Truslerne fra cyberspace

Af **Mikkel Storm Jensen**

Danmark er et af de mest gennemdigitaliserede lande i verden. Staten, virksomhederne og borgerne udnytter i stort omfang internettets muligheder for at effektivisere og optimere. Bagsiden af de mange gevinster er nye, alvorlige sårbarheder over for angreb eller ulykker. Stater har de farligste cybervåben, men betydelige incitamenter til ikke at bruge dem. Kriminelle har færre ressourcer til at udvikle cybervåben, men ingen hæmninger i forhold til at bruge dem. Terrorister og aktivister har hidtil ikke vist sig i stand til at gennemføre alvorlige cyberangreb. Uheld og menneskelige fejl vil altid være en mulighed.

Cyberspace gennemsyrer i dag alle aspekter af det danske samfund. IT gør de fleste aspekter af vores liv nemmere, hurtigere og billigere end nogensinde før. Så længe det virker. Hvad sker der i Danmark, hvis elnettet bliver angrebet og går ned som i Ukraine i 2015? Hvis hospitalernes data bliver krypteret som i Storbritannien i 2017? Hvis Maersks databaser bliver ødelagt, og firmaet pludselig ikke ved, hvad der er i alle deres containere verden over, hvor de er henne, og hvor de skal hen som i sommeren 2017?

Formålet med denne artikel er at give et kort overblik over truslerne mod det danske samfund, der udspringer fra cyberspace, ved at gennemgå de forskellige aktører. Endvidere giver artiklen et lille indblik i, hvorfor det er en meget vanskelig opgave for staten at håndtere truslerne, og den gør kort status over, hvorfor regeringens tiltag i form af de lancerede cyber- og informationssikkerhedsstrategier fra 2014, 2018 og 2019 er skridt i den rigtige retning. Skridt, der kan være politisk ubehagelige og kræver politisk mod at gennemføre.

Der er grundlæggende to kilder til trusler fra cyberspace: Angreb og uheld. Statslige organisationer, kriminelle og ideologisk motiverede angribere søger at opnå fordele ved at stjæle, true, ødelægge, forvrænge eller

Mikkel Storm Jensen er forsker ved Institut for Strategi ved Forsvarsakademiet.

kidnappe data eller fysiske enheder, der er tilknyttet internettet (eller andre netværk). Fejl, uforudsete konsekvenser, uheld og ulykker kan ramme data eller de fysiske dele af netværket.

For at tage det sidste først: I et digitaliseret samfund kan uheld eller fejl få meget alvorlige konsekvenser. I 2017 kom en medarbejder ved en underleverandør til British Airways til at slukke for strømmen til en server. British Airways havde forberedt sig på at overleve strømafbrydelser ved at placere back up-systemer, der kunne tage over, hvis elnettet gik ned – men ingen havde forudset den situation, at en uvidende person ville trække et vigtigt stik ud af en forlængerledning – og derpå i forskrækkelse satte det tilbage igen, inden servernes interne procedurer til at håndtere en strømafbrydelse og genstart var bragt til ende. Resultatet af den klodsede medarbejders uheld blev, at 75.000 passager blev forsinket i over et døgn, og at British Airways tabte fire pct. af sin aktieværdi samme dag, idet firmaet imødeså erstatningskrav på op mod 100 millioner pund.

Derfor kan digitaliserede samfund ikke nøjes med at forhindre, nedkæmpe og afskrække fjendtlige angreb i cyberspace; der må altid være et beredskab til at håndtere konsekvenserne af uheld og ulykker. Det er imidlertid mere de bevidste angreb, der fylder i den offentlige debat.

Begrebet cyberangreb bruges i debatten i både en smal og en bred forstand. I den smalle forståelse er et cyberangreb en hændelse, hvor en aktør gennem cyberspace sender et program med skadeligt indhold til et mål. Ved at køre det skadelige program på computere på målets netværk kan angriberen stjæle, forvrænge eller ødelægge data, eller måske endda sætte fysiske enheder, der er tiknyttet målets netværk, til at beskadige sig selv. Herved kan der ske yderligere skade i den fysiske verden.

I den bredere forståelse bruges udtrykket cyberangreb også om hændelser, hvor en fjendtlig handling har fundet sted via internettet uden at anvende et skadeligt program. For eksempel når en 'nigeriansk prins' via en email lokker kontooplysninger ud af en godtroende person, eller når det russiske Internet Research Bureau gennem kommunikation med falsk afsender på sociale medier forsøger at påvirke politiske stemninger i vestlige lande.

USA og Israel angreb sandsynligvis iranske anlæg til udvinding af beriget uran i en periode fra 2005 til 2010 med STUXNET, der fik de iranske centrifuger til at skifte hastighed, indtil de brød sammen.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed udgiver hvert år en trusselsvurdering, der grundigt og letforståeligt redegør for hvordan forskellige aktører truer os fra cyberspace, og hvor alvorlig truslen fra dem er.

Stater

Statslige aktører er på en måde de farligste, og på en anden måde dem, som

Meget groft sagt er den generelle internationale konsensus, at statslig spionage mod militære mål er i orden. Sådan har man altid gjort, og man kan argumentere for, at indsigt i modstanderens hensigter og kapaciteter kan forhindre misforståelser og i sidste ende krig.

andre stater har nemmest ved at håndtere. De er de farligste aktører på den måde, at de har de største ressourcer til rådighed til at gennemføre den spionage og forskning, der er nødvendig for at få den tilstrækkelige viden om andre staters digetale sårbarheder og udvikle programmer, der er målrettet til at kunne ramme dem. Stater er de nemmeste at håndtere for andre stater på den måde, at de som udgangspunkt er rationelle aktører, der kan bruge cyberangreb eller truslen om cyberangreb i konkurrencen med andre stater på samme måde, som man bruger mere traditionelle midler som spionage, propaganda eller – i sidste ende – væbnet magt. Derfor kan de også i et vist omfang afskrækkes eller overtales til ikke at gennemføre angreb.

Stater har brugt cyberangreb til at gennemføre sabotage for at påvirke andre staters handlinger. USA og Israel angreb sandsynligvis iranske anlæg til udvinding af beriget uran i en periode fra 2005 til 2010 med STUXNET, der fik de iranske centrifuger til at skifte hastighed indtil de brød sammen. Sandsynligvis svarede Iran igen i 2012 ved at angribe Saudi-Arabiens ledende oliefirma, Aramco, og ødelægge harddiskene på ca. 30.000 computere. Et russisk statsligt cyberangreb med programmet NotPetya, der skulle ødelægge ukrainske virksomheders data, spredte sig i 2017 til en lang række andre landes virksomheder, der gjorde forretninger med Ukraine. Angrebet ramte Maersks verdensomspændende netværk af servere. Maersk vidste i dagevis ikke, hvad der var i tusindvis af containere fordelt på 76 havne og 800 skibe verden over, eller hvor de skulle hen. Kun held i uheld – en server i Ghana var ikke blevet ramt af angrebet, fordi der var strømafbrydelse – gjorde, at angrebet 'kun' kom til at koste Maersk ca. 2 mia. danske kroner.

Cyberangreb er angiveligt også blevet brugt til at støtte angreb med traditionelle våben (angiveligt betyder i denne sammenhæng, at der ikke findes bekræftede, uklassificerede oplysninger, men at rygterne længe har været diskuteret alvorligt blandt forskere). Fx kunne israelske bombefly i 2007 uhindret bombe en atomreaktor, som Nordkorea var ved at bygge i det nordlige Syrien. En af de mulige forklaringer er, at israelerne – angiveligt – kan have gennemført et cyberangreb på de syriske varslingsradarer, så de ikke viste de israelske fly dybt inde over Syrien.

En anden form for statslige angreb er spionage. Her kan man dele spionage op i spionage mod militære eller andre sikkerhedspolitisk relevante mål og spionage mod økonomiske mål. Meget groft sagt er den generelle internationale konsensus, at statslig spionage mod militære mål er i orden. Sådan har man altid gjort, og man kan argumentere for, at indsigt i modstan-

derens hensigter og kapaciteter kan forhindre misforståelser og i sidste ende krig. Et land som USA er derfor ikke specielt interesseret i, at den form for cyberspionage bliver forbudt. Men det er et kæmpe problem for USA, at Kina anvender sine statslige spionagekapaciteter til at stjæle forskning og anden know-how fra amerikanske virksomheder og giver dem videre til kinesiske virksomheder, der derved opnår store fordele i konkurrencen med USA. I første omgang er problemet økonomisk, men efterhånden som den kinesiske økonomi vokser, og de kinesiske virksomheder gennem en blanding af stjålet, indkøbt og selvudviklet know-how bliver i stand til at udvikle både civile og militære produkter på linje med USA, bliver problemet i høj grad sikkerhedspolitisk. Der er også stater, der spionerer mod danske virksomheder. Det er en meget betydelig trussel mod Danmark, der i høj grad lever af vores virksomheders know-how.

En sidste form for statslige cyberangreb er at udnytte de sociale medier til målrettet at sprede halve sandheder og hele løgne med skjult eller falsk afsender til mennesker, hvis internetvaner viser, at de er modtagelige for budskaberne. Især Rusland har kombineret falske internetprofiler og moderne markedsføring til at skabe splid mellem befolkningsgrupper og vestlige regeringer ved at puste til utilfredshed med emner som indvandring, minoritetsrettigheder, EU's indflydelse på medlemsstaterne osv. Disse 'angreb' kan kombineres med traditionelle cyberangreb, som da Rusland først hackede det demokratiske partis emails i 2016 og derefter benyttede sociale medier til at undergrave Hillary Clintons valgkampagne.

Stater har altså ressorcerne til at udvikle de farligste våben i cyberspace – ligesom i den fysiske verden, hvor kriminelle og terrorister heller ikke har ressourcer til at udvikle og bygge jagerfly og atomvåben. Og det er sandsynligt, at nogle stater udvikler cybervåben, der kan ramme både fjendens våbensystemer og fjendens civile samfund i tilfælde af krig.

Men ligesom stater ikke uden videre anvender væbnet magt mod hinanden, er der også betydelige incitamenter til at udvise tilbageholdenhed i cyberspace. Cyberangreb kan foregå mere skjult og kan lettere benægtes end traditionelle metoder til spionage, sabotage eller andre former for undergravende virksomhed. Men det ændrer ikke ved, at kilden til angreb som regel kan spores, og at det er en politisk og ikke juridisk beslutning, når stater drager hinanden til ansvar. Således har USA længe haft som doktrin, at angreb fra cyberspace kan modsvares med angreb i de traditionelle domæner og i yderste konsekvens med atomvåben. Så mens stater generer hinanden i cyberspace under tærsklen for væbnet konflikt, er det usandsynligt, at en stat ud af det blå vil gennemføre et 'cyber-Pearl Harbour' mod en anden stat. Det giver kun mening, hvis man følger op med et konventionelt Pearl Habour og dermed indleder en 'almindelig' krig. Da der – heldigvis – ikke har været krig mellem moderne, velud-

viklede stater i digitaliseringens tidsalder, kan man stadig kun gisne om, hvor omfattende ødelæggelser det vil kunne medføre at supplere konventionelle våben med cybervåben.

Potentialet er stort, men som med atomvåben er der som sagt mange incitamenter til at udvise tilbageholdenhed.

Kriminelle og terrorister

Kriminelle aktører angriber mål i cyberspace for at tjene penge. Kriminelle aktiviteter varierer fra de helt primitive forsøg på bedrageri (mailen fra den nigerianske prins) over relativt simple angreb, der fx forhindrer målet i at kommunikere med omverdenen, til mere avancerede angreb, der kan stjæle, kidnappe eller ødelægge målets data. Kriminelle vil angribe så billigt som muligt og bruger derfor ofte 'standard'cyberangreb mod et stort antal mål i håb om, at nogen af målene har et dårligt cyberforsvar eller dårligt uddannede medarbejdere, der lader et angreb komme igennem.

Nogen få kriminelle netværk kan gennemføre meget avancerede angreb, der har krævet omfattende forberedelser i form af spionage mod målet samt udvikling og aflevering af programmer med skadeligt indhold. Sådanne angreb kan tage virksomheders, hospitalers eller hele byers data eller administration som gidsel for løsepenge. Det skete for den amerikanske storby Atlanta i marts 2018. Det tog Atlanta, der har 4,8 mio. indbyggere, flere måneder at komme nogenlunde på fode igen.

Af samme årsag har de kriminelle heller ingen interesse i at udvikle cybervåben, der overholder krigens love ved at være målrettet mod militære mål og begrænsede i deres virkning: Jo mere den kriminelle kan true et samfund, jo større løsesum kan denne kræve.

En særlig kategori af kriminelle aktører er Nordkorea, der bruger sine statslige hackere til at berige sig. Blandt andet har Nordkorea begået digitale bankrøverier i flere lande. WannaCry, der i 2017 bl.a. lammede et stort antal britiske hospitaler for at afpresse dem, var sandsynligvis et nordkoreansk angreb. Heldigvis har normale kriminelle aktører færre ressorcer til rådighed end stater, og deres mulighed for at investere i spionage mod potentielle mål og udvikle avancerede cybervåben er derfor begrænsede.

Antallet af kriminelle angreb er stort, og det vokser. Angrebene koster virksomheder og offentlige myndigheder mange penge. Der foreligger ikke overslag for den danske økonomi, men officielle rapporter fra USA anslår, at cyberangreb, hvoraf langt den overvejende del var kriminelt motiverede, kostede den amerikanske økonomi mellem 57 og 109 mia. dollar i 2016. Samtidig er risikoen fra kriminelles angreb på sin vis større for borgerne end risikoen fra staters angreb, fordi kriminelle (og Nordkorea) i modsætning til stater, ikke risikerer noget internationalt prestigetab ved fx at tage civile mål som hospitaler og anden kritisk infrastruktur som gidsler.

Danmark har siden 2001 haft statslige strategier for, hvordan stat, virksomheder og borgere kunne udnytte fordelene, men den første cyber- og informationssikkerhedsstrategi kom først i 2014.

Af samme årsag har de kriminelle heller ingen interesse i at udvikle cybervåben, der overholder krigens love ved at være målrettet mod militære mål og begrænsede i deres virkning: Jo mere den kriminelle kan true et samfund, jo større løsesum kan denne kræve.

På trods af en del bekymring i debatten om cybertrusler har terrorister og andre ideologisk motiverede aktører hidtil ikke været i stand til at gennemføre alvorlige cyberangreb, endsige gennemføre et 'cyber-9/11'. Selv terrorgrupper som ISIL, der i 2014-15 havde betydelige økonomiske ressourcer til rådighed, har ikke været i stand til at skaffe sig de nødvendige kompetencer. På trods af, at selve cybertruslen fra terrorgupper er lav, er det dog et stort problem at de i udstrakt grad bruger sociale medier i cyberspace til at sprede propaganda og kommunikere internt.

Danmarks cyberresiliens

Oven på denne gennemgang af truslerne fra cyberspace, vil det nok være på sin plads kort at gøre rede for Danmarks evne til at imødegå og overkomme dem – Danmarks cyberresiliens.

Bevidstheden om, at opbygningen af vores IT-baserede samfund har medført en række nye sårbarheder, er kommet til efter bevidstheden om alle fordelene. Danmark har siden 2001 haft statslige strategier for, hvordan stat, virksomheder og borgere kunne udnytte fordelene, men den første cyber- og informationssikkerhedsstrategi kom først i 2014.

Danmark har ikke været særligt bagud på denne front i forhold til andre gennemdigitaliserede lande. I 2008 udkom den første årlige trusselsvurdering fra de amerikanske efterretningstjenester, der for alvor nævnte cybertrusler. I 2010 havde Forsvarets Efterretningstjeneste cybertrusler med i den årlige risikovurdering for første gang. I 2012 kom cyber på forsiden af risikovurderingen, og i 2017 blev trusler fra cyberspace nævnt før alle andre trusler mod Danmark. Danmark har heller ikke været specielt langsom til at reagere på erkendelsen: I nordisk sammenhæng er regeringens tiltag på cyberområdet mindre konkrete og ambitiøse end Finlands, men mere end Sveriges og Norges.

Regeringens cyberresiliensstrategi tager udgangspunkt i sektoransvarsprincippet. I løbet af det 20. århundrede udviklede Danmark resiliensstrategier under overskrifter som 'Beredskab' eller 'Totalforsvar', hvor staten gennem komplicerede, indøvede kommandoveje kunne kontrollere kritiske dele af samfundsøkonomierne i tilfælde af krise eller krig. Da den kolde krig sluttede i 1989, faldt den politiske opmærksomhed omkring disse beredskabsstrukturer stærkt.

Samtidig havde globalisering og privatisering af kritisk infrastruktur en

positiv effekt på omkostninger og effektivitet, men udviklingen mindskede statens greb om den kritiske infrastruktur og gjorde det vanskeligere for staten at levere sikkerhed og håndtere kriser. Styringsmæssigt var problemet, at regeringen kunne udlicitere samfundskritiske opgaver, men ikke ansvaret for, at de blev udført. Samfundets stigende kompleksitet gjorde, at overvejelserne kom til at handle om det emergerende begreb 'resiliens'.

Hvor 1900-tallets beredskabstankegang så samfundet som en kompliceret maskine, der kunne styres og repareres udefra, er resilienstankegangen en dynamisk, selvregulerende tilgang inspireret af økologien. Den ser samfundet som en kompleks organisme, der kan reparere sig selv.

Sektoransvarsprincippet

Når staten ikke længere kan detailstyre via kommandoveje i tilfælde af krise, betyder det, at en stor del af opgaverne med at sikre resiliens – også på cyberområdet – må lægges ud i samfundets forskellige sektorer, fordi kun de har den nødvendige og opdaterede detailviden om deres egen situation. Princippet betyder, at den myndighed, virksomhed eller institution, som til daglig har ansvaret for et område, også har ansvaret for kriseplanlægning og opretholdelse af funktionerne under en krise. Statens nye rolle bliver at skabe rammerne for, at alle involverede aktører i det omfattende privatoffentlige samarbejde har forpligtigelse og incitamenter til at reagere optimalt på kriser.

Fordelen ved sektoransvarsprincippet er altså, at opgaven med beredskab og resiliens skal løses ude i sektorerne, hvor informationsniveauet om lokale forhold er højest. Hvad er ulemperne så?

Ved at decentralisere opgaverne med samfundets resiliens gennem sektoransvarsprincippet, bliver det let uklart hvad, der er kritisk infrastruktur, hvor højt et optimalt beredskab bør være, hvordan omkostninger til resiliens skal fordeles samt hvem, der er ansvarlig for, at opgaverne bliver løst. På det politiskstrategiske niveau kan det friste politikere på valg til at løbe en uhensigtsmæssigt stor risiko ved at nedprioritere ressourcer til fx cyberresiliens.

Det er lettere at demonstrere for borgerne, at man træffer beslutninger, som kommer dem til gode ved at afsætte ressourcer til infrastruktur, velfærd og skattelettelser, end ved at afsætte ressourcer til resiliens. De samfundsmæssige gevinster vil først vise sig, hvis der opstår en krise med udspring i cyberspace - en krise, der måske netop aldrig bliver rigtig alvorlig, hvis det ramte område har investeret og forberedt sig tilstrækkeligt. Og hvis det går galt, kan sektoransvaret misbruges til at placere ansvaret ude i sektorerne, langt væk fra de politikere, der ikke afsatte tilstrækkelige ressourcer eller tog ansvaret for at overføre dem fra sektorenes kerneopgaver.

Ude i sektorerne er udfordringen, at cyberresiliens ikke er sektorernes eller de individuelle aktørers kerneproduktion. Alt andet lige, vil ekstra omkostninger til formålet skulle tages fra kerneproduktionen eller fra virksomhedens overskud. Dermed vil det

have en tendens til at få mindre opmærksomhed og ressourcer, end hvad der fra et samfunsdmæssigt perspektiv er optimalt – især, hvis det ikke er en parameter, de ansvarlige chefer bliver målt på.

I 2014 blev en række myndigheder befalet til at implemetere en standard, ISO27001, som led i opbygningen af cyberresiliens. Da Digitaliseringsstyrelsen evaluerede implementeringen i 2017 fandt de, at selv om myndighederne generelt havde ledelsesmæssigt fokus på området, havde 43 pct. alligevel ikke gjort det i tilfredstillende omfang, angiveligt fordi området ikke blev prioriteret højt nok til, at der blev afsat ressourcer.

Det gælder også den private sektor: I A.P. Møller-Maersk blev cybersikkerhed og cyberresiliens angiveligt også nedprioriteret, fordi det ikke indgik direkte i evalueringen af chefer før NotPetya-angrebet i 2017. I den forbindelse udgør finanssektoren en undtagelse, fordi bankernes forretningsmodel kræver en så høj grad af cybersikkerhed, at markedskræfterne har kunnet drive udviklingen hurtigere og længere, end myndighederne har krævet.

Ny strategi

Danmark fik i foråret 2018 en ny strategi, der direkte omtaler problemerne med koordination og implementering og opstiller konkrete modtræk. Sektorerne fulgte op med deres individuelle delstrategier i januar 2019. Et par af elementerne i strategierne er, at det tværsektorielle overblik skal forbedres ved at oprette et cybersituationscenter og en oversigt over kritisk IT-infrastruktur. Tværsektoriel koordination søges forbedret ved at oprette en national styregruppe for cyber- og informationssikkerhed samt sektorenheder for udpegede samfundskritiske sektorer, og ved at foretage jævnlige tilstandsmålinger på området. Kontakten til borgere og virksomheder skal være lettere i det privat-offentlige samarbejde, bl.a. forenkles adgangen til at anmelde cyberangreb.

Tiltagene vil alt andet lige forbedre den tværgående kommunikation og det privat-offentlige samarbejde. Historisk har det dog altid været en udfordring at sikre prioriteringen af beredskab i sektorerne, og det vil det sandsynligvis også forblive på cyberområdet. I lyset af at kun Forsvaret er blevet tildelt ekstra midler til opgaven, er det sandsynligt, at de enkelte sektorer fortsat vil have svært ved at prioritere cyberresiliens i forhold til deres kerneopgaver.