En højteknologisk sikkerhedspolitik

Af Mathias Terp Jensen

Danmark er et af de mest teknologisk udviklede lande i verden. Vi anvender digitale løsninger i vores infrastruktur og dagligdag, og dansk rumfartsindustri omsætter for milliarder. Vores teknologiske begejstring og innovation skaber velstand og muligheder for Danmark. Men det skaber også en række sikkerhedspolitiske udfordringer, der ændrer de grundlæggende vilkår for sikkerhedspolitikken og kræver et strategisk svar.

Den teknologiske udvikling har flere gange ændret rammerne for udenrigs- og sikkerhedspolitik. Oceangående skibe muliggjorde fra det 16. århundrede nye handelsruter og koloniseringen af fjerntliggende nationer. I det 18. århundrede skabte udviklingen i tekstil- og jernindustrien grundlaget for den industrielle revolution, der markant forskød den økonomiske fordel til Vesten. Endnu senere skabte spredningen af atomvåben en ny strategisk dynamik mellem stormagterne.

I det 21. århundrede er turen til at forandre udenrigs- og sikkerhedspolitikken kommet til teknologien i cyberspace og det ydre rum. Den teknologiske udvikling på dette område har gjort kommunikation hurtigere, velstanden større og militære operationer mere præcise. Men vores afhængighed af cyberspace og det ydre rum udfordrer også den traditionelle forståelse af suverænitet og afskrækkelse. Samtidig ændrer det trusselsbilledet mod Danmark markant.

Den kendte strateg Lawrence Freedman definerer strategi som 'kunsten at skabe magt'. Som en lille stat med begrænsede midler er det derfor afgørende for Danmark at udvikle en strategi på området. Hvis Danmark skal fortsætte med at 'slå over vores vægtklasse', som skiftende amerikanske præsidenter har yndet at sige, i det 21. århundredes udenrigs- og sikkerhedspolitik, er det afgørende at prioritere de teknologiske områder, der kommer til at forme rammerne for sikkerhedspolitikken: cyberspace og det ydre rum.

Teknologisk afhængighed

Vi er utrolig afhængige af teknologien i cyberspace og det ydre rum. Ifølge Danmarks Statistik bruger 85 pct. af danskerne internettet hver dag. Hvad enten det er igennem emails på arbejdspladsen, fredagsfilmen fra Netflix eller vores kri-

Mathias Terp Jensen er bachelor i statskundskab ved Københavns Universitet. I øjeblikket studerer han til kandidat i International Affairs på Sciences Po i Paris og London School of Economics.

tiske infrastruktur er cyberspace en del af vores liv. Det er satellitter og rumteknologi også. Medier anvender kommunikationssatellitter, navigationssystemer og hæveautomater trækker på GPS-systemet, og når vejrudsigten en sjælden gang passer, skyldes det vejrsatellitter.

Afhængigheden gælder også for forsvaret. Vi sender og opbevarer fortrolige informationer i cyberspace, og flere af vores forsvarssystemer er afhængige af cyber- og rumteknologi. Vejrsatellitter bruges til at planlægge operationer, overvågningssatellitter til at vælge den korrekte strategi og taktik, og GPS-satellitter bruges til at guide fly, skibe og tropper.

Samtidig har Danmark opnået store velstandsgevinster grundet vores evne til udvikle løsninger inden for cyberspace og det ydre rum.

Danske it-virksomheder omsætter for flere hundrede milliarder, og i kommercialisering af det ydre rum er danske virksomheder med langt fremme. Betydningen af teknologien for Danmarks udenrigs- og sikkerhedspolitik understreges desuden af udpegningen af verdens første digitale ambassadør, som har hovedsæde tæt ved Silicon Valley.

Den amerikanske general Kevin Chilton kalder det amerikanske militær for afhængigt af det ydre rum. Det gælder også for det danske samfund og dets udenrigs- og sikkerhedspolitik. Af den årsag udgav regeringen også en national strategi for rummet i 2016, ligesom at der snart forventes en ny cyberstrategi til at afløse den sidste fra 2014.

Det er dog afgørende, at disse strategier også tænkes ind i den bredere udenrigs- og sikkerhedspolitiske strategi. For netop vores afhængighed af cyberspace og det ydre rum er med til at øge trusselsbilledet mod Danmark.

Et barn af globaliseringen

For at kunne forstå de udenrigs- og sikkerhedspolitiske udfordringer, der er forbundet med cyberspace og det ydre rum, er det afgørende at forstå et helt centralt element: Cyberspace og det ydre rum respekterer ikke landegrænser. På den måde bliver de teknologiske muligheder i cyberspace og det ydre rum på mange måder en inkarnation af globaliseringen. Cyberspace og satellitter er i deres natur grænseoverskridende og synes at understrege, at selv det, der sker på den anden side af jordkloden, påvirker os. Det udfordrer grundlæggende vores forståelse af suverænitet.

Et af de helt grundlæggende elementer i suverænitet er statens uafhængighed af andre. Men både i cyberspace og i det ydre rum er det langt fra sandheden. I cyberspace risikerer Danmark utilsigtet at blive ramt af cyberangreb i form af en virus.

Da USA og Israel i et forsøg på at forsinke Irans atomvåbenudvikling inficerede iranske computere med den såkaldte Stuxnet-virus, holdt den sig ikke pænt inden for Irans grænser, men spredte sig til computere i en række forskellige lande – herunder USA selv. Det samme gjorde det nordkoreanske ransomware-angreb WannaCry, der blev mest berygtet for i 2017 at kryptere britiske sundhedsdata og kræve løsepenge for at give adgang til dem.

Afhængigheden af andre lande gælder også i det ydre rum. Danmarks brug af det ydre rum er næsten udelukkende bundet op på amerikanske, europæiske og internationale satellitsystemer. Juridisk tilhører det ydre rum ikke nogen stater, men kan benyttes af alle til fredelige formål. Danmark opererer også enkelte satellitter selv.

De seneste år har en eksplosion i interessen for rummet dog gjort det trangt med plads, og rumaffald er blevet en trussel for danske interesser. Rumaffald er hele eller dele af gamle satellitter eller anden rumteknologi, der stadig opholder sig i det ydre rum, og som risikerer at kollidere med og ødelægge vitale satellitter. Det skabes både som en naturlig sideeffekt af øget aktivitet og missilangrebsøvelser på satellitter som Kinas i 2007. Der er for øjeblikket ca. 23.000 stykker sporet rumaffald. Til sammenligning er der ca. 1.200 satellitter.

Den gode nyhed er, at en lang række lande anerkender den grænseoverskridende natur af cyberspace og det ydre rum. Specielt cyberspaces grænseoverskridende natur fremhæves i EU's og USA's cybersikkerhedstrategier. Det understreger, at afhængigheden gælder for alle lande. Suveræniteten forsvinder således ikke for Danmark, den deles med resten af verden. Det indbefatter, at den bedste måde at regulere cyberspace og det ydre rum på er internationalt.

Et ændret trusselsbillede

De teknologiske forandringer i cyberspace og det ydre rum indbefatter en række effekter på trusselsbilledet for Danmark.

For det første kompliceres trusselsbilledet af en række nye mindre aktører og trusler. Groft sagt kræver det ikke meget mere end en computer og en person med indgående viden om informations- og computersystemer for at kunne lave et cyberangreb. Afhængigt af omfanget, målet og typen kan cyberangreb kræve mere eller mindre computerkraft og sofistikeret kode, men grundlæggende er adgangsbarrierne lave.

Adgangsbarrierne til det ydre rum er også faldet drastisk i de seneste år. Kommercialiseringen har medført stærkt faldende priser og mindre satellitter. Det betyder, at mens der i 1966 kun var seks lande, der havde satellitter, er der nu over 40 – herunder Danmark.

Det er dog stadig både svært og dyrt at opsende egne satellitter, og det er derfor stadig stormagterne, der dominerer opsendelser af satellitter.

I modsætning til opsendelsen er teknologi til at angribe satellitter relativt billig. Der findes generelt fire former for angreb mod satellitter. Mens missilangreb og dazzling – det vil sige midlertidigt at blænde en satellit med laser – både er dyre og komplicerede metoder, er cyberangreb og jamming – det vil sige at bruge elektromagnetisk energi til at overdøve satellittens signal – billige og relativt ligetil at anvende.

Den demokratisering af magtmidler giver en række mindre aktører midlerne til at true Danmark. Det gælder mest åbenlyst for hackergruppen Anonymous, der anvender cyberangreb som led i politisk aktivisme. Der har endda også været enkelte ubekræftede rapporter ude omkring Daeshs brug af jamming-angreb mod satellitter. Teknologien skaber dermed et mere komplekst trusselsbillede med flere aktører, der billigt og let kan udrette stor skade.

For det andet bliver sikkerhedspolitisk strategi baseret på mindre angreb og påvirkningskampagner. Mens NATO stadig har den klare militære fordel, anvender Kina, Rusland og Nordkorea med flere cyberspace til at skade Vesten igennem såkaldte death by a thousand cuts. Her bruges en kaskade af mindre i sig selv ubetydelige angreb til at skade Vesten i det lange løb. Den lille effekt af de enkelte angreb gør det svært at reagere kraftigt på angrebene, selvom de sammenlagt kan have store konsekvenser.

Ydermere giver teknologien fjendtligsindede aktører mulighed for at føre påvirkningskampagner mod Danmark ved at indsamle og lække oplysninger, der er med til at undergrave det politiske system uden at bruge militær magt. Disse påvirkningskampagner, som Rusland synes at stå bag, har specielt været tydelige ved amerikanske og europæiske valg. Målet med disse kan være at skabe splid i Vestens bærende institutioner, NATO og EU, hvilket vil tillade en mere aggressiv russisk udenrigspolitik.

Derudover udnytter fjendtlige stater, at det er særdeles svært at attribuere cyberangreb korrekt. Mens missiler eller troppebevægelser typisk har en returadresse, kan cyberangreb skjules og gennemføres igennem en række kompromitterede computere i andre lande. Dermed bliver det lettere for stater som Rusland og Kina at benægte deres involvering i cyberangreb.

For det tredje giver det dem en måde at mindske NATOs militære fordel. NATOs militære fordel er i høj grad bundet op på anvendelse af teknologi. I tilfælde af en større konflikt vil det første angreb derfor sandsynligvis være rettet mod cyberspace og det ydre rum. Hvis det lykkes, kan fjenden kraftigt reducere NATOs militære styrke eller få en afgørende fordel ved at angribe den vigtige militære infrastruktur.

Som resultat af den teknologiske udvikling i cyberspace og det ydre rum bliver trusselsbilledet dermed præget af en række mindre aktører, mindre angreb og påvirkningskampagner og en potentiel svækkelse af NATOs militære fordel.

Afskrækkelse i en ny tid

At vi i nu over 70 år har undgået en Tredje Verdenskrig tilskrives af mange eksperter afskrækkelse. Helt kort handler afskrækkelse om at påvirke fjendens strategiske kalkule, således at man undgår et angreb. Det kan man gøre ved at øge truslen om gengældelse eller ved at gøre det så tilpas svært at udføre angrebet, at det ikke er besværet værd.

Under den kolde krig afskrækkede sandsynligheden for gensidig tilintetgørelse Sovjetunionen og USA fra en atomkrig. Men i cyberspace og det ydre rum er flere af de elementer af det 20. århundredes afskrækkelse fraværende.

Under den kolde krig fungerede afskrækkelse i det ydre rum som en forlængelse af atomvåbenafskrækkelsen. Det ydre rum blev udforsket og bemandet som et led i sovjetiske og amerikanske missilforsvarssystemer, der advarede om forestående atomangreb. Angreb på satellitter ville derfor være blevet anset som starten på en atomkrig og gengældt med atomvåben.

I dag er situationen mærkbart anderledes. Det ydre rum er befolket med en række mindre vigtige satellitter fra vejrtil tv-satellitter, og de færreste tror, at amerikanerne, kineserne eller russerne, vil starte Tredje Verdenskrig, hvis tv-signalet ryger. Og da angrebsteknologien er relativt billig, er der ikke meget, der afskrækker fjender fra angreb på danske interesser i det ydre rum.

På samme måde mangler der også en troværdig afskrækkelse for cyberangreb. På trods af de seneste års gentagne cyberangreb mod Europa og USA er der ikke konsensus om en række vigtige spørgsmål om afskrækkelse. Det skyldes især problemet med at attribuere angreb, da der ikke er megen afskrækkelseseffekt over at gengælde over for det forkerte land.

Samtidig gør muligheden for, at en

række ikke-statslige aktører som Anonymous og Daesh kan bruge cyber- og rumangreb, at Danmark og NATO skal tage stilling til, hvordan man afskrækker dem. Det er nok svært at forvente, at Daesh, Al-Qaeda eller andre radikale ekstremistiske grupperinger vil lade sig afskrække af truslen om gengældelse.

Der er også problemer med at gøre det mere besværligt at angribe. Det er svært at dække alle potentielle indgange i cybersystemer, og da offensive våben er billige, risikerer en sådan strategi at ødelægge bæredygtigheden i det danske forsvarsbudget.

Det er således nødvendigt for Danmark at skabe en stærk og troværdig trussel om gengældelse mod fjendtligsindede. Men det kan kun lade sig gøre, hvis man i NATO etablerer en grundlæggende enighed om, hvor høj sikkerhed der skal være i attributionen af angrebet, samt hvilken gengældelse der vil være proportional.

Samtidig skal Danmarks defensive kompetencer styrkes for at gøre det så besværligt som muligt for mindre sofistikerede aktører, der som fx Daesh ikke kan afskrækkes, at kunne forårsage skade.

Strategiske principper

Den teknologiske udvikling inden for cyberspace og det ydre rum efterlader Danmark i en situation, hvor vi i er afhængige af resten af verden, hvor stormagterne er i konflikt, og hvor kun lidt afskrækker fjender. Det efterlader et klart behov for strategisk tænkning om dansk udenrigs- og sikkerhedspolitik på området. Jeg kommer nedenfor med mit bud på fire strategiske principper:

(1) Gør cyberspace og det ydre rum til strategiske topprioriteter i udenrigs- og sikkerhedspolitisk – specielt i forbindelse med EU og NATO.

Det absolut første skridt i løsningen på et problem er at anerkende, at det eksisterer. Cyberspace har i de senere år fået større opmærksomhed nationalt og internationalt. Det har udmøntet sig i en række nationale og internationale strategier. Der er ligeledes sat en proces i gang for at styrke NATOs afskrækkelse på cyberområdet. Den proces bør Danmark i videst mulige forstand forsøge at påvirke.

Regeringer og eksperter er også ved at få øjnene op for det ydre rums sikkerhedspolitiske betydning. Fx rummer både den amerikanske og den franske sikkerhedsstrategi afsnit om det ydre rum. I EU- og NATO-sammenhæng er der dog behov for en offensiv diplomatisk indsats for at prioritere emnet. Det kan Danmark blandt andet hjælpe på vej ved at øge sit bidrag til ESA (European Space Agency).

I EU kan det danske forsvarsforbehold dog stille Danmark ringere end andre lande, og regeringen bør derfor overveje en folkeafstemning, hvor der tages stilling til europæisk integration i udenrigs- og sikkerhedspolitikken, eller i endnu højere grad satse på USA og NATO som samarbejdspartnere.

En offensiv diplomatisk indsats vil også styrke Danmarks indflydelse på begge områder, der ellers grundet deres vigtighed risikerer at blive domineret af stormagterne. Specielt på cyberområdet kan Danmarks digitale ry som foregangsland bruges til at skabe øget indflydelse, mens at Danmarks erhvervsmæssige styrke kan bruges hvad angår det ydre rum.

(2) Arbejde for international koordinering og regulering samt internationale normer – specielt igennem NATO og EU.

Det er umuligt for en dansk regering

at håndtere truslerne i cyberspace og det ydre rum alene. Derfor skal regeringen arbejde for en bredere international koordinering af udenrigs- og sikkerhedspolitikken i forhold til cyberspace og det ydre rum. Koordineringen kan styrkes ved yderligere informationsudveksling imellem udenrigs-, forsvars- og efterretningstjenester. Det vil forbedre efterretningerne og forståelsen for cyberspace og det ydre rum samt forbedre grundlaget for attribution af angreb.

En stor del af truslen på cyberområdet, men også i det ydre rum, skyldes manglen på normer, hvilket øger usikkerheden og frygten for eskalation. Samtidig risikerer Danmarks interesser at blive negligeret, hvis stormagterne ikke begrænses. Derfor bør Danmark også arbejde for at etablere fælles normer, der kan hjælpe til at binde stormagterne. Det gælder især normer for, hvad der er acceptable reaktioner på et cyber- eller rumangreb. Herudover bør Danmark arbejde for at etablere en fælles forståelse af, hvor sikker et land bør være i attributionen af et angreb, før det svares igen. Ligeledes bør der arbejdes for at etablere en norm imod missilangreb på satellitter for at mindske mængden af rumaffald.

Danmark bør ydermere arbejde for at integrere en stor del af cybersikkerheden i internationale fora som NATO og EU, da det er tvivlsomt, om Danmark alene har kapaciteten til at forsvare sig imod eller afskrække angreb. Derfor bør Danmark arbejde for at gøre cybersikkerhed og sikkerhed i det ydre rum til et fælles anliggende. Fokus bør være at sikre afskrækkelse mod angreb på de vigtigste dele af infrastrukturen igennem NATO og EU, hvorefter Danmark selv kan styrke sit forsvar på mindre vigtige områder.

Danmark bør også arbejde for at etablere fælles standarder for hardware- og softwaresikkerhed i EU for at mindske muligheden for cyberangreb. Ligeledes bør Danmark arbejde i EU for at regulere mængden af rumaffald. Det kan blandt andet ske ved at stille krav til opsendelsesprocessen og arbejde for løsninger i ESA.

(3) Prioritere forsvaret af danske interesser i cyberspace og det ydre rum.

Det er afgørende, at forsvaret af danske interesser i cyberspace og det ydre rum forstærkes. På cyberområdet indebærer det store investeringer i teknologi og infrastruktur samt øget fokus på at mindske menneskelige fejl. I det ydre rum indebærer det en offensiv diplomatisk indsats i EU og over for blandt andet USA.

Samtidig er det urealistisk helt at sikre det danske samfund mod cyberangreb. Derfor bliver enhver strategi nødt til at indeholde hårde prioriteringer. Danmark bør videreudvikle et lagdelt cyberforsvar, hvor de mest vitale dele af samfundet – infrastruktur som sundhedsvæsen og el- og vandforsyning – beskyttes mest. Det gælder både igennem afskrækkelse fra NATO og egne forsvarskapaciteter. Ydermere bør man med tanke på Ruslands påvirkningskampagner overveje også at prioritere kommunikation internt i de politiske partier, da det kan bruges til propaganda mod Danmark.

Om end alvorlige angreb mod danske interesser i det ydre rum er mindre sandsynlige end cyberangreb, er de stadig mulige. Her bør Danmark igennem EU og NATO arbejde for at skabe en klar afskrækkelse af angreb på de vigtigste satellitter. Det indebærer, at de vigtigste satellitter identificeres – fx GPS-teknologi og vital kommunikation – og at der opbygges en afskrækkelse af angreb på dem

afhængig af deres vigtighed. Herefter kan Danmark i mindre fora lægge diplomatisk pres på enkelte lande for at beskytte de mindre betydningsfulde satellitter.

(4) Opmuntre en teknologisk kultur i befolkningen.

Cyberangreb rettes ofte mod individuelle personer og virksomheder, mens private virksomheder i stigende grad bliver en faktor i det ydre rum. Derfor bør Danmark skabe en teknologisk kultur i befolkningen for at mindske truslen mod det danske samfund samt for at øge Danmarks indflydelse i cyberspace og i det ydre rum.

Ved at skabe et internationalt forsknings- og innovationsmiljø i Danmark inden for cyber- og rumteknologi, kan vi øge innovation og viden relateret til cyberspace og det ydre rum. Af samme grund vil det være oplagt at skabe en række offentlig-private partnerskaber. Tilsammen kan det også lede til en større bevidsthed i den danske befolkning omkring sikkerhedsrisikoen i cyberspace og det ydre rum. Det kan ydermere komplementeres igennem informationskampagner, der sætter fokus på vigtigheden af den menneskelige faktor i specielt cybersikkerhed.