirektoratet har indkøbt kameraer fra Hikvision, som er delvist ejet af den kinesiske stat (40 pct.), selvom PET og CFCS advarer mod at indkøbe kinesisk producerede kameraer pga. risiko for overvågning, jf. artiklen "Dokumenter: Kinesiske kameraer overvåger danske militæranlæg og motorveje" fra Børsen.dk den 25. maj 2023?

Samrådsspørgsmål O:

Er ministrene enige i, at brugen af kinesisk-producerede kameraer involverer en risiko for spionage og overvågning foretaget af den kinesiske stat samt datahøst via den kinesiske sikkerhedslov, og vil ministrene i den forbindelse gennemføre tiltag, der skal forhindre indkøb af kinesisk produceret materiel, jf. artiklen "Dokumenter: Kinesiske kameraer overvåger danske militæranlæg og motorveje" fra Børsen.dk den 25. maj 2023?

Samrådsspørgsmål P:

Vil ministrene – på baggrund af at Materiel- og Indkøbsstyrelsen henviser til, at udbudsloven forhindrer en udelukkelse af Hikvision fra offentlige udbud – fremlægge begrundelser for, hvorfor der ikke i Udbudsloven og Udbudsdirektivet er muligheder for at udelukke indkøb, som kan være en trussel mod Danmarks sikkerhed?

Spørgsmålene er stillet efter ønske fra udvalget.

[Indledning]

Tak for ordet og tak for spørgsmålene.

Jeg vil gerne indlede med at sige lidt om den generelle spionagetrussel mod Danmark.

Dernæst vil jeg redegøre mere specifikt for spionagetruslen fra Kina.

Afslutningsvist vil jeg sige noget mere konkret om sikkerhedsrisikoen ved at anvende kinesisk produceret overvågningsudstyr og om politiets håndtering heraf.

[Generelt om spionagetruslen]

Helt generelt vil jeg sige, at Danmark er udsat for en markant, bredspektret og vedvarende trussel fra fremmede staters efterretningsvirksomhed.

Det fremgår også af den seneste "Vurdering af spionagetruslen mod Danmark, Færøerne og Grønland" (VSD), som Politiets Efterretningstjeneste (PET) offentliggjorde i maj 2023.

Der er ikke noget nyt i, at fremmede stater forsøger at spionere mod Danmark, men det gør selvsagt ikke spionagetruslen mindre alvorlig.

De fremmede efterretningstjenester, der er aktive i Danmark, er professionelle modstandere, som planlægger og gennemfører aktiviteter med en lang tidshorisont.

Det er modstandere, som har en høj kapacitet, og som udnytter mange forskellige fremgangsmåder til at udøve deres aktiviteter, herunder moderne teknologi.

Truslen fra fremmede staters efterretningsvirksomhed omfatter også forsøg på at anskaffe sig produkter, viden og teknologi. Det sker bl.a. for at udvikle de fremmede staters militære kapacitet.

For så vidt angår spionagen så kan den foregå ved hjælp af blandt andet menneskelige kilder, via cyberspionage eller aflytning af tele- og datatrafik.

Spionagetruslen retter sig mod politikere, embedsfolk i centrale ministerier, ansatte i efterretningstjenesterne og Forsvaret. Men den retter sig også mod andre offentlige

myndigheder, kritisk dansk infrastruktur, virksomheder og forskningsinstitutioner.

[Truslen fra Kina]

Truslen fra fremmede efterretningstjenester mod Danmark kommer først og fremmest fra Rusland og Kina.

Kina og det kinesiske kommunistpartis globale ambitioner og vilje til at udfordre Vesten afspejles også i trusselsbilledet i Danmark.

Det gælder særligt Kinas ambitioner om at blive førende inden for udviklingen af visse teknologier, hvor også Danmark er langt fremme.

Kina anvender en bred vifte af virkemidler til at understøtte sine strategiske og teknologiske interesser.

PET kan konstatere, at de kinesiske efterretningstjenester har meget vide beføjelser til at indsamle oplysninger i udlandet, heriblandt i Danmark.

Den kinesiske efterretningslovgivning giver de kinesiske efterretningstjenester mulighed for at pålægge kinesiske statsborgere og virksomheder at samarbejde med tjene-

sterne, uanset hvor i verden de måtte opholde sig. Det gælder også kinesiske teknologivirksomheder.

Spionagetruslen fra Kina er altså til stede og skal tages alvorligt.

Og jeg kan garantere, at både vores myndigheder og vi i regeringen tager truslen meget alvorligt.

PET arbejder – sammen med andre relevante myndigheder – hver dag for at imødegå spionagetruslen fra fremmede magter. Og PET har siden 2019 styrket sin indsats mod spionage markant.

Men vi skal alle sammen tage vores forholdsregler. Det gælder selvfølgelig også offentlige myndigheder, når de køber kameraer og andre former for overvågningsudstyr.

[Myndighedernes sikkerhedsvurdering af overvågningskameraer]

Center for Cybersikkerhed (CFCS) er national it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet.

Som forsvarsministeren har nævnt, så står Center for Cybersikkerhed til rådighed og kan vejlede og rådgive myndigheder om cyber- og informationssikkerhed i systemer til videoovervågning.

På Justitsministeriets område er det PET, der varetager opgaven som it-sikkerhedsmyndighed. Det er derfor også PET, som rådgiver Rigspolitiet og politikredsene i it-sikkerhedsspørgsmål.

PET's rådgivning på Justitsministeriets ressort vedrørende sikkerhedsspørgsmål sker i tæt samarbejde med CFCS

Det er begrænset, hvor meget jeg inden for rammerne af et samråd kan oplyse om PET's arbejde med at imødegå spionagetruslen.

Jeg kan dog nævne, at PET tidligere har udarbejdet en vurdering af mulige sikkerhedsrisici ved kameraer fra kinesiske producenter til politiet. Det har også været offentligt fremme tidligere.

PET anbefaler i den vurdering, at Rigspolitiet i forhold til overvågningskameraer anlægger en risikovurdering,

der tager højde for uvedkommendes adgang til både selve kameraet og til de konkrete systemer, der er tilknyttet det netværk, som kameraet er tilkoblet.

Uden at det skal blive alt for teknisk, så handler det bl.a. om, hvorvidt overvågningskameraet anvendes i internetforbundne systemer, og om er der andre systemer på det internetforbundne netværk, som overvågningskameraet er forbundet til.

[Politiets kortlægning af overvågningskameraer]
Rigspolitiet har på baggrund af PET's rådgivning udarbejdet en sikkerhedsvurderingsmodel for politiets overvågningskameraer.

Sikkerhedsvurderingsmodellen inddrager bl.a. tekniske sikkerhedsforhold, politioperative forhold og databeskyttelsesretslige forhold.

Desuden skelner modellen mellem kritiske og ikke-kritiske politifaglige funktioner for overvågningskameraerne.

Rigspolitiet har – med udgangspunkt i sikkerhedsvurderingsmodellen og PET's vurdering – kortlagt politikredsenes overvågningskameraer.

Kortlægningen har identificeret 136 overvågningskameraer fra kinesiske producenter.

På baggrund af en konkret sikkerhedsvurdering af hvert af de identificerede overvågningskameraer har Rigspolitiet truffet beslutning om, at 64 ud af de 136 overvågningskameraer udfases i politiet.

Rigspolitiet har oplyst, at 60 ud af 64 overvågningskameraer er udskiftet, og at de sidste 4 forventes at være udskiftet senest den 30. juni 2023.

Fjerner det så enhver sikkerhedsrisiko ved anvendelsen af overvågningskameraer? Nej, det gør det desværre ikke. Der vil være sårbarheder.

[Afslutning]

Derfor skal vi også være os truslen bevidst. Og vi skal alle sammen tage vores forholdsregler. Derfor er der også på Justitsministeriets område, herunder hos politiet, stort

fokus på, hvordan kritiske teknologier, herunder overvågningsudstyr, anvendes.

Samtidig kan jeg til fulde tilslutte mig det, som forsvarsministeren sluttede af med at sige: Nemlig, at der er behov for, at vi får undersøgt, hvordan vi konkret kan håndtere den generelle udfordring på det her område.

Og så kan jeg også kun opfordre til, at offentlige myndigheder rækker ud til sikkerhedsmyndighederne og søger rådgivning. Også om indkøb af teknologi.

Tak for ordet.