NATURVIDENSKAB OG TEKNOLOGI DIREKTE FRA FORSKNINGSVERDENEN

AKTUEL naturVIDENSKAB

Ivan har din ryg på internettet

40 års forskning har støbt fundamentet til fremtidens cybersikkerhed.

TEMA: Det digitale samfunds usynlige vagter

Uden sikkerhed ingen internet! I dette tema ser vi på teknologierne, udfordringerne og menneskene, der hjælper med at holder det digitale samfund kørende.

Verdens truede dyr er under pres

Forskere kortlægger, hvordan truslerne mod verdens dyr fordeler sig verden over.

Nr 03 · 2026

PRIS 50 KR

OM AKTUEL NATURVIDENSKAB

ANSVARSHAVENDE
Poul Nissen, prodekan,
Faculty of Natural Sciences, Aarhus Universitet.

REDAKTION
Carsten Rabæk Kjaer, redaktør
Jørgen Dahlgaard, redaktør
Rasmus Kerrn-Jespersen, kommunikationschef
Henriette Stevnhøj, journalist
Jeppe Kyhne Knudsen, journalist

ABONNEMENTSSERVICE
Har du fået ny adresse eller ønsker du at bestille et abonnement på bladet?
Kontakt os på telefon: 3036 0662
E-mail: abo@aktuelnaturvidenskab.dk
Abonnement kan også bestilles via hjemmesiden: aktuelnaturvidenskab.dk

UDGIVER
Aarhus Universitet, Faculty of Natural Sciences og Faculty of Technical Sciences.

KONTAKT
Aktuel Naturvidenskab,
Ny Munkegade 120, Bygning 1520,
DK-8000 Aarhus C
Tlf.: 3036 0660 / 8715 2094
E-post: red@aktuelnaturvidenskab.dk

LAYOUT
Gudrun Frost-Søgaard / Jørgen Dahlgaard

TRYK
Jørn Thomsen Elbo

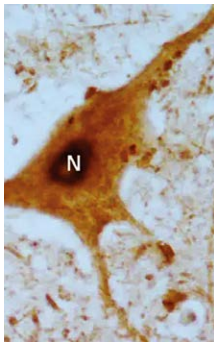
ISSN
1399-2309 (papirversionen),
1602-3544 (web)

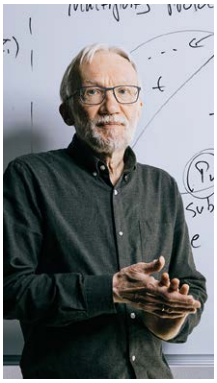
OPLAG
4.200

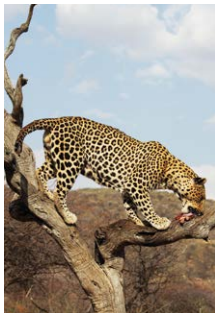
FORSIDEFOTO
Ivan Damgård, professor i datalogi ved Aarhus Universitet. Han forsker i kryptologi og datasikkerhed.
Foto: Liv Rohde, AU Foto.

AARHUS
UNIVERSITET

INDHOLD ■

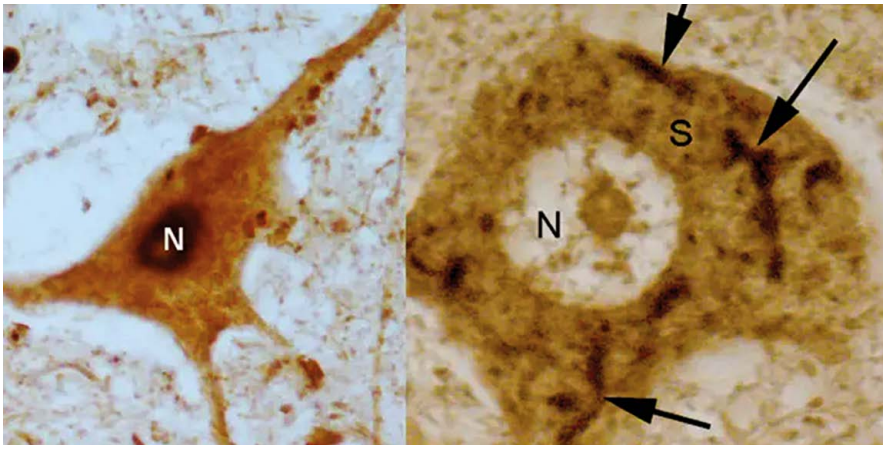






KORT NYT ■

FEJL I CELLERNES RENSESYSTEM KNYTTES TIL ALS



Billederne viser til venstre en rask motorneuron fra rygmarven, hvor proteinet TDP-43 (farvet med sort) er lokaliseret i cellekernen (N). Til højre ses en tilsvarende motorneuron fra en ALS-patient, hvor TDP-43 er unormalt ophobet i cellens cytoplasma (S). Fotos: Instituto de Neurociencias UMH CSIC

Amyotrofisk lateral sklerose (ALS) er en meget alvorlig sygdom, hvor de specialiserede nerveceller, der sender signaler til musklerne (motorneuroner) gradvist bliver nedbrudt. I de fleste tilfælde dør patienter få år efter diagnosen.

Forskere fra Instituto de Neurociencias i Spanien har i et nyt studium identificeret en mekanisme, som muligvis spiller en vigtig rolle i sygdommens udvikling: Et centralt cellulært rensesystem i nerveceller kaldet chaperone-medieret autofagi. Det er et rensesystem, der selektivt nedbryder bestemte beskadigede proteiner. Denne form for autofagi spiller en vigtig rolle for nervecellers overlevelse, fordi den fjerner specifikke potentielt giftige proteiner og medvirker til at opretholde cellernes indre balance.

Et kendetegn for sygdommen ALS er, at der i over 90 procent af tilfældene ophobes et protein kaldet TDP-43 uden for sin normale placering i motorneuronerne, hvor proteinet danner giftige aggregater. I raske mennesker kan chaperone-medieret autofagi selektivt nedbryde netop dette protein, men forskerne fandt, at aktiviteten af dette system er stærkt reduceret i motorneuroner fra ALS-patienter sammenlignet med raske kontrolpersoner.

Undersøgelsen er baseret på analyser af rygmarvsvæv fra både ALS-patienter og raske donorer. Forskerne målte niveauet af proteinet LAMP2A, som er en vigtig markør for aktiviteten af den selektive autofagi. Resultaterne viser høj aktivitet i raske motorneuroner og lav aktivitet i syge celler.

Ifølge forskerne tyder fundene på, at netop svigt i denne selektive proteinnedbrydning kan bidrage direkte til motorneuronernes død. Derfor peger studiet på chaperone-medieret autofagi som et muligt nyt mål for lægemidler, som potentielt vil kunne hæmme sygdommens udvikling.

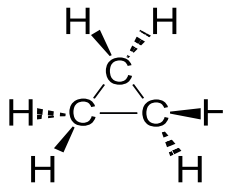
CRK, Kilde: acta neuropathol commun 14, 67 (2026)

KRAFTIGT LYS KAN NEDBRYDE PFAS

De er kendt som evighedskemikalier og udgør et stigende globalt problem for både natur og mennesker. Nu peger et nyt studie fra Aarhus Universitet imidlertid på, at PFAS kan nedbrydes ved hjælp af kraftigt lys uden brug af tilsatte kemikalier. I studiet har forskerne konkret undersøgt, hvordan meget reaktive partikler, som dannes fra vand under UV-lys – også kendt som hydrogenradikaler – spiller en afgørende rolle i nedbrydningen af PFAS. Tidligere var antagelsen, at andre reaktive partikler stod for at nedbryde de skadelige evighedskemikalier. Med den nye viden har forskerne fået et mere klart billede af de kemiske processer bag nedbrydningen, som gerne skulle bane vejen for mere effektive og kemikaliefrie løsninger til vandrensning.

Jeppe Kiel Revsbech, Kilde: AU Engineering.

KEMIKERE UDFOLDER POTENTIALET I "SPÆNDTE RINGE"



En af de mest simple former for "spændte ringe" er cyclopropan, som er vidt udbredt i kemisk syntese.

Kemikere bruger ofte såkaldte spændte ringe som udgangspunkt for at syntetisere komplekse molekyler. Spændte ringe er cirkulære molekyler, hvor vinklen mellem de kemiske bindinger er tvunget væk fra deres ideelle geometri. Det giver molekylerne en høj potentiel energi, der kan udnyttes i reaktioner. Problemet er dog, at når først den molekylære ring er åbnet, mister den normalt hurtigt sin reaktivitet.

Kinesiske kemikere har nu udviklet en ny metode, der gør det muligt at udnytte spændte molekylære ringe mere velkontrolleret og effektivt end før. Forskernes nye metode kombinerer stærke syrer og elektrokemi. Når ringen indledningsvist åbnes, danner de stærke syrer en række reaktive mellemtrin af såkaldte olefiner (også kaldet alkener), som er forbindelser, der udelukkende består af carbon og hydrogen, og hvor der er mindst én dobbeltbinding mellem to carbonatomer. Ved hjælp af elektrokemiske teknikker bringes disse mellemtrin til at afgive elektroner (de oxideres), hvilket gør det muligt gradvist at indsætte nye funktionelle kemiske grupper. I stedet for at reagere ukontrolleret på én gang, kan kemikerne styre reaktionen trin for trin, mens den foregår i samme reaktionsbeholder.

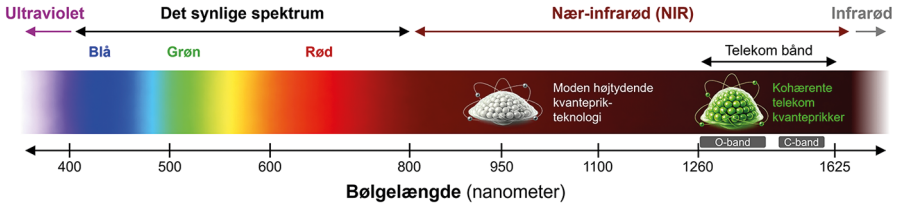
På den måde kan man ændre flere steder i det samme molekyle efter hinanden og indsætte op til fire nye funktionelle grupper meget præcist. Metoden gør det også muligt at aktivere bindinger, som normalt er svære at påvirke, uden at reaktionen løber løbsk.

Resultatet er komplekse og alsidige molekyler, som kan bruges som byggesten i blandt andet lægemiddeludvikling. Forskerne har blandt andet fremstillet forbindelser, der ellers er meget vanskelige at lave med traditionelle metoder.

Arbejdet viser, hvordan elektrokemi kan give kemikere langt større kontrol over kemiske reaktioner og peger på en ny tilgang til at opbygge komplekse molekyler mere effektivt og målrettet.

CRK, Kilde: Chemistry World/Y Li et al, Nat. Chem., 2026, 18, 656

FORSKERE FJERNER BARRIERE FOR KVANTEINTERNET



Kvanteprikker er små nanostrukturer, der består af nogle tusinder atomer. De fungerer i sig selv som kunstige atomer, som kan exciteres – dvs. når kvanteprikken rammes af laserlys kan en elektron løftes til et højere energiniveau, hvorefter den kort tid efter henfalder og udsender præcis én lyspartikel (foton). Netop denne egenskab gør kvanteprikker ideelle som sikre lyskilder til kvantekommunikation, da information lagret i en enkelt foton ikke kan kopieres.

En ulempe har dog hidtil været, at de bedste kvanteprikker kun fungerer ved bølgelængder omkring 930 nanometer. Og det er langt fra de bølgelængder i det såkaldte telekom-bånd fra omkring 1300 nanometer, som almindelig telekommunikation fungerer ved. Hidtidige forsøg på at arbejde med kvanteprikker i telekom-båndet har givet fotoner med for meget "støj". Hvis fotonerne skal bruges til kvantekommunikation, skal man nemlig kunne generere flere fotoner efter hinanden med nøjagtig de samme egenskaber – man siger, at fotonerne skal være kohærente.

I en afhandling i tidsskriftet *Nature Nanotechnology* rapporterer forskere fra Niels Bohr Instituttet i samarbejde med internationale kolleger nu, at det er lykkedes dem at fremstille kvanteprikker, som kan udsende fotoner, der både er næsten fuldstændigt ens og ligger i det rette bølgelængdeområde omkring 1300 nanometer, der anvendes i eksisterende fibernet.

Dette resultat fjerner reelt en af de største forhindringer for at bygge storskala kvantenetværk. Det åbner således for, at kvanteteknologi i form af kvantechips, kvante-forlængere og langdistance kvantekommunikation vil kunne bygges ind i verdens eksisterende fiberinfrastruktur uden komplicerede omveje.

CRK, Kilder: Niels Bohr Instituttet/ Nature Nanotechnology

VULKAN FJERNER SELV METAN FRA LUFTEN

Et voldsomt vulkanudbrud i det sydlige Stillehavet har afsløret en unik naturlig mekanisme, som muligvis kan hjælpe med at bremse den globale opvarmning. Takket være avancerede satellitmålinger har en international forskergruppe kortlagt, hvordan den undersøiske vulkan Hunga Tonga-Hunga Ha'apai ryddede op efter sig selv, da den gik i udbrud i januar 2022 og forårsagede massive metan-forureninger.

Studiet, som er publiceret i *Nature Communications,* viser konkret, at den enorme støvsky, der opstod i kølvandet på udbruddet, indeholdt store koncentrationer af formaldehyd, og det er ifølge forskerne et afgørende bevis: For når metan bliver nedbrudt i atmosfæren, dannes der formaldehyd som et kortvarigt mellemprodukt. Opdagelsen giver helt ny viden om atmosfærisk kemi, der kan inspirere udviklingen af nye metoder til at fjerne metan fra atmosfæren, fastslår studiet.

Jeppe Kiel Revsbech, Kilder: KU/Nature Communications.

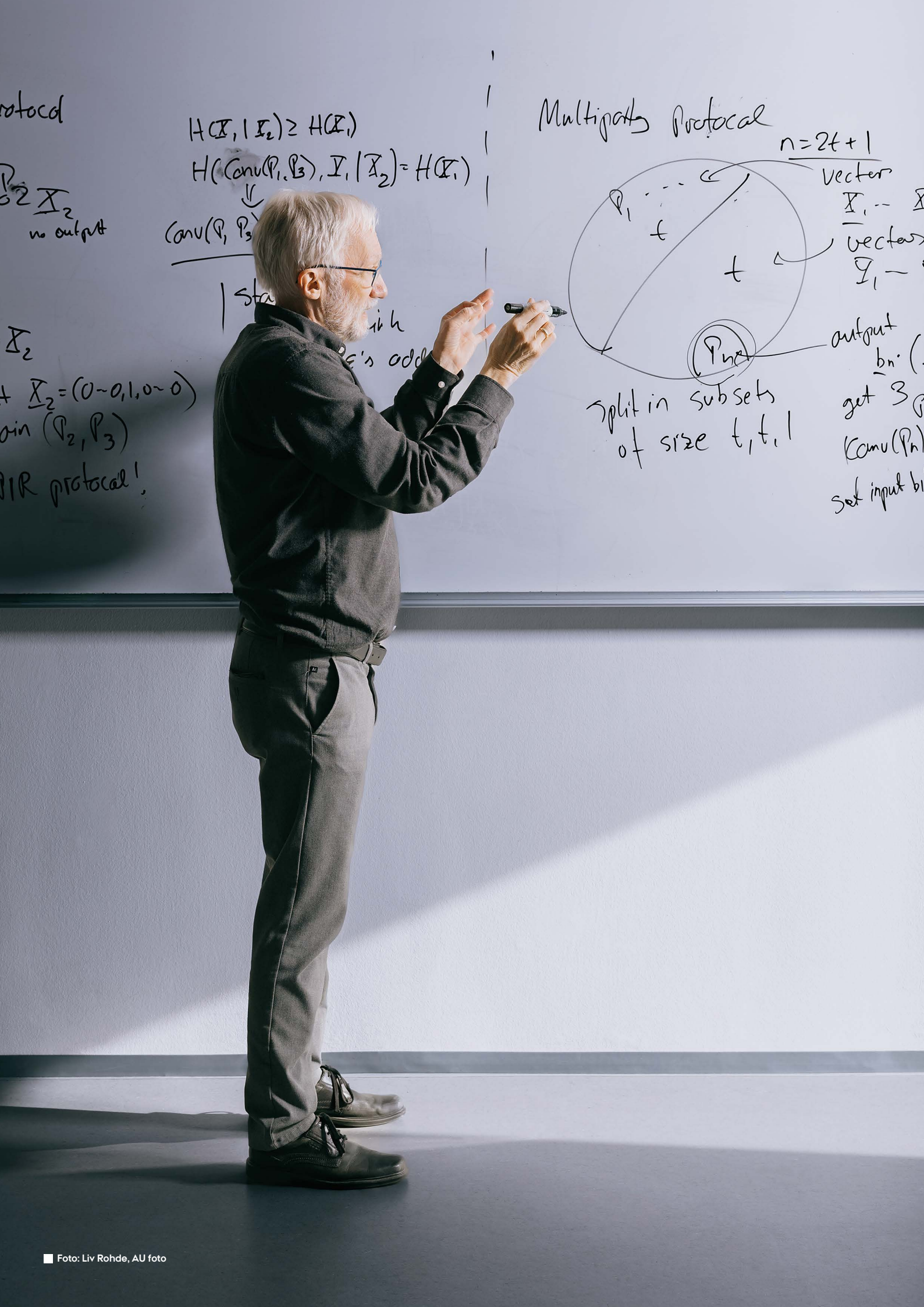
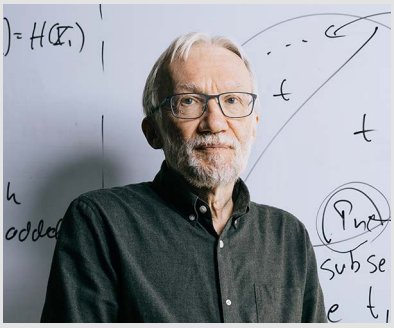


Foto: Liv Rohde, AU foto

Cybersikkerhed: Internettets fundament

Kunsten at sørge for, at kun de rette personer har adgang til den rette delmængde information, er en forudsætning for, at vi kan have et internet. Og dette fundament under internettet har professor Ivan Damgaard beskæftiget sig med hele sin karriere.

■ Carsten R. Kjaer, Aktuel Naturvidenskab.



OM IVAN DAMGAARD

Ivan Damgård er professor i datalogi ved Aarhus Universitet. Han forsker i kryptologi og datasikkerhed og den matematik der ligger bag. Et centralt emne i Ivans forskning er såkaldt multiparty computation – en teknologi der blandt andet kan sikre, at personlige data kun anvendes til de formål som ejeren har godkendt – uden at man behøver at stole på alle de aktører, der indgår.

Ivan er desuden medstifter af virksomhederne Cryptomathic, Partisia og Sepior.

ivan@cs.au.dk

Hvad tænker du, hvis jeg siger "cybersikkerhed"? Du vil måske umiddelbart tænke på hackere. Og deraf følger intuitivt, at forskning i cybersikkerhed må gå ud på, hvordan vi som individer og samfund beskytter os mod "onde" mennesker (eller måske stater), der vil bryde ind i vores computersystemer for at stjæle følsomme data eller overtage kontrollen med computeren. Når Ivan Damgaard på Computer Science i Aarhus tænker på cybersikkerhed, tænker han egentlig ikke så meget på hackere. For ham handler cybersikkerhed om noget mere grundlæggende – nemlig om den sikkerhed, der er nødvendig for, at vi kan have et internet og et digitalt samfund. For langt, langt de fleste af dem, vi skal "beskytte" os mod, er nemlig ikke hackere, men venner og bekendte, bankfolk, internetbutikker, forretningsforbindelser, ansatte i den offentlige forvaltning mv. – ja simpelthen "alle de andre", som vi ikke har lyst til at dele alle vores hemmeligheder med.

»Set i det helt store historiske perspektiv var kryptering oprindelig noget, der primært havde med militæret at gøre. Her var der en fjende, man ikke måtte afsløre hemmeligheder for, og dem, man kommunikerede med, var ens eget "hold", som man stolede på. I dag er verden meget mere kompliceret. Her kommunikerer vi på et internet, hvor alle i princippet kan læse med, hvis ikke vores data er krypterede. Og dem, vi kommunikerer med, deler vi ikke nødvendigvis interesser med. Derfor må vi sikre os, at vi altid kun giver modtagerne netop de informationer, vi ønsker at give dem«, forklarer Ivan Damgaard.

Cybersikkerhed handler om mange ting

Ivan Damgaard er professor i datalogi ved Aarhus Universitet, og han har siden 1980'erne forsket i kryptologi og datasikkerhed og den matematik, der ligger bag. Han er derfor en oplagt guide til at tage os med ind i det maskinrum, hvor fundamentet til nutidens og fremtidens teknikker til at håndtere cybersikkerhed bliver støbt.

Ivan Damgaards hjemmebane indenfor det brogede felt, vi overordnet kalder cybersikkerhed, er kryptologien. Det kan kort defineres som videnskaben om at hemmeligholde og autentificere information. Og det foregår grundlæggende ved at kode information ved hjælp af matematiske procedurer. Det sikrer, at kun den rigtige modtager kan læse informationen, og at ingen kan manipulere med den uden at blive opdaget. Kryptologi udgør derfor en hjørnesten i alt, hvad der har med cybersikkerhed at gøre.

Men cybersikkerhed handler ikke kun om kryptologi.

»Der er for eksempel også en meget praktisk orienteret del af feltet, der handler om, hvordan man sætter systemer op, så de er sikre mod indbrud. Men også sikre mod, at brugerne af et system, der burde være sikkert, tager forkerte beslutninger. Det, vi kalder "human-computer-interaction", forbinder vi normalt ikke med cybersikkerhed, men det bør vi gøre, for mennesker er ofte det svage led i kæden«, fortæller Ivan Damgaard.

Han illustrerer den pointe med, at da vi gik over til MitID i stedet for NemID, skete der et skift i, hvordan folk prøvede at svindle.

»Man gik over til at forsøge at snyde mennesker til at overføre penge. Simpelthen fordi MitID er svært at bryde. Hvis det nemmeste er at snyde mennesket – så er det det, man går efter«, siger Ivan Damgaard.

Er computeren sårbar, når den regner?

Hvis vi vender os mod Ivans eget felt, kryptologien, er det efter hans egne ord der, "hvor man laver værktøjerne". Behovet for krypte-

ring er som nævnt blevet så stort, fordi internettet fungerer, som det gør. Nettet består af en hulens masse computere, og de folk, der sidder bag dem, er alle mulige mennesker med mere eller mindre rent mel i posen. Hvis vi bare sendte vores data ud på nettet, uden at gøre noget ved dem, ville alle kunne se dem – og manipulere med dem.

»Man kan sige, at det, vi laver, er noget, som i første omgang skal lukke alle de store huller – altså så man ikke bare kan sidde derhjemme og høste alle mulige data«, siger Ivan Damgaard. »Den næste bekymring er så hackere. Og hackere findes jo kun fordi, der "nedenunder" nettet findes en hel masse kryptering, der får det til at fungere.«

Som eksempel på, hvad kryptologiske værktøjer skal kunne, nævner Ivan Damgaard, at data også skal være sikre, mens man regner på dem.

»De fleste vil nok tænke, at når en computer regner på nogle data, må disse data også være tilgængelige i computeren, mens den regner. Og så må man jo kunne få fat i de data, hvis man bryder ind i computeren, mens den regner på data. Men det kan vi godt sikre os imod« siger Ivan Damgaard.

Umiddelbart er der to forskellige metoder, man kan anvende. Den ene er, at computeren slet ikke "pakker data ud", når den regner på dem. Man regner altså på krypterede data, og man får dermed også et krypteret resultat, som først åbnes senere. Hvis nogen bryder ind og stjæler data i processen, vil de altså stadig være krypterede. Ivan Damgaard sammenligner metoden med en lukket kasse, hvor man gennem nogle handsker i kassen kan stikke hænderne ind og gøre forskellige ting ved det, der er i kassen – for eksempel trykke på nogle knapper inde i kassen – men selve genstanden i kassen kan man ikke se.

Når computere deler beregninger

Den anden metode kan illustreres med et eksempel. Hvis et flyselskab gerne vil vide, om der findes personer på deres passagerlister, der er terrormistænkte, vil efterretningstjenesten jo ligge inde med en liste over personer, der netop er terrormistænkte. Men hverken flyselskabet eller efterretningstjenesten vil bare udlevere deres respektive lister til den anden part. Så der er brug for en metode, der kan lave en fælles udregning på de samlede data, der kan fortælle, om der er en eller flere personer,

Foto: Colourbox

SUKKERROER SATTE GANG I MULTIPARTY COMPUTATION

Da Ivan Damgaard og kolleger i 1980'erne udviklede princippet i at regne på delmængder af fælles data på tværs af mange computere – multiparty computation – var det ren grundforskning. Her fandt de blandt andet også matematiske svar på, hvor mange indbrud, man maksimalt kan tåle, for at systemet stadig er sikkert.

Først i løbet af nullerne begyndte man for alvor at interesse sig for mulige praktiske anvendelser. Og i 2008 så den første industrielle anvendelse dagens lys – og det var i Danmark.

Baggrunden var behovet for en handelsplads, hvor man kunne købe og sælge kontrakter, som gav en landmand lov til at producere et bestemt antal tons sukkerroer med støtte fra EU. I 2006 var der en reform af EU-støtten til sukkerproduktion, hvilket reducerede støtten, og derfor opstod der et behov for i en fart at få flyttet produktionen hen til områder, hvor det bedre kunne betale sig at dyrke sukkerroer (støtten havde i udgangspunktet været så stor, at det kunne betale sig næsten overalt). Når man skulle handle på denne handelsplads, var det vigtigt, at det beløb, man ønskede at købe eller sælge for, forblev privat information. Opgaven var altså at finde ud af, hvem der skulle handle med hvem, uden at buddene blev afsløret for andre.

Det lykkedes ved hjælp af multiparty computation, og det var det første eksempel i virkelighedens verden på brug af denne teknik. Og det gav mange andre blod på tanden. Det udmøntede sig også i spin off firmaet Particia, som stadig findes i dag.

Der er siden sket en kæmpemæssig udvikling i hastigheden af disse løsninger, og mange virksomheder arbejder med udvikling af metoderne. For eksempel har industrigiganten Bosch en forskningsafdeling, der arbejder med det i forhold til forsyningskæder – altså hvordan man flytter varer rundt, uden at alle, der er med i kæden, skal offentliggøre deres forretningsstrategier. ■

Tegning: Susanne Rauff Møller

KAN MAN LYTTE SIG TIL DATA?

Hvis man vil stjæle data fra en computer, skal man bryde ind i den. Men er det nu også nødvendigt? Faktisk er det et af de spørgsmål, man bliver nødt til at overveje inden for cybersikkerhedsforskningen. For det kan jo være, at man ved at måle på computeren udefra – for eksempel på lyden eller på strålingen fra den, når den regner på data – kan afsløre noget om de data, den regner på. Der findes ifølge Ivan Damgaard eksempler på eksotiske angreb, hvor man netop har forsøgt at laver den slags målinger på computere. Derfor er der også brug for teknikker til at beskytte os mod det. Det kan for eksempel være at sørge for, at computeren bruger lige lang tid på at regne på data, uanset hvad den regner på. ■

	Per	Ulla	Hans	Signe	Løn	Gennemsnit:
Per	10000	2000	20000	18000	50000	
Ulla	3000	-5000	33000	24000	55000	
Hans	11500	9000	13000	15500	49000	
Signe	6000	-33000	48000	31000	52000	
Sum	30500	-27000	11400	88500	20600	51500

HEMMELIGE BEREGNINGER I FÆLLESSKAB

Hvordan kan flere personer være fælles om en udregning uden at afsløre information for hinanden? Lad os sige, at medarbejderne i en afdeling i en virksomhed gerne vil vide, hvad gennemsnitslønnen er i afdelingen, men de har ikke lyst til at afsløre, hvad netop de selv får i løn. Skemaet viser et eksempel med fire medarbejdere. Tricket er, at hver enkelt medarbejder deler sin egen løn op i et antal tilfældige tal (svarende til antallet af medarbejdere – her fire), der tilsammen summerer op til ens faktiske løn. Det ene tal beholder man selv (markeret med rødt i tabellen), mens man sender et af de andre tal til hver af de andre tre personer. Derefter lægger hver enkelt person de fire tal sammen, som de nu sidder med, og sender resultatet til alle de andre. Det smarte er nu, at hvis man lægger de fire beregningsresultater sammen, giver det den samlede løn i afdelingen (grøn) – og så skal man bare dividere med fire for at få gennemsnitslønnen. ■

der står på begge lister. Uden at afsløre andet end det. Princippet bag, at en beregning kan udføres på flere computere, som hver især kun har adgang til en delmængde af data – kaldet multiparty computation – udviklede Ivan Damgaard og hans kolleger allerede tilbage i 1980'erne.

»Dengang var det ren grundforskning,« siger Ivan Damgaard. »Vi var bare nysgerrige på, om det overhovedet kunne lade sig gøre. Ingen troede dengang på, at det ville komme ud og blive anvendt i praksis. Det var alt for langsomt og teoretisk. Men i 2008 var vi faktisk med til at udvikle verdens første løsning, hvor metoden blev brugt i praksis – nemlig til at handle sukkerroe-kontrakter i Danmark.« (se faktaboks).

I dag er værktøjer til multiparty computation vidt udbredte. For eksempel har Google en tjeneste, hvor de samler data ind fra mistænkelige steder, hvor huggede passwords er til salg på nettet. Google har derfor en stor database med lækkede passwords og en tjeneste, hvor man selv kan tjekke, om nogle af ens passwords findes på den liste. Vel at mærke uden at du skal sende alle dine passwords til Google.

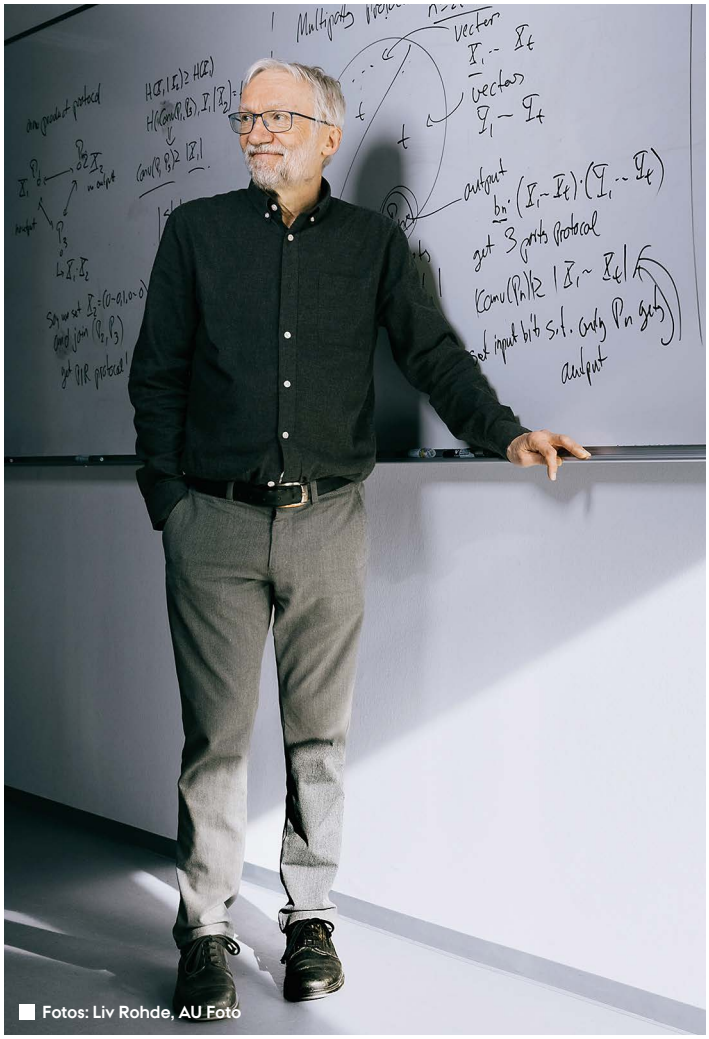
»Teknikken har selvfølgelig en pris: Sådanne beregninger kan ikke foregå lige så hurtigt, som hvis alle data var samlet i én computer. Det betyder i praksis, at vi ikke kan regne på "big data" på denne måde – men mellemstørrelse kan vi,« siger Ivan Damgaard.

Der foregår derfor også stadig udvikling indenfor feltet, der går ud på at kunne udføre den type beregninger hurtigere og mere effektivt.

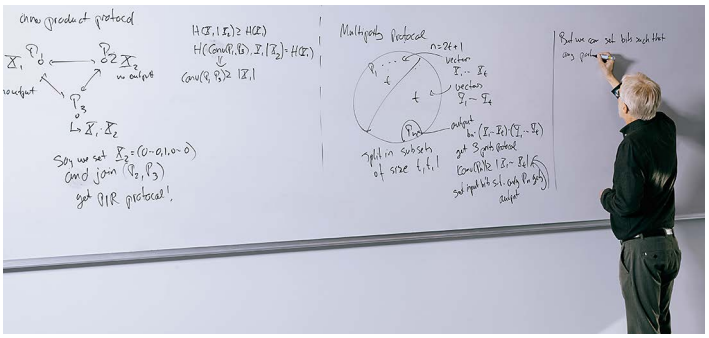
Truslen fra kvantecomputeren

Et af de store områder indenfor forskningen i cybersikkerhed handler om den potentielle trussel fra kvantecomputere. Kryptering er traditionelt bygget på en type matematisk bevis, som er meget vanskelig for en almindelig computer at løse, nemlig såkaldt faktorisering. Det tager udgangspunkt i, at det er meget vanskeligt at regne ud, hvilke to primtal, der ganget med hinanden giver et bestemt tal – for eksempel at tallet 8051 fremkommer ved at gange 83 med 97 (til gengæld er det meget nemt at kontrollere, at 83 ganget med 97 netop giver 8051). Jo større tal, jo sværere er det.

Problemet er nu, at en kvantecomputer i princippet er rigtig god til at regne lige præ-



Fotos: Liv Rohde, AU Foto



»For det mest grundlæggende – det der skal til, for at internettet kan fortsætte sine daglige funktioner – er løsningerne stort set på plads«.

cis den type matematiske problemer ud. Hvis det lykkes at udvikle kraftfulde kvantecomputere, vil utallige systemer verden over derfor være i fare for at blive hacket.

For at imødegå denne trussel, bliver vi derfor nødt til at bygge kryptering på beregningsproblemer, der er vanskelige at løse for en kvantecomputer — og som kan køre på helt almindelige computere. Sådanne krypteringsteknikker findes allerede.

»I princippet er denne overgang til "post quantum computing" en 1:1-udskiftning«, siger Ivan Damgaard. »I forskningsmiljøet er der allerede udviklet flere sæt af værktøjer, som er på vej ud i praktisk brug. For eksempel har et team i min egen forskningsgruppe foreslået en ny kvantesikker digital signatur, der lige nu evalueres af den amerikanske standardiseringsmyndighed NIST. Får den grønt lys dér, ender den næsten med garanti som industristandard — og dermed i alt fra offentlige systemer til private virksomheder verden over.«

Et gigantisk opgraderingsprojekt

Selvom teknologien findes, er det langt fra ligetil at få hele internettet over på kvantesikre løsninger. Der er utallige systemer, enheder og protokoller, som skal opdateres — både hardware og software.

Et eksempel er internetprotokollen TLS, som sikrer, at man kan browse sikker på nettet – den er aktiv, når du ser et lille hængelås-symbol i adresselinjen i din browser. Hvis en server bruger den nyeste version af denne protokol, er de kvantesikre algoritmer faktisk allerede indbygget. Browserne Chrome, Firefox og mange andre bruger den automatisk — hvis serveren i den anden ende altså understøtter det.

Problemet er bare, at der er et enormt efterslæb. Mange systemer ude i verden er ikke blevet opdateret endnu, og det kan tage år at få dem alle med.

»For det mest grundlæggende — det der skal til, for at internettet kan fortsætte sine daglige funktioner — er løsningerne stort set på plads. Standarder er på vej, og mange er begyndt at implementere dem. Men for de mere avancerede funktioner er der stadig store udfordringer,« siger Ivan Damgaard.

Han forklarer, at det for eksempel gælder mange af de små enheder, hvor softwaren er indbygget i hardwaren, og som for eksempel indgår i det, vi kalder "internet of things" (IoT). Udfordringen er her, at de nye kvantesikre algoritmer typisk fylder langt mere end de gamle, og så er der simpelthen ikke plads til at skifte dem ud. Det kommer til at give hardwareproducenterne designproblemer – medmindre forskere kan gøre algoritmerne meget mere kompakte, eller måske finde helt andre løsninger.

En stor forskningsopgave venter

»En anden udfordring er de systemer, hvor en hemmelig nøgle er fordelt mellem flere enheder – som telefon, computer og server. Det gør man for at undgå, at man kan hacke et system ved at bryde ind et enkelt sted. I dag fungerer løsninger på den slags kryptering elegant i klassiske systemer, men i kvantesikre algoritmer kan den samme proces ikke udføres lige så smidigt. Der er derfor behov for helt nye metoder,« siger Ivan Damgaard.

Endelig nævner han også systemer, der bygger på såkaldte zero-knowledge-beviser (det er også den type bevis, der ligger bag eksemplet med flyselskabet og terrormistænkte ovenfor). Det er teknologi designet til, at man kun afslører netop den delmængde af en større mængde information, som man ønsker. Det er i øvrigt også en teknik, der er vidt anvendt i hele block chain-sektoren (som jo blandt andet anvendes til kryptovaluta).

I øjeblikket arbejder EU på en fælles digital identitet – en såkaldt EU-wallet. Den skal EU-borgerne kunne bruge til at bevise ting om sig selv – for eksempel, at de er over 18 år og borgere i et EU-land – uden at afsløre mere end nødvendigt. Men også i den type systemer gælder det, at traditionelle algoritmer kører meget effektivt, mens de kvantesikre versioner bliver langt tungere. Der forestår derfor en stor forskningsopgave i at gøre dem brugbare i praksis.

Vi skal i gang nu!

I virkeligheden er der ingen der ved, hvornår – eller om der nogensinde – bliver udviklet en fungerende kvantecomputer, der vil kunne bryde de eksisterende krypteringsalgoritmer.
Men som Ivan Damgaard forklarer det, bliver vi nødt til at forberede os på det.

»Spørgsmålet er, hvordan vi forholder os til en sandsynlighed på for eksempel 10 % for, at der findes en kvantecomputer, der kan bryde vores nuværende kryptering i midten af 2030'erne. Den sandsynlighed kan lyde lav, men konsekvensen vil jo være en form for digital kollaps til den tid, hvis ikke vi har gjort noget i mellemtiden. Og det vil tage mindst ti år at gøre vores systemer kvantesikre, så derfor skal vi i gang nu.« ■

Jens Myrup Pedersen (th.) er professor i cybersikkerhed ved Aarhus Universitet og landstræner for det danske cyberlandshold. Han forsker i blandt andet netværkssikkerhed og udvikler cyber-øvelser, der træner unge talenter i at tænke kreativt og finde sårbarheder i digitale systemer. Foto: Mads Nielsen.

Et digitalt escape room: Sådan lærer unge at hacke

På det danske cyberlandshold træner unge talenter i at bryde ind i systemer, finde skjulte sårbarheder og tænke som hackere. Det kan ligne et ondsindet spil, men i virkeligheden handler det om at beskytte et af verdens mest digitaliserede samfund.

Jesper Bruun · journalist, AU Engineering, Aarhus Universitet

JENS MYRUP PEDERSEN

Jens Myrup Pedersen er professor i cybersikkerhed ved Aarhus Universitet og landstræner for det danske cyberlandshold. Han er uddannet cand.scient. i matematik og datalogi fra Aalborg Universitet og har en ph.d. i computernetværk.

Hans forskning fokuserer blandt andet på netværkssikkerhed og på, hvordan man kan opdage og håndtere sårbarheder i komplekse digitale systemer. Derudover arbejder han med at udvikle realistiske cyberøvelser og konkurrencer, som træner evnen til at tænke kreativt og finde fejl i systemer. Som landstræner er han med til at udvikle unge talenter og styrke Danmarks kompetencer inden for cybersikkerhed.

jensmyrup@ece.au.dk

En profil på et socialt medie. Et billede af en burger. Et navn: Mr. Beef.
Umiddelbart ligner det bare endnu en bruger på endnu en platform, der poster alt lige fra jokes til memes og madopskrifter til mere eller mindre privat indhold.
Men noget stemmer ikke helt.
Måske har brugeren brugt det samme password flere steder? Måske afslører opslaget lidt for meget? Måske ligger svaret gemt i små detaljer, som kun den opmærksomme opdager?
Opgaven lyder enkel: Find ud af, hvem Mr. Beef er i virkeligheden. Men vejen dertil er alt andet end simpel.
Velkommen til træning i cybersikkerhed.

At tænke som en hacker

Rundt omkring ved computere sidder unge mennesker og leder efter spor. De klikker, analyserer, tænker sig om, tester og kombinerer informationer. Ikke for at bryde loven, men for at forstå, hvordan systemer kan brydes.

For Jens Myrup Pedersen, professor ved Aarhus Universitet og landsholdstræner for cyberlandsholdet, er det netop den måde at arbejde på, der gør cybersikkerhed fascinerende. Hvor man prøver forskellige veje og tænker kreativt for at finde løsninger.

»Hvad nu hvis man gør ting på en anden eller tredje eller fjerde måde? Eller i en rækkefølge, som ingen har prøvet før? Hacking er ikke bare en teknisk disciplin, men først og fremmest en kreativ disciplin. Det handler om, at man prøver noget af, som der ikke er nogen, der har tænkt på før,« siger han.

Cyberlandsholdet består af 10 unge i alderen 15 til 25 år, som udvælges gennem konkurrencer og træningsforløb. De repræsenterer Danmark ved internationale mesterskaber og træner gennem realistiske cyberopgaver.

De opgaver, landsholdet arbejder med, er dog væsentligt mere avancerede end de eksempler, man umiddelbart kan gennemskue. Her kræver det ofte, at man kombinerer flere teknikker, arbejder på tværs af systemer og holder overblik over komplekse sammenhænge.

»Grunden til, at vi har landsholdet, er også at give synlighed til cybersikkerhed og vise, at det er et spændende område for unge mennesker,« siger Jens Myrup Pedersen.

Sådan bliver en cyberopgave til

En god opgave starter ikke med kode. Den starter med en idé.

»Den gode opgave begynder tit ved et whiteboard, hvor der er en original idé og en god historie bag,« forklarer Jens Myrup Pedersen. Historien er afgørende. For hvis opgaven føles som et univers, bliver den også mere engagerende at løse.

»Vi laver opgaver, som man har lyst til at gå på opdagelse i. Det skal ikke bare være teknisk, men en oplevelse,« siger han.

Det kan være et socialt medie, en webshop eller et digitalt system. Men de er ikke bygget korrekt:

»Vi bygger faktisk sårbarhederne ind i den hjemmeside eller de systemer, man bruger til konkurrencen. Deltagerne skal så finde sårbarhederne og udnytte dem,« siger Jens Myrup Pedersen.

I de svære opgaver skal flere ting gå op på én gang.

»Hvis det skal være svært, skal der gerne være flere brikker, der skal falde på plads på samme tid, hvor man skal udnytte flere redskaber og sårbarheder på samme tid,« forklarer han.

Det er også her, forskellen for alvor viser sig: Hvor begynderniveauet kan handle om at finde enkelte spor, arbejder landsholdet med opgaver, hvor mange lag af systemer spiller sammen, og hvor løsningen kræver både erfaring, kreativitet og vedholdenhed. Det er kun de allerdygtigste, der når til det niveau.

Hvem er Mr. Beef?
Tilbage til opgaven med at finde ud af, hvem Mr. Beef er:

Her har nogle af folkene bag De Danske Cybermesterskaber bygget et helt netværk af brugere, opslag og relationer. Det ligner en rigtig platform, men er i virkeligheden en nøje konstrueret opgave.

Mr. Beef er én af brugerne. Han poster billeder. Kommenterer. Liker opslag. Ved første øjekast er det ligegyldigt. Men for en hacker er det spor. Et opslag kan afsløre en vane. Et like kan afsløre en interesse. Et billede kan afsløre noget i baggrunden.

»Det kan være, at en bruger poster et billede, hvor man kan ane en post-it med brugernavn og password,« siger professoren.

Et andet spor kan være mere subtilt.

»Man kan måske gennemskue sammensatte spor og i sidste ende gennemskue password til en af brugerne, fordi vedkommende liker en post, hvor der står, at man kan lave passwords efter navnet på ens kæledyr og fødselsår eller sådan noget lignende,« forklarer han.

Så begynder arbejdet. Man finder kæledyrets navn. Man finder fødselsåret. Man tester kombinationer. Langsomt samler billedet sig.

»Ved at lægge de informationer sammen kan man så bruge det til at finde frem til ting, der gør, at man kan komme ind i systemet. Lige som et escape-room med små spor, der samlet giver en opgave, der gør, at man føler, at man kommer tættere og tættere på.« Opgaverne er ikke tilfældige. De afspejler virkeligheden.

»Vi træner ikke folk i at være ondsindede hackere, men noget af det, vi træner folk i, er at lære sårbarhederne at kende, så man ikke laver dem i de systemer, man selv laver, og at finde sårbarhederne hurtigt, så man kan lukke dem, før ondsindede hackere finder dem,« siger Jens Myrup Pedersen.

Den type fejl findes overalt: Genbrugte passwords. For mange oplysninger på sociale medier. Systemer, der ikke er tænkt sikkert fra starten. Det er ikke avancerede hacks. Det er blot menneskelige utilsigtede fejl.

Eksemplet med Mr. Beef er en forsimplet version af den type opgaver, deltagerne møder. I virkeligheden er opgaverne på cyberlandsholdets niveau langt mere komplekse og kræver, at man kombinerer flere forskellige sårbarheder, arbejder på tværs af systemer og ofte løser flere trin i den rigtige rækkefølge for overhovedet at komme videre.

Når 400 unge hacker hinanden
Cybersikkerhed har ry for at være svært og snævert. Det forsøger cyberlandsholdet at ændre.

»Vi vil gerne gøre det endnu mere tilgængeligt for alle, også dem, der kun har en halv time af en arbejdsdag på en måned, de kan dedikere til cybersikkerhed,« siger Jens Myrup Pedersen og fortsætter:

»Vi vil gerne tale til alle og ikke kun de allermest nørdede drenge, så vi kan få mere diversitet ind.« Derfor handler opgaverne også om for eksempel sociale medier, data og privatliv.

»Hvis man åbner det op og inddrager data og måden, man bruger sociale medier på, og beskyttelse af privatliv, så er der pludselig en meget større gruppe, som synes, det er spændende. Cybersikkerhed er super vigtigt for hele samfundet,« forklarer han.

Ved de europæiske mesterskaber skifter tempoet.

»Når vi holder de europæiske mesterskaber, er der både opgaver og attack-defence dage, hvor 400 unge mennesker sidder og hacker hinanden på kryds og tværs. Det er mega fedt,« siger professoren.

Her arbejder holdene både med at angribe og forsvare. De skal beskytte deres egne systemer og samtidig forsøge at bryde ind hos de andre. Cybersikkerhed i praksis.

AI: En ny med- og modspiller
Tilbage til Mr. Beef. Forestil dig nu, at du ikke selv behøvede finde sporene. Forestil dig, at du kunne få en kunstig intelligens til at gøre det for dig. Den kunne analysere opslag. Finde mønstre i adfærd. Gætte sandsynlige passwords. Alt sammen på få sekunder. Det er ikke science fiction. Det er virkeligheden i dag. I løbet af få år har kunstig intelligens ændret cybersikkerhed markant.

»AI betyder rigtig meget i den her verden. Det ændrer både angrebet og forsvaret,« siger Jens Myrup Pedersen.

Hvor phishing-mails tidligere ofte var lette at gennemskue med dårligt sprog og generiske formuleringer, kan AI i dag eksempelvis skrive beskeder, der er sprogligt korrekte og tilpasset den enkelte modtager.

Med dens hjælp kan en angriber for eksempel analysere dine sociale medier og lave målrettede angreb og skrive personlige phishing-mails. Og AI kan efterligne stemmer eller personer eller teste tusindvis af password-kombinationer intelligent.

»Det kan for eksempel være i phishing-angreb, hvor AI'en kan være rigtig stærk til at skrive gode phishing-mails, der er målrettet enkelte personer, så det fremstår meget troværdigt,« siger professoren.

Det, der tidligere krævede tid og ekspertise, kan nu udføres hurtigere og med færre ressourcer. Én person kan potentielt ramme tusindvis af mål med skræddersyede angreb. Det gør angreb hurtigere, billigere og mere præcise. Og ved at analysere store mængder kode eller netværkstrafik kan algoritmer

Jens Myrup Pedersen sammen med det danske cyberlandshold i 2025. Landsholdet består af unge talenter fra hele landet, som trænes i at finde og forstå sårbarheder i digitale systemer og repræsenterer Danmark ved de europæiske cybermesterskaber. Foto: Lasse Møller Badstuen

■

FAKTA OM CYBERLANDSHOLDET

Det danske cyberlandshold består af 10 unge i alderen 15 til 25 år, som udvælges gennem konkurrencer og træningsforløb. De trænes i at finde og udnytte sårbarheder i digitale systemer med det formål at lære, hvordan man opdager og forebygger cyberangreb.

Landsholdet repræsenterer Danmark ved de europæiske cybermesterskaber, European Cybersecurity Challenge (ECSC), hvor unge fra hele Europa konkurrerer i cybersikkerhed. Her arbejder deltagerne både med at analysere sårbare systemer og med at angribe og forsvare digitale infrastrukturer i realistiske scenarier.

Formålet er både at udvikle de bedste talenter og at skabe interesse for cybersikkerhed i en tid, hvor behovet for kompetencer er kraftigt stigende. Cyberlandsholdet er finansieret af Industriens Fond.

identificere svage punkter langt hurtigere end et menneske.

»Efter min vurdering har det gjort det klart lettere for angriberne,« siger Jens Myrup Pedersen. Samtidig bliver forsvaret sværere.

»Det hænger sammen med, at cybersikkerhed er en asymmetrisk konkurrence, hvor vi på forsvarssiden skal vinde hver gang. Bare angriberne kommer igennem én gang, har de vundet. Det forsvar, vi laver, skal virke hver gang,« forklarer han.

AI forstærker den ubalance.

Derfor er det vigtigt

Cybersikkerhed er blevet en forudsætning for samfundet, og behovet for mennesker, der forstår det, vokser.

»Der er rigtig meget brug for talenter,« siger Jens Myrup Pedersen. Men det kræver, at flere får lyst til at engagere sig.

»Hvis vi ikke har de der elementer med gamification og rewards og escaperoom, så er der mange, der allerede fra starten siger: "Nej det er for svært, det kan jeg ikke finde ud af", så det kan virkelig noget,« forklarer han.

Når det bliver en oplevelse, ændrer det noget. Når deltagerne forsøger at afsløre Mr. Beef – eller langt mere komplekse opgaver på landsholdsniveau – handler det ikke kun om at løse en opgave.

De lærer at tænke. At stille spørgsmål. At se mønstre. At være nysgerrige. Og vigtigst af alt: At digitale systemer aldrig er perfekte. Det er den erkendelse, der gør dem i stand til at bygge bedre løsninger.

Cyberlandsholdet fungerer samtidig som en form for talentudvikling på et område, hvor behovet for kompetencer vokser, og hvor samfundet i stigende grad er afhængigt af, at flere kan forstå og arbejde med cybersikkerhed. For i sidste ende handler det ikke om at hacke. Det handler om at forstå og beskytte. ■

»Det føles lidt som at være spion« Luccas jagter en plads på cyberlandsholdet

Luccas Sukul har arbejdet med cybersikkerhed siden folkeskolen og har flere gange været tæt på at komme med på det danske cyberlandshold. Nu gør han endnu et forsøg, drevet af nysgerrighed, konkurrence og lysten til at blive bedre.

Jesper Bruun · journalist, AU Engineering, Aarhus Universitet

LUCCAS CONSTANTIN-SUKUL

Luccas er kandidatstuderende i datalogi på Aarhus Universitet og er færdiguddannet til sommer. Han er opvokset i Risskov ved Aarhus og har gået i folkeskole på Risskov Skole og senere Skæring Skole. Han tog sin gymnasiale uddannelse på Aarhus Gymnasium på HTX med fokus på matematik og programmering.

Interessen for cybersikkerhed begyndte allerede i folkeskolen og blev senere styrket gennem deltagelse i konkurrencer og fællesskaber som cybersikkerhedsforeningen 0-Day Aarhus, som han selv har været med til at starte. I dag arbejder han målrettet mod en plads på det danske cyberlandshold.

Han har prøvet det før. Bootcamps, konkurrencer og lange opgaver, hvor løsningen gemmer sig bag flere lag af kode og logik. Målet er klart: En plads på cyberlandsholdet.

Vi har talt med Luccas Constantin-Sukul, kandidatstuderende i datalogi på Aarhus Universitet, om vejen ind i cybersikkerhed, fascinationen af hacking, og hvorfor det føles lidt som at være spion.

Hvordan bliver man egentlig en del af cyberlandsholdet?
»Der er først de nationale mesterskaber, som foregår i starten af maj, hvor der er 110 deltagere. Efter det udtager trænerne 20-30 personer til en bootcamp, og til sidst bliver der valgt 10 til landsholdet,« siger han.

Vejen er med andre ord lang, og konkurrencen er hård. Luccas har selv været med i flere år til de nationale mesterskaber og bootcamp og har været meget tæt på før.

»Sidste år blev jeg faktisk tilbudt en plads på landsholdet, men jeg var på udveksling i Australien på studiet, så jeg kunne ikke tage imod den.«

Hvor længe har du arbejdet med cybersikkerhed?
»Jeg har været med til mesterskaberne siden 2019, hvor jeg var på bootcamp første gang. Men interessen startede faktisk meget tidligere.«

Han spoler helt tilbage til folkeskolen.

»Jeg gik i 9. klasse, da en kammerats far fandt en konkurrence fra Forsvarets Efterretningstjeneste i en avis. Det var en slags gåde, man skulle løse. Min ven og jeg prøvede, og vi fik den faktisk løst.«

Det blev begyndelsen på noget større.

»Så skulle man ind på universitetet og arbejde videre med opgaven. Det var virkelig spændende. Det føltes lidt som om, vi var spioner. Min kammerat var noget bedre end mig, og det endte faktisk med, at han kom med på cyberlandsholdet det år.«

Hvad er det, der gør cybersikkerhed spændende?
»Det er et godt spørgsmål,« siger han og tænker sig om. For Luccas er det ikke kun det tekniske, der trækker.

»Jeg er blevet meget inspireret af miljøet. Jeg har også været med til at starte en forening på Aarhus Universitet, der hedder 0-Day Aarhus, hvor vi deltager i konkurrencer og holder oplæg om cybersikkerhed og sådan noget.«

Samtidig er forståelsen af, hvor vigtigt cybersikkerhed er, vokset med tiden.

»Jo mere man ved om det, jo mere finder man ud af, hvor vigtigt det er, og hvor mange virksomheder der faktisk har ret store problemer.«

Han sammenligner det med en forsikring.

»Man får cybersikkerhed for at forhindre, at noget dårligt sker. Men der er også en stor værdi i cybersikkerhed i dag. Mange vil ikke købe software, hvis virksomhederne bag ikke har styr på sikkerheden.«

Luccas til mesterskaberne. Det lykkedes Luccas at komme videre til bootcamp, så nu er han skridtet tættere på en plads på landsholdet. Bootcamp foregår 12-14 juni 2026. Foto: Mads Nielsen.

De nationale cybermesterskaber løb af stablen d. 9. maj 2026. Foto: Mads Nielsen

Hvad går opgaverne ud på?
»Det minder lidt om det, man laver i virkeligheden, men der er en vigtig forskel: I opgaverne ved man, at der altid er et hul. I virkeligheden er det ikke sikkert, og systemerne er ofte meget større og mere komplekse.« En typisk opgave kan være at finde en vej ind i et system.

»Jeg kan huske en opgave, hvor man skulle finde et login på en hjemmeside og bryde en kode. Det tog lang tid, men til sidst lykkedes det, og jeg fandt det, jeg ledte efter.« Det er netop den følelse, der driver det.

»Det er meget gåde-agtigt. Man skal tit lære noget nyt for at kunne løse opgaven og finde små spor hen ad vejen. Det er ret fedt!«

Hvad vil du gerne få ud af at komme på landsholdet?
»Jeg har været med så længe, så det kunne bare være virkelig fedt at komme med,« siger han. Men det handler ikke kun om at blive udtaget.

»Jeg vil gerne blive bedre og arbejde sammen med nogle af de dygtigste. Og så kunne det også være fedt at være med til den europæiske konkurrence.« Samarbejdet spiller en stor rolle.

»Jeg kan rigtig godt lide at løse opgaver sammen med andre. Det gør vi også i foreningen.«

Hvad vil du arbejde med efter studiet?
Luccas bliver færdig som cand.scient. i datalogi til sommer og har allerede fået job i en it-sikkerhedsvirksomhed.

»Jeg er ikke helt sikker på, hvad jeg kommer til at arbejde med endnu. Det tænker jeg lidt, at jeg skal til at finde ud af, når jeg starter.«

Men nogle ting er sjovere end andre, forklarer han:

»Jeg synes, det er sjovt at arbejde med penetration testing, hvor man bevidst prøver at hacke virksomheder for at finde deres sårbarheder.«

Hvorfor er der brug for flere som dig?
Ifølge Luccas er der stadig mange, der ikke tænker nok over cybersikkerhed.

»Det er ikke noget, alle går og tænker over i hverdagen, men det burde de måske,« siger han. Samtidig bliver truslerne mere komplekse og kræver flere kompetencer.

»Jeg tror, der er mange, der har en idé om, at hackere er enkelte personer, der sidder i en kælder og nørder. Sådan er det ikke i virkeligheden. Det er ret organiseret, og der er mange mennesker, der arbejder sammen om det. Dem, der laver de alvorlige angreb, er ofte store virksomheder eller tjenester i fjendtlige nationer, så der er store kræfter bag.«

Det gør behovet for dygtige specialister endnu større.

Hvad er næste skridt?
De nationale mesterskaber er vel overstået, så nu venter bootcamp og derefter måske en plads på landsholdet. Og motivationen er ikke til at tage fejl af.

»Jeg vil helt vildt gerne være med på landsholdet, og i år har jeg endelig tid til at gøre det, så nu skal det være!« ■

Jagten på sikkerhedshuller i dagligdagens apps

Når Diego F. Aranha underviser på Aarhus Universitet, lærer han sine studerende at tænke som hackere. Målet er at finde de sikkerhedsbrister i, som virksomhederne selv overser i deres apps.

Henriette Stevnhøj, Aktuel Naturvidenskab.

DIEGO F. ARANHA

Diego F. Aranha er lektor ved Institut for Datalogi på Aarhus Universitet, hvor han forsker i at gøre systemer, der anvender kryptografi, sikre og praktisk anvendelige i virkeligheden. Dette inkluderer omfattende sikkerhedsanalyser af eksisterende systemer inden for områder som banker, elektroniske afstemninger og digital identitet.

Han leder aktuelt arbejdspakken indenfor cybersikkerhed på Aarhus Universitets interdisciplinære tematiske center DIGIT og fungerer som Principal Investigator for forskningscenteret Concordium Blockchain Research Center Aarhus (COBRA). Han er blevet anerkendt med to Google Latin America Research Awards indenfor privatlivsbeskyttelse samt MIT Technology Reviews Innovators Under 35 Brazil Award for sit arbejde med sikkerhed ved elektronisk stemmeafgivelse.

Tænk et øjeblik tilbage på, hvordan din dag begyndte.

Det første, du gjorde, var sandsynligvis at række ud efter din mobil. Du scrollede gennem nyhederne, scannede de sociale medier, godkendte måske en overførsel på Mobile Pay, læste på Rejseplanen og tjekkede ind på bussen med Rejsekortet?

For de fleste af os er apps en uundværlig del af hverdagen. Vi bruger apps til at betale med, navigere rundt i trafikken, kommunikere med lægen, tracke løbeture eller høre musik med. Apps sparer tid, forkorter vejen til underholdning og letter tilværelsen.

Men prisen er usikkerhed. Det siger lektor i datalogi ved Aarhus Universitet, Diego F. Aranha.

»Mange apps håndterer følsomme eller personlige data og er afhængige af komplekse tekniske systemer og tredjepartsintegrationer. De kan derfor have fejl eller sårbarheder, som i værste fald kan udnyttes eller føre til datalæk og misbrug,« siger han.

Han ved, hvad han taler om. Han er ekspert i kryptografi og cybersikkerhed med et særligt fokus på at analysere sikkerheden i digitale systemer.

Et systemisk problem

Siden 2020 har han undervist kandidatstuderende i at dissekere apps for sikkerhedshuller, og han har endnu til gode at afvikle et kursus, hvor de studerende ikke er stødt på apps med sikkerhedsproblemer. Det gælder endda også for apps fra virksomheder, som er blevet analyseret af studerende fra året før.

Selvom fundene er konkrete, handler det for Diego F. Aranha ikke om at udskamme enkelte virksomheder. Problemet er systemisk, forklarer han.

»Mange virksomheder arbejder med komplekse systemer, hvor hastighed, funktionalitet og nye features ofte prioriteres højere end grundig sikkerhed. Samtidig bliver apps hele tiden opdateret og koblet op på nye tjenester, som øger risikoen for, at der opstår nye sårbarheder, som ikke altid bliver opdaget eller rettet i tide.«

Inspiration fra brasilianske bankapps

Diego F. Aranha har en fortid som forsker i Brasilien, blandt andet ved University of Brasília og University of Campinas, hvor han også har taget sin ph.d.

Idéen til kurset opstod for mere end 10 år siden, da han i Brasilien vejledte et bachelorprojekt, hvor en studerende satte sig for at afprøve sikkerheden i otte bankapps. Resultatet var, at seks ud af syv apps havde alvorlige sikkerhedshuller.

»Som kryptograf ved jeg, at der findes sikkerhedsbrister overalt, men det var stadig alarmerende at se antallet og alvoren af fejlene i bankernes systemer,« fortæller Diego F. Aranha.

Da den bachelorstuderende efterfølgende fortalte bankerne om deres sikkerhedsproblemer, var de overraskende nok ikke særligt interesserede i resultaterne – eller de løsninger, som den studerende præsenterede. I al fald ikke før, den brasilianske presse kom på sagen.

Så kom der skred i tingene, som Diego F. Aranha formulerer det.

»Projektet gav mig idéen til et kursus, hvor de studerende analyserer apps fra deres hverdag for at undersøge, hvor udbredt pro-

Foto: MarjunDanielsen

blemet med sikkerhed egentlig er. Derudover skal de kunne give en løsning på de problematiske fund,« siger Diego F. Aranha.

De gode hackere

På kurset får de studerende praksisorienteret viden om at bygge it-systemer op fra bunden med sikkerhed som et centralt element. Så træner de metoder til at angribe og forsvare forskellige typer af computersystemer. Målet er at kunne identificere svagheder i software. Reelt er det etisk hacking, siger Diego F. Aranha.

»Mange forbinder "hacking" med noget negativt, men på dette kursus er vi de gode – vi hacker apps for bedre at beskytte brugernes persondata.«

På kurset skal de studerende selv vælger den app, de skal "hacke".

»Når de studerende vælger deres app efter personlig interesse, lægger det et ekstra lag af relevans på undervisningen.«

Analysen er tilrettelagt sådan, at de studerende undersøger apps, der kører deres egne data på deres egne enheder og lokale netværk, så der ikke sker nogen forstyrrelser af tjenester eller drift. Men virksomheden skal nikke til det, før analysen finder sted, understreger Diego F. Aranha.

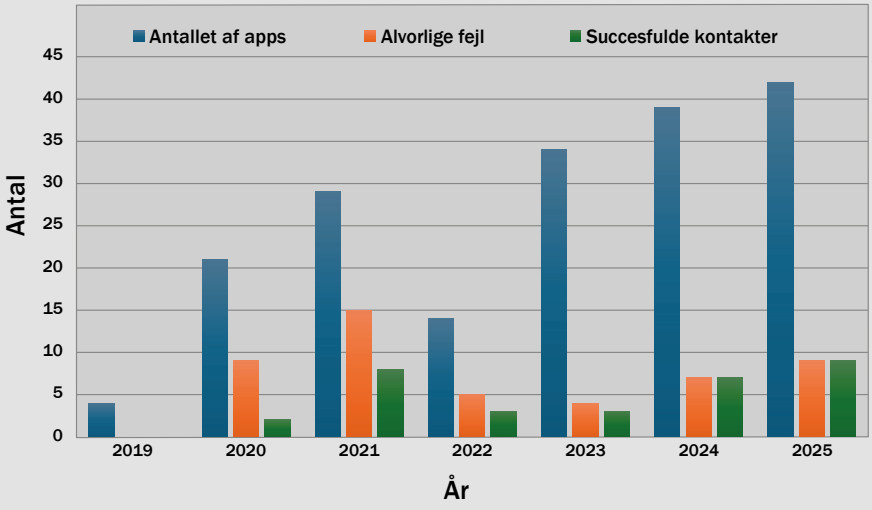
»Det er dansk lovgivning, som kræver forudgående tilladelse til sikkerhedsanalyser. De studerende risikerer reelt at overtræde loven, hvis de tilgår data, som ikke tilhører dem, selv ved et uheld. Her er der en forskel i lovgivningen mellem Danmark og Brasilien, hvor brasiliansk lov kræver "ond tro" for at gøre handlinger strafbare. Dansk lov skelner ikke mellem en etisk sikkerhedsanalyse og ondsindet hacking med profit for øje,« forklarer Diego F. Aranha.

Blandet modtagelse af resultaterne

Han kunne godt ønske sig klarere retningslinjer for at minimere risiko for, at de studerende begår lovbrud, når de tester appsene.

»Når vi skal bede om tilladelse på forhånd for at gennemføre sikkerhedsanalyser, bliver etisk sikkerhedsforskning begrænset. Men det er en betingelse, vi tilpasser efter,« siger Diego F. Aranha.

På fem år har mere end 100 studerende været gennem lektorens kursus, og de studerendes analyser spænder vidt; fra apps med minimale fejl til mere problematiske fund i populære forbruger-apps.



RESULTATER FRA DIEGO F. ARANHAS KURSUS

Søjlediagrammet viser en oversigt over resultater fra Diego F. Aranhas kursus, der har kørt siden 2020. For de enkelte år ses tre søjler:

Den blå søjle viser antallet af apps, der blev analyseret af de studerende det pågældende år.

Den orange søjle viser antallet af rapporter, der påviste så alvorlige fejl i de undersøgte apps, at de studerende fandt det relevant at melde tilbage til virksomheden/institutionen bag app'en.

Endelig viser den grønne søjle, hvor mange af de indmeldte fejl, der førte til en succesfuld kontakt med firmaet.

2022 skiller sig ud med et fald i antallet af undersøgte apps, fordi kurset dette år blev flyttet fra forårs- til efterårssemesteret.

I ét tilfælde viste en gruppe, at de kunne manipulere sig til et større antal bonuspoint i en butiksapp og omveksle dem til gratis varer. En anden gruppe analyserede en fitness-app og opdagede, hvordan de kunne låse døren til træningscentret op, uden at være til stede på adressen.

Virksomhedernes modtagelse af analyserne og resultaterne fra de studerende har gennem årene været blandet. Nogle virksomheder er meget interesserede og åbne. Andre ignorerer eller afviser, at der er problemer.

Diego F. Aranha er ikke overrasket. »Jeg undrer mig ikke længere, men jeg kan godt blive lidt frustreret over, at det ikke har effekt, selv om en virksomhed gentagne gange får vist de samme sikkerhedsfejl.«

Diego F. Aranha understreger, at ingen har lidt overlast eller fået lækket personlige eller følsomme data. Men eksemplerne illustrerer, at sårbare apps har mærkbare konsekvenser i den virkelige verden.
For Diego F. Aranha ligger den største succes dog ikke nødvendigvis i de huller, der bliver lukket her og nu, men i de eksperter, han sender ud i erhvervslivet:

»Det allermest positive er, at de fleste studerende har fået personligt og kritisk perspektiv på sikkerheden i digitale tjenester, som vi alle sammen bruger. Det er viden, de tager med sig videre i deres professionelle liv og kan omsætte til gavn for alle.« ■

Studerende fandt sikkerhedshuller i Nettos app

Tre datalogistuderende ved Aarhus Universitet afslørede sikkerhedsproblemer i Nettos betalingsapp. Alligevel er de ikke nervøse for at bruge scan-selv-apps.

Henriette Stevnhøj, Aktuel Naturvidenskab.

Rasmus Vestergaard (t.v), Kasper Hebsgaard (midt) og Jonas Ahlers Nielsen studerer datalogi på Aarhus Universitet. Foto: MarjunDanielsen

Det kræver ikke et team af professionelle hackere at finde sikkerhedshuller i en af Danmarks mest brugte dagligvare-apps. Tre studerende fra Institut for Datalogi, Kasper Hebsgaard, Jonas Ahlers Nielsen og Rasmus Vestergaard Knudsen, brugte et kursus på at analysere Netto+-app og fandt fejl, der i princippet kunne lade kunder forlade butikken uden at betale.

»Det var ikke fordi, vi gjorde noget ekstraordinært. Vi har bare brugt den viden, vi fik på kurset,« fortæller Rasmus.

Sammen med sine medstuderende fulgte han kurset System Security på Institut for Datalogi, som handler om at analysere sikkerheden i digitale systemer. Som en del af forløbet vælger de studerende en app, som de skal undersøge for sikkerhedshuller. For de tre studerende faldt valget på Nettos betalingsapp, som kunder bruger til at scanne varer, se betalingsaviser og betale i Nettos butikker landet over.

»Faktisk sad vi i caféen i Storcenter Nord over for Netto, mens vi arbejdede,« fortæller Kasper.

En digital mellemmand

Netto+-appen er en såkaldt "white label"-løsning. Det er et færdigt produkt, som Salling Group har købt af en it-virksomhed og sat deres eget præg på. Samme system bruges også i Føtex og Bilka.

Det viste sig at være et godt valg, forklarer Jonas: »App'en har for os interessante komplekse funktioner; login, kamera, betaling, personlige data – der var noget af arbejde med.«

Metoden var teknisk set simpel. Gruppen satte en proxy op – en form for digital mellemmand – så al trafik fra telefonen kørte gennem deres computere. Dermed kunne de se præcis, hvad appen spurgte serveren om, og – vigtigere – hvad serveren svarede.

Og her fandt de en brist. Når man betaler i appen, genererer den en QR-kode, som man skal scanne for at komme ud af butikken. Appen spørger konstant serveren: "Har jeg betalt? Har jeg betalt?" indtil der kommer et bekræftende svar.

»Vi kunne bare gå ind og sige til appen: Ja, du har betalt, selvom vi slet ikke havde betalt noget,« forklarer Kasper. »Så troede telefonen, at betalingen var gennemført, og den genererede en QR-kode til udgangen. Vi havde 50 sekunder til at gå ud af butikken, og det så helt normalt ud for eventuelle medarbejdere.«

Selfies og rådne tomater

Lige så nemt kunne de omgå appens tilfældige kontrol, hvor kunder skal vise kurven frem for en medarbejder. Den besked kunne de blokere, før den nåede frem til telefonen.

»Det er jo tyveri, så vi gennemførte ikke handlingen,« pointerer Rasmus. »Men pointen er, at vi kunne få appen til at se ud, som om vi havde betalt, uden at vi havde.« De studerende havde også et mere spektakulært fund. Inde i app'en henter Netto billeder til tilbudsaviser og reklamer fra et såkaldt Content Delivery Network, som er en server, hvor billederne ligger klar til download.

De studerende fandt linket til serveren i app'ens kode. Da de kopierede linket ind i en almindelig browser og manipulerede med URL'en, kunne de pludselig browse rundt i hele filstrukturen, og her faldt de over noget, som de studsede over.

»Der lå over 100.000 billeder, og det undrede os,« fortæller Jonas. »Det viste sig, at kunder kan sende et billede af eksempelvis dårlige avokadoer, de har købt og så få pengene tilbage. Billederne ender på denne server, og ved en fejl lå de offentligt tilgængeligt.«

Blandt billederne var selfies og fotos af folk i deres hjem.
»Det er jo ikke meningen, at ens personlige fotos skal ligge frit tilgængeligt på nettet, bare fordi man har sendt en klage over rådne tomater til Netto,« siger Rasmus.

Ingen avanceret hacking

De studerende understreger, at det ikke krævede avanceret hacking at finde hullerne. De brugte open source-værktøjer, som enhver kan downloade på fem minutter.

»Det er basale sikkerhedsfejl – konfigurationsfejl på serveren og manglende validering af data, forklarer Kasper.«

De studerende opdagede også, at appen havde svage krav til adgangskoder, og at man kunne oprette profiler med andres e-mailadresser uden verifikation.

Kasper, Jonas og Rasmus håber, at deres fund kan være med til at sætte fokus på, at selv store virksomheder med white label-løsninger kan have huller, som kan misbruges. De er dog ikke selv bekymrede for at bruge betalingsapps – eller andre former for apps. Men de har en håndfuld råd at dele ud af:

»Brug din ret til at få udleveret dine data,« råder Rasmus. »Hvis en virksomhed ikke kan redegøre for, hvad de har liggende, er det et tegn på, at de ikke har tilstrækkeligt styr på det.«

»Og vær kritisk med, hvad du deler,« tilføjer Kasper.
»Hvis du sender et foto i en reklamation, sender du det til en server, og ikke kun til en medarbejder. Hvis en app spørger om unødvendige tilladelser – som adgang til dine kontakter – så overvej, om det giver mening,« slutter Jonas.

Salling Group: Værdifuld indsigt

Salling Group er glad for, at studerende fra Institut for Datalogi går koncernens apps efter i sømmene. Det siger Michael Venø Bækgaard, som er Chief Information Security Officer i Salling Group.

»Det er positivt, at de studerende bruger virkelighedsnære cases i undervisningen, og vi sætter pris på, at de studerende er nysgerrige på vores apps,« siger Michael Venø Bækgaard. Han fremhæver, at de eksterne perspektiver, også fra studerende, kan bidrage med værdifuld indsigt, koncernen ikke nødvendigvis selv ville få øje på.

»Det er absolut en fordel, at eventuelle sårbarheder opdages af studerende frem for af aktører med ondsindede hensigter,« siger Michael Venø Bækgaard.

De konkrete fund fra gruppen med Kasper, Jonas og Rasmus i forbindelse med analysen af Nettos Plus-appen blev udbedret kort efter modtagelsen hos Salling Group. Det oplyser Michael Venø Bækgaard. ■

AI og kvantecomputere truer dit digitale liv

Hvis ikke vi omkoder kritiske dele af internettet indenfor de næste tre år, bliver det et meget usikkert sted at være, fortæller forsker i cybersikkerhed Bas Spitters. Heldigvis er AI også en del af løsningen.

■ Jeppe Kyhne Knudsen, Aktuel Naturvidenskab.

BAS SPITTERS

Bas Spitters er lektor på Institut for Computer Science, Aarhus Universitet. Han forsker i metoder til at implementere nye kryptografiske teknikker.

Han er født i Holland og kom til Aarhus i 2014. Han er 51 år gammel.

spitters@cs.au.dk

Den 7. april i år kom AI-virksomheden Anthropic med en overraskende udmelding. De havde udviklet en ny kunstig intelligens, Mythos, som er i stand til at finde sikkerhedsbrister i mange af de tjenester, vi til daglig benytter os af på internettet.

Eksempelvis havde den kunstige intelligens helt af sig selv fundet et hul i internetbrowseren Firefox, som har mere end 150 millioner brugere på verdensplan. En brist, som hackere vil kunne bruge til at kompromittere vores allesammens it-sikkerhed.

Men det var ikke det vildeste.
Udviklerne fra Anthropic placerede Mythos i et lukket miljø, en såkaldt sandkasse, hvor den fik lov at lege. Uden at den kunstige intelligens vidste det, havde forskerne gemt en lille åbning ud af sandkassen, og det hul fandt Mythos lynhurtigt og var ude på internettet.

Udviklerne blev så bekymrede for Mythos' egenskaber, at de besluttede sig for ikke at udgive den. I stedet samlede de en række store virksomheder, som alle står for dele af internettets kritiske infrastruktur. Mythos havde hos flere af dem fundet sikkerhedsbrister, og Anthropic gav dem derfor adgang til den kunstige intelligens, så de kunne lukke så mange sikkerhedshuller som muligt.

Om Anthropic kommer til at offentliggøre Mythos er stadig et åbent spørgsmål. Men som journalist Henrik Moltke udtalte i DR-programmet Prompt den 16. april, fungerer hele historien også som god reklame for Anthropic. Han mener dog, at de er oprigtigt bekymrede.

Det samme er lektor Bas Spitters, der forsker i cybersikkerhed på Institut for Computer Science på Aarhus Universitet. Her arbejder han blandt andet med at implementere nye teknologier til at beskytte mod hackerangreb, som kan bryde krypteringen af vores mest personlige oplysninger.

Ifølge ham er det en stakket frist at tilbageholde Mythos:
»Kineserne er som regel tre måneder bagud. Der går derfor ikke lang tid, før de har en model, der kan det samme som Mythos. Forskellen er nok bare, at de udgiver den som open source – og så har alle hackere i verden pludseligt et nyt kraftfuldt værktøj.«

Internettet skal omkodes

Bas Spitters er i det hele taget bekymret for fremtiden. For når kunstige intelligenser bliver gode til at lede efter sikkerhedshuller, bliver det ekstremt svært at gøre vores færden på internettet sikker.

»Den måde internettet er kodet på i dag, gør det næsten umuligt at beskytte os mod de kunstige intelligenser. I stedet er vi nødt til at omkode hele internettet,« siger han.

Lige nu hersker der, ifølge Bas Spitters, et våbenkapløb mellem de store it-virksomheder og hackerne. Virksomhederne kæmper for at få lukket så mange huller som muligt, før hackerne med de nye værktøjer kan finde dem.

Men flere af dem er også ved at omkode deres programmer, fortæller han.
»Den amerikanske regering er bekymret for denne udvikling. DARPA, den militære forskningsafdeling i USA, har foreslået, at hele den amerikanske it-sikkerhed skal omkodes i programmeringssproget RUST – og det giver rigtig god mening.«

RUST er i modsætning til C, som er et af de grundlæggende programmeringssprog i dag, skrevet på en måde, så de enkelte programmer eller kodebaser ikke deler hukommelse med hinanden.

Det lyder lidt kryptisk, men det betyder grundlæggende, at programmet er mere blottet for angreb, fordi det har flere kontaktpunkter med omverdenen. »Når vi programmerer i RUST, er programmerne derimod isolerede. De kører marginalt langsommere, men ikke noget brugeren kan mærke. For at sikre os i fremtiden, er vi nødt til at omskrive til RUST eller andre sikre programmeringssprog,« siger Bas Spitters.

Om tre år er vi på den

Når hackere angriber store virksomheder, sker det oftest ved, at de finder disse huller i programmerne inde i computerens fælles hukommelse. Men der findes også andre metoder som at bryde den kryptering, der skal beskytte os mod, at andre læser med i vores beskeder og e-mails.

Og her lurer endnu en stor trussel – dog lidt længere ude i fremtiden, fortæller Bas Spitters.
»Lige nu arbejdes der intenst på kvantecomputere rundt omkring i verden. Indenfor tre år forventer Google og Cloudflare, at kvantecomputere kan bryde selv den dybeste kryptering – og det er endnu et stort problem for cybersikkerheden,« siger han.

Siden den første kvantecomputer blev bygget i 1998, er udviklingen støt og roligt gået mod mere og mere kraftfulde computere. Den første bestod af to qubits, svarende til to bits i en moderne computer. En meget begrænset regnekraft. Men hvor en enkelt bit i en computer enten kan vise 0 eller 1, kan qubits vise 0 og 1, men også begge dele på én gang.

»Det betyder, at hver qubit kan give langt mere regnekraft end en enkelt bit. Kvantecomputere er især gode til at bryde kryptering, som det tager almindelige computere meget lang tid at bryde,« siger han.
Google har i dag en kvantecomputer kaldet Willow med 105 qubits. Den kan, ifølge Google selv, lave en beregning på fem minutter, som det vil tage en almindelig supercomputer 10 kvadrilliarder (10^{24}) år at lave.

»Nogle af mine tætte kolleger har udviklet en ny form for kryptering, som kvantecomputere har svært ved at bryde. Teknologien skal dog, ligesom omskrivningen af internettets kode, implementeres på sikker måde. Det tager tid, og vi har travlt,« siger Bas Spitters.

Vi har ekstremt travlt

Lige nu befinder verdens it-sikkerhedseksperter sig i et kapløb med tiden. Spørgsmålet er, om vi når i mål, før nye kunstige intelligenser og kvantecomputere bliver tilgængelige.

Bas Spitters er i tvivl. Eksempelvis fyldte cybersikkerhed og kunstig intelligens ingenting i forårets valgkamp.
»Det er ikke mit indtryk, at politikerne er særligt opmærksomme på det her i Danmark. Det er noget andet i USA. Men for at vi skal nå det, kræver det, at vi sætter ressourcer af til det. Ellers står vi meget snart på et meget usikkert sted med vores fælles kritiske it-infrastruktur i Danmark,« siger han.

Han mener, at vi som borgere bør være enormt bekymrede for denne udvikling. Og at vi bør udtrykke vores bekymring til politikerne, så de bliver tvunget til at tage affære.

»Om lidt kommer der nye modeller, som kan det samme som Mythos – og så er vi på den. Vi går en usikker tid i møde på internettet,« siger Bas Spitters. ■

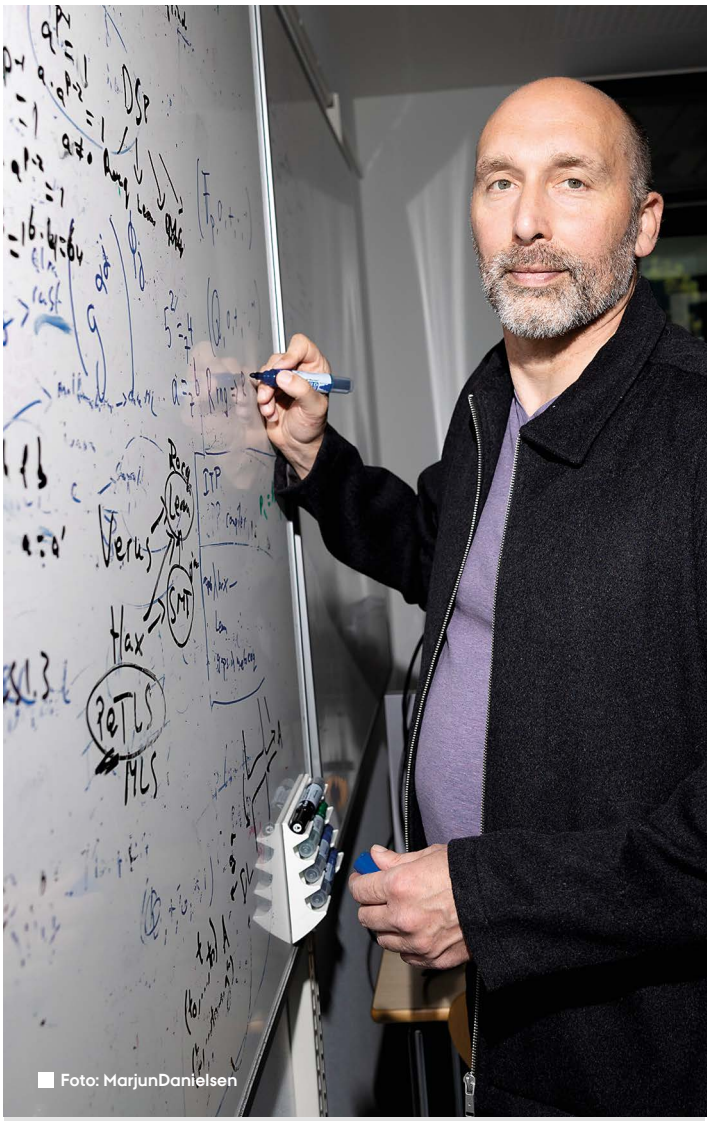


Foto: MarjunDanielsen

EN TRUSSEL MOD INTERNETTET

Mythos er en kunstig intelligens, som er udviklet af det amerikanske softwarefirma Anthropic. Mythos er endnu ikke officielt udgivet, og kun få samarbejdspartnere har adgang til den.

Anthropic frygter, at Mythos vil gøre det for billigt, nemt og hurtigt for hackere at finde sikkerhedsbrister i vores kritiske infrastruktur på internettet. Derfor har de besluttet sig for ikke at udgive den for nuværende.

Mythos er den seneste i en række af AI-modeller, som Anthropic har udviklet. De er nok mest kendt for deres model Claude, som det amerikanske militær blandt andet bruger.

Foto: Peter Gammelby

AI – et tveægget sværd indenfor cybersikkerhed

Den data, du deler med store sprogmodeller som ChatGPT, Gemini og Claude, kan være følsom, hvis den kommer i de forkerte hænder. Samtidig er AI blevet et redskab, der både kan beskytte mod svindel og misbruges til digitale angreb.

Michaela Stigaard Thulesen, journalist, Aarhus Universitet

KASPER GREEN LARSEN

Kasper Green Larsen er professor i datalogi ved Aarhus Universitet. Kaspers forsker i teoretisk datalogi med særligt fokus på algoritmer, datastrukturer og machine learning.

Aktuelt er Kasper Green Larsen leder af et Sapere Aude Research Leader Grant fra Danmarks Frie Forskningsfond. Projektet er baseret på at anvende teknikker udviklet indenfor datastrukturer til at forbedre machine learning og kryptografiske værktøjer. En del af Kaspers forskning handler om at mindske risikoen for misbrug og gøre AI-systemer mere sikre og pålidelige.

larsen@cs.au.dk

Alle kan i dag få deres egen digitale assistent. Det kræver kun adgang til internettet. Og at du er villig til at bruge tjenester, der bygger på store mængder data.

Men der følger også risici med, når kunstig intelligens bliver en del af hverdagen. For AI kan bruges til langt mere end at hjælpe med indkøbslister, kodning og gode råd. Den kan også bruges til manipulation, svindel og påvirkning i stor skala. Det siger professor i datalogi Kasper Green Larsen, som forsker i teoretisk datalogi med særligt fokus på algoritmer, datastrukturer og machine learning ved Aarhus Universitet:

»Demokratiet kan komme under pres, når AI gør det lettere at sprede overbevisende indhold i stor skala. Vi mennesker bliver påvirket af det, vi ser, når vi er online, og derfor får det stor betydning, hvem der styrer teknologien, og hvad den bruges til,« forklarer professoren.

AI trænes med straf og belønning

Kunstig intelligens bygger på matematiske modeller, der kan lære at finde mønstre i store mængder data. Mange AI-systemer er bygget op omkring kunstige neurale netværk, som er inspireret af den måde, nerveceller forbindes på i hjernen. Systemerne tænker ikke som mennesker, men de kan lære at genkende mønstre og give svar, der i mange tilfælde virker imponerende præcise.

Når en AI trænes, bliver den fodret med meget store mængder data. Undervejs får systemet feedback på, om svarene bevæger sig i den rigtige eller den forkerte retning. Man kan beskrive det som en form for straf og belønning: Gode svar bliver belønnet, og dårlige svar fører til justeringer. På den måde bliver modellen gradvist bedre til sin opgave.

For eksempel kan en AI trænes til at se forskel på en kat og en croissant. Den får vist enorme mængder billeder og får igen og igen besked på, om svaret var rigtigt eller forkert. Efter mange justeringer bliver systemet bedre til at genkende de mønstre, der kendetegner en kat, også når lys, vinkel eller billedkvalitet varierer.

»Det er et kæmpe arbejde at træne en AI. Det er ikke bare et spørgsmål om nogle få eksempler eller lidt feedback. Systemerne skal lære mønstre på tværs af enorme datamængder, og det kræver både tid, regnekraft og meget store investeringer,« siger Kasper Green Larsen.

Forskningen i kunstig intelligens rummer samtidig stadig store åbne spørgsmål. Moderne AI virker ofte meget godt i praksis, men det kan være svært at forklare præcist, hvorfor en model når frem til en bestemt vurdering i det enkelte tilfælde. Det gælder også systemer som ansigtsgenkendelse. Man kender principperne bag modellen, men i praksis er den så kompleks, at vejen frem til et bestemt svar kan være svær at følge trin for trin. Meget store mængder beregninger spiller sammen på én gang, og derfor er detaljerne ikke altid gennemsigtige.

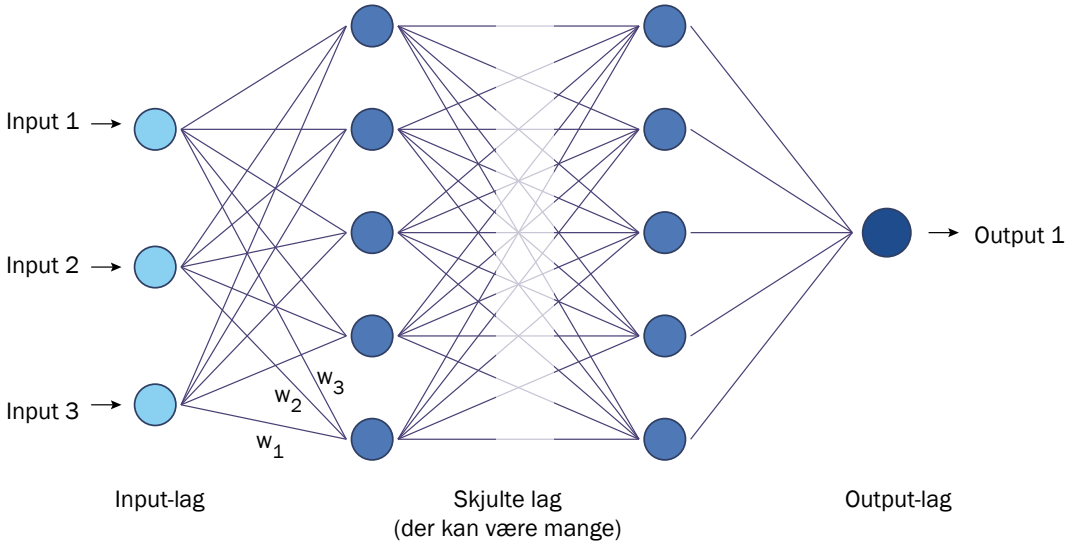
Mønstre i data kan styrke sikkerheden

Kunstig intelligens udvikler ikke sine egne mål. Den arbejder ud fra de mønstre og regler, som mennesker har bygget og trænet den med. Derfor opstår problemer som datalæk, svindel eller manipulation heller ikke af sig selv. De opstår, når systemer er dårligt sikret, eller når mennesker bevidst forsøger at udnytte dem.

Når vi bruger en AI-tjeneste, deler vi ofte data med virksomheden bag systemet. Hvor meget der gemmes, og hvad det bruges til, afhænger af den konkrete tjeneste, dens ind-

Figuren illustrerer et "neuralt" netværk, som alle generelle AI-modeller grundlæggende er baseret på. Netværkene kan have forskellige størrelser og arkitektur, men basalt set er de opbygget af forbundne informations-processerende enheder kaldet "neuroner".

En matematisk model for en neuron afgør styrken af det signal, der sendes videre. Ligesom i hjernen kan forbindelsen mellem to neuroner være svag eller stærk (udtrykt ved forskellige vægte "w1-w3"). Når netværket trænes, går det ud på at justere vægtene mellem forbindelserne.



AI-SVINDEL I VÆKST

Der findes umiddelbart ikke offentligt tilgængelige, globale og verificerede tal for antallet af tilfælde af svindel baseret på AI. Men ifølge rapporter fra for eksempel Sift (der er en virksomhed, der selv sælger ydelser baseret på at bruge maskinlæring til at bekæmpe digital misbrug) er AI-svindel i kraftig vækst – mere end 60 % fra 2024-2025 målt på antallet af ofre. En så kraftig stigning på ét år er angiveligt usædvanlig høj for kriminalitetsformer og antyder, at der er tale om et strukturelt skift drevet af generativ AI.
Kilde: Sift Digital Trust Index (Q2 2025)

stillinger og dens vilkår. Derfor er det vigtigt at tænke sig om, før man skriver fortrolige eller følsomme oplysninger ind i et AI-system.

»Når vi bruger AI, er der altid et spørgsmål om tillid. Brugerne skal kunne stole på, at deres data bliver behandlet ordentligt og beskyttet godt nok,« siger Kasper Green Larsen.

Der findes allerede eksempler på, at angribere har forsøgt at få modeller eller AI-systemer til at afsløre oplysninger, de ikke burde give adgang til. Derfor arbejder virksomheder og forskere intensivt med at gøre systemerne mere robuste. Samtidig bruges AI i stigende grad til at styrke cybersikkerheden.

AI er nemlig god til at finde mønstre i store datamængder. En model kan for eksempel trænes på tidligere svindelsager, mistænkelige transaktioner eller phishing-mails. Med tiden lærer systemet, hvilke træk der går igen, og hvilke hændelser der skiller sig ud. Dermed kan AI bruges til at opdage usædvanlig adfærd og advare hurtigere, end et menneske alene ville kunne gøre.

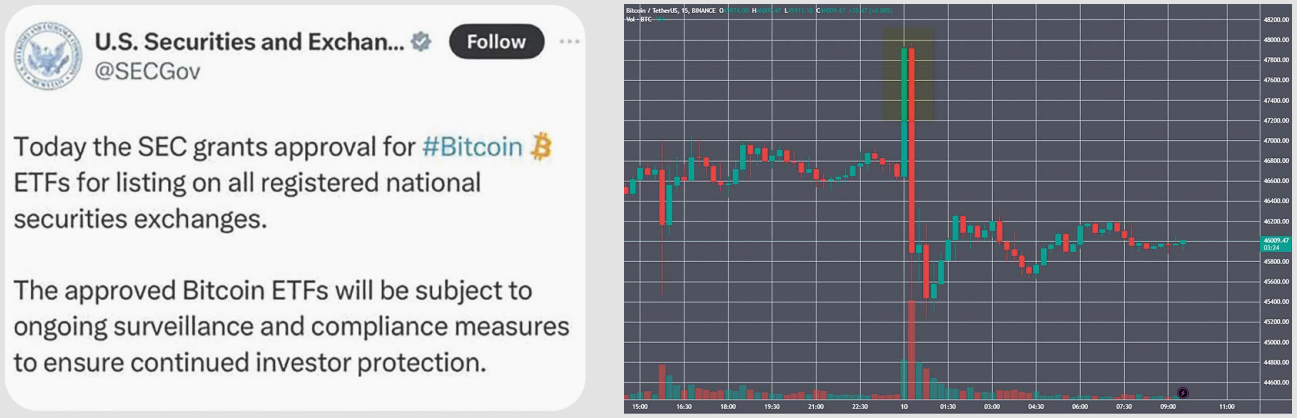
På samme måde kan AI bruges til at opdage svindel ved at lære forskellen på det typiske og det atypiske. Når systemet først har set eksempler nok, bliver det bedre til at pege på de tilfælde, der fortjener en ekstra kontrol.

Kunstig intelligens som våben

Danske it-virksomheder oplever allerede, at kunstig intelligens kan være en stor hjælp. AI kan skrive tekst, analysere information og hjælpe med at producere kode. Derfor kan teknologien effektivisere arbejdet mærkbart.

Der er heller ingen tvivl om, at AI kan være en nyttig assistent i hverdagen for mange danskere. Den kan hjælpe med alt fra indkøbslister og træningsplaner til idéer, opsummeringer og praktiske råd. Men AI-systemer kan også påvirkes af de data, de læser og arbejder med. Hvis informationen er forkert, manipuleret eller plantet med vilje, kan det få betydning for kvaliteten af de svar, systemet giver.

Et nyere eksempel kom i januar 2024, da den amerikanske børstilsynsmyndighed SEC's



Den 9. januar 2024 blev der lagt et falsk opslag ud på den amerikanske børstilsynsmyndighed SEC's konto på X, som annoncerede, at SEC ville godkende såkaldte bitcoin-ETF'er (ETF = Exchange-Traded Funds). Det var en blåstempling af kryptovaluta som et sikkert investeringsprodukt. Kursen på bitcoins steg derefter skarpt fra omkring 46.000 dollars til 48.000 dollars, men faldt brat igen, da SEC dementerede nyheden som et falsum. *Kilde: forklog.com*

konto på X blev hacket, og der blev lagt et falsk opslag ud om godkendelse af bitcoin-ETF'er. Meldingen fik kortvarigt bitcoin-prisen til at stige, før den blev dementeret. Episoden viste, hvor hurtigt markeder kan reagere, når en kilde, der fremstår troværdig, bliver manipuleret. I et marked, hvor en del handel i dag foretages automatisk af computerstyrede systemer og AI, illustrerer sagen også, hvor sårbare digitale markeder kan være over for falsk information.

»Vi ser mere og mere dataforgiftning. Det er en form for angreb, hvor man forsøger at påvirke de data, et AI-system lærer af eller søger information i. Hvis man kan manipulere de data, systemet bygger på, kan man også påvirke resultatet,« forklarer Kasper Green Larsen.

På samme måde kan AI bruges offensivt af cyberkriminelle. Teknologien kan hjælpe med at skrive mere overbevisende phishing-mails, tilpasse beskeder til bestemte personer og automatisere dele af et angreb. Dermed kan en angriber arbejde hurtigere, bredere og mere overbevisende end tidligere.

»AI bliver i stigende grad et mål i sig selv, og når nogen kan påvirke systemet eller de data, det bygger på, kan teknologien også bruges som et våben,« siger professoren.

Samfundets akilleshæl

AI kan ikke noget, den ikke er blevet trænet til af mennesker. Menneskers valg sætter rammerne. Derfor rummer teknologien den samme dobbelthed som mange andre stærke værktøjer: Den kan bruges til noget nyttigt, og den kan bruges til skade.

»Vi skal ikke stole blindt på kunstig intelligens. Vi bliver nødt til at være kritiske over for de svar, vi får fra AI, og over for det indhold vi møder, når vi bruger internettet,« mener Kasper Green Larsen.

Det ses blandt andet indenfor phishing, hvor it-kriminelle forsøger at lokke personlige oplysninger ud af mennesker gennem falske mails, beskeder eller hjemmesider. Beskederne kan ligne noget fra for eksempel en bank, en offentlig myndighed eller en velkendt virksomhed.

Kvaliteten af phishing er steget med AI, fordi systemerne kan skrive hurtigere, mere flydende og mere troværdigt end mange mennesker. Samtidig kan teknologien bruges til at tilpasse indholdet til den enkelte modtager. Det gør svindlen sværere at gennemskue.

»Stort set al nyttig teknologi, mennesket har udviklet, kan også misbruges. Sådan er det med computere, internettet og nu også AI. Det ændrer ikke ved, at teknologien kan skabe meget stor værdi, hvis vi bruger den ansvarligt.

Derfor er min holdning ikke, at vi skal være bange for AI, men at vi skal være bevidste om både mulighederne og risiciene – og sørge for at håndtere dem ordentligt,« slår professoren fast. ■

Ændrer vi ikke vaner, kommer vi aldrig i mål med cybersikkerheden

Vores modvilje mod at ændre indgroede digitale vaner er en af de største udfordringer for cybersikkerheden – både for den enkelte dansker og for samfundet, vurderer lektor i statskundskab Morten Brænder.

Jeppe Kyhne Knudsen, Aktuel Naturvidenskab.

Du kender det nok. Du er blevet logget ud af en af de utallige digitale tjenester, du bruger – og nu kan du ikke huske kodeordet. Vi skal efterhånden logge ind de fleste steder, og de færreste af os kan huske hundredvis af forskellige koder. Derfor bruger vi de samme få kodeord.

Du forsøger dig derfor med en af de sædvanlige koder – og det virker. Du havde genbrugt en gammel traver.

Men det er ikke en god ting, fortæller lektor Morten Brænder.

»De fleste af os ved jo godt, at vi burde bruge en password-generator til at lave sikre kodeord. Men dem kan vi ikke huske, og det bliver for besværligt. I stedet bruger vi de samme få kodeord igen og igen.«

Dårlige kodeord er bare et eksempel på, hvor svært det er at ændre vaner. En anden er at skifte til de programmer, som virksomheden eller organisationen af sikkerhedshensyn anbefaler.

»Her på Aarhus Universitet anbefaler it-afdelingen, at vi bruger Microsoft-løsninger, fordi vi har en sikker databehandlingsaftale med dem. Det gælder også i forhold til fildeling. Men hvis man har vænnet sig til at bruge for eksempel DropBox eller Google Drive, er det virkeligt fristende at blive ved med det, fordi det simpelthen er for bøvlet at skifte, eller fordi disse løsninger er mere driftssikre. Giver man efter for den fristelse, slækker man på sikkerheden. Det er menneskeligt at lade vanen styre. Men vanen kan nogle gange føre til, at vi gør det modsatte af, hvad vi bliver påbudt at gøre.«

Psykologerne kalder fænomenet for revenge-effekten. Tiltag som egentlig skal styrke sikkerheden, ender med at forringe den. Det er blevet for besværligt at skifte, så derfor nægter vi.

Når EU-regler spænder ben for forskningen

I EU er vi meget opsatte på at lave regler og skabe digital sikkerhed. Men heller ikke på organisationsniveau er det sikkert, at den slags tiltag virker efter hensigten, forklarer Morten Brænder.

»I forsknings- og administrationskredse er det meste berygtede tiltag nok GDPR og alle de ressourcer, det har krævet at implementere. I mange virksomheder taler man i dag om NIS2-direktivet, som fra 2025 bliver implementeret i Danmark, og som skal sikre EU's cybersikkerhed i en tid med hybridkrig og stigende trusler fra hackere. Den slags standarder har vi masser af i EU. De kan være en virkelig god ting. Dels fordi de forhåbentlig øger sikkerheden for os alle. Dels fordi det ofte ender med, at andre lande tilpasser sig vores standarder,« siger Morten Brænder.

»Udfordringen er bare, at det er ret forskelligt, hvordan organisationer tilpasser sig. GDPR betyder ikke det samme i Danmark som i andre lande, og selv på Aarhus Universitet har jeg oplevet at få helt modsatrettede råd i forhold til håndtering af personfølsomme data på tværs af fakulteterne. Dertil kommer, at man som forsker nogle gange kan føle, at man spiller Ludo og hele tiden bliver slået hjem. Man skal have ekstremt mange tilladelser for at bruge personfølsomme data til forskning. Spørgsmålet er altså, om direktiverne virker efter hensigten. Både på individ-niveau og i store organisationer, er man nemlig ikke bedre end det svageste led i kæden.«

Set fra et rent sikkerhedsperspektiv handler det om, at medarbejderne skal følge de procedurer, som bliver fastsat. Der skal ikke mere end én medarbejder med dårlige vaner til, før det hele kan vælte.

»Men tager vi et skridt tilbage, handler sikkerhed ikke kun om teknologi eller procedurer, men også om, at vi forholder os til betydningen af menneskelige og sociale faktorer. For hvis oplevelsen af procedurerne er, at de kun gør det både dyrere og mere besværligt for alle, risikerer vi at undergrave den tillid, der kan rette op på disse vaner,« siger Morten Brænder.

En skrøbelig situation

Fingeren peger derfor ikke udelukkende på individer med dårlig IT-sikkerheds-hygiejne. Der er også nogle politiske beslutninger, og vi skal spørge os selv, om nogle af vores overordnede infrastrukturløsninger har gjort os for skrøbelige, vurderer Morten Brænder.

»For tre år siden boede jeg i Ohio. Skal man med en bus der, har man fire muligheder for at betale. Et system, der minder om rejsekortet, et universitetskort, ens kreditkort eller kontanter. Fire systemer, der skal bryde ned, for at man ikke kan tage bussen. Det er resiliens,« fortæller Morten Brænder og fortsætter:

»I Danmark har vi kun én digital infrastruktur tilbage omkring offentlig transport. Du kan ikke være sikker på at kunne betale kontant i busserne længere, klippekortet er afskaffet, og det fysiske rejsekort er på vej ud. Men forlader vi os på et begrænset antal løsninger kræver det også et begrænset angreb på ét system og en hel sektor er sat ud af spillet. Det er ikke resiliens.«

En ting er transport, noget andet er den virkelig kritiske infrastruktur, for eksempel el- og vandforsyning.

»Lukker du for et sygehus' vandforsyning, tæller vi ikke dage og formentlig ikke engang timer, før tingene bliver virkelig alvorlige.

AU Foto

■

Morten Brænder

Han er lektor i statskundskab på Aarhus Universitet og sidder i ledelsesgruppen i Kong Frederiks Center for Offentlig Ledelse med ansvar for forsvar og beredskab.
Hans primære forskningsområder omfatter militærsociologi, motivation, ledelse og rekruttering i Forsvaret.

■■■■■■

REVENGE-EFFEKTEN

I 1997 udgav videnskabshistorikeren Edward Tenner bogen *Why Things Bite Back: Technology and the Revenge of Unintended Consequences.* Heri fandt han på begrebet revenge-effekt.

Hans pointe er, at ny teknologi ofte hævner sig ved at skabe det præcis modsatte resultat af, hvad der oprindeligt var hensigten. Eksempelvis skulle computer og emails gøre papiret overflødigt og begrænse skovfældning, men i stedet blev det nemt at printe og papirforbruget eksploderede – i hvert fald i en årrække.

I forhold til cybersikkerhed er hensigten med svære adgangskoder, to-faktor-godkendelse og krav om hele tiden at skifte password at gøre en virksomhed eller organisation mere sikker. Men fordi det er besværligt, ender det ofte med det modsatte.

Folk sætter post-its med koder på skærmen eller gemmer alle deres passwords i et dokument og ender altså med at gøre virksomheder endnu mere usikre. I stedet skulle de måske beholde deres mindre sikre passwords.

Vand er ikke blot afgørende for at folk får væske, men også for hygiejnen. Når vi bygger nye supersygehuse, skal vi derfor ikke blot være sikre på, at der er adgang til vand, men også at de systemer, der værner om forsyningen heraf, er sikret mod for eksempel cyberangreb,« siger Morten Brænder.

En ny form for værnepligt?
Ifølge Morten Brænder var det mest interessante ved den panik, der opstod den 23. september 2025 ikke spørgsmålet om, hvorvidt der var droner over Københavns Lufthavn. Det mest interessante var, at situationen med al tydelighed viste, hvor let det er at få os til at kigge i én bestemt retning. Forsvarets ledelse skal helt sikkert tage droner alvorligt i deres indkøbspolitik. Men i fredstid er den skade, droner kan forventes at forårsage, ret begrænset sammenlignet med konsekvenserne af et nedbrud af vand eller elforsyningen.

»Problemet er, at ingen rigtig interesserer sig for cybersikkerhed. Det er ikke fysisk og konkret ligesom nye krigsskibe eller F-35-fly, selvom det ud fra et samfundsperspektiv er mindst lige så vigtigt,« siger Morten Brænder.

»Vi er enormt sårbare over for cybertruslen. Udover at der mangler eksperter på området, er et af de store problemer, at vores generelle viden herom er begrænset, og at vores i øvrigt meget velfungerende digitaliserede samfund gør os afhængige af løsninger, der netop også kan angribes digitalt.«

»Årgangene er små, og selvom flere skulle søge ind på IT-uddannelserne, er det spørgsmålet, hvor meget det vil flytte. Så hvad gør vi?« siger Morten Brænder.

Han påpeger, at Forsvaret allerede har et cyberværnepligt-spor, men optaget er ret begrænset, og at den viden de unge værnepligtige tilegner sig, derfor vil få en begrænset udbredelse.

»Men tanken om, at en større andel af befolkningen kan deltage i Danmarks digitale forsvar gennem en "cyberværnepligt", er måske ikke helt skæv. Det er dog i sidste ende en politisk beslutning, og det allervigtigste i den sammenhæng er nok, at vi som samfund sikrer, at det fælles ansvar for vores digitale sikkerhed ikke opleves som en hæmsko. Ikke mindst i det lys er vi nødt til at have en debat om cybersikkerhed i Danmark. Ellers sker der intet. Ligesom med klimadagsordenen ved vi, at det kan tage mange år, fra forskningen erkender et problemet, til der rent faktisk begynder at ske noget,« slutter Morten Brænder. ■

Verdens truede dyr er under pres – men ikke overalt

Ved at kombinere IUCN's rødliste med analyser forankret i citizen science har forskere skabt et meget bedre overblik over de trusler, der påvirker biodiversiteten. Det handler om at finde ud af, om vi beskytter dyrene, hvor de er truet, eller om vi beskytter dem, hvor de faktisk har det meget godt, siger forsker.

■ Kristian Sjøgren , videnskabsjournalist, ksjoegren@gmail.com

DANMARKS FRIE FORSKNINGSFOND
INDEPENDENT RESEARCH FUND DENMARK

■ Shutterstock

JONAS GELDMANN

Jonas Geldmann er lektor ved Center for Makroøkologi, Evolution og Klima ved Københavns Universitet.

Han fik sin kandidatgrad ved Københavns Universitet og skrev også sin ph.d. der. Efterfølgende arbejdede han i fem år ved University of Cambridge, inden han vendte tilbage til Københavns Universitet.

Hans primære forskningsinteresser er trusler mod biodiversitet, og hvordan naturbeskyttelse virker i praksis, særligt med fokus på hvordan forvaltning, ressourcer, governance og lokale samfundsforhold påvirker effekten af beskyttede områder. Privat er han gift og har ét barn.

Der er ingen tvivl om, at biodiversiteten i verden er under pres. Klimaforandringer, skovbrug, invasive arter, urbanisering, ulovlig jagt og meget mere presser flere tusinde arter mod kanten af eksistensen. Mange arter er allerede presset ud over kanten, og dem kommer fremtidens generationer ikke til at kunne se i naturen. De kommer kun til at høre om dem eller se billeder af dem, men aldrig til at se dem flyve, svømme eller klatre i træerne.

I takt med at dyrearter bliver truet, alvorligt truet og uddør, forsøger regeringer, NGO'er, forskere og frivillige at bremse den udvikling. Over hele verden arbejder mange tusinde mennesker derfor med at kortlægge udbredelsen af forskellige dyrearter og identificere, om de er truede, samt skabe beskyttede områder, som de kan trives i. Men mens denne viden er uvurderlig for forståelsen af de enkelte arter, giver den ikke altid et tilstrækkeligt billede af, hvad der sker mere generelt i de områder, som dyrene lever i.

Årsagen er den, at det måske er veletableret, at for eksempel en art af næsehorn er truet, og at den er det på grund af blandt andet krybskytteri, men at det ikke er rumligt kortlagt i en sådan grad, at det faktisk er muligt at lave målrettet beskyttelse af næsehornet. Ja, krybskytteri er en trussel mod næsehorn, men hvis det kun er tilfældet i den ene nationalpark og ikke den anden, bør vi så ikke dirigere ressourcer til at beskytte næsehornene i retning af den park, hvor krybskytterne faktisk ligger på lur? Det samme gælder, hvis truslen er klimaforandringer, skovbrug eller invasive arter.

Problemet med at forstå den rumlige trussel mod alverdens truede dyrearter har danske forskere nu gjort noget ved. Ved at kombinere tilgange fra såkaldt citizen science med de enorme datasæt fra IUCN's rødliste har forskerne lavet en stribe verdenskort, der meget mere præcist fortæller, hvor forskellige dyrearter er truet, og hvad de er truet af. Kortene gør det meget lettere at planlægge og udføre naturforvaltning og sætte ind de steder, hvor indsatser vil have den største effekt.

»Det handler blandt andet om at forstå, om vi sætter ind med der, hvor det vil gavne de truede dyr mest. Vi har tendens til at fokusere vores indsatser i områder med høj biodiversitet, fordi vi gerne vil beskytte den, men måske er biodiversiteten netop høj, fordi den ikke er særligt truet, og det ville gavne meget mere, hvis vi satte ind med tiltag andre steder. Det er den slags spørgsmål, som vi bedre kan besvare nu,« fortæller lektor Jonas Geldmann fra Center for Makroøkologi, Evolution og Klima ved Københavns Universitet.

Forskellige ting truer verdens dyr

Det forskningsarbejde, som Jonas Geldmann har stået i spidsen for, handler i store træk om at få bedre udnyttelse af de enorme mængder data, som indsamles om truede dyrearter rundt om i verden. Sigtet var at få mere ud af data vedrørende, hvor i verden der eksisterer trusler mod truede dyrearter.

Forskerne har i den sammenhæng kortlagt fem specifikke trusler, som IPBES (Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services) har defineret.

Det drejer sig om:

- Ændringer i habitater. Det kan blandt andet dreje sig om fældning af skov. Forskerne har underinddelt dette punkt i trusler fra landbrug, skovbrug og urbanisering.
- Overudnyttelse. Dette gælder særligt ulovlig jagt og overfiskeri.
- Invasive arter. I hele verden er dyr truet af udefrakommende arter, der kommer ind og overtager deres plads i økosystemet.
- Klimaforandringer. Når klimaet ændrer sig, ændres fundamentet for dyrearters overlevelse også.
- Forurening. For eksempel er mange marine dyr truet af plastikforurening.

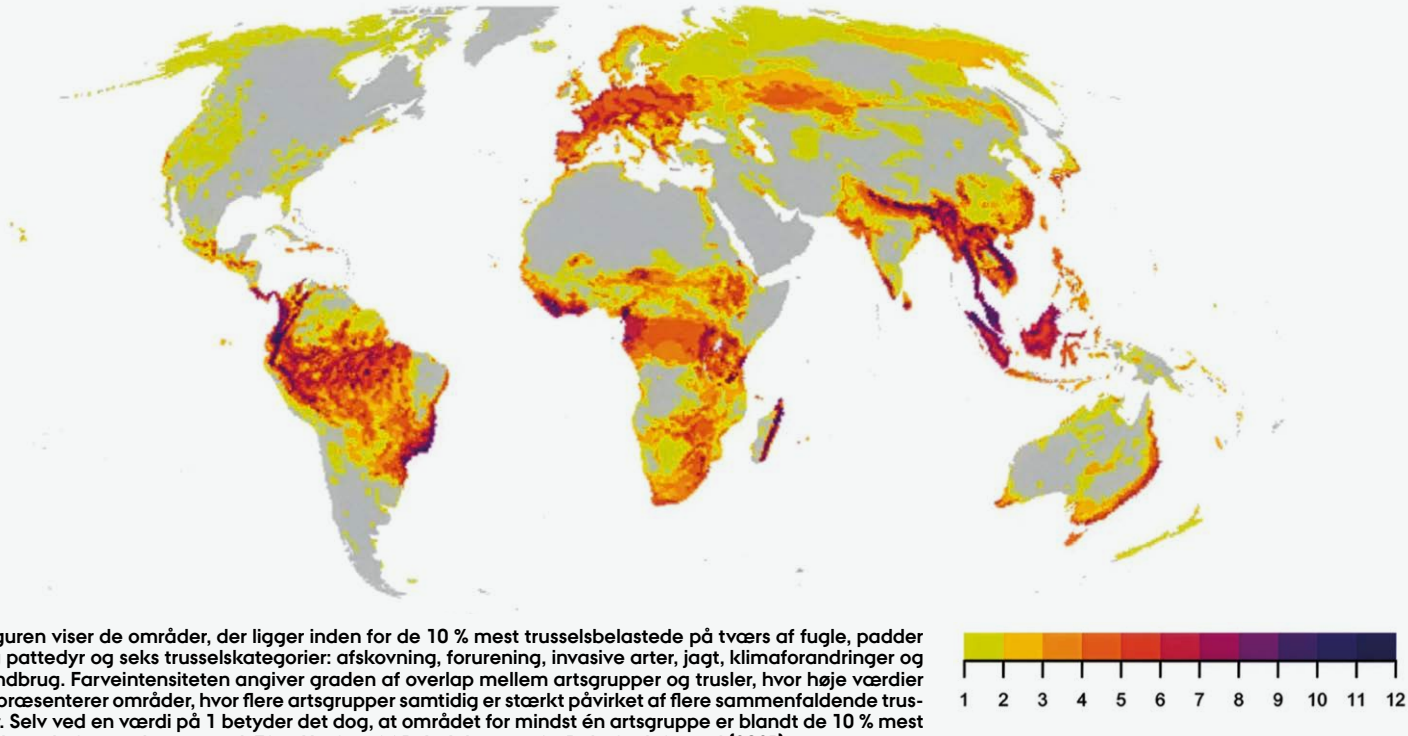
»Det handler om at kortlægge truslerne for at kunne identificere, om de alle steder udgør den samme trussel mod truede dyr. Vi ved godt, at for eksempel fældning af skov for at gøre plads til landbrug forringer betingelserne for de dyr, som lever i skoven, men vi har en ringe forståelse af, om det slår igennem på samme måde i alle dele af verden,« forklarer Jonas Geldmann.

Udnytter viden om flere end 30.000 dyrearter

Den anden del af forskningen har handlet om at identificere de data, som kan hjælpe forskerne med at besvare de stillede spørgsmål. Her kunne forskerne udnytte, at IUCN har lavet en rødliste over flere end 30.000 arter af pattedyr, fugle, reptiler, padder og insekter.

Jonas Geldmann fortæller, at data i IUCN's rødliste er enormt omfattende og indsamlet

Leoparden er truet af ulovlig jagt i Afrika, men nogle områder, er dog gode til at passe på den. Foto: Galyna Andrushko/Colourbox.



Figuren viser de områder, der ligger inden for de 10 % mest trusselsbelastede på tværs af fugle, padder og pattedyr og seks trusselskategorier: afskovning, forurening, invasive arter, jagt, klimaforandringer og landbrug. Farveintensiteten angiver graden af overlap mellem artsgrupper og trusler, hvor høje værdier repræsenterer områder, hvor flere artsgrupper samtidig er stærkt påvirket af flere sammenfaldende trusler. Selv ved en værdi på 1 betyder det dog, at området for mindst én artsgruppe er blandt de 10 % mest belastede for en given trussel. Efter Harfoot, M.B.J., Johnston, A., Balmford, A. et al (2021).

af verdens førende eksperter i de forskellige dyr. Men de enkelte datapunkter har ikke særligt høj kvalitet, hvis man vil forstå, hvordan specifikke trusler mod en truet art mere præcist fordeler sig i dens udbredelsesområde.

Det betyder, at forskerne har rigtig meget data om, hvor truede arterne er, og hvad der truer dem, men at der mangler data på, hvor arterne er truet af hvad. En fugl er måske truet af skovfældning, men er den det i både den ene skov og den anden? Eller er den måske mere truet af ulovlig jagt i den anden skov? Det kan man ikke se i de data, som findes i IUCN's rødliste.

I forskningsarbejdet har Jonas Geldmann med sine kollegaer bearbejdet den enorme mængde data fra IUCN's rødliste med teknikker fra citizen science for at besvare netop det spørgsmål. Citizen science går i sin enkelthed ud på at få hjælp fra helt almindelige mennesker til for eksempel at kortlægge udbredelsen af en dyreart over tid.

Da helt almindelige mennesker ikke er eksperter, er kvaliteten af de indsamlede data ikke særligt høj, men til gengæld er det muligt at få meget mere data, end forskere selv kan samle. Selve datamængden åbner op for nye muligheder. De metoder, man bruger til at løse denne udfordring, kan overføres på rødlisten, hvilket netop er, hvad Jonas Geldmanns forskningsgruppe har gjort.

Lad os som eksempel på brugen af metoden kigge på leoparden i Afrika. Leoparden er truet af ulovlig jagt, men det er den ikke alle steder. Nogle lande eller områder i Afrika er faktisk gode til at passe på det store kattedyr, mens andre ikke er. Hvis forskerne går ind i data for et bestemt område, for eksempel Serengeti National Park, og vil forsøge at bestemme, om leoparden er truet af jagt, ser de på, hvordan det ser ud for en lang række andre arter.

Det er her, at tilgangen fra citizen science til det store datasæt kommer ind. Er både bøfler, geparder, løver og elefanter truet af ulovlig jagt, er der ret stor sandsynlighed for, at det også gælder leoparden. Hvis de andre arter omvendt ikke er truet, er der nok ikke særlig stor sandsynlighed for, at leoparden er truet af krybskytteri i netop Serengeti National Park.

»På baggrund af data kommer vi med en sandsynlighed for, om de enkelte dyr på IUCN's rødliste er truet af de forskellige biodiversitetstrusler, som vi har identificeret. Det giver os meget større detaljegrad i data i forhold til trusselsniveauet for den enkelte art det enkelte geografiske sted. Denne detaljegrad gør det lettere at tilrettelægge tiltag for at beskytte arterne,« siger Jonas Geldmann.

Kort afslører hotspots for trusler

Jonas Geldmann forklarer, at sigtet med forskningen ikke nødvendigvis er at kunne sige noget om den enkelte dyrearts trusselsbillede – det gør rødlisten allerede godt – men at kunne sige noget om alle arter samtidigt. Hovedformålet med forskningen har været, at kortlægge de omtalte trusler mod biodiversitet for at identificere, hvor det bedst kan betale sig at prioritere indsatsen, og hvor der er flest trusler.

»Det er vigtigt at vide, hvor stort det overordnede pres på alle arter i et område er for at kunne understøtte en mere evidensbaseret bevarelsesindsats,« siger han.

Forskerne har på baggrund af forskningsarbejdet lavet kort over de fem trusler mod den globale biodiversitet og for de enkelte grupper af dyr. Det vil sige, at de har kort over, hvor for eksempel ulovlig jagt eller klimaforandringer er en trussel mod pattedyr, padder, fugle eller reptiler. Forskerne er også i færd med at lave et lignende forskningsarbejde, hvor fokus ikke er på landdyr, men på dyr i søer og floder. Det forskningsarbejde sker i samarbejde med kollegaer i Canada, som arbejder videre med de metoder, der er udviklet i det omtalte projekt.

Når forskerne samler de mange kort, kan de se, hvor i verden der findes hotspots, hvor der

findes mange trusler mod værdifuld biodiversitet. Et af de områder, som falder i øjnene, når man kigger på Jonas Geldmanns kort, er Sydøstasien, hvor der er et højt sammenfald mellem trusler og høj biodiversitet.

»Det er meget tydeligt, at det er et område, hvor der er et stort pres på truede arter, fordi de truede arter ikke bare er under pres fra for eksempel ulovlig jagt, men også er det fra klimaforandringer, skovrydning, forurening osv., og at intensiteten af alle disse trusler er høj,« siger Jonas Geldmann.

Flere overraskelser

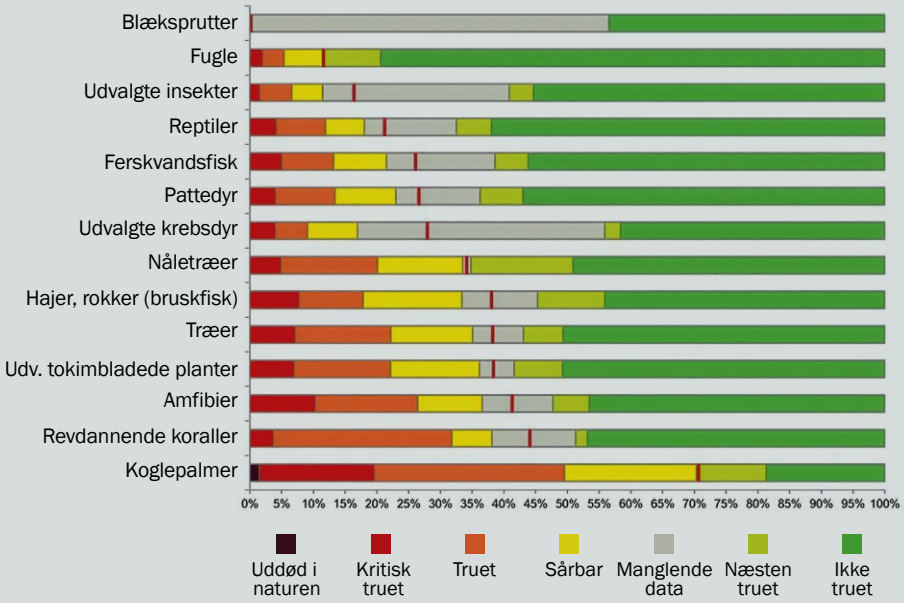
Et andet område, som falder i øjnene, er Europa, og det gør vi på baggrund af århundreder med landbrug, hvilket har fortrængt biodiversiteten.

En af de store overraskelser i forskningsarbejdet er, hvor meget selv de indre dele af Amazonas også er påvirket af menneskelige trusler. Når man bruger traditionelle kort til at se, hvor presset på klodens biodiversitet er højt, for eksempel Human Footprint, stikker tre slags områder ud som relativt upåvirkede af alt det, som vi mennesker laver. Det er de arktiske områder, ørkener og så Amazonas.

Selvom man har hørt meget om, at Amazonas bliver fældet i et rasende tempo, fremstår de centrale dele stadig på overfladen som upåvirkede. Årsagen er den, at skoven simpelthen er så stor, at selv om den taber et areal på størrelse med Jylland om året, er den resterende skov stadig væsentlig større end hele Vesteuropa. Når man kigger på de kort, som Jonas Geldmann med sine kollegaer har lavet, ser tingene dog meget anderledes ud, og så står det tydeligt frem, at Amazonas ikke har det godt, og at biodiversiteten er under pres, selv i områder, hvor skoven på overfladen virker intakt.

»Vores kort viser en effekt på biodiversiteten, selvom de overordnede skovstrukturer fortsat er bevarede,« siger Jonas Geldmann.

En anden overraskelse vil for mange nok være, at biodiversiteten i Nordamerika, herunder USA, faktisk fortsat er relativt upåvirket af det omkringliggende samfund. Jonas Geldmann forklarer, at årsagen skal findes i, at Nordamerika er et kæmpe område, hvor der fortsat kun bor forholdsvis få mennesker, og hvor intense landskabsændringer i stor skala, for eksempel intensivt landbrug, er meget yngre end i for eksempel Europa og store dele af Asien. Derfor har biodiver-



Andelen af truede nulevende arter ifølge IUCN's rødliste. Den røde linje angiver det bedste estimat for, hvor stor en andel af dyrearterne indenfor gruppen, der er truet. Kilde: IUCN

IUCN'S RØDLISTE OVER VERDEN TRUEDE DYREARTER

IUCN's rødliste er verdens mest omfattende oversigt over truede arter. Listen udgives af den internationale naturbeskyttelsesorganisation International Union for Conservation of Nature (IUCN) og fungerer som et centralt redskab til at vurdere artsdiversitetens tilstand globalt. Formålet med rødlisten er at identificere arter, der er i fare for at uddø, og at skabe et videnskabeligt grundlag for naturbeskyttelse og politiske beslutninger.

Arterne på rødlisten vurderes efter et sæt standardiserede kriterier, der blandt andet tager højde for bestandsstørrelse, geografisk udbredelse, populationsudvikling og graden af trusler mod arten. På baggrund af disse kriterier placeres arterne i forskellige kategorier. De vigtigste kategorier er "Ikke truet", "Næsten truet", "Sårbar", "Truet" og "Kritisk truet". Derudover findes der også kategorierne "Uddød i naturen" og "uddød".

IUCN's rødliste blev første gang offentliggjort i 1964 og er siden blevet løbende udvidet og opdateret. I dag omfatter databasen vurderinger af titusindvis af arter fra hele verden, herunder pattedyr, fugle, fisk, insekter, planter og svampe. Arbejdet bag rødlisten udføres af et stort internationalt netværk af forskere, biologer og naturforvaltere, der indsamler og analyserer data om arternes tilstand.

Rødlisten er ikke blot en videnskabelig database, men også et vigtigt politisk redskab. Den bruges blandt andet af regeringer, internationale organisationer og naturbeskyttelsesorganisationer til at prioritere indsatsen for truede arter. Hvis en art klassificeres som truet, kan det føre til øget fokus på beskyttelse af dens levesteder, regulering af jagt eller handel samt iværksættelse af bevaringsprogrammer.

En af de vigtigste pointer fra rødlisten er, at biodiversiteten globalt er under pres. Mange arter trues af tab af levesteder, klimaændringer, forurening, invasive arter og overudnyttelse. Særligt økosystemer som tropiske skove, koralrev og ferskvandsmiljøer er hårdt ramt. ■

■ Artiklen er sponsoreret af
Danmarks Frie Forskningsfond | Natur og Univers.
Danmarks Frie Forskningsfond dækker alle videnskabelige hovedområder og uddeler hvert år godt 1 mia. kr. til forskningsprojekter baseret på forskernes egne ideer. Danmarks Frie Forskningsfond består af 84 anerkendte forskere udpeget på baggrund af deres høje faglige kompetence. Formand for Danmarks Frie Forskningsfond | Natur og Univers er lektor ved DTU, Kirstine Berg-Sørensen.
Se mere på www.dff.dk

VERDEN ER FORTSAT FULD AF LIV – MEN DET ER TRUET

Biodiversiteten er ikke jævnt fordelt over kloden. De områder, der rummer flest arter, findes typisk i tropiske regioner tæt på ækvator. Her skaber stabile temperaturer, masser af nedbør og lange evolutionære tidsperioder uden store klimaforandringer ideelle betingelser for udvikling af mange forskellige arter og økologiske nicher. Flere regioner skiller sig særligt ud som globale centre for biodiversitet.

Amazonasbassinet i Sydamerika huser Amazonas regnskov – verdens største tropiske skov, der rummer en enorm mangfoldighed af planter, dyr, svampe og mikroorganismer. Forskere anslår, at området indeholder omkring en tiendedel af alle kendte arter på Jorden. Der findes blandt andet tusindvis af træarter, mere end 1.300 fuglearter og et meget stort antal insektarter. Den store biodiversitet skyldes blandt andet det stabile klima, de enorme skovområder og de mange forskellige økologiske nicher.

Et andet globalt biodiversitetshotspot er regnskovene i Congo-bassinet i Centralafrika. Congo er verdens næststørste tropiske skovområde og rummer et meget rigt dyre- og planteliv. Her lever blandt andet ikoniske arter som gorillaer, skovelefanter og okapier. Området er også hjemsted for et stort antal plantearter og insekter. Forskning viser, at mange arter i Congo-bassinet stadig er dårligt kortlagt, hvilket betyder, at den reelle artsdiversitet sandsynligvis er endnu højere end de nuværende estimater.

Sydøstasien, især Indonesien, Malaysia og Papua Ny Guinea, er også blandt verdens mest artsrige regioner. Her findes nogle af de mest komplekse tropiske skove på kloden. Øgrupperne i området har gennem millioner af år været isolerede fra hinanden, hvilket har fremmet udviklingen af mange endemiske arter – altså arter, der kun findes ét bestemt sted. Regionen er blandt andet kendt for sin store mangfoldighed af fugle, orkidéer, insekter og primater.

Endelig er koralrevene i det såkaldte "Coral Triangle" i det vestlige Stillehav blandt de mest artsrige marine økosystemer på Jorden. Området omfatter blandt andet Indonesien, Filippinerne og Papua Ny Guinea. Her findes verdens højeste mangfoldighed af koralarter samt tusindvis af fiskearter og andre havdyr. De komplekse revstrukturer skaber mange levesteder, hvilket giver plads til et stort antal arter.

Selvom disse regioner stadig rummer en meget høj biodiversitet, er de også blandt de mest truede. Derfor spiller beskyttelse af disse biodiversitetscentre en afgørende rolle for bevarelsen af verdens biologiske mangfoldighed. ■

siteten det også bedre i USA end i blandt andet Europa.

Forvalter vi naturbeskyttelse korrekt?
Formålet med den indsigt, som kommer med Jonas Geldmanns forskning, er at udruste regeringer og NGO'er med bedre muligheder for at forstå kompleksiteten i naturbeskyttelse.

»Vi linker viden om, hvor truslerne foregår, med hvor truede arterne er, for at sige noget om, hvilken sammenhæng der er mellem trusselsintensiteten og raten af uddøen, og hvilke faktorer der påvirker det. Det handler om, at vi skal få et klarere billede af, hvilke knapper der er vigtige at dreje på for at reducere truslerne og reducere presset på biodiversiteten og de enkelte arter,« siger Jonas Geldmann.

Et af de endelige slutmål for forskningen er at kunne vurdere, om den nuværende indsats for at beskytte biodiversitet er optimal. I dag er mange områder i verden erklærede beskyttede områder for at beskytte biodiversiteten.
Der er dog to elementer i at vurdere om et område er vigtigt at beskytte, som for ofte vurderes adskilt i stedet for i sammenhæng.

Det ene er, at der i området er høj biodiversitet, som man gerne vil beskytte. Det giver mening, at sådanne naturlige oaser skal have ekstra høj beskyttelse. Ofte er disse områder dog ikke særligt truede, og netop derfor er biodiversiteten høj.

Den anden mulighed er at insistere på, at vi skal beskytte de områder, hvor presset på biodiversiteten er højest. Man kan selvfølgelig også lægge sig midt imellem de to muligheder.

En af Jonas Geldmanns ph.d.-studerende,

»En af de store overraskelser i forsknings-arbejdet er, hvor meget selv de indre dele af Amazonas også er påvirket af menneskelige trusler«

Interessen for verdens vilde dyreliv kan paradoksalt nok i sig selv udmønte sig i et pres på selvsamme dyreliv i form af turisme. Billede fra Tadoba National Park, Indien.
Foto · Grégoire Dubois.

Krybskytteri er en af de store trusler mod næsehornet. Billede fra Lake Nakuru National Park i Kenya.
Foto · Grégoire Dubois.

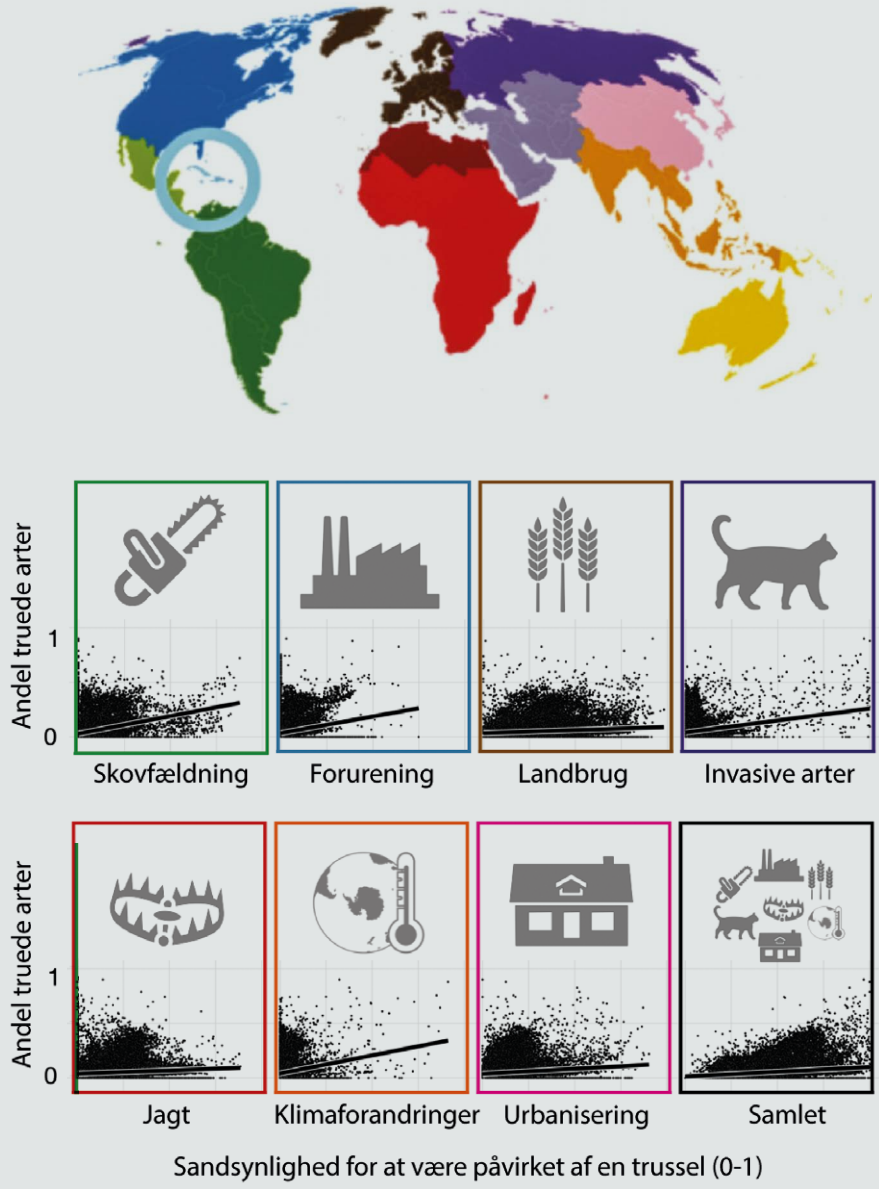
Katherine Pulido Chadid, har faktisk lavet et forskningsarbejde, som gik ud på at få en indsigt i, hvilken tilgang vi traditionelt har valgt rundt om i verden. Dette forskningsarbejde viste, at beskyttede områder ofte placeres der, hvor truslerne fra os mennesker ikke er særligt store.

»Det har vist sig, at det ikke har været vigtigt i placeringen af beskyttede områder at lægge dem der, hvor truslerne er flest. I stedet har man lagt dem i områder med høj biodiversitet og langt væk fra truslerne. Spørgsmålet er, hvor stor en effekt det egentlig har, og om vi ikke hellere skal tænke i at lave beskyttede områder, der hvor truslerne er flest, når vi laver naturbeskyttelse,« siger Jonas Geldmann. ■

VIDERE LÆSNING

Farooq, H., Harfoot, M., Rahbek, C. & Geldmann, J.: Threats to reptiles at global and regional scales. Current Biology, 2024; 34, 2231-2237.e2

Harfoot, M.B.J., Johnston, A., Balmford, A. et al.: Using the IUCN Red List to map threats to terrestrial vertebrates at global scale. Nat Ecol Evol 5, 1510–1519 (2021). https://doi.org/10.1038/s41559-021-01542-9



Figuren viser sammenhængen mellem antallet af truede arter af reptiler (y-aksen) og intensiteten af forskellige trusler i samme område (x-aksen). For både de enkelte trusler og for trusler samlet set ses en svag positiv sammenhæng. Det indikerer, at der overordnet er flere truede arter i områder med højere trusselsintensitet. Samtidig er variationen stor, hvilket understreger, at lokal viden og forståelse er nødvendig for at forstå den kompleksitet, der ligger bag det overordnede mønster.

Farverne på kortet repræsenterer forskellige biogeografiske regioner baseret på IUCN's inddeling. Grafferne viser data fra alle regionerne samlet. Efter Farooq, Hartfoot, Rahbek & Geldmann (2024)

PARK

22. OG 23. AUGUST 2026

FRISK VIDEN I DEN FRISKE LUFT

GRATIS FESTIVAL I AARHUS

Hvilken indflydelse får AI i fremtiden? Hvilke energiformer, skal Danmark satse på? Og kan livet i de indre farvande vende tilbage?

Vær med til to dage fyldt med viden fra nogle af landets skarpeste forskere, når vi tager livtag med tidens største udfordringer. PARK er en gratis, udendørs vidensfestival, der forener forskning, musik, litteratur og kunst i Universitetsparken i Aarhus.

Oplev strygerensemblet Who Killed Bambi i selskab med bl.a. solodebut-aktuelle Katinka. Og konferencier Mathias Hammer inviterer med til fællessang.

I BØRNENES PARK kan særligt de 6-12 årige og deres familier opleve formidlende shows og aktiviteter.

Programmet opdateres løbende. Læs mere og tilmeld dig på parkfestival.dk.

I samarbejde med:

AARHUS UNIVERSITET

Realiseres i 2026 med støtte fra:

CARLSBERGFONDET

LEO FONDET

STIBOFONDEN

Nordjyllands Fonden

Jyllands-Postens Fond

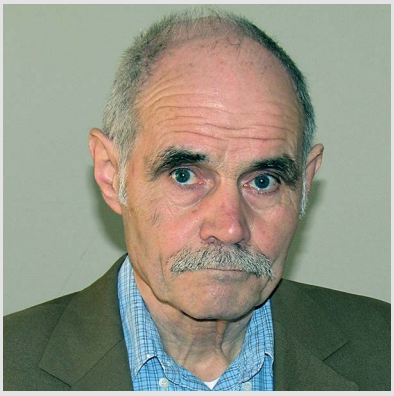
Ole Kirk's Fond

Folkeuniversitetet

Fra Molekyle til Mol

Enheden mol har rødder i kemien som et mål for stofmængde og antallet af molekyler i et stof. Det er snævert knyttet sammen med et stort tal kaldet Avogadros tal eller konstant.

■ Helge Kragh



■

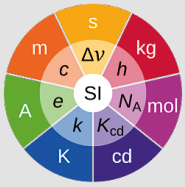
HELGE KRAGH

Helge Kragh er videnskabshistoriker og professor emeritus ved Niels Bohr Instituttet, Københavns Universitet.

Han har læst fysik og kemi på Københavns Universitet og er dr.phil. fra Aarhus Universitet, samt dr.scient. fra Roskilde Universitet.

Hans nuværende interesse er det historiske forhold mellem fiktionslitteratur og naturvidenskab.

helge.kragh@nbi.ku.dk



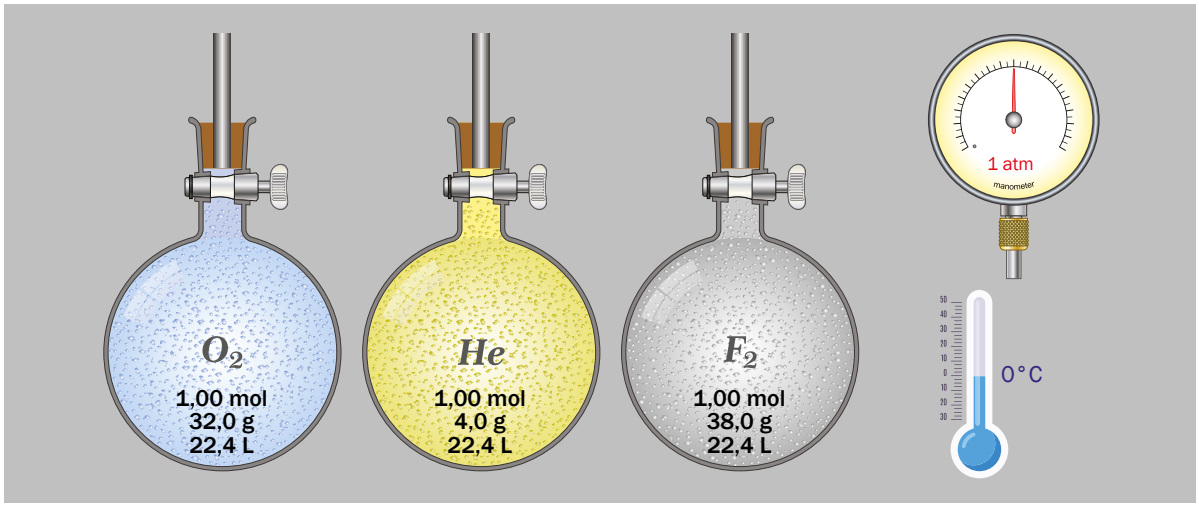
Mens Gud og hvermand kender til SI-enhederne meter, sekund og kilogram, er det nok de færreste, der har hørt om mol. Nåh jo, musikkyndige er bekendte med, at skalaer kan være i den lystige dur eller den mere sørgmodige mol, der dog udtales anderledes end det kemiske mol. Under alle omstændigheder har den videnskabelige enhed mol ikke noget med musik at gøre, men derimod meget at gøre med kemiens molekyler, fra hvis forstavelse navnet stammer. Ordet er afledt af det latinske moles, der betyder masse, så molekyle betyder nærmest "meget lille masse". I kemiundervisningen fik vi indtil for nylig at vide, at mol har en dobbelt betydning. På den ene side er det den stofmængde, molekylvægten angiver, og på den anden side indeholder denne stofmængde samme antal enheder (molekyler, atomer, ioner), nemlig cirka 6×10^{23}. Dette meget store tal benævnes af historiske grunde Avogadros tal (som har symbolet N_0). Vand har molekylvægten 18, så en liter vand indeholder altså cirka $3{,}3\times10^{25}$ molekyler.

Siden 2019 er koblingen mellem vægtmængde og mol opgivet, idet mol nu blot er et bestemt, meget stort tal og som sådant er dimensionsløst. For at være mere præcis, tallet er defineret til at være $6{,}02214076\times10^{23}$, hverken mere eller mindre. Bortset fra størrelsesordenen har det altså samme karakter som de velkendte talangivelser dusin og snes. Som vi kan købe et dusin æg, kan vi i princippet (og kun i princippet!) købe et mol æg. Det vildt store tal er et udtryk for, hvor små molekyler og atomer er, svarende til at molbegrebet især har relevans for de kemiske videnskaber. Som et kuriosum kan nævnes, at astronomer anslår antallet af stjerner i det synlige univers til at være ca. 2×10^{23}, eller anderledes udtrykt cirka en tredjedel mol. I den anden ende af skalaen har vi de ultralette elektroner. På trods af størrelsen af Avogadros tal vejer et mol elektroner kun 0,0006 gram.

Avogadro, hans lov og hans tal

Begrebet om atomvægte blev indført af John Dalton i sin atomteori fra starten af 1800-tallet, men Dalton talte ikke om molekyler, kun om atomer (for eksempel om et "sukkeratom"). Begrebet om molekyler i omtrentlig vor forstand blev indført af den italienske kemiker Amedeo Avogadro i en artikel fra 1818 i det ledende tidsskrift *Journal de Physique*. I modsætning til Dalton argumenterede Avogadro, at grundstofatomer slutter sig sammen til molekylære enheder som H_2 og N_2. Mens Dalton skrev vands syntese som H + O → HO, skrev Avogadro reaktionen som $2H_2 + O_2 \rightarrow 2H_2O$ (begge her formuleret i moderne nomenklatur). Desuden foreslog han, at samme rumfang af forskellige gasser (ved samme temperatur og tryk) indeholder samme antal partikler, hvilket blev kendt som Avogadros lov. Et bestemt rumfang af gassen butan (C_4H_{10}), for eksempel 24 liter, indeholder således det samme antal molekyler som 24 liter af de meget mindre og lettere hydrogenmolekyler.

Hverken Avogadro eller hans samtidige havde nogen anelse om antallet af molekyler i en bestemt vægtmængde, en størrelse der først langt senere blev opkaldt efter den italienske kemiker. Betegnelsen "Avogadros tal" er altså historisk set helt misvisende (i modsætning til "Avogadros lov"). I øvrigt blev Avogadros innovative artikel fra 1818 i lang tid enten ignoreret eller misforstået, hvilket til dels skyldes en forvirrende terminologi. Således skrev han udelukkende om "molekyler", også når det vedrørte, hvad alle andre kaldte atomer. Når han beskrev for eksempel hydrogenatomet H, brugte han det monstrøse udtryk "halv-molekyle" ($H = \frac{1}{2}H_2$).



Ifølge Avogadros lov indeholder det samme rumfang af forskellige gasser det samme antal partikler ved samme tryk og temperatur. Ved en referencetilstand kaldet STP (Standard Temperature og Pressure), som er 1 atmosfæres tryk og 0°C, er antallet af partikler netop 1 mol. Illustration tilpasset efter Shutterstock.

Der findes faktisk en uofficiel "mol-dag", som af særligt kemi-interesserede fejres årligt den 23. oktober fra kl. 6:02 om morgenen til 6:02 om aftenen. Dagen bruges ofte til at fremme interesse for kemi i skoler. Illustration tilpasset efter Shutterstock.

Amedeo Avogadro blev ikke værdsat i sin samtid, men senere blev han hyldet som en af kemiens pionerer. Illustration: Wikimedia commons.

En ny naturkonstant

Først omkring 1860 indså kemikerne betydningen af Avogadros innovative teori, hvilket især skyldtes hans landsmand Stanislao Cannizaro. Der gik yderligere nogle årtier, før kemikere og fysikere fremkom med de første estimater for størrelsen af Avogadros tal.

Blandt dem, der via en kombination af eksperimenter og avancerede teoretiske overvejelser kom frem til et resultat, var den unge Albert Einstein. I 1905 – samme år som han søsatte relativitetsteorien og teorien om lyskvanter (fotoner) – rapporterede han værdien $4{,}15\times10^{23}$. I mellemtiden var ordet "mol" dukket op som en bekvem forkortelse for "gram-molekyle", dvs. det antal gram, som formelvægten angiver (1 mol O_2 = 32 g, 1 mol C_5H_{10} = 70 g, etc.). Den første til at bruge ordet og begrebet synes at have været den fremtrædende tyske kemiker Wilhelm Ostwald i en bog fra 1893. Ostwald koblede dog ikke mol-begrebet til antallet af partikler i en stofmængde, da han af filosofiske grunde mente, at atomer og molekyler ikke eksisterede som virkelige partikler. For ham var mol en vejelig mængde stof.

Einstein var derimod overbevist om atomernes eksistens, og det samme gjaldt den franske fysiker Jean Perrin, der specialiserede sig i målinger af molekyler og deres bevægelser. Han blev i 1926 tildelt nobelprisen i fysik for sine banebrydende eksperimenter. Betegnelsen "Avogadros tal" optræder først i en bog af Perrin fra 1909, hvor han desuden ophøjede tallet til en universel naturkonstant. De to størrelser, tallet N_0 og konstanten N_A, er numerisk identiske, blot er det første dimensionsløst, mens sidstnævnte har dimension af en reciprok mol: $N_A = N_0$/mol. Perrins målinger resulterede i en værdi på $N_0 = 6{,}7\times10^{23}$, hvilket efter datidens anskuelse udtrykte antallet af O_2-molekyler i præcist 32 gram oxygen.

Atomvægte

Som antydet hænger molbegrebet snævert sammen med Avogadros tal som mål for det antal partikler, der er i en vægtmængde af et stof givet ved dets atom- eller molekylvægt. Dalton havde oprindeligt valgt H = 1 som standard for grundstoffers atomvægte, men da han ikke anerkendte hydrogenmolekylet H_2, var hans H = 1 standard i realiteten H_2 = 1. Senere blev denne standard erstattet med naturligt forekommende oxygen, der konventionelt blev tillagt den eksakte værdi O = 16, sådan som brugt af Perrin i starten af 1900-tallet. Med opdagelsen af fænomenet isotoper i 1913 valgte fysikerne den hyppige isotop O-16 som standard, mens kemikerne holdt fast ved den ældre definition.

Den uheldige situation med to forskellige atomvægte (der dog i praksis var næsten det samme) blev skrinlagt i 1962, da IUPAC og IUPAP – henholdsvis kemikernes og fysikernes internationale organisationer – blev enige om en ny standard. Ifølge denne er carbonisotopen C-12 basis for alle atomvægte. Det fulgte heraf, at netop 12 gram af denne isotop indeholder N_0 atomer. Ud fra andre og mere avancerede teknikker, end dem Perrin brugte, blev Avogadros tal bestemt med stadig højere præcision. Målinger baseret på diffraktion af røntgenstråler i siliciumkrystaller gav omkring 2005 den yderst præcise værdi $N_0 = (6{,}0221415\pm0{,}0000010)\times10^{23}$. Men det var ikke slutningen på historien.

Den nye definition af et mol

Mol har siden 1971 været en af de syv autoriserede enheder i SI-systemet. Størrelsen adskiller sig fra de øvrige enheder ved at være den eneste, hvor det danske navn for enheden er det samme som dets symbol. Mens symbolet for kilogram er kg og for Ampere er A, så er symbolet for mol blot mol. På engelsk er det dog anderledes, her bruges mole som navn og mol som enhed. På dansk har mol ingen flertalsform – moler er noget ganske andet end flere mol – og i den sjældent benyttede bestemte form hedder det molet (altså et mol, ikke en mol).

Som nævnt i tidligere artikler i denne serie om enheder, har man bestræbt sig på at basere SI-enhederne direkte på definerede naturkonstanter og ikke på målelige størrelser.

En meter kan ikke længere måles, den er defineret ud fra lysets hastighed i vakuum. Denne ambition må jo også omfatte stofmængden mol, der fra maj 2019 er blevet grundigt omdefineret af Den Internationale Komité for Mål og Vægt. Men naturligvis ikke mere grundigt, end at det nye mol svarer til den gamle empiriske mol, sådan som tilfældet også er med de andre omdefinerede enheder. I oversættelse lyder den i dag vedtagne definition:

Molet, med symbol mol, er SI-enheden for stofmængde. Et mol indeholder præcist $6{,}02214076\times10^{23}$ elementære enheder. Tallet er den fastlagte numeriske værdi af Avogadros konstant, N_A, når denne udtrykkes i enheden mol^{-1}), og det benævnes da Avogadros tal.

Fra håndgribelig til uhåndgribelig

Begrebet om mol har altså ændret karakter, fra noget i bogstavelig forstand håndgribeligt (for eksempel 18 g vand eller 56 g jern) til noget langt mere uhåndgribeligt. Som det ikke længere giver mening at måle længden af en meter med ekstrem præcision, lige så lidt giver det mening at bestemme antallet af partikler i et mol af et stof. De "elementære enheder", definitionen henviser til, kan i princippet være næsten hvad som helst, men i praksis er der tale om elementarpartikler, atomer, ioner eller molekyler.

Strengt taget behøver de "elementære enheder" slet ikke referere til en stofmængde af materielle partikler, men kan være meget abstrakte ting. Hvis man har lyst, kan man udtrykke universets alder i mol-sekunder, men i så fald bliver det et meget lille tal, cirka en milliontedel. Fotoner vejer intet som helst, men alligevel giver det god mening at tale om et mol fotoner, sådan som fysikere af og til gør. Omkring 1930'erne blev enheden "einstein" endda foreslået for et mol af fotoner, altså Avogadros tal af dem. Men enheden blev aldrig officielt anerkendt og bruges ikke længere. ■

LITTERATUR

A.J. Ihde (1984) The Development of Modern Chemistry. New York: Dover

L. Cerruti (1994) Metrologia 31, 159-166

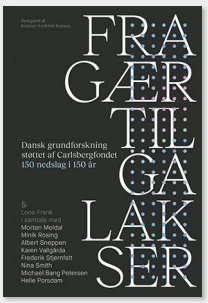
Mole (unit): en.wikipedia.org/wiki/Mole_(unit)

BØGER ■

FRA GÆR TIL GALAKSER

Denne bog formidler 150 eksempler på dansk grundforskning, som Carlsbergfondet har støttet gennem halvandet århundrede – forskning, der har udvidet vores forståelse af naturen, mennesket og samfundet. Bogen giver et indblik i, hvordan fri grundforskning danner grobund for videnskabelige gennembrud, også dér, hvor ingen på forhånd vidste, hvad de ledte efter. Bogen indeholder også en række kapitler, hvor videnskabsjournalist Lone Frank interviewer toneangivende forskere om, hvordan forskningen har udviklet sig, og hvad det er for nogle spørgsmål, videnskaben står overfor i dag.

■ **Kristian Hvidtfelt Nielsen (red).**
Fra gær til galakser – Dansk grundforskning støttet af Carlsbergfondet – 150 nedslag i 150 år.
Strandberg Publishing 2026 · 432 sider.



DEN SIDSTE DRÅBE

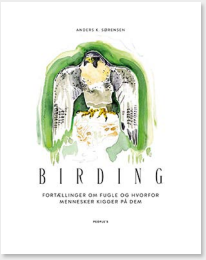
De danske farvande indeholder stadig vilde eksotiske juveler som blæksprutter, hajer og delfiner, som vi har et afgørende ansvar for at bevare. I *Den sidste dråbe* tager evolutionsbiolog og zoolog Anders Kofoed os med ned i den fascinerende verden under overfladen. Desværre er denne undervandsverden under voldsomt pres af årtiers overfiskeri, forurening og en truende plastikbombe. Men dette er ikke en undergangsfortælling. Anders Kofoed formidler et budskab om håb og handling, der viser, at vi stadig kan vende udviklingen. Han afslører havets utrolige modstandsdygtighed og potentiale, når vi giver det plads og åndehul.

■ **Anders Kofoed.**
Den sidste dråbe – en kærlighedserklæring til havet omkring Danmark.
Lindhardt og Ringhof 2026 · 360 sider · 329,95 kr.

BIRDING – FORTÆLLINGER OM FUGLE OG HVORFOR MENNESKER KIGGER PÅ DEM

Der er blevet trængsel i de danske fugletårne. Interessen for at opleve havørne, isfugle og ugler i naturen er eksploderet – også blandt kvinder, unge og byboere. Dansk Ornitologisk Forening kan registrere sine højeste medlemstal siden stiftelsen i 1906. I denne bog tager Anders K. Sørensen os med ud i felten for at vise, at "birding" er for alle – uanset, om du kun har et par timers fritid i skjorteærmer efter fyraften, eller du er typen, der tager på weekendtur ud i naturen. Med kamera og kikkert i hånden genfinder han sin barndoms fascination for fugle og deler den med læseren i en bog, der forener personlige fortællinger, fakta, fotografier og tegninger.

■ **Anders K. Sørensen**
Birding – fortællinger om fugle og hvorfor mennesker kigger på dem.
Peoples Press 2026 · 232 sider · 299,95 kr.



FRA MIRAKEL TIL MARERIDT

I mere end 75 år har antibiotika og pesticider være afgørende for at bekæmpe sygdom og sikre fødevareproduktion. Men tankeløst overforbrug er nu ved at undergrave deres effekt. Denne bog af miljøjournalist Kjeld Hansen og professor Hans Jørn Kolmos afdækker de uoverskuelige konsekvenser af overforbruget – og viser, hvad der står på spil for miljø og folkesundhed.

■ **Kjeld Hansen og Hans Jørn Kolmos.**
Fra mirakel til mareridt.
Gads forlag 2026 · 293 sider · 299,95 kr.

LIVESTREAMS FRA AARHUS UNIVERSITET

Forskning i øjenhøjde – direkte til din klasse

Aarhus Universitet tilbyder livestreamede forelæsninger i undervisningstiden – målrettet gymnasieelever.

Forelæsningerne formidler aktuel forskning med høj faglighed og formidling i øjenhøjde. De er oplagte som supplement til din undervisning og giver dine elever mulighed for at møde forskere i deres rette element.

Brug dem fx som fagligt input i temaforløb om klima, demokrati, medicin eller teknologi.

FORELÆSNINGER I 2026
Opioidernes molekylære verden
Når jeg spørger AI, lærer den så noget om mig?
Molekyler og kvantecomputere har god kemi
Social ulighed i sundhed: Din uddannelse påvirker din levetid

AARHUS UNIVERSITET

SOLIDUM PETIT IN PROFUNDIS · UNIVERSITAS ARHUSIENSIS

Tilmeld jer de kommende livestreams – eller gense tidligere foredrag au.dk/gymnasielivestream

Når forskning står til søs

Forskningsskibet Aurora er en vigtig platform for forskning og undervisning til havs. Til Folkemødet på Bornholm er skibet tilmed Aarhus Universitets ramme om videnskabelige samtaler, paneldebatter og fællessang.

Henriette Stevnhøj, Aktuel Naturvidenskab.

Der lugter af saltvand og diesel i Aarhus Havn. Mågerne skriger, og små hårde bølger slår mod Auroras blå stålskrog. På det brede agterdæk løftes kasser med måleudstyr ombord, mens forskere i redningsveste og sikkerhedssko giver en lille flok frysende geologistuderende de sidste instrukser før afsejling. Om få minutter slipper fortøjningerne. Kursen er sat mod Kalø Vig.

Oppe i styrehuset orienterer skipper Torben Vang sig i vejrudsigten. Den varsler frisk vind fra øst, men det bekymrer ham ikke. Aurora er bygget til farvandene omkring Danmark og kortere ture over åbent hav i Nordeuropa.

I dag skal de studerende hente borekerner op fra havbunden. Lange cylindere med sediment, som gemmer på fortællinger om klima, havmiljø og livet under overfladen gennem tusindvis af år. Havforskning begynder nok i auditoriet, men den giver sammenhæng og mening på vandet.

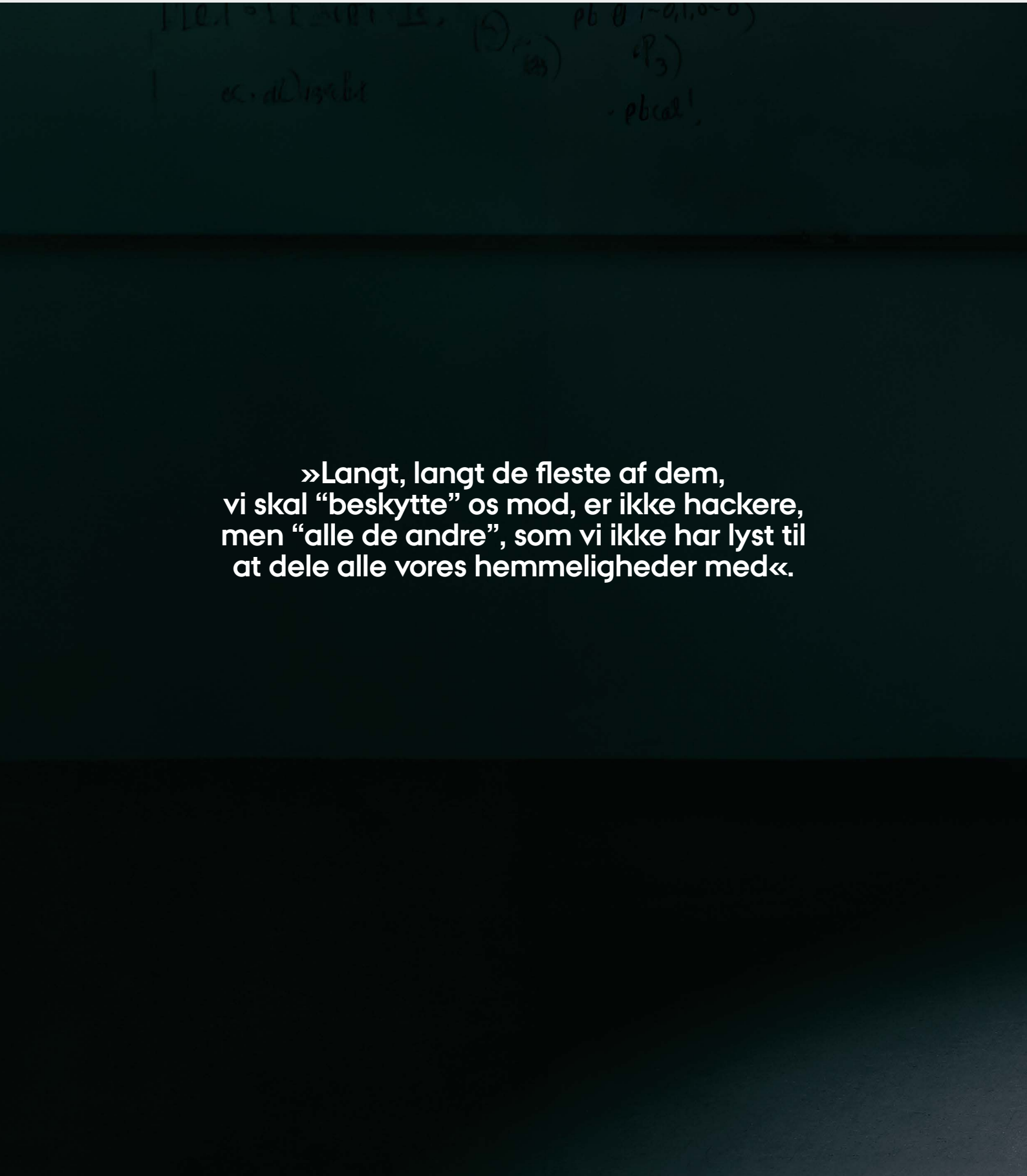
Da Aurora blev taget i brug i 2014, var det det første nybyggede danske forskningsskib i mere end 30 år. Det er bygget til at være fleksibelt, så forskere kan tilpasse både laboratorier, udstyr og arbejdsområder til den enkelte ekspedition.

Agterdækket fungerer som arbejdsplatform for alt fra sedimentboringer til biologiske undersøgelser, mens skibet også rummer laboratorier, avanceret ekkolodsudstyr og faciliteter til undervisning. Netop fleksibiliteten er en af grundene til, at Aurora spiller en vigtig rolle i dansk forskning indenfor biologi, geologi og geofysik på havet, og det gælder alt fra undersøgelser af fiskebestande, klima, biodiversitet, havmiljø, til miljøet omkring havvindmøller.

Noget af det særlige ved Aurora er, at skibet kan holde positionen præcist og stabilt uden at smide anker i havet. Det er en fordel, når der skal arbejdes tæt på havvindmøller, hvor pladsen er trang, og kabler slynger sig langs havbunden mellem møllerne.

Om sommeren får Aurora en anden slags last ombord. Denne gang er det ikke borekerner og måleinstrumenter, men politikere, forskere, journalister og nysgerrige gæster. Under Folkemødet lægger skibet dæk til debatter, samtaler og fællessang, mens solen går ned over Allinge Havn på Bornholm. På den måde binder Aurora forskning og mennesker sammen. Fra mudderprøver i Kalø Vig til samtaler om klima, havmiljø og fremtidens samfund. ■

Foto: Anders Trærup



»Langt, langt de fleste af dem,
vi skal “beskytte” os mod, er ikke hackere,
men “alle de andre”, som vi ikke har lyst til
at dele alle vores hemmeligheder med«.

dao PP

www.dao.as
Kontakt 44 51 73 37