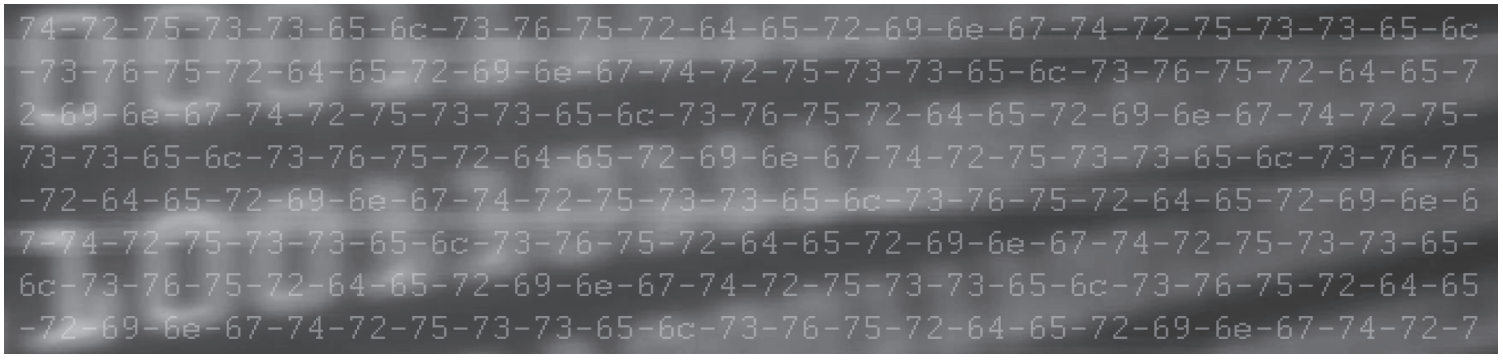
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod Danmark



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Marts 2019

CENTER FOR CYBERSIKKERHED

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. udgave
25.03.2019

Trusselsvurdering: Cybertruslen mod Danmark 2019

Formålet med denne årlige, nationale trusselsvurdering er at redegøre for den samlede cybertrussel, der møder danske myndigheder og virksomheder. Truslen er størst fra cyberspionage udført at stater og fra cyberkriminalitet.

Hovedvurdering

- Truslen fra cyberspionage er **MEGET HØJ**. Truslen er særligt udtalt mod de dele af staten, der beskæftiger sig med udenrigs, sikkerheds- og forsvarspolitik. Truslen er også rettet mod myndigheder og virksomheder i samfundsvigtige sektorer, da hver sektor har forskellige typer viden, som fremmede stater har interesse i. Flere stater forsøger at udføre cyberspionage mod danske interesser, og det er en udvikling, der fortsætter, i takt med at flere stater opbygger og udvikler deres cyberkapaciteter.
- Truslen fra cyberkriminalitet er **MEGET HØJ**. Myndigheder og virksomheder i samtlige sektorer i Danmark kan forvente løbende at blive udsat for cyberkriminalitet. Visse typer cyberkriminalitet kan have alvorlige konsekvenser for myndigheder og virksomheder i samfundsvigtige sektorer og derfor for det danske samfund.
- Truslen fra cyberaktivisme er **MIDDEL**. Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige kapaciteter. Truslen kan derfor stige pludseligt, hvis danske myndigheder eller virksomheder kommer i cyberaktivisters søgelys.
- Truslen fra cyberterror er **LAV**. Militante ekstremister har i få tilfælde vist interesse i at udføre cyberterror, men de har fortsat ikke kapacitet til dette.
- Det er mindre sandsynligt, at fremmede stater har til hensigt at rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark på kort sigt. Det er dog muligt, at danske virksomheder og myndigheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark.
- Teknologiske udviklinger, såsom Internet of Things og kunstig intelligens, vil medføre nye muligheder til gavn for samfundet, men vil også åbne for en større angrebsflade for hackere. Der vil også være en øget risiko for, at cyberangreb kan medføre fysiske ødelæggelser, da enheder koblet til internettet i højere grad styrer fysiske systemer.

Indledning

Cybertruslen er blevet et grundvilkår for danske myndigheder og virksomheder. Cybertruslen har i 2018 fortsat været meget aktiv, selvom der ikke har været så store sager som i 2017, hvor WannaCry og NotPetya-angrebene forstyrrede alt fra sygehuse til havneterminaler verden over. CFCS vurderer, at trusselsbilledet ikke vil ændre sig i en mere positiv retning, da den teknologiske udvikling og digitalisering af samfundet løbende giver hackere nye muligheder. Udviklingstendenser med betydning for cybertruslen foldes ud i sidste kapitel af dette års vurdering af cybertruslen mod Danmark.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Anden brug af internettet med ondsindet formål, såsom rekruttering til terrorgrupper via sociale medier eller salg af narkotika på internettet, indgår ikke i denne definition af cybertrusler.

Trusselsbilledet kan beskrives fra flere vinkler. I denne vurdering er fokus på, hvad formålet med cyberangrebene er. CFCS beskriver og vurderer aktiviteter, der har til formål at udføre cyberspionage, cyberkriminalitet, cyberaktivisme eller cyberterror. Desuden beskriver CFCS hackeres brug af destruktive cyberangreb og hack og læk.

Trusselsniveauerne er baseret på en analyse af aktørernes intention og cyberkapaciteter. CFCS vurderer en aktørs cyberkapacitet ud fra de menneskelige og materielle ressourcer, aktøren har til rådighed. Det kan være teknisk dygtige hackere og udviklere af malware eller viden om mål, der kan bruges til eksempelvis social engineering. Det kan også være it-infrastruktur, tid, penge og adgang til information. Hvor stor en cyberkapacitet, en aktør har, vil derfor afhænge af flere forskellige forhold og aktørens evne til at udnytte dem.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede, som har en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Cyberspionage

Truslen fra cyberspionage er **MEGET HØJ**.

Cyberspionage udgør en betydelig sikkerhedspolitisk og samfundsøkonomisk trussel mod danske myndigheder, sektorer og virksomheder. CFCS vurderer, at truslen især kommer fra fremmede stater og deres efterretningstjenester, som løbende forsøger at stjæle information fra danske myndigheder og virksomheder.

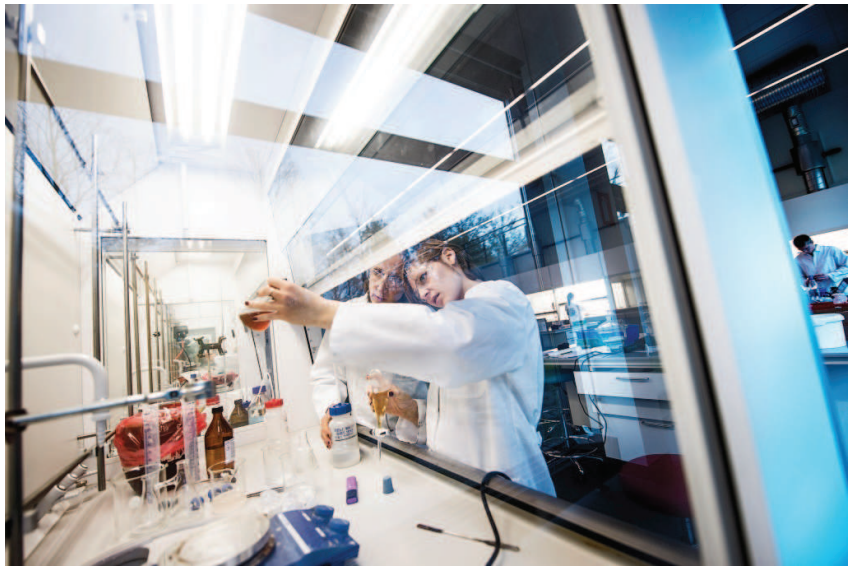
Truslen fra cyberspionage er særligt udtalt mod dele af staten. Det gælder især Udenrigsministeriet, Forsvarsministeriet og disses myndighedsområder samt institutioner og individer, der er tilknyttet Forsvaret og NATO-samarbejdet.

Truslen fra cyberspionage er også rettet mod myndigheder eller virksomheder i samfundsvigtige sektorer i Danmark, herunder energi-, finans-, sundheds-, søfarts, tele- og transportsektoren. CFCS vurderer, at truslen fra cyberspionage er MEGET HØJ for energi-, sundheds- og søfartssektoren, hvor den er HØJ for finans-, tele- og transportsektoren. Truslen fra cyberspionage er således ikke lige høj mod alle samfundsvigtige sektorer, men fremmede stater har både intention om og kapacitet til at udføre cyberspionage mod samtlige sektorer.

Cyberspionagen mod myndigheder og virksomheder i de samfundsvigtige sektorer kan både være politisk og økonomisk motiveret. Hver sektor har forskellige typer viden, som fremmede stater har interesse i. For eksempel er truslen for sundhedssektoren særligt rettet mod sundhedsdata, -forskning og -teknologi, som kan bruges til at udvikle og forbedre fremmede staters sundhedssektor og deres befolkningers levestandard. Truslen for energisektoren er derimod særligt rettet mod viden, der kan fremme andre landes energipolitik og -sektor, men også mod systemer og netværk, der kan udnyttes til at udføre destruktive cyberangreb.

Fælles for sektorerne er, at de fremmede stater både kan stjæle informationerne for at udnytte dem selv, eller for at videregive dem til deres hjemlige virksomheder. Udover at skade den berørte danske virksomhed eller myndighed kan det også udgøre en samfundsøkonomisk risiko for Danmark. Det kan skade den danske konkurrenceevne, når udenlandske virksomheder får adgang til stjålen viden om forskning, systemer, eller udbud og kontrakter, som danske virksomheder har brugt ressourcer på at udvikle eller forhandle.

Truslen mod virksomheder er derfor særligt rettet mod forskningstunge virksomheder samt virksomheder, der er i kraftig vækst på internationale markeder, er aktive i konfliktområder eller driver virksomhed inden for strategiske ressourcer, såsom naturressourcer eller kritisk infrastruktur.



Fremmede stater har bl.a. interesse i at spionere mod forskning, som Danmark bruger ressourcer på at udvikle

Hvis en fremmed stat kompromitterer danske virksomheder eller myndigheder for at udføre cyberspionage mod dem, kan organisationerne også være mere sårbare overfor andre typer trusler. Cyberspionage kan bl.a. give en modstander adgang til følsomme oplysninger, der senere kan lækkes til offentligheden for at påvirke meningsdannelsen enten i forbindelse med afholdelse af valg, politiske eller højaktuelle sager. Cyberspionage anvendes også forud for destruktive cyberangreb, særligt hvis spionagen giver adgang til kritiske systemer eller informationer af særlig karakter.

Flere stater udgør en cybertrussel mod Danmark
CFCS vurderer, at stadigt flere stater udgør en cybertrussel mod Danmark, og at denne udvikling vil fortsætte i takt med, at cyberangreb bliver et centralt værktøj i den politiske værktøjskasse i flere lande. Både mere og mindre magtfulde stater udvikler og anvender deres cyberkapaciteter, fordi cyberspionage er en relativt risikofri måde for stater at få adgang til eftertragtede oplysninger.

CFCS vurderer, at nogle få stater forsøger at udføre cyberspionage mod myndigheder og virksomheder over hele verden, herunder i Danmark. Disse stater udgør den største cybertrussel mod Danmark. Særligt Rusland og Kina råder over avancerede cyberkapaciteter og er yderst aktive aktører på cyberområdet. Det er sandsynligt, at Iran og Nordkorea også er stater, der anvender deres cyberkapaciteter mod mål verden over.

Andre stater anvender primært deres cyberkapaciteter mod myndigheder, virksomheder og borgere i deres regionale nærområde. CFCS vurderer, at disse stater også udgør en cybertrussel mod Danmark, da de sandsynligvis forsøger at spionere mod danske repræsentationer, der er til stede i regionen. I maj 2018 blev en medarbejder på en dansk ambassade i Asien f.eks. udsat for forsøg på spear phishing af en hackergruppe, der muligvis er knyttet til en stat, der også ligger i Asien. Forsøget lykkedes ikke. CFCS vurderer, at disse stater forsøger at kompromittere repræsentationerne, dels for at få adgang til viden om dansk sikkerheds- og udenrigspolitik i regionen og dels for at få adgang til viden om det land eller den region, repræsentationen ligger i. Nogle danske repræsentationer kan også have fremmede staters interesse, fordi de har en særlig rolle i internationale organisationer.

Stater, der primært bruger deres cyberkapaciteter i deres nærområde, udgør også en cyberspionagetrussel mod Forsvarets udsendte bidrag. Fremmede stater kan f.eks. forsøge at stjæle følsomme oplysninger om Forsvaret ved at kompromittere udsendte danske styrker.

Statsstøttede hackergrupper udfører cyberspionage mod underleverandører
Statsstøttede hackergrupper retter deres cyberangreb mod underleverandører, som de kan bruge som springbræt til at få adgang til informationer, der tilhører deres egentlige mål.

Hackergrupperne har bl.a. rettet deres opmærksomhed mod underleverandører, der tilbyder forskellige cloud-løsninger og datalagringstjenester. Ved at kompromittere disse underleverandører har fremmede stater haft fjernadgang direkte ind i kundernes netværk, hvorfra de har kunnet

stjæle informationer. Fordi hackerne misbrugte underleverandørernes betroede netværk og brugte legitime brugernavne og kodeord, har det været vanskeligt for ofrene at skelne mellem legitim og illegitim aktivitet. I visse tilfælde har aktørerne også haft adgang til de kundedata, der lå på underleverandørernes egne servere.

De fleste myndigheder og virksomheder benytter sig af underleverandører, og i alle sektorer er det relevant at have et godt overblik over, hvilken adgang underleverandører har til myndigheder eller virksomheders netværk.

Cyberangreb mod underleverandører

APT10 er en hackergruppe, der i flere år har stjålet informationer fra deres ofre ved at angribe underleverandører. Gruppen har f.eks. stået bag en kampagne kaldet Cloudhopper. Kampagnen fik det kaldenavn, fordi APT10 bl.a. angreb udbydere af cloud-tjenester for at bruge dem som springbræt til at kompromittere disses kunder.

APT10 er gået efter myndigheder og virksomheder i mange forskellige sektorer verden over bl.a. for at stjæle intellektuel ejendom.

Den 20. december 2018 anklagede det amerikanske justitsministerium og FBI to kinesiske statsborgere for at være tilknyttet hackergruppen APT10.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ.**

Det er en kompleks trussel bestående af mange forskellige typer af cyberkriminalitet. Truslen indeholder alt fra simple cyberangreb udført at kriminelle, der nærmest ikke har it-kompetencer, til avancerede cyberangreb, udført af velorganiserede hackergrupper, der sandsynligvis er statsstøttede. Cyberkriminalitet er i denne vurdering en fællesbetegnelse for handlinger, hvor gerningsmanden bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk berigelse.

Typerne af cyberkriminalitet har forskellige konsekvenser, og det er ikke alle myndigheder eller virksomheder, der vil blive udsat for alle de forskellige angrebsformer. Myndigheder og virksomheder i samtlige sektorer i Danmark kan dog forvente løbende at blive udsat for en eller flere former for cyberkriminalitet.

Hyppige angreb fra cyberkriminelle udgør en vedvarende trussel mod hele Danmark

Én type af cyberkriminelle netværk forsøger at kompromittere så mange ofre som muligt for at maksimere deres profit. Angrebene er typisk mindre avancerede og giver et mindre afkast per offer, men til gengæld angriber hackerne mange på en gang, og de angriber igen og igen. Disse kriminelle netværk udgør en vedvarende trussel mod myndigheder, virksomheder og borgere.

For at ramme så mange som muligt spreder cyberkriminelle deres malware gennem phishing-mails eller inficeringer af hjemmesider, som ofrene besøger. Nogle kriminelle udsender phishing-mails i stor volumen med mange tusinder modtagere. Bag disse angreb er der typisk et økosystem af kri-

minelle, der har specialiseret sig i bl.a. udvikling af malware, udvikling og drift af teknisk infrastruktur eller håndtering af kompromitterede ofre. Udvekslingen af tjenester mellem disse kriminelle muliggør også, at kriminelle med relativt begrænsede it-kompetencer kan begå cyberkriminalitet.

Hvilke malwaretyper, de cyberkriminelle spreder, afhænger af indtjeningsmulighederne. Noget malware kombinerer endda egenskaber fra forskellige typer malware for at maksimere profit fra deres ofre. Den Android-baserede malware kaldet Svpeng er et eksempel på en mobil malware, som både kan stjæle informationer fra ofrets mobiltelefon og kryptere telefonens indhold. Hackerne bag Svpeng-malwaren kan således både tjene penge ved f.eks. at misbruge loginoplysninger til bank-apps og ved at forlange en løsesum for at dekryptere indholdet på telefonen.

I 2018 har der været en generel tendens til, at ransomware-angreb er faldet i hyppighed samtidig med, at der er sket en stigning i spredning af malware, der misbruger it-systemer til at generere kryptovaluta, såkaldt crypto mining malware. I de seneste år har der også været en stigning i tyverier af kryptovalutaer fra kryptovalutabørser og privatpersoner. Denne stigning skyldes sandsynligvis den generelt øgede værdi af og spekulation i kryptovalutaer.

Hackere forsøger også at kompromittere virksomheder, som opbevarer personlige oplysninger om borgere, der kan misbruges på forskellige måder til at skabe profit. Oplysningerne kan f.eks. være personnumre eller oplysninger fra betalingskort.

I slutningen af 2018 har cyberkriminelle både i Danmark og i udlandet inficeret netbutikker for at aflæse brugernes betalingsoplysninger, når de har købt varer. Det er sket ved, at hackerne har indlejret ondsindet kode på netbutikkernes hjemmesider, som stjæler kundernes betalingsoplysninger. Konkurrencen blandt kriminelle om at stjæle oplysninger fra betalingskort er så udbredt, at forskellige cyberkriminelle grupper i visse tilfælde saboterer hinanden på de samme kompromitterede netbutikker.

Eksempler på datatyveri

I juni 2018 offentliggjorde Ticketmaster UK, at betalingsoplysninger tilhørende deres kunder muligvis var blevet kompromitteret. Danske kunder, der havde handlet hos Ticketmaster i en bestemt periode, blev som en sikkerhedsforanstaltning opfordret af Ticketmaster til at overvåge deres kontoudskrifter for muligt bedrageri.

I efteråret 2018 blev den danske virksomhed Bahnes netbutik angrebet af hackere, der forsøgte at stjæle kunders betalingsoplysninger. Virksomheden opfordrede deres kunder til præventivt at spærre betalingskort, som var blevet brugt til køb på netbutikken, da oplysningerne kunne blive misbrugt af cyberkriminelle. Som følge af angrebet var Bahnes netbutik nede nogle timer på udsalgsdagen Black Friday. I starten af januar 2019 blev netbutikken igen angrebet og blev derfor lukket i ca. to måneder og flyttet til en ny platform.

Cyberkriminelle udfører også afpresningsforsøg, der ikke benytter malware. Flere danskere er i år eksempelvis blevet ramt af afpresningsforsøg, såkaldt sextortion, hvor cyberkriminelle afpresser ofret ved at påstå at have private oplysninger om eller billeder og videooptagelser af ofret. I mange tilfælde angiver de kriminelle en adgangskode, som ofret har brugt på en hjemmeside, for at øge troværdigheden af truslen. Adgangskoden stammer, i de tilfælde som CFCS er bekendt med, fra tidligere læk eller hackede databaser, der er tilgængelige på nettet, og som typisk er flere år gamle.

I nogle af afpresningsforsøgene ser det ud som, at afpresningsmailen er sendt fra modtagerens egen e-mailadresse, og de kriminelle påstår, at det beviser, at de har adgang til ofrets mailkonto. Det er dog et trick, hvor de kriminelle har forfalsket afsenderadressen med en teknik kaldet spoofing.

I de tilfælde af sextortion, som CFCS er bekendt med, har der været tale om påstande og tomme trusler. CFCS anbefaler, at man ikke besvarer afpresserne og ikke betaler løsesum.

Cyberangreb fra kriminelle kan ramme samfundsvigtige funktioner

Der er cyberkriminelle netværk, som udgør en trussel mod virksomheder og myndigheder med samfundsvigtige funktioner. Disse netværk angriber mere målrettet og har derfor færre ofre. Til gengæld kan de opnå væsentligt højere profit per angreb, da de i højere grad lykkes med at kompromittere centrale netværk og systemer. For de hackergrupper, der anvender ransomware eller stjæler data, kan deres målrettede cyberangreb lægge et stort pres på ofret ift. at betale høje løsesummer for deres data.

Cyberangreb fra disse kriminelle netværk kan få alvorlige konsekvenser for virksomheder og organisationer, der varetager samfundsvigtige funktioner. Mulige konsekvenser er blandt andet forsyningsstop, tab af store pengebeløb, nedetid eller tab af omdømme. Det kan i værste fald have samfundsmæssige konsekvenser og føre til tab af tillid til samfundsvigtige funktioner. Truslen fra mere målrettede cyberkriminelle angreb gælder også for virksomheder, der ikke er samfundsvigtige. Det kan have store konsekvenser for den berørte virksomhed, men de samfundsmæssige konsekvenser er mindre udtalte.

Et eksempel er den cyberkriminelle gruppe, der står bag ransomwaren SamSam. SamSam-angrebene har især ramt sundhedsvæsnet, uddannelsesinstitutioner og offentlige institutioner i flere lande, dog fortrinsvist i USA. SamSam-ransomwaren har i flere tilfælde ramt hospitaler, hvor det har påvirket den samfundsvigtige ydelse, hospitalerne udfører. Et amerikansk hospital, der blev ramt af et målrettet angreb med SamSam-ransomwaren i starten af 2018, valgte at betale løsesummen, der svarede til omtrent 300.000 kroner. Ifølge amerikanske myndigheders anklage mod to mænd, der angiveligt har udført SamSam-angrebene, har hackerne i alt tjent, hvad der svarer til omtrent 40 millioner kroner på deres angreb.

De seneste år har der også været en række målrettede cyberangreb mod udenlandske banker, hvor det er lykkedes kriminelle at stjæle betragtelige beløb. Hackerne har kompromitteret bankers it-systemer og derefter foretaget uautoriserede overførsler via finansielle netværk, bl.a. SWIFT. I august 2018 mistede en indisk bank eksempelvis, hvad der svarer til cirka 85 millioner kroner, i et cyberangreb. Flere sikkerhedsfirmaer har tilskrevet en del af disse digitale bankrøverier til hackergrupper, som CFCS vurderer har tilknytning til Nordkorea.

Nogle af angrebene har påvirket de finansielle virksomheders tjenester. Det var f.eks. tilfældet den 13. februar 2019, hvor den maltesiske bank Bank of Valletta midlertidigt stoppede sine bankforretninger for at imødegå et cyberangreb, hvor hackere forsøgte at stjæle, hvad der svarer til tæt på 100 millioner kroner. Banken lukkede bl.a. sine filialer og hæveautomater på Malta og lukkede sin hjemmeside.

I enkelte tilfælde har hackerne slettet eller krypteret finansielle virksomheders data i forbindelse med sådanne digitale bankrøverier. Det er sandsynligvis gjort i forsøg på at slette spor eller forhindre ofret i at reagere på tyveriet.

Cyberaktivisme

Truslen fra cyberaktivisme er **MIDDEL**.

Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige evner og ressourcer til at udføre cyberangreb. Truslen kan derfor stige pludseligt, hvis danske myndigheder eller virksomheder kommer i cyberaktivisters søgelys.

Formålet med cyberaktivisme er at skabe størst mulig opmærksomhed om en given sag. Det medfører, at angreb i en del tilfælde bliver varslet eller opfordret til på bl.a. sociale medier, i modsætning til eksempelvis cyberspionage, hvor hackere forsøger at skjule deres aktiviteter.

Netværk med interesse i Danmark
Der er et begrænset cyberaktivistisk miljø med interesse i eller aktiviteter rettet mod danske myndigheder og virksomheder. Der er få sager med danske cyberaktivister, og NC3 har i nogle af disse sager identificeret aktivisterne og bidraget til, at de blev retsforfulgt.

Cyberaktivisme motiveres af alt fra dyrevelfærd til anti-kapitalisme
Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver. Aktivistiske hackere fokuserer ofte på personer eller organisationer, som de opfatter som modstandere af deres

sag. De angriber til tider også myndigheder og virksomheder, der ikke har direkte tilknytning til aktivisternes sag, men som aktivisterne opfatter som symbolske mål.

Det kan være særdeles svært at forudsige, hvad der vil udløse cyberaktivisme og mod hvem. Cyberaktivister er drevet af meget forskellige motiver og synspunkter. I løst sammensatte netværk som f.eks. Anonymous er der aktivister, der fokuserer på så forskellige emner som internetfrihed, dyrevelfærd, klima, støtte til whistleblowere, anti-kapitalisme og bekæmpelse af militante islamister og højreekstremisme. Der er også eksempler på nationalistiske hackergrupper samt netværk, der støtter terrorgrupper.

Dyrevelfærd var motiv for angreb

Under en kampagne med slogannet OpDenmark og OpBeast blev omkring 350 danske hjemmesider ramt af bl.a. overbelastningsangreb i perioden 2013-2014. Kampagnen gik efter at ændre dansk lovgivning om dyresex.

I udlandet bliver mange cyberaktivistiske angreb udført i forbindelse med diplomatiske eller militære konflikter. Truslen mod Danmark kan derfor også stige, hvis danske myndigheder eller virksomheder pådrager sig opmærksomhed i relation til sådanne konflikter i udlandet.

Tilbagevendende kampagner og fysisk politisk aktivisme kan varsle cyberaktivisme

Mens cyberaktivistiske angreb ofte er relativt spontane, vil der i nogle tilfælde være bedre muligheder for at forudse cyberaktivistiske angreb. Det er særligt tilfældet ved tilbagevendende kampagner og i forbindelse med fysisk politisk aktivisme, der i stigende grad ledsages af cyberaktivisme.

En række cyberaktivistiske kampagner gentages år efter år. Et eksempel på dette er gentagne overbelastningsangreb, også kaldet DDoS-angreb, udført af Anonymous-affilierede hackere mod centralbanker og andre finansielle institutioner i forbindelse med den anti-kapitalistiske #OpIcarus kampagne. Denne kampagne er vendt tilbage flere gange siden 2016.

Cyberaktivister angreb franske myndigheder og virksomheder for at støtte De Gule Veste-protesterne

Cyberaktivisme ledsager også i stigende grad mere traditionel politisk aktivisme. Det skete eksempelvis i slutningen af 2018, da hackere i sympati med De Gule Veste i Frankrig udførte flere overbelastningsangreb og hack og læk angreb mod en række franske myndigheder og virksomheders hjemmesider, herunder det franske politi, udenrigs- og forsvarsministerium.

Cyberaktivisters kapaciteter og grad af organisering varierer

Der er stor forskel på cyberaktivistiske aktørers kapacitet og organisering, eller mangel på samme. Det kan gøre det svært at forudsige, hvor stor en cyberkapacitet aktivister har til rådighed i forskellige kampagner.

Det løst sammensatte hackernetværk Anonymous består eksempelvis både af strukturerede hackergrupper med kapacitet til og intention om at udføre cyberangreb og sympatisører uden kapacitet eller intention om selv at udføre cyberaktiviske angreb. Nogle aktivistiske cyberangreb bliver således udført af hackergrupper, der består af forholdsvis permanente medlemmer, mens andre bliver udført af individuelle hackere. Individuelle hackere, hackergrupper og netværk slår sig til tider også sammen om specifikke kampagner.

Individuelle hackere kan med relativt simple metoder dog også udføre cyberaktivistiske angreb, der får stor opmærksomhed. For eksempel fik det stor opmærksomhed i Tyskland, og også i Danmark, da op imod 1000 tyske politikere og offentlige personer fik offentliggjort personlige informationer på Twitter i december 2018. En ung tysk mand, der blev anholdt i januar 2019, tilstod at have hacket sig til nogle af informationerne. De tyske myndigheder udtalte, at manden havde brugt relativt simple metoder til at hacke sig ind i ofres konti. Ifølge medier havde han bl.a. udnyttet, at mange af hans ofre havde svage passwords.

Eksempler på cyberaktivistiske angrebsmetoder

DDoS-angreb: Det er fortsat en udbredt metode blandt cyberaktivister at forsøge at gøre hjemmesider utilgængelige ved brug af overbelastningsangreb.

Defacement: Med denne metoder hacker cyberaktivister hjemmesider eller profiler på sociale medier, hvor de indsætter budskaber eller billeder.

Hack og læk angreb: Nogle cyberaktivister lækker følsomme oplysninger fra hacking af f.eks. personlige mailkonti for at skabe opmærksomhed om deres sag.

Statsstøttede hackere står bag faketivisme

I nogle tilfælde benytter stater cyberaktivistiske grupper som dække i forsøg på at påvirke den folkelige meningsdannelse i andre lande. I populær tale kaldes sådanne statsstøttede hackere, der udgiver sig for at være ikke-statslige cyberaktivister, for faketivister.

Truslen fra faketivisme kan stige i forbindelse med sager af særlig politisk, strategisk eller økonomisk karakter, hvis udfald fremmede stater har en væsentlig interesse i at påvirke. Truslen kan også stige i forbindelse med en skærpet politisk eller militær konflikt.

Et eksempel på faketivisme var, da World Anti-Doping Agency (WADA) og flere andre anti-doping organisationer blev hacket af en gruppe, der kaldte sig Fancy Bear Hack Team og udgav sig for at være cyberaktivister. Gruppen lækkede oplysninger, de havde hacket sig til, bl.a. om den danske svømmer Pernille Blume. I oktober 2018 blev flere russiske efterretningsofficerer offentligt anklaget af amerikanske myndigheder for at stå bag disse og flere andre hack og læk angreb.

Cyberterror

Truslen fra cyberterror er **LAV.**

Militante ekstremister har i få tilfælde vist interesse i at udføre cyberterror, men CFCS vurderer, at de fortsat ikke har kapacitet til dette. De er på nuværende tidspunkt alene i stand til at udføre simple cyberangreb, der især har til formål at skabe opmærksomhed om og sprede propaganda for ISIL og andre militante ekstremistiske grupper. Der er derfor en lav trussel mod Danmark fra cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

Flere hackergrupper, der støtter terrororganisationen Islamisk Stat i Irak og Levanten (ISIL), har de seneste år forsøgt at styrke deres cyberkapaciteter ved at slå sig sammen i forskellige hackernetværk. Det mest kendte af disse netværk blev dannet i 2016 under navnet United Cyber Caliphate (UCC). Det har indtil nu ikke øget militante ekstremisters evner eller ressourcer til at udføre cyberangreb.

ISIL's ledelse har indtil nu ikke officielt anerkendt UCC eller andre hackergrupper. Truslen fra hackere, der støtter ISIL eller andre ekstremistiske terrorgrupper, kan stige, hvis grupper som ISIL i fremtiden vælger at støtte UCC eller andre hackergrupper. Det er mindre sandsynligt, at ISIL eller andre sunniekstremistiske terrorgrupper på kort sigt vil støtte udviklingen af cyberkapaciteter i en sådan grad, at det vil øge truslen fra cyberterror.

Militante ekstremister med tilstrækkelig finansiel styrke kan købe sig til mere avancerede kapaciteter end dem, de råder over nu. De værktøjer, de vil kunne købe sig til på nuværende tidspunkt, er dog ikke tilstrækkeligt avancerede til at udføre så alvorlige cyberangreb, at de kan få samme effekt som konventionel terror.

Destruktive cyberangreb

CFCS vurderer, at det er mindre sandsynligt, at fremmede stater har til hensigt at rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark på kort sigt. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt med lande, der har evnen til at gennemføre destruktive cyberangreb.

Destruktive cyberangreb

CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er død, personskade, betydelig skade på fysiske objekter eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

CFCS vurderer, at det er muligt, at fremmede stater har forsøgt at kompromittere danske samfundsvigtige virksomheder for at kunne opbygge kapacitet til at rette destruktive cyberangreb mod samfundsvigtig infrastruktur på et senere tidspunkt. CFCS ser derfor med alvor på, at der i 2017 var flere målrettede forsøg på at få uautoriseret adgang til organisationer i den danske energisektor.

Danske organisationer kan blive påvirket af destruktive cyberangreb mod mål udenfor Danmark

Det er muligt, at danske virksomheder og myndigheder på kort sigt kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske virksomheder og myndigheder, der er til stede i lande såsom Saudi-Arabien, Sydkorea og Ukraine, hvor fremmede stater sandsynligvis har stået bag destruktive cyberangreb.

NotPetya-angrebet i Ukraine i 2017 viste, at destruktive cyberangreb kan sprede sig til organisationer uden for disse lande. Virksomheder, der har aktiviteter i disse lande, kan også blive udset som specifikke mål for destruktive cyberangreb. Det viser det destruktive cyberangreb i december 2018 mod en italiensk underleverandør til olieindustrien, Saipem. Saipem er bl.a. underleverdør til det saudiarabiske olieselskab, Saudi Aramco. Saudi Aramco har to gange tidligere været udsat for destruktive cyberangreb med varianter af den samme malware, kaldet Shamoon, som blev brugt mod Saipem. Det destruktive cyberangreb, som ramte Saipem, slettede data på flere hundrede af virksomhedens computere verden over.

Destruktive cyberangreb er sjældne og ødelægger for det meste data

CFCS' definition af destruktive cyberangreb dækker cyberangreb med meget forskellige konsekvenser, rangerende fra sletning af data til fysisk ødelæggelse. Destruktive cyberangreb har oftest medført ødelæggelse af data, der er blevet slettet eller gjort utilgængelige af malware og værktøjer, der i fagsprog kaldes wipere. Ødelæggelse og manipulation af data i industrielle kontrolsystemer har i nogle tilfælde ført til driftsforstyrrelse og nedbrud. I et enkelt tilfælde for flere år siden har et destruktivt cyberangreb medført fysisk ødelæggelse udenfor it-systemer.

Destruktive cyberangreb er sjældne sammenlignet med andre typer cyberangreb og har som ovenfor nævnt primært fundet sted i Saudi-Arabien, Sydkorea og Ukraine. CFCS vurderer, at angrebene i disse lande sandsynligvis blev udført af statslige aktører, og at de overvejende blev anvendt som led i regionale konflikter og spændinger.

Hackere benytter også simple destruktive cyberangreb uafhængigt af politiske og militære konflikter. I få tilfælde har hackere i forbindelse med cyberkriminalitet de seneste år vist vilje til at slette eller kryptere finansielle virksomheders data i forbindelse med digitale bankrøverier, sandsynligvis i et forsøg på at slette deres spor eller forhindre virksomhederne i at reagere på tyveriet. Sletning eller kryptering af data i digitale bankrøverier er foreløbigt et relativt sjældent fænomen, men det kan have store konsekvenser for den berørte finansielle institution.

Angrebet mod Triconex

Et cyberangreb, der potentielt kunne have medført fysisk ødelæggelse, fandt sted i Saudi-Arabien i 2017. Angrebet blev først offentligt kendt i 2018. Cyberangrebet var rettet mod en petrokemisk industrivirksomhed og et bestemt system kaldet Triconex, som virksomheden brugte.

Systemet Triconex sørger bl.a. for, at produktionssystemer bliver lukket ned på en kontrolleret og sikker måde, hvis der opstår kritiske fejl eller problemer. I det konkrete tilfælde i Saudi-Arabien medførte nogle bestemte forhold, at sikkerhedssystemerne lukkede ned på en ufarlig måde, hvilket gjorde at malwaren blev opdaget.

Hvis sikkerhedsmekanismerne derimod var blevet slået fra eller manipuleret med, kunne det i værste fald have øget risikoen for udslip af farlige gasser eller eksplosioner.

Hack og læk angreb

Visse lande benytter også hack og læk af politisk følsomt materiale i forsøg på at påvirke meningsdannelsen. Her er cyberangreb igen et instrument i den politiske dagsorden og magtkamp. Det er bl.a. sket i forbindelse med afholdelse af valg i udlandet, hvor angrebene har haft til formål at påvirke befolkningens holdning og tillid til bestemte politikere samt skabe mistro til den demokratiske proces. Det er sket i en grad så vestlige lande i dag generelt forbereder sig på at blive udsat for cyberangreb i forbindelse med afholdelse af valg.

I disse tilfælde har cyberangreb været ét blandt flere virkemidler i bredere informations- og påvirkningskampagner, der også har inkluderet f.eks. falske nyhedshistorier og aktiviteter på sociale medier. Det er muligt, at cyberangreb, såsom hack og læk af følsomme oplysninger, vil blive brugt som virkemiddel i en eventuel påvirkningskampagne i Danmark. Truslen fra sådanne cyberangreb kan stige i forbindelse med politiske sager, hvis udfald fremmede stater har en væsentlig interesse i at påvirke eller i forbindelse med en politisk eller militær konflikt.

Udviklingstendenser med betydning for cybertruslen

Cybertruslen mod det danske samfund er i høj grad afhængig af de eksisterende teknologiske og samfundsmæssige forhold. Nedenfor beskrives en række teknologiske og strukturelle tendenser, som forventes at have betydning for cybertruslen de kommende år.

Generelt vil flere områder blive digitaliseret, og der vil ske en stadig større sammensmeltning af den fysiske og digitale verden. Derudover vil computere med såkaldt kunstig intelligens i stigende grad udføre opgaver med væsentlig betydning for samfundet og den enkelte borger. Det medfører, at samfundets afhængighed af digitale systemer øges.

Cyberangreb kan i stigende grad få konsekvenser i den fysiske verden

Indenfor de seneste to år er der i Danmark implementeret nye netværk, som Narrowband IoT, Sigfox og LoRaWAN, der sammen med internettet og de traditionelle mobilnet understøtter et stadig stigende antal digitale løsninger, der kobler den digitale og fysiske verden sammen, også kaldet "tingenes internet" eller Internet of Things (IoT). Et eksempel er udviklingen af de såkaldte Smart Cities, hvor områder som renovation, transport og forsyning er effektiviseret ved hjælp af IoT-løsninger. I Danmark arbejder flere kommuner med smart city aktiviteter. Eksempelvis findes der skraldespande, som selv fortæller, hvornår de er fyldte og skal tømmes. Et andet eksempel er en kommune, der løbende regulerer fjernvarme og vandforsyning på baggrund af realtidsdata om den enkelte husstands vand- og varmeforbrug.

Den kommende 5G mobilteknologi, som bl.a. er designet til at kunne understøtte selvkørende biler og autonome produktionssystemer, forventes at øge denne kobling af den digitale og fysiske verden yderligere.

Teknologien vil medføre nye muligheder til gavn for samfundet, men vil også åbne for en større angrebsflade for hackere. Hvis hackere afbryder eller manipulerer med signaler, som sendes til og fra IoT-enheder, kan det potentielt medføre fysiske ødelæggelser, da enheder koblet til internettet i stadig højere grad styrer fysiske systemer.

Begreber

Machine learning: It-systemer som behandler nye data på baggrund af maskinelle analyser af et tidligere datasæt (læring) frem for gennem eksplicit programmering (instrukser).

Kunstig intelligens: Teknologier som efterligner menneskelig intelligens, herunder sprog, syn, læring og evnen til at generalisere.

Internet of Things: Internet of Things, forkortet IoT, er et udtryk for hverdagsobjekter som f.eks. køleskabe og kameraer, der er koblet til internettet. Det gør, at enhederne kan styres centralt og kan interagere mere automatiseret med hinanden uden menneskelig involvering.

Cloud Computing: Cloud computing er it, som leveres via internettet og er kendetegnet ved at være skalérbart og fleksibelt. Cloud computing kan bestå af virtuel infrastruktur, softwareplatforme, applikationer eller tjenester, som lejes efter behov.

Det stigende antal IoT-enheder kan føre til flere og mere alvorlige cyberangreb
Der ses i disse år en stor stigning i antallet af enheder, der ikke traditionelt har været forbundet til internettet, som nu kobles på. Nogle estimater anslår, at der inden 2020 vil være mere end 20 mia. nye enheder koblet på internettet, og andre estimater er langt højere. Der er tale om alt fra køleskabe til store industrielle kontrolsystemer, som kobles på internettet.

Der er flere risici forbundet med det stigende antal IoT-enheder, som kobles på internettet, og IoT-enheder anslås allerede nu at være blandt den type af enheder på internettet, der bliver udsat for flest cyberangreb.

Et cyberangreb på en IoT-enhed kan påvirke enhedens funktion eller medføre en kompromittering af det netværk, som enheden er installeret i. Målet er ofte at installere malware på enheden, som gør det muligt for angriberen at fjernstyre den, så den kan udnyttes i andre cyberangreb. Kompromitterede IoT-enheder har typisk været brugt som led i overbelastningsangreb, hvor angriberen retter et meget stort antal enheders netværkstrafik mod en server og derved forsager et nedbrud.

IoT-enheder er ofte sårbare, fordi de bliver udviklet med et specifikt formål for øje, og de netværksfunktioner, som gør det muligt for enheden at kommunikere via internettet, er kun sekundære funktionaliteter. Derfor har enhederne ofte en utilstrækkelig netværkssikkerhed sammenlignet med traditionelt it-udstyr, der er udviklet med henblik på at blive koblet på internettet. Derudover er mange IoT-enheder ikke designet til at kunne modtage sikkerhedsopdateringer. Det betyder, at de sårbarheder, der bliver opdaget i produktets levetid, ikke kan rettes og derfor kan udnyttes af hackere, så længe produktet er i brug. Det er især et problem for IoT-enheder, der er designet til at kunne fungere i flere år uden menneskelig indblanding.

Kunstig intelligens kan hackes til at tage skadelige beslutninger
Over hele verden forskes der i kunstig intelligens, og mange lande kan se en strategisk fordel i teknologien. Det gælder også for Danmark. Egentlig kunstig intelligens findes endnu ikke og har nok lange udsigter. Begrebet anvendes dog bl.a. om computerprogrammer, som via machine learning er i stand til at udføre specifikke analytiske opgaver, der tidligere har krævet involvering af menneskelig intelligens.

Brugen af kunstig intelligens kan dog også øge samfundets sårbarhed overfor cyberangreb. Når kunstig intelligens i stigende grad anvendes til at tage rutinemæssige beslutninger og udføre handlinger, som tidligere har været foretaget af mennesker, er det vigtigt, at systemerne er robuste overfor cyberangreb, så hackere ikke kan påvirke dets beslutninger. Hvor outputtet fra traditionelle computerprogrammer er en følge af fastlagte og sporbare algoritmer, så kan det ved systemer med kunstig intelligens være vanskeligt at påvise, hvordan computeren præcis er kommet frem til et bestemt resultat. Det kan gøre det vanskeligt at efterprøve validiteten af resultatet.

Eksempler på områder, hvor kunstig intelligens forventes at spille en stadig større rolle, er inden for selvkørende biler, autonome industrisystemer og diagnosticering og medicinering i sundhedssektoren.

Stigende outsourcing kan gøre cybersikkerhed vanskeligere
Den stigende kapacitet og kommunikationshastighed på internettet har løbende øget muligheden for, at myndigheder og virksomheder kan outsource infrastruktur og driftsopgaver til underleverandører. Det har medført, at danske såvel som internationale virksomheder i stigende grad har lagt dele af deres digitale forretning ud til underleverandører, også uden for landets grænser. Det er f.eks. tilfældet i forbindelse med lagring af data i centrale datacentre, udflytning af it-løsninger til cloud-leverandører eller drift af samfundskritisk infrastruktur.

Det kan på mange måder give god mening ud fra et forretningsmæssigt synspunkt, da det kan optimere flere arbejdsgange, og virksomheden eller myndigheden kan fokusere sine ressourcer. Det kan dog også give sikkerhedsmæssige udfordringer, da man i nogle situationer reelt fralægger sig kontrollen med de outsourcede it-systemer og overlader beskyttelsen af forretningskritiske data og it-systemer til underleverandøren. Det kan også medføre, at det i forbindelse med sikkerhedshændelser bliver mere vanskeligt både teknisk og juridisk at genetablere it-systemerne og finde årsagerne til hændelsen. Eksempelvis lykkedes det i februar 2019 en hacker at slette indholdet på servere hos webmail udbyderen VFEmail. Angrebet medførte, at kundernes e-mails blev slettet og mange af dem kunne ikke gendannes, da backup-filer også var slettet. Grundlæggeren af tjenesten tweetede kort efter, at virksomheden formodentlig ikke ville overleve angrebet.

Centralisering af data og it-infrastruktur gør det muligt at kompromittere mange ofre på én gang
For den enkelte virksomhed kan outsourcing til udbydere af it-infrastruktur, datacentre og cloudløsninger bidrage til at øge virksomhedens cybersikkerhed. Det skyldes, at en markedsførende underleverandør med en stor kundebase kan investere mange ressourcer i at beskytte sin infrastruktur mod cyberangreb.

En negativ effekt af denne centralisering er dog, at et effektivt cyberangreb mod en sådan underleverandør potentielt kan berøre et stort antal myndigheder og virksomheder på samme tid, hvilket derfor kan have en stor effekt på samfundet. Tendensen til, at markedet for cloud computing i stadig højere grad domineres af færre, men større, globale udbydere, kan øge denne problematik.

Simple angrebsmetoder er stadig blandt de mest effektive
Selvom cybertruslen hele tiden udvikler sig, angriber hackere dog ofte med de samme metoder, som de har brugt i årevis. Det skyldes, at de samme angrebsmetoder stadig er effektive, da mange myndigheder og virksomheder fortsat er sårbare overfor dem.

Eksempelvis er phishing-mails fortsat en af de mest effektive måder for hackere at få uautoriseret adgang til organisationers oplysninger, netværk eller systemer. Hackere lykkes også fortsat med at

bryde eller gætte sig til simple eller genbrugte adgangskoder. Gamle sårbarheder giver også fortsat hackere adgang til myndigheders og virksomheders netværk, fordi systemer ikke bliver opdateret eller udskiftet rettidigt.

På CFCS' hjemmeside, www.cfcs.dk, ligger der vejledninger ift., hvordan disse angrebsmetoder kan imødegås. CFCS deler også løbende nyheder af relevans for imødegåelsen af cybertruslen via sine Twitterkonti.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynlighed i analyser:

Billedfortegnelse

Side 4 Fremmede stater har bl.a. interesse i at spionere mod forskning, som Danmark bruger ressourcer på at udvikle
Rode Joachim/Ritzau Scanpiz/Ritzau Scanpix

Side 10 Cyberaktivister angreb franske myndigheder og virksomheder for at støtte De Gule Veste-protesterne
Michel Spingler/AP/Ritzau Scanpix