11 år med Tor: Mine erfaringer som Tor-exit operatør

Henrik Kramselund

Forlaget Zencurity ApS
August 2026

Indhold

Om bogen

Titel: 11 år med Tor: Mine erfaringer som Tor-exit operatør

Udgivelsesdato: Første udgave 2026-08-14, Zencurity ApS, Hundested

Forlaget: Zencurity Aps
Lynghøjvej 26, 3390 Hundested
info@zencurity.com
CVR 3294 1184
http://www.zencurity.com

Bogen er udarbejdet uden støtte fra andre organisationer, men et antal frivillige læsere har doneret tid til at læse og forbedre indholdet. Vi takker mange gange - alle tilbageblevne fejl er vores egne.

ISBN-13 978-87-976479-0-5 Trykt udgave

9788797647905

ISBN-13 978-87-976479-1-2 e-bog

Kapitel 1

Dedikation

Denne bog er dedikeret til alle dem som gennem mit liv har hjulpet mig med at forstå hvor privilegeret jeg er - som hvid, danskfødt, heteroseksuel CIS-mand. Det er ikke noget jeg har fortjent. Det er noget jeg er født ind i.

I har vist mig at styrke forpligter. At dem der kan, bør. At det at stå frem - med Tor exit-servere, med holdninger, med sin krop og sit navn - ikke er et offer, men et valg man træffer fordi man har råd til at træffe det, mens andre ikke har.

I har påvirket mig i en positiv retning, og det er jer jeg tænker på når jeg overvejer om det er umagen værd at fortsætte. Det er det.

Nogle af jer er ikke her mere. Men I huskes.

Kapitel 2

Forord

Kære læser - venner og folk jeg ikke kender.

Vi har alle sammen nogle grundlæggende behov for privatliv. Det er bare ikke noget vi tænker særligt meget over i hverdagen. Privatliv er lidt som ilt: usynligt og selvfølgeligt, indtil det pludselig mangler. Først når vores frihed konkret begrænses - når staten kigger med, når platformen lukker ned, når nogen bruger vores digitale spor imod os - opdager vi hvor meget vi egentlig holdt af den frihed vi havde.

Dette lille hæfte er til dig der er nysgerrig på Tor. Hvad er det? Hvorfor eksisterer det? Og hvorfor har en dansk datalog brugt over ti år af sit liv på at drive en exit-server for fremmede mennesker på den anden side af kloden?

Jeg vil bede dig om at læse ét ord og lade det blive i dig: *solidaritetskryptering*.

Det er måske ikke et ord du lige finder i ordbogen. Men det beskriver noget virkeligt. Når du bruger Tor, bruger du ikke bare et redskab til dit eget privatliv - du er med til at skjule alle de andre der bruger det samme netværk. Princippet kaldes inden for privatlivsforskning også for ‘‘anonymity loves company’’: anonymiseringsnetværk som Tor er mere sikre og mere anonyme jo flere mennesker der bruger dem.

Du hjælper således ikke bare dig selv - men alle. Journalisten i Ankara. Aktivisten i Minsk. Den unge kvinde der søger hjælp til at komme væk fra en voldelig partner. De er alle afhængige af at nok mennesker bidrager til netværket og bruger det - fordi et anonymiseringsnetværk kun er stærkt når mange bruger det.

Du kan være med. Ikke nødvendigvis ved at drive en server. Men ved at bruge fælles værktøjer som Tor og Signal. Ved at kæmpe imod masseovervågning når den forklædes som sikkerhedspolitik. Ved at stille krav til dine politikere om proportionalitet og retsgarantier.

Privatliv er ikke noget vi har. Det er noget vi aktivt må vælge at beskytte - for os selv og for hinanden.

God læsning.

Henrik Kramselund

2.1 Målgruppe

Denne lille bog er rettet mod mine venner, og kan måske have interesse for andre aktivister, forkæmpere for privatliv og andre mennesker.

Specielt er den skrevet til alle der har berøring med Tor projektet som brugere, operators og udviklere.

Tor er ikke ulovligt at bruge eller drive i Danmark - det vil jeg gerne underbygge og dokumentere så officielt jeg kan med ISBN som en *trykt bog*

Jeg frygter, eller måske forventer, flere sager om Tor i fremtiden og jeg vil gerne stå på mål for mine erfaringer med Tor, klager og specielt officielle politisager. Hvis du en dag står anklaget - som jeg gjorde - så tøv ikke med at række ud.

Vi er heldigvis mange der stadig betragter privatliv som noget vigtigt!

2.2 Hvorfor

Privatliv er en menneskeret.

Den Europæiske Menneskerettighedskonvention (EMRK) er et vigtigt dokument, men er også i dagligdagen vigtigt for os allesammen.

> Europarådet vedtog EMRK i 1950, og i dag er medlemskab af Europarådet betinget af ratifikation af EMRK. Som en del af konventionen oprettede staterne i 1959 Den Europæiske Menneskerettighedsdomstol (EMD). Her kan borgere i medlemsstaterne rejse sager, hvis de oplever, at en stat krænker menneskerettighederne.
>
> I Danmark betyder EMRK meget. Den blev inkorporeret i lovgivningen i 1992, og danske domstole har dermed pligt til at håndhæve den. Desuden betyder det, at borgere kan klage til myndighederne eller lægge sag an med direkte henvisning til EMRK.

Kilde: Institut for Menneskerettigheder https://menneskeret.dk/om-os/menneskerettigheder/menneskerettigheder-eu/europaeiske-menneskerettighedskonvention

2.3 Referencer

Der er mange referencer, kilder og andre steder man kan finde information.

Hvis man er interesseret i privatlivsbeskyttelse vil jeg anbefale at læse disse to vigtige dokumenter:

- *Bugs in our pockets: The risks of client-side scanning*
- *Keys under doormats: Mandating insecurity by requiring government access to all data and communications ‡*

Hvis man ønsker en blid introduktion til emnet kryptering anbefales denne bog: *The code book: The evolution of secrecy from mary, queen of scots, to quantum cryptography* af Singh

Leder man efter en teknisk introduktion til moderne kryptering er denne bog en god reference: *Serious cryptography: A practical introduction to modern encryption*. Den kan finde hos forlaget No Starch Press https://nostarch.com/serious-cryptography-2nd-edition

2.4 Brug af generativ AI

Der er til denne bog brugt generativ AI - Claude fra Anthropic - som partner og forskningsassistent til at strukturere indholdet og samle informationer. Det har hjulpet med at producere bogen på relativt kort tid og gjort det til en overkommelig opgave - som ellers ville være svær at nå igennem med.

Alle fakta omkring politisager, retten i Helsingør, vidnesbyrd m.v. er mine, og valg i forhold til tone, vægtning og herunder kritik af politiet står jeg bag og er ophavsmand til.

Alle fejl og unøjagtigheder er naturligvis mit ansvar.

Da jeg er bevidst om ressourceforbruget ved brug af AI har jeg valgt ikke at generere et stort antal illustrationer, så bogen fremstår måske mere teksttung end den kunne være.

Kapitel 3

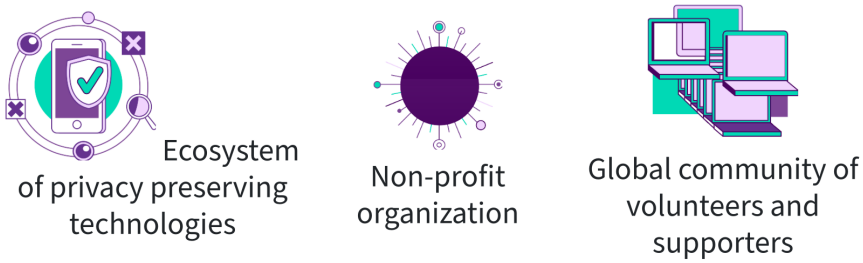
Hvad er Tor

Tor er et netværk designet til ét formål: at gøre det svært at spore hvem der kommunikerer med hvem på Internet. Navnet var oprindeligt en forkortelse af *The Onion Router* - løg-routeren - og løget er faktisk en god metafor for hvordan det virker.

Når du normalt besøger en hjemmeside, går din forbindelse direkte fra din computer til serveren. Din internetudbyder kan se hvad du laver. Hjemmesiden kan se hvem du er. En lang række mellemled kan logge, analysere og gemme data om din færden. Det er standard-internet teknologi pakkerne sendes mellem routere.

Tor fungerer anderledes. Din trafik pakkes ind i flere lag af kryptering - som et løg - og sendes gennem en kæde af mindst tre frivilligt drevne servere rundt om i verden, kaldet *noder* eller *relæer*. Hvert led i kæden kan kun se det foregående og det næste led, aldrig hele ruten. Ingen enkelt server kender både afsender og modtager på samme tid.

*En note om stavning: gennem hele denne bog bruges betegnelsen **Tor** - med stort T og lille or - når der refereres til netværket, projektet og dets servere. Det er den korrekte stavning og afspejler at Tor ikke længere er et akronym, men et egennavn.*



Figur 3.1: Tor er teknologier, en organisation og et community

3.1 Oprindelsen - fra militær teknologi til folkelig infrastruktur

Tor er ikke opfundet af idealister i en kælder. Det er opfundet af det amerikanske forsvar.

I midten af 1990'erne arbejdede forskere ved det amerikanske *Naval Research Laboratory* på et problem: hvordan beskytter man efterretningsagenter i marken når de kommunikerer over internet? En agent der sender en rapport fra Moskva eller Beijing efterlader digitale spor - og de spor kan koste liv. Løsningen var løg-routing: en teknik der krypterer og omdirigerer trafik gennem flere led, så ingen enkelt punkt i kæden kender hele billedet.

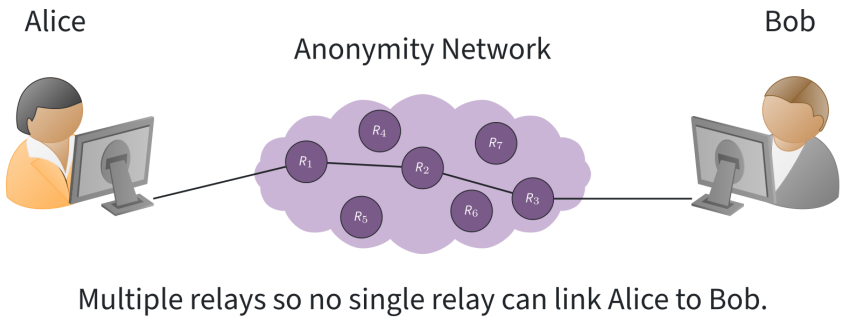
Den tidlige forskning blev offentliggjort i 1996, og den første egentlige implementering fulgte kort efter. Men forsvaret indså hurtigt et paradoks: et anonymiseringsnetværk der kun bruges af agenter er let at identificere. Hvis al trafik i netværket kommer fra efterretningstjenester, er det ikke svært at gætte hvem afsenderen er. For at teknologien virker, skal den bruges af flere - studerende, journalister, aktivister, helt almindelige borgere.

Derfor blev koden gjort offentligt tilgængelig. I 2002 udgav forskerne Roger Dingledine og Nick Mathewson en tidlig version af det vi i dag kender som Tor, og i 2006 blev *The Tor Project* grundlagt som en non-profit organisation i USA.

Siden da har projektet været uafhængigt af det amerikanske forsvar - om end det i en periode modtog dele af sin finansiering derfra, hvilket stadig er et diskussionsemne i miljøet.

I dag drives Tor-netværket af tusindvis af frivillige med servere over hele verden, koordineret af The Tor Project med hovedsæde i USA. Det er et af de mest robuste anonymiseringsværktøjer der eksisterer, og det bruges dagligt af millioner af mennesker.

3.2 De tre typer servere



Figur 3.2: Vejen gennem tor går gennem flere servere

Tor-netværket består af tre slags noder, og de spiller hver sin rolle.

Den første er *entry-noden* - eller *guard-noden* - som er det punkt hvor din trafik flyder ind i netværket. Den kender din rigtige IP-adresse, men ved ikke hvad du laver eller hvor du er på vej hen.

Den anden er *midterste relæer*, som videresender trafik uden at kende hverken afsender eller destination. Det er den usynlige og ufarlige midterste del af kæden.

Den tredje - og den mest udsatte - er *exit-noden*. Det er her trafikken forlader Tor-netværket og sendes videre ud på det almindelige internet. Exit-noden er den eneste der ved hvad du forbinder til, men den ved ikke hvem du er. Til gengæld er det exit-nodens IP-adresse verden ser. Ikke din.

3.3 Klienten bestemmer

Det er vigtigt at forstå at det er Tor-klienten på din egen computer der vælger hvilke tre noder der bruges i hver forbindelse - ikke Tor-netværket centralt. Klienten henter en liste over tilgængelige noder fra Tor's directory-servere og sammensætter selv den kæde den vil bruge.

Klienten skifter løbende til nye noder - en ny kæde etableres typisk hvert tiende minut, eller når du åbner en ny forbindelse. Det betyder at selv hvis nogen observerer trafikken på ét punkt i kæden, er billedet konstant skiftende og svært at følge over tid.

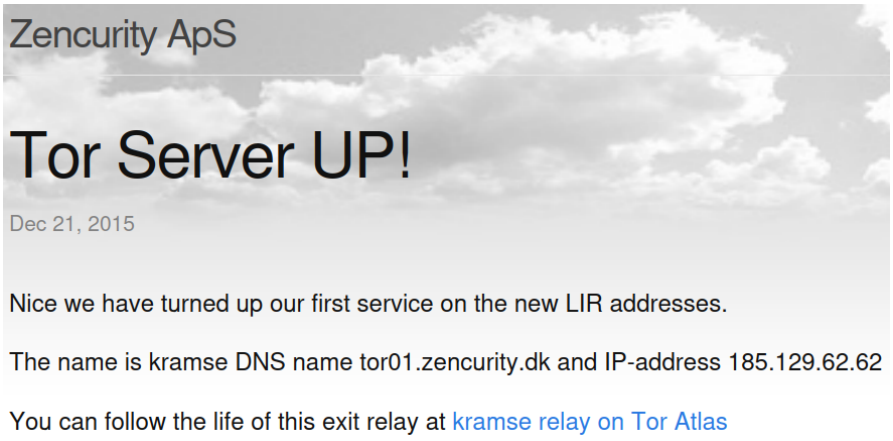
Denne arkitektur er bevidst: ingen central instans beslutter hvem der kommunikerer med hvem. Det er en af grundene til at Tor er robust mod forsøg på at lukke eller kontrollere netværket udefra.

3.4 Mine servere

Jeg kørte vist min første server omkring 2010erne som medejer i et firma - og vi fik en klage fra Tysk politi indenfor 24 timer. Det var en mindre svindelsag, og jeg har ikke detaljerne mere. Firmaet var sammen med en partner og selvom han ikke var vild med klagen, så accepterede han at vi kørte Tor.

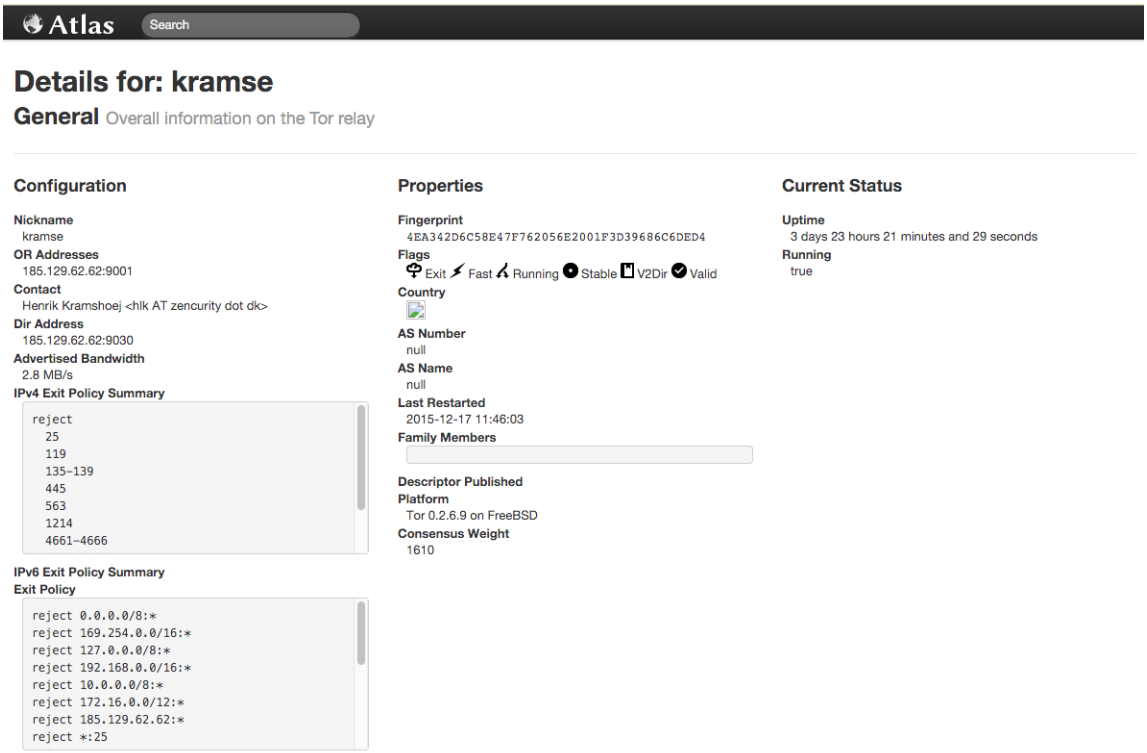
Da jeg senere omkring 2015 genstartede på egen hånd, med fuld kontrol over mit eget firma Zencurity Aps valgte jeg straks at køre Tor exit server.

En af grundene til at jeg ved det så præcist er at jeg lavede et post på min nyopsatte infrastruktur, som her er genfundet.



Figur 3.3: Nyhedsopslag på zencurity.com i 2015 - her gengivet fra archive.org

Jeg havde også postet et fint screenshot fra Tor Atlas, hvor man kan se den er online.



Figur 3.4: Tor Atlas 2015 - her gengivet fra archive.org

Den pågældende IP adresse bruges stadig til Tor exit. Det er således den rolle jeg har spillet i mange år ihvertfald i mere end 11 år.

3.5 Hvem bruger Tor - og hvorfor?

Tor bruges af mange forskellige mennesker med mange forskellige formål. Det er vigtigt at understrege, fordi netværket ofte omtales i medierne i forbindelse med kriminalitet og det såkaldte *dark web*. Det billede er skævt.

De største brugergrupper er langt mere jordnære: journalister der kommunikerer sikkert med kilder i lande med overvågning og censur. Aktivister der organiserer sig under autoritære regimer. Whistleblowere der ønsker at videregive oplysninger uden at blive identificeret. Helt almindelige borgere i lande som Iran, Kina, Rusland og USA, der bare vil have adgang til et frit internet.

Tor bruges også af efterretningstjenester, virksomheder og forskere - og ja, af en minoritet med ulovlige hensigter. Men det samme gælder for telefonen, e-mailen og kontanter. Teknologien er neutral. Det er brugen der afgør værdien.

3.6 Et netværk der hviler på frivillighed

Det centrale ved Tor er at det ikke ejes af nogen. Der er ingen central server, ingen virksomhed der styrer det, ingen enkelt stat der kan lukke det ned. Det er et decentraliseret netværk, der udelukkende fungerer fordi frivillige rundt om i verden stiller serverressourcer til rådighed.

Alle servere i netværket har en funktion og er vigtige, men det som andre ser er typisk IP-adressen på Exit noden. Det er også derfor Tor exit-servere er så vigtige - og så sjældne. At drive en Tor exit-server kræver mere end teknisk kunnen. Det kræver mod, ressourcer og vilje til at stå på mål for noget man tror på.

Det vender vi tilbage til.

Kapitel 4

Hvorfor jeg gik ind i det

Min interesse for privatliv på Internet starter ikke med Tor. Den starter meget tidligere - i begyndelsen af 1990'erne, på Datalogisk Institut ved Københavns Universitet, DIKU.

Jeg blev optaget i 1990 og afsluttede min kandidatgrad i datalogi i 2002. Mit speciale handlede om IPv6 - den næste generation af internetprotokollen - og havde ikke direkte med Tor at gøre. Men studietiden formede mig på en anden måde. Det var her jeg for alvor begyndte at forstå hvordan internet og Internet er skruet sammen, og hvad det betyder når infrastruktur designes på én måde frem for en anden. Netværk er ikke altid neutrale. De er også politiske.

I studietiden læste jeg bredt. Engelske artikler, akademiske papers, mailinglister. Emner som IT-sikkerhed, hacking og kryptering optog mig, og jeg fandt hurtigt vej til de steder på nettet hvor den slags blev diskuteret seriøst. To kilder husker jeg særligt tydeligt fra de tidlige år: *Cryptome* og *Cryptogram*.

Cryptome var - og er - et arkiv der publicerer dokumenter om overvågning, efterretning og statshemmeligheder, ofte materiale som magthavere hellere så forblive lukket. Cryptogram var Bruce Schneiers nyhedsbrev om kryptografi og sikkerhed. Schneier er en af de mest indflydelsesrige stemmer inden for feltet, og hans evne til at forklare komplekse sikkerhedsspørgsmål på en måde der gav mening - ikke bare teknisk, men politisk og menneskeligt - har haft stor betydning for hvordan jeg selv tænker om disse emner. Han og andre fra det miljø har på mange måder formet min karriere.

Det var også i dette miljø jeg første gang stødte på forskningen fra *Naval Research Laboratory* - NRL - omkring løg-routing og beskyttelse af kommunikation over åbne netværk. Jeg husker ikke det præcise tidspunkt, men det var en naturlig del af den verden jeg allerede bevægede mig i. Idéen om at designe anonymitet ind i selve netværksstrukturen fascinerede mig fra første færd.

Da Tor siden hen dukkede op som et konkret projekt og netværk, var det derfor ikke som noget helt fremmed. Det var som at en idé jeg havde hørt om allerede blive til virkelighed. Så henover årene læste jeg om Tor og privacy.

Men interesse alene driver ikke en Tor exit-server i 11 år. Det kræver også de rette forudsætninger - og dem havde jeg senere.

En smule kontekst er også at logningsbekendtgørelsen blev indført i Danmark i løbet af 2000'erne og pålagde internetudbydere at registrere og gemme oplysninger om deres kunders netværkstrafik - ikke indholdet af kommunikationen, men metadata: hvem forbandt sig hvornår, til hvad og fra hvilken adresse. Som studerende deltog jeg i møder hvor bekendtgørelsen blev diskuteret, blandt andet med teknisk personale fra internetudbydere som Cybercity. De var ikke glade for at blive pålagt at bygge overvågningsinfrastruktur - og det var jeg heller ikke.

Jeg fik gennem arbejde adgang til serverressourcer i et professionelt datacenter. Det lyder måske teknisk, men det betyder i praksis meget: en exit-server der kører fra en privat hjemmeadresse er sårbar på en helt anden måde end én der kører bag et cvr-nummer i et datacenter. Juridisk, teknisk og praktisk. Jeg drev driften under et anpartsselskab, hvilket gav en klar og professionel ramme for aktiviteten - og en vis beskyttelse, hvis myndighederne en dag kom på besøg med spørgsmål.

Det var måske noget andre ville have affejet som paranoia. Jeg havde hørt historierne om private der fik besøg af politiet tidligt om morgenen, hvor hele familien blev involveret. Alexander Janssen i Tyskland oplevede det to gange og opgav til sidst sin server. Han bloggede om det.

Valget om at drive Tor exit-servere fra et professionelt datacenter under et ApS var derfor ikke tilfældigt.

Et anpartsselskab giver en vigtig juridisk adskillelse mellem mig som privatperson og den virksomhed der driver serverne. Henvendelser og klager er rettet mod firmaet - ikke mod Henrik Kramselund privat. Det giver en klar ramme for kommunikation og ansvar, og det sender samtidig et professionelt signal: dette er ikke en hobbyist der eksperimenterer

hjemmefra, men en registreret virksomhed med CVR-nummer, adresse og kontaktoplysninger i offentlige registre. Det er sværere at ignorere - og burde være sværere at misforstå.

Dertil kommer noget jeg ikke vil lægge skjul på: jeg er mere ressourcestærk end mange andre, der måske deler min overbevisning om privatliv og ytringsfrihed. Det forpligter. Hvis de der *kan* bidrage til Tor-netværket ikke gør det, er det dem med færre ressourcer - aktivister, journalister, dissidenter - der betaler prisen i form af et svagere og mere sårbart netværk.

Sådan så jeg det. Sådan ser jeg det stadig.

Kapitel 5

Når staten vil kigge med - før krypteringen

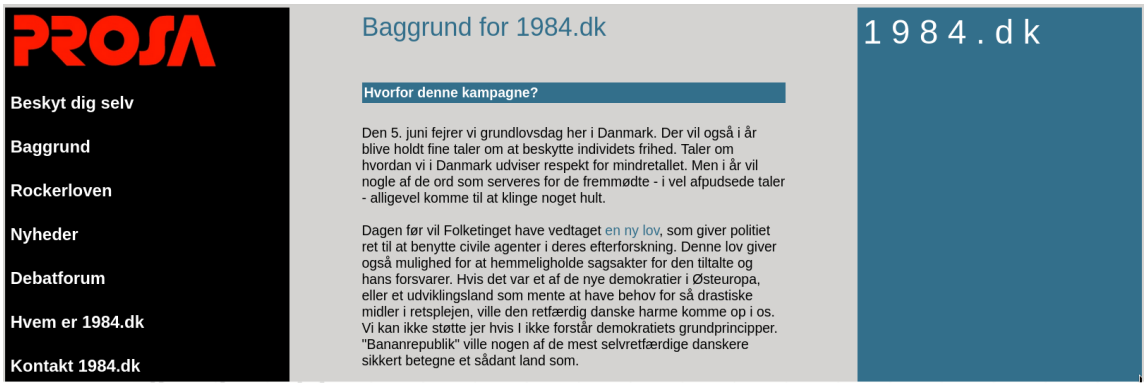
Logningsbekendtgørelsen var ikke den eneste begivenhed der formede min holdning i de år.

I forbindelse med Tvindsagerne omkring 2001 løb dansk politi ind i et problem de ikke brød sig om: krypterede harddiske. Data der var utilgængelige. Efterforskning der gik i stå fordi mistænkte havde beskyttet deres data med kryptering. Politiets frustration var forståelig - men løsningen de pegede på, var ikke god.

Den 23. april 2003 fremlagde justitsminister Lene Espersen lovforslag L218, officielt kaldet et forslag om bekæmpelse af rockerkriminalitet og organiseret kriminalitet. Men indlejret i forslaget lå noget langt mere vidtrækkende: en hjemmel til såkaldt *dataaflæsning*. Med lovforslagets egne ord fik politiet mulighed for at ‘‘læse elektroniske meddelelser, som sendes fra en mistænkt via en computer, før der sker kryptering.’’ Konkret ved brug af snifferprogrammer - software installeret på en borgers computer uden dennes vidende, der logger tastetryk og data inden de krypteres og sendes afsted.

En bagdør. Bare med et juridisk navn.

Forslaget blev mødt med modstand. Fagforeningen PROSA og en gruppe privatlivsinteresserede stod bag websitet *1984.dk* - opkaldt efter Orwells roman - der dokumenterede og kritiserede de løbende angreb på borgernes retssikkerhed og digitale privatliv. Det var et miljø jeg kendte og var en del af.



Figur 5.1: 1984.dk - her gengivet fra archive.org

5.1 Chatcontrol er en bagdør

Det der gjorde - og stadig gør - dette særligt alvorligt er ikke den konkrete sag. Det er mønsteret. Argumentet om at bagdøre er nødvendige for at bekæmpe kriminalitet dukker op igen og igen. I dag kender vi det konkret i EU som debatten om *chatkontrol* - EU-Kommissionens forsøg på at pålægge beskedtjenester at scanne al privat kommunikation for ulovligt indhold. Teknologien er en anden, retorikken er den samme: vi gør det kun mod de skyldige, kun i alvorlige sager, kun under kontrol.

Men en bagdør der er åben for myndighederne er en bagdør der er åben for alle. Der er ingen teknisk måde at garantere at den kun bruges af de rigtige, kun i de rigtige situationer. Det er ikke en holdning - det er en kendsgerning som de fleste med teknisk indsigt vil bekræfte.

Specielt kan den samme teknologi der scanner efter udlovligt materiale være den samme der identificerer politiske modstandere, hvis ikke bare man gør det at være modstander ulovligt i et land.

Det var den erkendelse der over tid førte mig fra at *læse om* privatliv og anonymitet til aktivt at *bidrage* til det. En Tor exit-server er ikke et politisk statement. Det er et stykke infrastruktur. Men infrastruktur er aldrig neutral - og det vidste jeg godt da jeg satte den op.

Kapitel 6

Opsætning af Tor og det praktiske

Jeg ved ikke præcist hvornår jeg satte min første Tor exit-server op. Mine emails fra 2012 og 2013 indeholder tegn på at det startede tidligere end jeg umiddelbart husker - men siden 2015 ved jeg med sikkerhed at jeg har drevet Tor exit-server næsten uafbrudt. Det er den periode jeg husker tydeligst, og det er den jeg kan stå inde for.

Det jeg husker klart er en sommer på *Thecamp* - et dansk community-arrangement for folk med interesse for teknologi, kultur og fællesskab. Jeg er direktør i det lille netværksfirma Solido Networks, jeg har adgang til serverressourcer i et professionelt datacenter, og jeg har besluttet mig: nu sætter jeg en Tor exit-server op.

Det tog ikke lang tid. En Tor exit-server er teknisk set ikke raketvidenskab for én med min baggrund. Software installeres, konfigureres, startes op. Serveren melder sig ind i Tor-netværket og begynder at videresende trafik.

Mindre end 24 timer senere ringede telefonen. Tysk politi havde henvendt sig. En klage over et hackingforsøg mod en hjemmeside - det der i praksis viste sig at være temmelig banal internetsvindel. Men det var nok til at min forretningspartner var lidt nervøs.

Lad mig understrege: han var ikke imod Tor. Han forstod idéen og sympatiserede med formålet. Men en henvendelse fra udenlandsk politi, mindre end et døgn efter opstart, er en reminder om at en Tor exit-server ikke er et usynligt projekt. Det sætter dit navn og din virksomheds navn på noget - og det kræver at man har tænkt det igennem.

Det havde vi en samtale om, og vi nåede frem til nogle spilleregler.

6.1 Spillereglerne - hvordan man driver ansvarligt

Det første og vigtigste princip er synlighed. En Tor exit-server bør aldrig ligne noget mystisk eller skjult. Tværtimod. Jo tydeligere det fremgår hvem der driver den, hvad den er, og hvordan man kommer i kontakt, desto bedre - for alle parter.

I praksis betyder det en række konkrete tiltag som The Tor Project selv anbefaler til exit-operatører:

En informationsside på serveren. På port 80 - den samme port som almindelige hjemmesider bruger - skal der ligge en side der forklarer at denne IP-adresse er en Tor exit-server, hvad det betyder, og hvem man kan kontakte ved spørgsmål eller klager.

Opdaterede Whois- og reverse DNS-oplysninger. Whois er den offentlige database over hvem der ejer en given IP-adresse. Reverse DNS er det navn en IP-adresse ''svarer med'' når man spørger om den. Begge skal pege præcist og tydeligt på dig og din server - gerne med ord som *tor-exit* eller *anonymous-relay* i selve navnet.

En reduceret exitpolitik. En Tor exit-server kan som udgangspunkt videresende trafik på alle netværksporte. Det er ikke hensigtsmæssigt. En reduceret exitpolitik begrænser hvilke porte serveren tillader trafik på - og udelukker eksempelvis port 25 SMTP til afsendelse af email, som bruges til e-mail. Åben SMTP på en exit-server er en invitation til spam-misbrug og medfører klager i hobetal. Det betyder også at ens infrastruktur heller ikke så nemt kan bruges til port scan af systemer.

Det er ikke kompromisser. Det er god praksis, plus det er den praksis jeg har fulgt siden jeg startede.

6.2 Fra første server til løbende drift

Efter den indledende snak med min partner fortsatte serveren. Med de rette oplysninger på plads og en klar ramme for hvem der drev den og hvordan man henvendte sig, ændrede karakteren af henvendelserne sig. De fleste var - og er - automatiserede rapporter fra sikkerhedssystemer der har registreret trafik fra min IP-adresse. Langt størstedelen håndteres

med en standardbesvarelse der forklarer hvad en Tor exit-server er, og at operatøren ikke har adgang til eller kendskab til den konkrete trafik der har passeret igennem.

Det er lidt som at være vært for en telefonboks. Du ved at folk bruger den. Du ved ikke hvad de siger.

Siden da har jeg drevet Tor exit-server næsten uafbrudt - under betegnelsen *Tor server operator*. Infrastrukturen har ændret sig undervejs, konfigurationer er blevet justeret, og erfaringerne har hobet sig op. Dem vender vi tilbage til i de følgende kapitler.

Kapitel 7

Hvad sker der bag kulisserne

At drive en Tor exit-server er ikke det samme som at drive en almindelig server. Det er en særlig position i et netværk designet til at beskytte anonymitet - og den position giver et unikt og samtidig begrænset indblik i hvad der foregår.

Lad mig forklare hvad jeg faktisk kan se.

7.1 Det jeg ser - og det jeg ikke ser

Som exit-operatør sidder jeg på det sidste led i kæden. Trafikken ankommer krypteret fra Tor-netværkets indre, og jeg sender den videre ud på det åbne internet - hen til den webserver, den tjeneste eller den ressource som brugeren ønsker at tilgå. Det betyder at jeg teknisk set kan se destinationen: hvilken server der forbindes til, og DNS-oplysningerne der hører med.

Hvis forbindelsen sker over almindelig HTTP - uden kryptering - ville jeg i princippet kunne læse alt. Indhold, loginoplysninger, beskeder. Alt.

Hvis forbindelsen derimod går over HTTPS - med kryptering - kan jeg se certifikaterne, men ikke indholdet. Præcis som en hvilken som helst internetudbyder.

Det jeg til gengæld *ikke* kan se, er den oprindelige afsenders IP-adresse. Det er hele pointen med Tor. Den er skjult bag netværkets løg-struktur, og den når aldrig frem til mig. Brugeren er anonym. For mig er der ingen afsender - kun trafik.

Men - og dette er vigtigt - at *kunne* se noget er ikke det samme som at *gøre* det.

Jeg sniffer ikke trafik. Ikke noget. Ikke nogensinde.

Det er et stærkt etisk princip jeg har holdt fast i gennem hele min tid som exit-operatør. Der har desværre været dokumenterede tilfælde hvor andre exit-operatører har misbrugt deres position til at opsnappe følsomme oplysninger der passerede ukrypteret gennem deres servere. Det er et alvorligt tillidsbrud mod de brugere der er afhængige af Tor til at beskytte deres kommunikation - diplomater, journalister, aktivister, mennesker i lande hvor det at søge information kan have konsekvenser. At udnytte den position er ikke bare uetisk. Det er en direkte trussel mod de mest sårbare brugere af netværket.

Note: ovenstående bruger HTTP/HTTPS som eksempel fordi de er let genkendelige, men der er også andre typer af ukrypteret og krypteret trafik som kan sendes gennem netværket. De samme betragtninger gør sig gældende.

7.2 Tor browser

Her er det også på sin plads at nævne en positiv udvikling der har ændret forudsætningerne markant: Internet er generelt gået stærkt imod at alle websites bruger kryptering via HTTPS.

I 2015 var kun 39 % af websider krypterede. I dag er det omvendt - over 90 % af al trafik i moderne browsere er krypteret. En stor del af æren tilfalder Let's Encrypt, en non-profit certifikatautoritet grundlagt i 2013 med støtte fra bl.a. EFF og Mozilla. Før Let's Encrypt kostede SSL-certifikater penge, krævede manuel fornyelse og var besværlige at installere. Det holdt især mindre websites væk. Let's Encrypt gjorde det gratis og automatisk - og er i dag verdens største certifikatautoritet med over 700 millioner websites. Kilde: Let's Encrypt - 10 år: https://letsencrypt.org/2025/12/09/10-years

Tor-projektet har bidraget aktivt til denne udvikling gennem initiativet HTTPS Everywhere - et browserudvidelse udviklet i samarbejde med EFF, der automatisk tvang forbindelser over på HTTPS hvor det var muligt. Det er siden blevet integreret direkte i Tor Browser og i mange andre browsere som standardadfærd.

Det betyder at meget af den trafik der i dag sendes gennem Tor allerede er krypteret - og dermed utilgængelig for en exit-operatør uanset hensigt.

7.3 Hvad verden sender igennem

Min infrastruktur består i dag af tre egne servere under firmaet Zencurity ApS - kramse01, kramse02 og kramse03 - med en samlet annonceret båndbredde på knap 125 MiB/s. Derudover har jeg udlånt IPv4-adresser til den danske frivilligorganisation dotsrc i Aalborg. Det er en non-profit organisation der stiller serverressourcer til rådighed for open source-miljøet. Dotsrc driver på det grundlag en række Tor-servere med en samlet kapacitet på knap 400 MiB/s.

Tilsammen repræsenterer det over 520 MiB/s - et betydeligt bidrag til Tor-netværkets samlede kapacitet.

Med den mængde trafik kunne man forvente et tilsvarende stort antal klager og henvendelser. Det er ikke tilfældet.

Fra februar 2020 til april 2026 har jeg modtaget omkring 8.000 henvendelser på mine egne servere. Det lyder af meget - men fordelt over mere end seks år, og set i forhold til den datamængde der har passeret igennem, er det bemærkelsesværdigt lidt. Det har overrasket mig positivt.

Links:

- Zencurity ApS servere (kramse): https://metrics.torproject.org/rs.html#search/kramse
- Dotsrc Tor-servere: https://dotsrc.org/tor og https://metrics.torproject.org/rs.html#search/dotsrc

7.4 Hvem klager - og hvad klager de over

Mønsteret i henvendelserne er ret konsistent. Langt størstedelen handler om deling af piratkopieret materiale - film, serier, software. Disse klager kommer overvejende fra amerikanske organisationer, typisk på vegne af filmindustrien. De er som regel automatiserede, genereret af systemer der scanner nettet for IP-adresser der deler copyrightbeskyttet indhold, og som sender klagerne videre uden menneskelig vurdering af den konkrete situation.

Svaret hvis jeg overhovedet sender et, er standardiseret og faktuelt: denne IP-adresse er en Tor exit-server. Vi har ingen oplysninger om hvem der har benyttet den, eller hvornår. Her er dokumentation for at adressen er registreret som Tor exit-node.

Den anden store kategori er forsøg på hacking - brute force-angreb mod webservere, automatiserede forsøg på at udnytte kendte sårbarheder, scanning af porte. Disse henvendelser kommer fra hele verden, fra serveradministratorer der har set mistænkelig trafik i deres logs. Det de ser i deres logs er ikke noget særligt for Tor. Det er præcis det samme som sker fra det åbne internet hver eneste dag.

Ingen af disse ovenstående henvendelser har ført til juridiske konsekvenser. Det er infrastruktur, og infrastruktur behandler trafik uden at kende afsenderens hensigt.

Kapitel 8

Juridiske og etiske dilemmaer

8.1 Hvornår er det lovligt

Da jeg startede med at drive en Tor exit-server undersøgte jeg så grundigt jeg kunne - uden at være jurist - om det var ulovligt. Jeg læste logningsbekendtgørelsen, kiggede på krav til logning, og vurderede min størrelse og rolle som de facto internetudbyder. Jeg fandt ingen klar lovhjemmel der forbød det, men jeg ville være sikker.

Jeg spurgte derfor en ekstremt dygtig IT-advokat. Svaret var klart: det er ikke ulovligt at drive en Tor exit-server i Danmark.

Det er et svar jeg har holdt fast i - og løbende genovervejet. For lovlighed er ikke en statisk tilstand. Regler ændrer sig, praksis udvikler sig, og det politiske klima omkring kryptering og anonymitet er i konstant bevægelse. At drive Tor exit ansvarligt kræver at man følger med.

Der er også noget at sige om det faktum at jeg nu har drevet Tor exit-servere i mere end ti år - åbent, registreret og med fulde kontaktoplysninger i offentlige databaser. Politiet har i den periode haft kendskab til mine servere. Der har været henvendelser. Der har været sager hvor de har spurgt efter data og fået beskeden, det er en Tor server, jeg har ikke noget at give jer.

Det gør ikke noget automatisk lovligt fordi man har gjort det længe. Men det er ikke uden betydning. Hvis der var en klar lovhjemmel der forbød det, og myndighederne kendte til aktiviteten, ville man forvente at det afspejlede sig i en sigtelse eller i hvert fald en formel advarsel. Det er ikke sket.

Den eneste sigtelse jeg har modtaget vedrørte ikke driften af Tor - den vedrørte en specifik IP-adresse der viste sig at tilhøre en af mine exit-servere. Og den sigtelse kollapsede i samme samtale den opstod i.

8.2 Eksempel på sag omkring Tor server

Et eksempel på noget jeg formoder er svindel i forbindelse med køb i en web shop og mit svar er nedenfor.

```
From: Henrik Lund Kramshøj <hlk@zencurity.dk> (mit tidligere navn)
To: Axxxxx@politi.dk
Subject: Re: Anmodning om oplysninger: 3700-76151-00900-16
Date: Wed, 22 Feb 2017 12:01:55 +0100

Hej Anders / politi

Den pågældende IP adresse blev på det pågældende tidspunkt brugt til en Tor Exit node. Det er en
fast IP som er tildelt denne funktion.

Tor er anonymiseringssoftware som har til hovedformål at maskere brugerens IP adresse, og I kan
læse mere om Tor her: https://www.torproject.org/

Softwaren har mange gode brugssituationer, eksempelvis for journalister, stalking-ofre, diplomater
og andre offentlige myndigheder

Vi er selvfølgelig kede af når er opstår sager hvor det vil være nyttigt at kunne finde personer,
men softwaren er designet til at dette ikke skal kunne lade sig gøre.

Vi har derfor ikke yderligere oplysninger at bidrage med.
```

```
Jeg kan kontaktes telefonisk på 2026 6000 eller svar tilbage hvis der er flere spørgsmål

Mvh

Henrik


> On 22 Feb 2017, at 11:37, <Axxxx@politi.dk> <Axxxxx@politi.dk> wrote:
>
> Hej Zencurity
>
> I verserende straffesag ved journalnummer 3700-76151-00900-16, ønsker politiet at få udleveret
brugeroplysninger vedr. brug af IP adresse 185.129.62.62
>
> Den har kommunikeret med hjemmesiden www.frishop.dk (52.84.24.22) den 11-10-2016 kl. 2100.
>
> Vi kan ikke supplere med et portnummer.
>
> Såfremt der er tale om en dynamisk IP adresse anmodes om postnummer og by.
>
> Såfremt der er tale om en fast IP adresse anmodes om fuldstændige brugeroplysninger.
>
> På forhånd tak,
>
> Med venlig hilsen
>
> Anders Kxxxx Lxxxx
> Politibetjent
>
> <image001.png>
> Økonomisk Kriminalitet
> Efterforskningscenter Midt
> Skolegade 3A
> 7100 Vejle
```

Anders kvittede senere med kort svar,

```
Hej Henrik

Tak for din mail.

Det notere jeg til sagen.

Det er jo desværre nok fremtiden :)

Med venlig hilsen

Anders Kxxxx Lxxxx
Politibetjent
```

I mine *abuse indbakker* som går tilbage til 2016 finder jeg under 10 tilsvarende emails fra politiet.

8.3 De alvorlige sager

Der er perspektiver ved at drive en Tor exit-server som ikke kan fejes til side med statistik og standardsvar. De kræver at man ser dem i øjnene.

Alvorlig kriminalitet foregår i verden. Det har det altid gjort. Så ligesom alle andre kommunikationsnetværk - telefonen, e-mailen, det åbne internet - bruges Tor også af en minoritet med kriminelle formål. Det mest alvorlige eksempel, og det der oftest fremhæves i den offentlige debat, er seksuelt misbrug af børn og deling af overgrebsbilleder - internationalt betegnet CSAM, *Child Sexual Abuse Material*.

Det er et emne jeg ikke kan eller vil forholde mig til på afstand. Som forælder selv er det ikke abstrakt. Det er virkeligt, det er alvorligt, og det er forbrydelser mod de mest sårbare.

Men netop fordi emnet er så alvorligt, er det vigtigt at forholde sig præcist til det - ikke emotionelt, men faktabaseret.

Tor-netværket er lille. Det er en kendsgerning der sjældent nævnes i de sammenhænge hvor Tor omtales som et fristed for kriminelle. Den samlede båndbredde og det samlede antal brugere på Tor er så beskedent sammenlignet med det åbne internet, at selv en overfladisk analyse viser at langt størstedelen af deling af overgrebsbilleder sker på helt almindelige platforme - lukkede grupper på sociale medier, krypterede beskedtjenester, fildelingstjenester. Ikke på Tor.

Det ændrer ikke ved at det sker på Tor også. Men det sætter det i proportion.

Betegnelser som *mørkenettet* og *the dark web* har fået et liv i medierne, der er løsrevet fra den tekniske virkelighed. Påstande som ‘‘størstedelen af trafikken på Tor er kriminel’’, ‘‘det er kun hackere der bruger det’’ eller den implicit og eksplicit fremsatte kobling mellem Tor-brug og pædofili - de er ikke underbyggede. De er udtryk for en forsimpling der tjener en bestemt fortælling, men som ikke holder stik over for kendsgerningerne.

Tor bruges primært af journalister, aktivister, whistleblowere, borgere under censur og mennesker der ønsker et privatliv på nettet. Det er dokumenteret af The Tor Project og understøttet af uafhængig forskning. Den kriminelle minoritet eksisterer - som den gør overalt på Internet - men den definerer ikke netværket.

Som exit-operatør har jeg ikke mulighed for at identificere eller blokere specifikt kriminelt indhold. Det er en konsekvens af det samme design der beskytter den iranske journalist og den danske whistleblower. Man kan ikke have den ene uden den anden. Det er et reelt dilemma - og det er ærligere at sige det højt end at lade som om det ikke eksisterer.

Kapitel 9

Når myndighederne banker på

9.1 Ransagningen

En af grundene til at jeg skriver denne bog er at den kan udgives med et ISBN-nummer som et trykt medie og dermed stå som et dokumenteret vidnesbyrd. Det følgende er et konkret eksempel på hvad det i praksis kan betyde at drive en Tor exit-server i Danmark.

I sommeren 2023 blev der ved Retten i Helsingør fremsat en anmodning om ransagning af min adresse - som er både min privatadresse og den adresse mit ApS er registreret på. Helsingør ret sagsnr. 9-2376/2023, politiets nr. 0900-72387-00258-22. Baggrunden var en sag om to billeder med CSAM indhold som en person havde uploadet til Bing Image Search - formentlig for at finde lignende materiale.

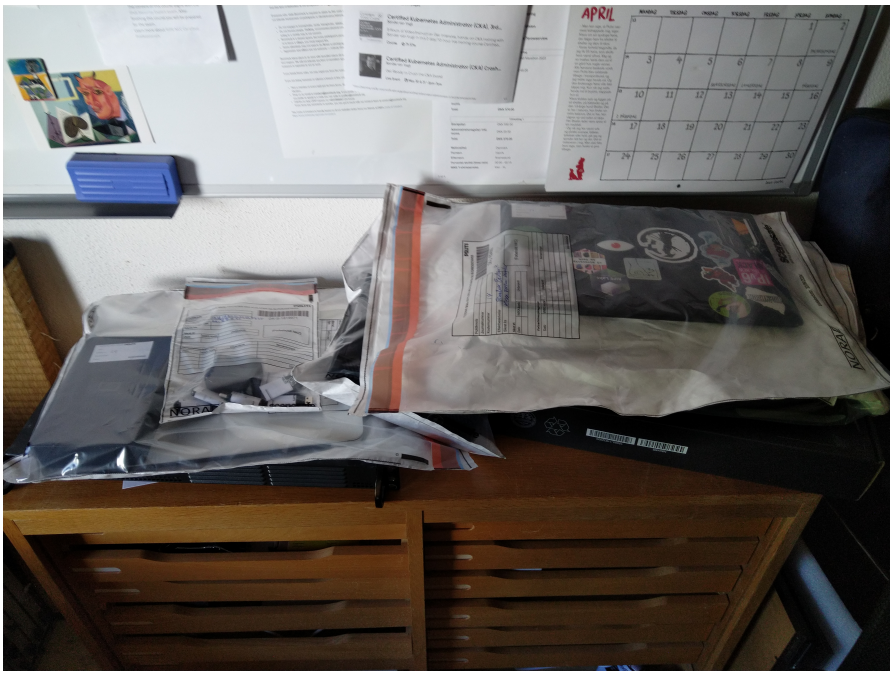
En dag hvor jeg ikke var hjemme dukkede politiet op. Uniformerede betjente og civile efterforskere - omkring fem personer i alt, en hel formiddag. Min ekskone var i huset og lukkede dem ind, som man jo ikke kan modsætte sig. Hun blev bedt om at udpege eget udstyr og dernæst gik de igang. Der var strenge ordrer om ikke at informere mig. Så jeg fandt først ud af det klokken cirka 15, da jeg kom hjem og stod med to A4-sider fra retten i hånden. Der var ikke engang kontaktoplysninger til efterforskerne på papirerne.

Der blev sat mærkater på en masse udstyr og noget blev samlet i bevisposer - men intet blev taget med. Det efterlader et spørgsmål jeg stadig ikke har et godt svar på: hvorfor brugte man fem personer i timevis på at gennemgå og mærke udstyr - for dernæst at efterlade det hele?

Jeg modtog ingen kvittering. Der var måske efterladt et visitkort, men hvor det er endt er uvist. Det er aldrig dukket op.

Figur 9.1: Effekt nr. 11 - Nordsjællands Politi. Mærkaten er udfyldt i hånden, journalnummer (JNR) og beskrivelse står tomme.

Figur 9.2: Fire bevisposer med udstyr sat i stand til beslaglæggelse - intet blev taget med. Laptop, tablet, USB sticks



Figur 9.3: Udstyr samlet i bevisposer på en reol i hjemmet - fotograferet samme eftermiddag 14. juni 2023.

9.2 Første samtale med Michael fra politiet

Jeg kontaktede Nordsjællands Politi, vagthavende var imødekommende og skabte kontakt til sagsbehandleren, efterforskeren Michael. Vi talte samme dag i telefon.

Jeg fortalte præcist hvem jeg var - direktør i et IT-sikkerhedsfirma, med mange IP-adresser registreret under mit CVR-nummer. Michael svarede at de vidste det godt - men oplyste stadig ikke den konkrete IP-adresse som mistanken vedrørte, på trods af at retsbogen eksplicit angav at ‘‘mistænkte er identificeret via sin IP-adresse.’’

Jeg fortalte Michael at jeg drev Tor exit-servere, da jeg naturligvis havde en klar formodning om at det kunne være forklaringen. Hans svar var utvetydigt: det drejede sig om min *hjemme-IP-adresse*.

Den oplysning satte gang i en uge der var svær for alle involverede. En hjemme-IP-adresse peger ikke på en server i et

datacenter - den peger på en husstand. På alle der havde haft adgang til netværket. På familiemedlemmer. Det er ikke en abstrakt juridisk skelnen. Det mærkes.

At min ekskone blev bedt om at udpege sit eget udstyr - for at adskille det fra mit - siger noget om grundigheden af forberedelserne til ransagningen. Der var mange spørgsmål den dag. Nogle af svarene har jeg fået siden, og de findes i dette skriv. Andre er stadig ubesvarede.

Kort tid efter fik jeg den konkrete IP-adresse oplyst. Det var ikke min hjemme-IP. Det var en af mine Tor exit-servere - med adressen `2a06:d380:0:103::62`. En adresse Michael havde haft adgang til at slå op fra første dag.

9.3 Hvad er en adresse

Inden vi fortsætter vil jeg dykke lidt ned i teknikken. Hidtil har meget været på et niveau hvor mange kender begreberne - men nu er vi nødt til at være enige om terminologien, for den er afgørende for at forstå hvad der faktisk skete.

Hvad menes der egentlig med ‘‘Mistænkte er identificeret via sin IP-adresse’’?

IP-adresser er ikke tilfældige tal - de er hierarkisk organiseret og tildelt gennem et internationalt system. Øverst sidder organisationen IANA, som har fordelt store adresseblokke til fem regionale organisationer kaldet Regional Internet Registries (RIRs) der tilsammen dækker hele verden.

For Europa, Mellemøsten og dele af Centralasien er det RIPE NCC med hjemsted i Nederlandene. Enhver virksomhed eller organisation kan blive medlem af RIPE NCC og dermed få tildelt og registreret egne IP-adresser. Når man gør det, bliver man det der hedder en Local Internet Registry - en LIR. Det er præcis hvad Zencurity ApS er. Vores adresser er registreret direkte hos RIPE NCC under firmaets navn.

En almindelig internetudbyder fungerer på samme måde - de er også LIR, og de uddeler adresser videre til deres slutkunder. Min hjemmeforbindelse var på tidspunktet for sagen leveret af en helt almindelig udbyder via TDC's fibernet. Den IP-adresse var registreret til udbyderens netværk. Jeg var så kunde hos den pågældende udbyder.

Det er altså to helt forskellige adresserum med to helt forskellige ejere og registreringer. Og alligevel endte politiet med at banke på den forkerte dør.

Der er en fundamental skelnen man bør gøre sig klart når man efterforsker via IP-adresser: er det et firma eller en privatperson der er tale om?

Mine Tor-servere kører på adresser registreret til Zencurity ApS - et firma med CVR-nummer, registreret adresse og offentlige kontaktoplysninger. Hvis politiet mente at den pågældende IP-adresse tilhørte Zencurity ApS, burde retsbogen have nævnt firmaet. Det gjorde den ikke. Den nævnte udelukkende mistænkte Henrik Kramselund og min privatadresse.

Man kan ikke på den ene side bruge en IP-adresse registreret til et firma som grundlag for en dom om ransagning - og på den anden side udstede dommen mod en privatperson på en privatadresse. De to ting hænger ikke sammen. Og det burde retten have opdaget.

9.4 IPv6 og et enkelt Whois-opslag

Her er det tekniske hjerte af sagen - og det er både alvorligt og en smule absurd.

Whois er en af Internettets ældste administrative tjenester - protokollen har været defineret siden 1982 og i Europa har den været brugt hos RIPE NCC siden 1990erne. Det giver enhver mulighed for at slå op hvem der administrerer netværket bag en given IP-adresse eller et domænenavn. Det kræver ingen særlige værktøjer og ingen adgangskode. Det er åbent og offentligt tilgængeligt - og det er præcis det redskab enhver efterforsker bør kende når en IP-adresse skal identificeres.

Et Whois-opslag på den pågældende IP-adresse tager under ti sekunder og det fulde Whois opslag står i sagen, men jeg har desværre ikke mulighed for at kopiere fra det.

Et opslag på mine Tor servere ser nogenlunde sådan ud - IPv6 og IPv4:

```
inet6num:       2a06:d380::/29
netname:        DK-ZENCURITY-20151130
country:        DK
org:            ORG-ZA135-RIPE
admin-c:        ZEN8-RIPE
tech-c:         ZEN8-RIPE
status:         ALLOCATED-BY-RIR
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         dk-zencurity-1-mnt
```

```
mnt-lower:      dk-zencurity-1-mnt
mnt-routes:     dk-zencurity-1-mnt
created:        2015-11-30T16:54:53Z
last-modified:  2021-02-17T16:34:30Z
source:         RIPE

inetnum:        185.129.62.0 - 185.129.62.255
netname:        SERVICE-NET1
descr:          Various servers including Tor servers
remarks:        This network includes Tor servers and we are sorry for any inconvenience
remarks:        We consider Tor a benefit for the internet even though some abuse will come through
remarks:        Contact abuse@zencurity.dk regarding abuse
country:        DK
admin-c:        ZEN8-RIPE
tech-c:         ZEN8-RIPE
status:         ASSIGNED PA
mnt-by:         dk-zencurity-1-mnt
created:        2015-12-17T06:18:18Z
last-modified:  2023-11-14T08:00:05Z
source:         RIPE
```

Politiet brugte en web Whois, og der ligger udskrifter fra denne i sagen.

I dag har jeg valgt at opdatere begge objekter i databasen for at gøre det endnu tydeligere at der er tale om to lokationer, datacenter og kontor:

```
inet6num:       2a06:d380::/29
netname:        DK-ZENCURITY-20151130
country:        DK
org:            ORG-ZA135-RIPE
remarks:        Data center: AdeoDC, Herstedvang 8, DK2620 Albertslund, Danmark
remarks:        Office: Lynghoejvej 26, DK3390 Hundested, Denmark
```

og samme for IPv4.

Note: De nævnte fysiske adresser er de nuværende, og jeg boede på en anden da sagen rullede. Den kan findes på CVR og mange andre steder. Adressen tilhører Zencurity ApS. Med fulde kontaktoplysninger, dansk adresse og en dedikeret abuse-kontakt. Alt hvad politiet behøvede at gøre var at køre én kommando - eller blot åbne en browser.

9.5 En doven efterforsker

Når man undersøger en IP-adresse og slår den op i Whois er man ikke færdig. Så er efterforskningen kun lige begyndt.

Der er mange whois oplysninger der ikke er opdateret, der er falske oplysninger, og det er et velkendt og udbredt problem som enhver erfaren efterforsker bør tage højde for.

I det her tilfælde peger mine IP-adresser på *rigtig information* - de pågældende IP-adresser er ganske rigtigt allokeret til mit firma/LIR med Reg ID hos RIPE NCC: dk.zencurity som er et firma med CVR, adresse i Danmark og en ejer.

Det er dog ingen garanti for at adresserne, allesammen eller dele benyttes i Danmark, jeg kan snildt vælge at drive min forretning fra et datacenter i Europa, så hvor mine adresser er aktive er kritisk.

Dernæst er selve ideen med en LIR, et firma, at drive forretning, så det er oftest kunderne der benytter servere bagved disse adresser.

9.6 Hvor findes serveren

Når man står med en IP-adresse og en bagvedliggende server bør man dykke dybere ned i hvor den pågældende server reelt findes. Specielt hvis man ønsker at lave en ransagning!

Måske bør de som minimum lave en traceroute, for at undersøge om en given IP-adresse ligger i Danmark eller udlandet. I mit tilfælde med mine tor servere har jeg gjort mit bedste for ikke at skjule hvor de er, men også gøre det tydeligt at de drives i et data center.

Traceroute er en funktion og et program som findes på alle PCer. Det viser med nogen nøjagtighed hvordan trafik i et netværk løber hen mod en IP-adresse. Det er et simpelt værktøj og viser ofte bynavne på centraler undervejs.

En kort traceroute fra en hjemme IP-forbindelse mod en Tor server med navnet tor01.zencurity.com kan ses nedenfor:

```
shito$ traceroute tor01.zencurity.com
traceroute to tor01.zencurity.com (185.129.62.62), 64 hops max, 40 byte packets
 1  46-32-xxx-xxx.static.kviknet.net (46.32.xxx.xxx)  2.129 ms  2.258 ms  2.706 ms
 2  taa9-edge1.kviknet.dk (185.107.12.126)  2.766 ms  2.623 ms  2.751 ms
 3  netnod-ix-cph-green-9000.globalconnect.dk (212.237.193.22)  2.683 ms  2.577 ms  2.776 ms
 4  lo1-cr1.hamb.gc-net.eu (77.243.32.5)  2.575 ms  2.51 ms  2.448 ms
 5  194.182.31.154 (194.182.31.154)  2.383 ms  2.525 ms  2.661 ms
 6  * * *
 7  185.150.199.178 (185.150.199.178)  2.631 ms  2.437 ms  2.591 ms
 8  tor01.zencurity.com (185.129.62.62)  2.267 ms  2.592 ms  2.513 ms
```

Den viser en omvej via Taastrup (taa9?) gennem Global Connect udstyr, et smut omkring Hamborg (hmb.gc-net.eu) som også er registreret med 194.182.31.154 og 185.150.199.178 er adressen på udstyr leveret af mit datacenter. Det datacenter ligger forøvrigt i Albertslund. Så vi er et smut fra Hundested, over Tyskland og tilbage til vestegnen omkring København. 60km fugleflugtslinie bliver en tur omkring Hamborg.

Specielt for denne sag er måske at min hjemme adresse på daværende tidspunkt blev servicereret af en helt almindelig internetudbyder. Jeg havde en fysisk fiberforbindelse gennem TDC fibernet og en ISP på deres netværk. Derfor var min hjemme IP-adresse registreret til et kundeforhold med en fysisk adresse som bestemt IKKE tilhører eller er registreret til mit firma! Så hvordan man kan ‘‘forveksle’’ mine IP adresser i datacenter og hjemme med hinanden er en gåde.

9.7 Moderne teknologi IPv6 fra 1990erne

Min vurdering er at IPv6-adressen var årsagen til forvirringen. IPv4-adresser er velkendte og ser ud som 192.0.2.0 - fire tal adskilt af punktummer. IPv6-adresser er nyere og skrives med hexadecimale tal og kolon, som `2a06:d380:0:103::62`. De er ikke sværere at slå op, men de ser anderledes ud - og det er tilsyneladende nok til at skabe usikkerhed hos efterforskere der ikke arbejder med dem dagligt.

Pudsigt og måske lidt illustrativt: heksadecimale tal har værdien 0 til 15, repræsenteret med cifrene 0-9 og bogstaverne a-f. Efterforskeren Michael læste adressen op som ‘‘2 lille a 0 6…’’ - hvilket viser at man kan læse en adresse op uden at forstå hvad man læser. Lille a og stort A er jo samme hexadecimale værdi.

IPv6 er ikke ny teknologi. Jeg arbejdede med det på IBM AIX-systemer i 1990’erne, hvor jeg kørte mine første `ping6 ::1` og traceroute kommandoer dengang adresserne stadig var eksperimentelle. Mit kandidatspeciale fra 2002 handlede netop om IPv6. Vi taler om en teknologi der har været i aktiv brug i mere end 20 år - omend udbredelsen i Danmark stadig halter bagefter hvad man kunne ønske.

At en efterforsker i 2023 ikke genkender en IPv6-adresse er derfor ikke et spørgsmål om ny eller svær teknologi. Det er et spørgsmål om forberedelse.

9.8 Erfaringer og overvejelser

Resultatet var fem politifolk i en hel formiddag og en ransagning af et privat hjem. Jeg var den mistænkte - hvilket i sig selv er tankevækkende, for hjemmet var delt med andre mennesker der havde samme adgang til internetforbindelsen. Den første telefonsamtale med Michael førte ikke til sigtelse - den førte til forvirring om hvilken IP-adresse der overhovedet var tale om.

En uge senere blev jeg sigtet - over telefonen. Først da fik jeg den konkrete adresse oplyst. Jeg forklarede at den tilhørte en Tor exit-server. Michael lød træt. Sagen kollapsede i løbet af den samme samtale.

Kort efter kom de officielle papirer i min e-boks. Jeg har ikke hørt mere til sagen.

Politiets besøg satte naturligvis tanker i gang. Juridisk genovervejer jeg regelmæssigt min rolle som Tor exit-operatør - ikke fordi jeg er i tvivl om lovligheden, men fordi det er det ansvarlige at gøre. Regler og praksis ændrer sig.

Operationelt reagerede jeg konstruktivt. Jeg har nu opdateret mine Whois-oplysninger for at gøre det endnu tydeligere hvem der driver infrastrukturen og hvor man henvender sig - datacenterets adresse, kontorets adresse, kontaktoplysninger. Sådan mere aktivistisk startede jeg som en slags aktiv modreaktion en tredje Tor exit-server.

Den bredere overvejelse er mere principiel. Med jævne mellemrum evaluerer jeg om det at drive Tor exit reelt hjælper Internet og verden - uanset at der sker misbrug. Faktisk er misbrug i sig selv et nuanceret begreb. Det der betragtes som kriminelt afhænger af hvilken stat der kigger. At give borgere adgang til frie nyhedsmedier er en grundlæggende ret i Danmark. I andre lande er det en forbrydelse. Tor-netværket er det samme netværk i begge tilfælde.

Ét politibesøg, én kort sag, over mere end ti år som operatør. Den balance har fået mig til at fortsætte.

Til information findes der mere end 200 definitioner af hvad terror er, og terrorlisterne i forskellige lande er ikke et samlet register - de afhænger af hvem magthaverne er. Det der er frihedskæmper ét sted, er terrorist et andet. Tor-netværket skelner ikke.

Kapitel 10

Politiets og Retternes arbejde

Jeg drømte som barn om at blive politimand, fortæller min mor fra tid til anden. Min storebror og jeg skulle være motorcykelbetjente. Det er dog mange år siden, og den drøm forsvandt efterhånden som jeg blev ældre - og heldigvis.

Der er ikke i min optik ret meget godt at sige om det danske politi. Det er et negativt billede jeg har af dem. Der er så mange møgsager omkring vold, manglende ageren i reelle sager. Hertil kommer embedsmisbrug, korruptionssager og statslig indblanding i eksempelvis Tibetsagen. Selv højtrangerede politifolk er anklaget og dømt, men ofte er det meget milde straffe. Der er sågar reel stalking med misbrug af registre, opslag i data som ikke har noget med politiets arbejde at gøre.

Hvis man ikke fjerner de dårlige æbler, er allesammen at betragte som rådne. Alternativt må vi snakke om hvilke værktøjer de skal have til rådighed. Jeg har været opmærksom på at selv politifolk har svært ved at styre nysgerrigheden siden ihvertfald 2003. Det var nemlig deromkring at mordet på Anna Lindh skete i Sverige. Der var massiv politiindsats, men det kom efterfølgende frem at der var misbrugt adgange og data i stor stil - af politifolk!

Der er nok mange der vil være uenige, men jeg synes det er fair at fokusere på de steder hvor politiet gør fejl og forbedre sagernes tilstand. Et sted man kunne starte var eksempelvis hos Den Uafhængige Politiklagemyndighed (Politiklage-myndigheden) - det burde være muligt at identificere flere som overtræder reglerne, og det er nødvendigt at det får konsekvenser!

En af de nylige sager fortæller om hvordan kriminelle med bestikkelse, penge til ansatte, kunne få slået data op i politiets registre. Det ledte heldigvis til dom og straf, men ofte sker det ikke. Så selvom vi stoler på politiet, er det allerede ved opsamlingen af data at vi risikerer misbrug.

I de konkrete sager med Tor, som omhandler trafik der har passeret mine servere, er det jo sager der involverer mig. Det involverer også andre områder at IT, netværk og sikkerhed hvor jeg har +30 års erfaring. Pudsigt nok har jeg også i de mange år været i kontakt med netop politifolk i flere sammenhænge, endda uddannet nogle stykker indenfor de emner.

I relation til mine Tor servere har der også løbende været flere sager, hvor jeg er blevet kontaktet af politiet, og der er sager hvor jeg ikke er kontaktet. Jeg ville ønske politiet indenfor egne rækker vidste mere om Tor generelt.

10.1 Aktindsigten

Næsten to år efter ransagningen søgte jeg aktindsigt i sagen med politiets nr. 0900-72387-00258-22. Det skete den 7. oktober 2025 - og det var ikke en sag jeg bare kunne få tilsendt digitalt eller pr. post. Svaret fra Nordsjællands Politi var at aktindsigt ville kunne ske ved gennemsyn hos dem. Fysisk fremmøde. Med opsyn.

Afgørelsen ses her - men det er værd at læse den grundigt, for den siger også noget om systemet:

> Afgørelse
>
> Vi kan imødekomme din anmodning om aktindsigt i sagens dokumenter.
>
> Aktindsigt vil kunne ske ved gennemsyn af akterne hos Nordsjællands Politi, Prøvestensvej 1, 3000 Helsingør.
>
> Det bemærkes, at retten til aktindsigt ikke omfatter personnumre. Personnumre er derfor undtaget fra sagen. Dette følger af retsplejelovens paragraf 729 d, stk. 8.
>
> Det bemærkes endvidere, at interne dokumenter er undtaget fra retten til aktindsigt, jf. retsplejelovens paragraf 729 d, stk. 2. Vi har derfor valgt at undtage interne dokumenter.

Endvidere skete det under strenge regler:

> En medarbejder fra Advokaturen for Kvalitet og Udvikling vil holde opsyn under gennemsynet. Det er ikke tilladt under gennemsynet at afskrive, udtage eller affotografere dokumenter eller på lignende måde hjemtage dele af sagen.

Man fik altså lov til at læse om sig selv - men ikke til at tage noget med hjem. Ikke en fotokopi, ikke et billede, ikke en afskrift. Noget af det følgende er derfor rekonstrueret fra noter skrevet umiddelbart efter besøget.

10.2 Aktindsigt ved gennemsyn

Den 12. maj 2026 mødte jeg således op på politistationen.

En medarbejder - tilsyneladende en studerende - tog imod mig og fulgte mig til et mødelokale. På bordet lå en medium stak papirer i et blåt omslag. Reglerne for hvad jeg ikke måtte blev gentaget.

Det som følger er rekonstrueret fra noter skrevet umiddelbart efter besøget. Hvis du kære læser tilfældigvis er ansat i politiet eller har adgang til disse registre, giver jeg dig hermed samtykke til at slå sagerne op om min person.

Sagen tog sin begyndelse den 11. maj 2022 med en henvendelse fra USA: der var fundet et positivt match for CSAM i en af myndighedernes databaser med misbrugsmateriale. Dansk politi fik henvendelsen via NCMEC og begyndte efterforskning - reelt ca. otte måneder senere, i 2023. De lavede et Whois-opslag på IP-adressen og fandt Zencurity ApS. Dernæst et opslag i firmaoplysninger, sandsynligvis på proff.dk.

På den baggrund besluttede efterforskeren - efter at have rådført sig med mindst en kollega - at *besøge mig* med en ransagning 14. juni 2023. Det var dokumenteret i en ransagningsrapport. Bemærk at hvis jeg husker datoerne rigtigt er der således også gået mere end et år fra forbrydelsen til ransagningen!

10.3 Ransagningsrapporten

Rapporten fortalte sin egen historie - og den passede ikke helt med virkeligheden.

Ifølge papirerne havde politiet holdt sig til forkontor og kontor. Men udstyr var fremfundet andre steder i huset - blandt andet en tablet og en 4G router fra første sal. Der var påsat mærkater på et bredt udvalg: PC-systemer, laptops, switche, tablets, USB-sticks. Ret mange.

De ankom først som to, derefter to mere, og en femte stødte til undervejs. Et sted i dokumentet stod der noget i stil med følgende beskrivelse af situationen: ‘‘det oversteg deres IT-kompetencer’’. Det er en bemærkelsesværdig formulering - men jeg har også en del forskelligt udstyr hjemme. Herunder en lille server der fungerer som virtualiseringsplatform og som stod tændt.

Intet udstyr blev slukket. Det er formentlig ikke tilfældigt. Inden for computer forensics - den disciplin der handler om at sikre digitale beviser - er det grundlæggende princip at tændt udstyr ikke slukkes, fordi computerens arbejdshukommelse indeholder flygtige data der forsvinder ved strømafbrud. Passwords, krypteringsnøgler, aktive forbindelser - alt det kan i princippet udlæses fra RAM på en kørende maskine, men er borte for altid når den slukkes. Det kræver specialudstyr og viden at gøre det, men princippet er velkendt. At de ikke slukkede noget tyder på at de i hvert fald kendte den grundregel.

Ransagningen stoppede da de fik besked fra centralt hold om at lade alting være. Jeg kender ikke den præcise rækkefølge, men antager at de ringede for at rådføre sig - og at svaret var at stoppe.

Jeg ved ikke om de ville have taget mere med hvis de ikke var blevet stoppet. Alt var pakket og mærket - klar til beslaglæggelse. Hvad det ville have betydet for mit arbejde er svært at sige. En del af udstyret bruges dagligt i min forretning. Men det er en hypotetisk situation, og jeg nøjes med at konstatere at intet faktisk blev taget.

10.4 En klar fiasko

Jeg betragter forløbet som en fiasko på flere fronter - og har svært ved ikke at kalde det for fejl:

Flere politifolk havde været indover sagen, og der er referencer til NC3 som kendte til Henrik, altså mig. Jeg har undervist politifolk adskillige gange i min karriere, og mine Tor-servere har kørt i årevis - åbent og registreret.

Man vurderede at det gav mening at ransage en adresse på jagt efter en Tor exit-server - en server der af design og natur aldrig indeholder brugbart data. Tor er nævnt gentagne gange i sagens dokumenter.

Af ukendte grunde antog man at jeg kørte Tor-serveren hjemmefra. Det er aldrig en god idé. Det er ikke noget man normalt gør med en exit-server. Det burde et bedre efterforskningsarbejde have afsløret fra starten.

10.5 Udlevering af dokumenter - nægtes

Under gennemsynet anmodede jeg om kopi af fire dokumenter:

- Forhold 1, bilag 1 (anmeldelsesrapport).
- Forhold 1, bilag 6 (rapport indledende efterforskning).
- Forhold 1, bilag 7 (rapport ransagningsrapport).
- Forhold 1 bilag 10-2 (rapports kontakt NC3).

Anmodningen blev afslået med besked i e-boks kort efter.

10.6 Sagen fra 2020?!

Undervejs i gennemsynet stødte jeg på noget uventet - en anden sag, nævnt ved nummer, som lå tilbage i 2020. Den var en stor overraskelse at læse. Jeg vidste slet ikke at jeg havde været genstand for en undersøgelse.

Desværre var det en trist affære at læse sagen og hvilke data der var samlet, hvad der var opsummeret på de få sider.

Den gamle sag havde afsender Telia og drejede sig om chat mellem to profiler nævnt ved profilnavn. Ingen af de to profilnavne gav anledning til at forbinde dem med mig. Der var intet der pegede på mig eller mit firma - kun en IP-adresse, 185.129.62.63, der tilhørte en af mine Tor-servere.

Samme fejlantagelse var allerede cementeret : at jeg drev Tor exit-server hjemmefra, denne gang på min adresse på Amager. Der stod at man havde overvejet ransagning. Flere personer havde været indover sagen, og der havde været tale om overvågning. Rigspolitiet NC3 var kontaktet. Et sted stod der noget i stil med at Tor er en blindgyde efterforskningsmæssigt. Det vidste man altså allerede i 2020.

Jeg har aldrig fået oplyst at denne sag eksisterede. Det var en ubehagelig opdagelse. Mit bedste gæt er at 2020-sagen kan have bidraget til at man i 2023 mente der nu var grundlag for en ransagning - at to sager med samme IP-adresse vejede tungere end én.

Selvom du føler du er paranoid, kan det være at nogen overvejer at overvåge dig. Jeg formoder ikke de iværksatte overvågning. Men det er en ubehagelig tanke. Der er naturligvis søgt aktindsigt også i denne sag, men formoder ikke det giver nye oplysninger af betydning.

10.7 Hvad skal Retten i Helsingør gøre

Jeg er ikke jurist. Men jeg har en holdning.

En ret der godkender en ransagning eller overvågning bør sikre at det sker det rette sted - helt konkret og fysisk: hvem er det rettet imod, og hvor. Er det et firma eller en privatperson? Er det et datacenter eller et hjem? Det er ikke detaljer - det er fundamentet for hele indgrebet.

Dernæst bør retten kræve dokumentation for mistanken. Hvad er beviset? Hvad er undersøgt, og hvad er ikke? I et retssamfund skylder staten borgeren en forklaring - ikke bare en tilladelse stemplet og underskrevet.

I det pågældende tilfælde kom politiet med hovedet under armen. De bad om tilladelse til at ransage et privat hjem på baggrund af en IP-adresse tilhørende et firma de ikke havde undersøgt til bunds. Det er minimalt hvad der var udført af forarbejde - og retten godkendte det alligevel.

Efter min mening burde kravet til dokumentation fra politiet, samt den dokumentation som skrives ind i retsbogen være mere klar og tydelig.

Havde retsbogen blot indeholdt den konkrete IP-adresse der lå til grund for afgørelsen, havde jeg straks kunnet afmystificere sagen. Det tog én telefonsamtale at afklare hvad simpel efterforskning ville have vist fra starten.

Det burde retten have krævet, inden de gav carte blanche til at banke på og vade ind. Det gjorde den ikke.

10.8 Krav til ransagning

Lad os se på hvad loven rent faktisk kræver. Reglerne om ransagning findes i retsplejelovens kapitel 73, særligt paragraf 794. To betingelser skal begge være opfyldt:

Mistankekravet. Den pågældende skal med rimelig grund være mistænkt for en lovovertrædelse undergivet offentlig påtale. Det er mere end en fornemmelse - der skal være konkrete, objektive holdepunkter. For ransagning af en bolig skal lovovertrædelsen desuden kunne medføre fængselsstraf.

Her mener jeg politiet grundlæggende misser hvordan IP-adresser registreret til en udbyder eller virksomhed faktisk bruges. I retsbogen står:

> ''Mistænkte er identificeret via sin IP-adresse.''
> Kilde: Udskrift af retsbogen Rettens nr. 9-2376/2023 Politiets nr. 0900-72387-00258-22

Kort, men upræcist. Gennem aktindsigten ved jeg nu hvad der lå til grund: et opslag i WHOIS og CVR-registret. Intet i de oplysninger koblede den pågældende IP-adresse til min fysiske hjemmeadresse. Den IP-adresse sagen handlede om er aktiv i et datacenter i Albertslund. Min hjemme-IP-adresse gik gennem en TDC-fiberforbindelse med en anden udbyder i Nordsjælland. Identificeret er løst formuleret - det er en konklusion der ikke følger af det fremlagte grundlag.

Indikationskravet. Ransagningen skal antages at være af væsentlig betydning for efterforskningen - der skal med andre ord være bestemte grunde til at tro at den konkret vil give noget.

Det sidste krav er særligt interessant i min sag. Som tidligere nævnt gentagne gange, en Tor exit-server indeholder per design ingen brugbare data om hvem der har brugt den. Det er ikke en tilfældighed - det er hele arkitekturen bag Tor. Der er intet at finde. Der har aldrig været noget at finde.

Hvis man accepterer præmissen om at jeg drev en Tor exit-server hjemmefra, bliver det endnu mere absurd. En Tor-bruger sender sin trafik gennem tre servere netop for at skjule sin identitet. Teorien ville kræve at jeg var kyndig nok til at drive en exit-server - men samtidig så uduelig at jeg sendte min anonymiserede trafik gennem to servere ude i verden og tilbage til min egen server på min egen internetforbindelse. Det giver ikke mening.

Indikationskravet burde have afskåret ransagningen fra starten. Retten burde have spurgt: hvad forventer I konkret at finde? Og hvad er grunden til at tro det befinder sig der?

I stedet ligner det at politiets anmodning er en standardiseret tekst med de juridisk korrekte ord - men uden at specificere hvad man præcist søger efter:

> Det er i den forbindelse Nordsjællands Politis vurdering, at en ransagning vil være af væsentlig betydning for sagen, idet der er bestemte grunde til at antage, at der ved ransagning kan findes genstande, som vil kunne tjene som bevis i sagen i form af telefon, computer og lagringsenheder.

og

> Politiet må foretage ransagning af lejlighed, andre lokaliteter eller genstande, herunder mobiltelefoner, computere og elektroniske enheder til lagring hos Henrik Kramselund på adressen ….

Man havde ikke engang udskiftet lejlighed med hus. Alligevel sendte man fem mand ud på adressen i timevis.

10.9 Hvad skal politiet gøre

De bør være dygtige nok til at genkende et værktøj der har været i brug i mere end 20 år.

De bør kunne finde ud af hvor en service reelt leveres fra - hvilket land, hvilken by, hvilket datacenter.

De bør kende forskel på en Tor exit-server i et professionelt datacenter og en server i et privat hjem.

De bør vide at en Tor exit-server per design ikke indeholder brugbare data - og at en ransagning derfor er spild af ressourcer, tid og borgernes tillid.

Jeg har siden 2010 haft kontakt med politiet i flere lande i forbindelse med mine servere. Svaret har hver gang været det samme. Det er ikke kompliceret. Men det kræver at man ved hvad Tor er.

Basalt set: de bør efterforske sagerne effektivt. Det gør de ikke i dag - i hvert fald ikke i sager som denne. Det er ikke et spørgsmål om ressourcer eller vilje. Det er et spørgsmål om viden og metode.

En ransagning der bygger på et Whois-opslag og et CVR-tjek - uden traceroute, uden kontakt til operatøren, uden at afklare om IP-adressen overhovedet er aktiv på den pågældende adresse - er ikke efterforskning. Det er en gætteleg med et magtmiddel.

Vi kan ikke som samfund acceptere at borgere ransages på så løst et grundlag. Det koster tillid.

10.10 Er det chikane eller inkompetence

Når jeg forsøger at forklare ovenstående med god vilje og åbent sind, har jeg svært ved at nå frem til en flatterende konklusion om politiets arbejde. Det er inkompetent, på grænsen til at jeg tror det er chikane.

En Tor exit-server er aldrig et oplagt mål for en ransagning. Det ved enhver der har sat sig ind i hvordan Tor fungerer. Serveren har ingen viden om hvem der har brugt den. Der er intet at finde. Det er spild af alles tid - og det står der tilmed allerede i politiets egne dokumenter.

Tor softwaren er bygget med kryptografiske værktøjer, opdateres løbende og der gøres en stor indsats for at beskytte brugerne. Det betyder at hvis man forsøger at hente data om brugerne møder mange forhindringer.

Jeg havde hørt og læst historierne om tysk politi der mødte op hos Tor-operatører tidligt om morgenen. Alexander Janssen opgav sin server. Foreningen Artikel 5 eV blev også ransaget to gange. Nu skete noget lignende i Danmark.

Så hvad er forklaringen? Enten ved man ikke hvad man laver. Eller også ved man præcis hvad man laver.

Hvad vil du helst tro på?

Kan det være at det er en torn i øjet på deres efterforskning som de er trætte af?

Ønsker man et skræmme borgere fra at udøve deres menneskeret til privatliv?

Kapitel 11

Journalister og aktivister - hvem har brug for Tor

11.1 De fire apokalyptiske ryttere

Når politikere, embedsmænd og medier skal begrunde hvorfor kryptering og anonymiseringsværktøjer er farlige, vender de igen og igen tilbage til de samme eksempler. Hvad der i fagmiljøet er blevet kaldt *the Four Horsemen of the Infocalypse* - de fire apokalyptiske ryttere der altid stilles frem når nogen vil begrænse digital frihed.

Der er lidt forskellige udgaver, men i nyere tid har eksempelvis aktivisten Cory Doctorow brugt ‘‘software pirates, organized crime, child pornographers, and terrorists’’. Kilde: https://en.wikipedia.org/wiki/Four_Horsemen_of_the_Infocalypse

Børn, og beskyttelse af børn har således gennem årtier været spydspids for drakoniske forslag om begrænsning af ytringsfrihed og indførelse af overvågning - og det fortsætter idag. Se bare chatcontrol som forsøges indført ved at henvise til børnene! ‘‘Tænk på børnene!’’ - nu en kliché men bruges aktivt gennem årtier.

Chatkontrol er et godt eksempel på hvordan ‘‘tænk på børnene’’-argumentet bruges til at presse lovgivning igennem som ellers ikke ville have flertal. EU-Kommissionen har siden 2022 forsøgt at indføre obligatorisk masseovervågning af private beskeder - angiveligt for at bekæmpe deling af overgrebsbilleder af børn.

Det parlamentariske forløb er sigende. I marts 2026 stemte Europa-Parlamentet med 311 stemmer mod 228 for at afvise forslaget. Det burde have været slut. Men ved en proceduremæssig manøvre blev lovforslaget genoplivet og sat til afstemning igen den 9. juli 2026 - sidste dag før sommerferien. Ved andenbehandling kræver afvisning et absolut flertal af alle MEP’er: 361 stemmer. Af de 607 MEP’er der stemte, stemte 314 for at afvise loven - et klart flertal af de tilstedeværende. De manglede 47 stemmer for at nå de krævede 361, og loven passerede derfor per default. Flertallet stemte nej. Loven vedtages alligevel.

Så mønsteret er at man bliver ved til det lykkedes, i denne sag er tidslinien - Chat Control - vigtigste afstemninger:

- August 2021 - Chat Control 1.0 (frivillig scanning) vedtages som midlertidig undtagelse, udløber august 2024
- Maj 2022 - EU-Kommissionen fremsætter Chat Control 2.0 forslaget
- November 2023 - Europa-Parlamentets LIBE-komité stemmer for at blokere masseovervågning og beskytte kryptering
- April 2024 - Chat Control 1.0 forlænges til april 2026 da 2.0 ikke er vedtaget
- Juni 2024 - COREPER-afstemning i Rådet fejler - intet flertal for obligatorisk scanning
- Oktober 2025 - Danmark som rådsformandskab forsøger at presse det igennem - Tyskland og Luxembourg danner blokerende mindretal
- 26. marts 2026 - Parlamentet stemmer 311-228 for at afvise forlængelse
- 9. juli 2026 - Anden afstemning - **314 mod 276, men loven vedtages pga proceduren**

Hvem er det som ønsker kontrol, og kontrol med hvad? eller hvem?

EU-Kommissionens egen evalueringsrapport fra 2025 viser at 48 % af de indberettede chats til tysk politi var kriminelt irrelevante, og at omkring 40 % af efterforskningerne endte med at ramme teenagere for frivillig sexting. Systemet der skulle beskytte børn kriminaliserer dem i stedet.

Logikken er simpel og effektiv: hvis du forsvarer kryptering eller Tor, forsvarer du også det allerværste. Det er et retorisk greb der har fungeret mange gange siden PGP-krypteringen i begyndelsen af 1990'erne, da Phil Zimmermann udgav sit gratis krypteringsprogram og prompte blev efterforsket af det amerikanske justitsministerium. Det gjorde ham altså til genstand for en tre år lang federal efterforskning. Han blev aldrig tiltalt.

Logikken var den samme dengang: stærk kryptering til alle er en gave til fjenden.

Men logikken holder ikke. Brevhemmelighed beskytter også kriminelle. Et telefonsystem der ikke kan aflyttes ulovligt beskytter også kriminelle. Infrastruktur er ikke neutral - men den er heller ikke ond fordi nogen misbruger den.

11.2 Crypto Wars

Dette har givet anledning til begrebet *Crypto Wars* som har været en regelmæssig diskussion mellem frihed til at kryptere, privatliv og staters mulighed for at begrænse brugen af stærk kryptering. Specielt USA har med eksport regulering forsøgt at begrænse udbredelsen af krypteringssoftware.

> The controversy unofficially dubbed the ''Crypto Wars'' involves attempts by the United States (US) and allied governments to limit access to cryptography strong enough to thwart decryption by national intelligence agencies, especially the National Security Agency (NSA), and the response to protect digital rights by privacy advocates and civil libertarians.[1][2]

Kilde: https://en.wikipedia.org/wiki/Crypto_Wars

Selvom kampene først fik navnet senere har der helt tilbage fra 1970erne været diskussioner om hvem der måtte beskytte data med kryptering, først kommercielle virksomheder, men sidenhen også privates brug af stærk kryptering.

NSA forsøgte allerede i 1970'erne at begrænse civil kryptografiforskning ved at lægge hemmeligholdelsesordrer på patentansøgninger og presse universiteter til at stoppe publicering. Da IBM udviklede krypteringsstandarden DES i 1974 med 112-bit nøgler, endte den efter NSA's *evaluering* med kun 56-bit - svag nok til at efterretningstjenester kunne bryde den.

I 1980'erne var der åben strid i NATO om hvorvidt GSM-mobiltelefoni overhovedet måtte bruge stærk kryptering. Sikkerhedsforsker Ross Anderson rapporterede i 1994 at der havde været en ''voldsom strid'' mellem NATO's efterretningssignaltjenester om netop det spørgsmål i midten af 1980'erne - og at resultatet var et kompromis der bevidst svækkede krypteringen.

Højdepunktet kom i 1990'erne med Clipper Chip - en NSA-designet chip med en indbygget bagdør som den amerikanske regering forsøgte at tvinge telefonproducenter til at adoptere. Det mislykkedes. Kort efter kom Phil Zimmermanns PGP - og den føderale efterforskning af ham.

Vi har altså haft denne diskussion i årtier, og den er ikke slut.

11.3 Polippix og den danske debat

Danmark har haft sin egen version af denne debat. I 2006 udgav IT-Politisk Forening i samarbejde med fagforeningen PROSA en CD-ROM kaldet *Polippix* - et værktøj der gjorde det muligt for brugeren at surfe anonymt og beskytte sit privatliv. Cirka 12.000 eksemplarer blev distribueret med PROSAs medlemsblad.

Reaktionen fra daværende justitsminister Lene Espersen var prompt. Hun udtalte til TV 2 at Polippix var en hjælp til kriminelle såsom pædofile og mordere.

Det er en bemærkelsesværdig udtalelse. Ikke fordi bekymringen for kriminalitet er illegitim - det er den ikke. Men fordi den sætter lighedstegn mellem et lovligt privatlivsværktøj og de værste forbrydelser man kan forestille sig. Det er præcis den samme logik som *the Four Horsemen* - og det er en logik der, hvis den følges til sin konsekvens, betyder at ingen bør have ret til privatliv overhovedet.

Polippix var lovlig, sammensat udelukkende af open source-programmer. Det var ikke et hackingværktøj. Det var en CD med software til anonymt internet brug - det samme som Tor giver adgang til i dag.

11.4 Hvem har egentlig brug for Tor

Min holdning er jordbundet og hverdagsagtig. Alle har behov for et vist mål af privatliv - ikke fordi vi har noget at skjule, men fordi privatliv er en forudsætning for at være et frit menneske. Vi lukker ikke alle vores vinduer op og inviterer staten indenfor i vores hjem. Vi hvisker ikke altid. Vi skriver breve i lukkede kuverter.

Det digitale rum bør ikke være anderledes.

Men lad os også tale om de konkrete brugergrupper der i særlig grad er afhængige af Tor.

Journalister og kilder. En journalist der arbejder med følsomme historier har brug for at kommunikere sikkert med sine kilder. En kilde der videregiver oplysninger om korruption, overgreb eller magtmisbrug har brug for anonymitet - ikke fordi det er ulovligt, men fordi det kan koste dem deres job, deres frihed eller i yderste konsekvens deres liv. Tor er et af de få tekniske værktøjer der kan give denne beskyttelse.

Aktivister under autoritære regimer. I lande som Iran, Kina, Rusland og USA er Tor ikke et privatlivs-nicheprodukt. Det er adgang til et frit internet. Det er muligheden for at organisere sig, kommunikere og modtage information uden at staten ser med. For disse brugere er Tor ikke et valg - det er en nødvendighed.

Whistleblowere. Edward Snowden brugte Tor. De medier der modtog hans dokumenter brugte Tor. Det er ikke en tilfældighed. Tor er en del af den infrastruktur der muliggør at oplysninger af almen interesse kan komme frem uden at kilden kan identificeres og straffes. Der findes speciel software som SecureDrop der kan benyttes af eksempelvis medier til at modtage anonyme tip fra whistleblowere.

Stalkingofre og partnervolds-ramte. For mennesker der flygter fra en voldelig partner eller en stalker er digital anonymitet ikke et spørgsmål om principper - det er et spørgsmål om fysisk sikkerhed. En IP-adresse kan afsløre en geografisk placering. En søgning på et krisecenter, en advokat eller en flugtrute kan i hænderne på den forkerte person betyde at offeret bliver fundet. Tor giver disse mennesker mulighed for at søge hjælp, orientere sig og planlægge uden at efterlade spor der kan bruges imod dem. Det er måske den brugergruppe der oftest glemmes i debatten om anonymitet på nettet - og en af dem der har mest brug for det.

Helt almindelige borgere. Og så er der alle de andre. Mennesker der ikke ønsker at deres internetudbyder sælger data om deres adfærd. Mennesker i lande med masseovervågning der bare vil søge på nettet uden at efterlade spor. Folk der ikke er kriminelle, ikke er aktivister, ikke er journalister - men som synes at retten til at færdes privat på Internet burde være en selvfølge.

Ingen af dem har gjort noget forkert. De vil bare have lov til at være sig selv - uden at nogen kigger med.

Det er ikke bare en rimelig forventning - det er en rettighed. Privatliv er beskyttet af Den Europæiske Menneskerettighedskonvention, vedtaget af Europarådet i 1950 og inkorporeret i dansk lovgivning i 1992. Danske domstole har pligt til at håndhæve den. Det betyder at retten til privatliv ikke er noget staten giver dig - det er noget staten er forpligtet til at beskytte.

Et konkret eksempel fra USA illustrerer hvor hurtigt ‘‘almindelig’’ information kan blive farlig afhængigt af hvor man befinder sig. Efter Højesterets Dobbs-afgørelse i 2022 afskaffede en række amerikanske stater retten til abort og kriminaliserede medvirken hertil. Det betyder at en kvinde der søger information om abort online, en læge der vejleder over telefonen, eller en person der hjælper med at finansiere en rejse til en anden stat - alle potentielt kan efterforskes og straffes. Myndighederne i disse stater har aktivt efterspurgt lokationsdata og søgehistorik fra tech-virksomheder som bevis i sager.

I Danmark taler vi åbent om abort. Det er en rettighed vi tager for givet. Men det digitale spor du efterlader når du søger på nettet kender ingen grænser - og data indsamlet i dag kan bruges i en retssag i morgen, i en anden stat, under en anden lov.

Det er ikke et hypotetisk scenarie. Det sker.

Kapitel 12

Overvågning, censur og modmagt

12.1 Før og efter 9/11

Presset mod kryptering og anonymiseringsværktøjer har eksisteret så længe de har eksisteret. Men det er accelereret markant efter terrorangrebene den 11. september 2001. I Danmark betød det antiterrorpakker, udvidede overvågningsbeføjelser og en politisk stemning hvor sikkerhed og frihed igen og igen blev præsenteret som et nulsumsspil: mere af det ene er automatisk mindre af det andet.

Det er en falsk præmis. Masseovervågning af alle borgere er ikke et effektivt redskab mod en lille gruppe kriminelle. Det er et redskab mod den brede befolkning - og det er staten der vinder, ikke sikkerheden.

At drive Tor servere er idag en modstand imod det pres. Ikke det eneste, ikke det perfekte - men et konkret, teknisk svar på et konkret, politisk problem. For den sikkerhedsbevidste internet bruger er det at bruge Tor også en tydelig måde at begrænse data der kan opsamles.

Det er derfor jeg driver det, og det er værd at kæmpe for.

12.2 Verden set fra en exit-server

Når man driver en Tor exit-server over mange år, får man et særligt perspektiv på verden. Man ser ikke indholdet af trafikken - men man ser mønstrene. Man mærker når noget sker.

I Tyrkiet har præsident Erdogan gentagne gange forsøgt at begrænse adgangen til sociale medier og uafhængige nyhedsmedier. Censuren har været så konsekvent at borgere begyndte at skrive IP-adresser på alternative DNS-servere som graffiti på husmure - en analog løsning på et digitalt problem, og et stærkt billede på hvad der sker når staten forsøger at kontrollere informationsstrømmen. I Myanmar, Tunesien og en lang række andre lande har Tor spillet en direkte rolle i at give borgere adgang til et frit internet under politiske kriser og militærkup.

Det arabiske forår er et andet eksempel. De folkelige opstande i 2011 var tæt forbundet med sociale medier - og dermed også med platforme der kan lukkes ned. Da myndighederne blokerede adgangen til Facebook og Twitter, søgte mange borgere alternative veje. Det illustrerer noget vigtigt: vi er i stigende grad afhængige af private platforme til vores offentlige kommunikation, og de platforme kan begrænse adgang - enten på myndighedernes opfordring eller af egne kommercielle årsager. Det er en af grundene til at jeg mener at Tor er nødvendigt. Ikke som et alternativ til det åbne internet, men som en sikkerhedsventil når det åbne internet lukker sig.

12.3 Danmark og Europa - ikke så langt fra

Det er let at pege på Tyrkiet, Myanmar og Kina. Det er sværere - men vigtigere - at pege på sig selv.

Danmark og Europa er ikke immune over for de samme tendenser. Vi bevæger os, om end langsommere og mere diskret, i en retning der bør bekymre enhver der holder af frihed og retsstat.

I Danmark har der været alvorlige sager hvor politiet og PET har haft adgang til data om borgere som de ikke burde have haft. Den politiske reaktion har i flere tilfælde ikke været at sætte grænser for efterretningstjenesterne - men at ændre loven med tilbagevirkende kraft, så adgangen blev lovlig. Uden en bred demokratisk diskussion. Uden proportionalitetsvurdering.

Det seneste eksempel er L 218 (2024-25) - *Forslag til lov om ændring af lov om Politiets Efterretningstjeneste (PET) - Understøttelse af PETs mulighed for at udføre data- og analysebaseret efterretningsvirksomhed m.v.*, fremsat 25. april

2025. Institut for Menneskerettigheder har kaldt det et paradigmeskift i den måde PET indsamler data om borgere på. Med lovforslaget lægges der op til en markant udvidelse af efterretningstjenestens muligheder for at masseindsamle og analysere data om helt almindelige borgere - uden konkret mistanke og uden domstolskontrol. Som Institut for Menneskerettigheder formulerede det under høringen i Folketinget: PET tildeles meget vidtgående beføjelser, og der følger ikke de nødvendige retsgarantier med.

Hvis politiet og PET mener de har brug for disse beføjelser, er det en diskussion vi skal have - åbent, demokratisk og inden loven vedtages. Det er ikke et spørgsmål om at være for eller imod efterretningstjenester. Det er et spørgsmål om rækkefølge og retsgarantier.

Et demokrati er ikke et tag-selv-bord hvor man hjælper sig og beder om tilgivelse bagefter. Beføjelser til masseindsamling af data om borgere kræver et mandat. Det mandat skal komme fra en informeret befolkning og et velfungerende folketing - ikke fra en bekendtgørelse vedtaget i stilhed.

Yderligere er det vigtigt at vurdere negativ konsekvenser overfor andre dele af samfundet.

Det er ikke kun privatlivsorganisationer der har rejst bekymringer. På høringen i Landstingssalen den 28. august 2025 hvor jeg var til stede fremførte tre sundhedsfaglige organisationer - Lægeforeningen, Det Etiske Råd og Dansk Selskab for Almen Medicin (DSAM) - alvorlige advarsler mod at give PET adgang til sundhedsdata.

Lægeforeningens formand Camilla Rathcke har formuleret det præcist i et brev til justitsministeren: sundhedspersoners tavshedspligt er en central forudsætning for et velfungerende sundhedsvæsen, og tillid mellem patient og sundhedspersonale er afgørende. Hvis denne tillid svækkes risikerer man at patienter undlader at søge nødvendig behandling eller tilbageholder oplysninger af væsentlig betydning - hvilket i sidste ende kan føre til fejldiagnoser, forværring af sygdomsforløb og i alvorlige tilfælde unødige dødsfald.

Det er en konkret og målbar konsekvens af masseovervågning der sjældent indgår i den politiske risikovurdering, eller skal vi sige politiets/PETs risikovurdering. Når jeg siger det sådan er det fordi daværende justitsminister udtrykte *fuld tillid* til politiet/PET og stiller ingen spørgsmål - forholder sig ikke konkret til det fremsatte forslag.

12.4 Masseovervågning virker ikke - og Krudttønden beviser det

Et af de tilbagevendende argumenter for udvidet overvågning er at det forebygger terror og alvorlig kriminalitet. Det er et argument der ikke holder.

Krudttønde-attentatet i København i februar 2015 er et konkret eksempel. Gerningsmanden var kendt af myndighederne. Han var på deres radar og alligevel endte han med at kunne udføre et angreb. Netop fordi masseovervågning ikke er et effektivt redskab mod en enkelt person der beslutter sig for at handle. Gerningsmanden efterlod simpelthen telefonen hjemme.

Det samme billede tegner sig fra San Bernardino-angrebet i USA samme år. Også her var gerningsmændene ikke ukendte for myndighederne. Også her hjalp den eksisterende overvågning ikke.

Netop mens denne bog blev gjort færdig, skete der et angreb ved Berlin Pride i juli 2026. En 21-årig tysk statsborger kørte en varevogn ind i en menneskemængde og dræbte én person og sårede 29. Gerningsmanden, Abdul Ballout, var allerede kendt af myndighederne - han var tidligere blevet fængslet for at forberede et angreb og løsladt i maj. Systemet kendte ham. Det hjalp ikke.

William Binney, tidligere teknisk direktør i NSA, har formuleret det bedre end de fleste. Jeg hørte ham selv tale ved CPH:DOX i november 2014 - i forbindelse med premieren på Laura Poitras' Citizenfour, hvor han selv optræder. Hans pointe var enkel: problemet er ikke at der mangler data. Problemet er at bunken er for stor til at man kan se hvad der er vigtigt. Målrettet efterforskning virker. Masseindsamling skaber støj.

Alligevel er svaret fra politisk hold næsten altid det samme: vi har brug for mere adgang, mere data, færre begrænsninger. Det er som at behandle en fejlslået strategi med en større dosis af den samme medicin.

Masseovervågning rammer ikke de skyldige. Det rammer alle.

12.5 Hvad kan du gøre

Til den journalist, aktivist eller bekymrede borger der læser dette: du behøver ikke at acceptere at dit digitale liv er et åbent vindue.

Et godt sted at starte er EFF's Surveillance Self-Defense - en gratis, praktisk guide der hjælper dig med at vurdere din personlige risiko og vælge de rigtige værktøjer. Den findes på mange sprog og er bygget op fra begynder til øvet. Start

med deres grundlæggende guides på https://ssd.eff.org/module-categories/basics - særligt Your Security Plan der hjælper dig med at tænke over hvad du konkret har brug for at beskytte og mod hvem.

Brug kryptering. Signal til beskeder. HTTPS overalt. Brug specielt Tor når du har brug for at bevæge dig og kun efterlade få spor.

Støt organisationer der arbejder for digitale rettigheder. IT-Politisk Forening i Danmark. Electronic Frontier Foundation internationalt. The Tor Project.

Stil krav til dine politikere. Proportionalitet er ikke et teknisk begreb - det er et demokratisk princip. Overvågning af alle for at finde de få er ikke proportionalt. Det er ikke acceptabelt i et demokrati, uanset hvor mange gange det forklædes som sikkerhedspolitik.

Og hvis du har ressourcer og teknisk kunnen: overvej at drive en Tor-node. Ikke nødvendigvis en exit-server - det kræver mod og forberedelse som denne bog forhåbentlig har illustreret. Et lille bidrag til den infrastruktur der holder netværket kørende for dem der har brug for det.

Friheden på Internet er ikke gratis. Den kræver at nogen aktivt bidrager til at bevare den.

Kapitel 13

Afslutning: 11 år efter kører serverne stadig

Da jeg satte min første Tor exit-server op, vidste jeg ikke helt hvad jeg gik ind til. Jeg vidste at det var det rigtige at gøre. Jeg vidste at jeg havde ressourcerne til det. Jeg vidste at privatliv på Internet ikke er noget der bevarer sig selv - det kræver at nogen aktivt bidrager til at holde infrastrukturen oppe.

Det jeg ikke vidste var at jeg mange år senere stadig ville sidde med det. At der ville komme politibesøg. At der ville komme tusindvis af klager. At jeg ville blive sigtet og reelt frikendt i samme telefonsamtale. At jeg alligevel ville fortsætte.

Jeg håber at du med denne bog - om du har læst den fra ende til anden eller skimmet de kapitler der interesserede dig mest - har fået et mere nuanceret billede af Tor end det medierne normalt tegner. Tor er ikke et mørkt hjørne af Internet forbeholdt kriminelle. Det er et stykke infrastruktur bygget af frivillige, til gavn for mennesker der har brug for at bevæge sig frit og privat på nettet.

Nogle af dem lever i lande vi ikke vil bytte med. Lande hvor det at søge information, organisere sig eller tale frit kan have alvorlige konsekvenser. Men proportionalitetsdebatten hører ikke kun hjemme der. Den hører også hjemme her - i Danmark, i Europa - hvor alvorlige indgreb i borgernes data alt for ofte vedtages uden den demokratiske diskussion de fortjener. Uden at staten behøver at argumentere grundigt for hvorfor. Uden at vi som borgere stilles til regnskab for hvad vi accepterer.

Det bekymrer mig, og det er en af grundene til at jeg stadig driver mine servere.

Hvis du går fra denne bog med ét spørgsmål i baghovedet, så lad det være dette: hvad er du villig til at gøre for at bevare det privatliv du endnu ikke ved at du holder af?

Bilag A

Ordliste

CSAM - Child Sexual Abuse Material. Internationalt begreb for billeder og videoer der dokumenterer seksuelt misbrug af børn.

DNS - Domain Name System. Internet ‘‘telefonbog’’ der oversætter adresser som ‘‘torproject.org’’ til IP-adresser. Kan blokeres af autoritære stater for at forhindre adgang til bestemte websites.

Entry-node / Guard-node - Den første server i en Tor-forbindelse. Kender brugerens rigtige IP-adresse, men ikke destinationen.

Exit-node / Exit-server - Den sidste server i en Tor-forbindelse. Sender trafik ud på det åbne internet. Dens IP-adresse er den verden ser - ikke brugerens.

HTTP - Ukrypteret webforbindelse. Al trafik kan i princippet læses af enhver der sidder på forbindelsen, herunder en exit-operatør.

HTTPS - Krypteret webforbindelse. Beskytter indholdet af kommunikationen, men ikke nødvendigvis hvem der kommunikerer med hvem.

IANA- den overordnede organisation der fordeler IP-adresser og andre talværdier der bruges på Internet

IP-adresse - En unik adresse der identificerer en enhed på et internet. IPv4 skrives som fire tal adskilt af punktummer (fx 192.0.2.0). IPv6 skrives med hexadecimale tal og kolon (fx 2a06:d380:0:103::62).

IPv4 / IPv6 - adresseformater og internet protokoller til data transmission på Internet

LIR - Local Internet Registry, eksempelvis en Internetudbyder

Middle node / Relay - Servere i midten af Tor-kæden. Kender hverken afsender eller destination.

NC3 - Nationalt Cyber Crime Center, Dansk politi

Reduceret exitpolitik - En konfiguration der begrænser hvilke netværksporte en Tor exit-server videresender trafik på. Reducerer misbrug markant.

Reverse DNS - Det navn en IP-adresse ‘‘svarer med’’ når man slår den op. Bør for Tor exit-servere indeholde ord som ‘‘tor-exit’’ eller ‘‘anonymous-relay’’.

RIPE NCC - den europæiske registreringsorganisation for IP-adresser

RIR - Regional Internet Registry, fx RIPE NCC

SMTP / Port 25 - Protokol og port brugt til afsendelse af e-mail. Blokeres ofte i reducerede exitpolitikker for at forhindre spam.

Tor Atlas / Tor Metrics - web sider hvor man slå data op om Tor netværket

Tor Browser - den specielle browser der giver adgang til Tor-netværket

Traceroute - program der viser ruten trafik tager gennem netværk/Internet

Whois - Offentlig database der viser hvem der er registreret administrativt som *ejer* af en given IP-adresse eller et domænenavn.

Bilag B

Kilder og referencer

Der findes mange ressourcer omkring privatliv, værktøjer, litteratur, nyhedsartikler m.v.

Nedenfor er en bred liste over nogle af de ressourcer, historier og ideer som har influeret mit syn på privatliv.

B.1 Tor-netværket

- The Tor Project: https://www.torproject.org
- Tor exit-guidelines for operatører: https://community.torproject.org/relay/community-resources/tor-exit-guidelines/
- Tips til at drive en exit-server: https://blog.torproject.org/tips-running-exit-node/
- Tor Metrics - se aktive servere: https://metrics.torproject.org/rs.html
- Tor (netværket) - Wikipedia: https://en.wikipedia.org/wiki/Tor_(network)
- Tor Abuse Templates: https://community.torproject.org/relay/community-resources/tor-abuse-templates/
- EFF's juridiske FAQ for Tor-operatører: https://community.torproject.org/relay/community-resources/eff-tor-legal-faq/
- Anonymity Loves Company: Usability and the Network Effect, Roger Dingledine and Nick Mathewson, The Free Haven Project https://www.freehaven.net/doc/wupss04/usability.pdf

B.2 Tor servere nævnt i denne bog

- Zencurity ApS servere (kramse): https://metrics.torproject.org/rs.html#search/kramse
- Dotsrc Tor-servere: https://dotsrc.org/tor og https://metrics.torproject.org/rs.html#search/dotsrc

B.3 Privatliv og digitale rettigheder i Danmark

- IT-Politisk Forening: https://itpol.dk
- PROSA - Forbundet af IT-professionelle: https://www.prosa.dk
- Institut for Menneskerettigheder: https://menneskeret.dk , Menneskerettighedskonventionen https://menneskeret.dk/om-os/menneskerettigheder/menneskerettigheder-eu/europaeiske-menneskerettighedskonvention , Politi og efterretningstjenester: https://menneskeret.dk/status/politi-retningstjenester
- 1984.dk (arkiveret 2003): https://web.archive.org/web/20030603193643/http://www.1984.dk/
- Polippix - Wikipedia: https://da.wikipedia.org/wiki/Polippix og archive.org https://web.archive.org/web/20080917131857/http://www.polippix.org/

B.4 Danske love og lovforslag

- Lovforslag L218 (2002/2003) - dataaflæsning og bekæmpelse af rockerkriminalitet: https://www.retsinformation.dk/eli/ft/200212L00218
- Lovforslag L218 (2002/2003) med betænkning: https://www.retsinformation.dk/eli/ft/200213L00218
- L 218 (2024-25) - Forslag til lov om ændring af lov om Politiets Efterretningstjeneste (PET) - Understøttelse af PETs mulighed for at udføre data- og analysebaseret efterretningsvirksomhed m.v., fremsat 25. april 2025: https://www.retsinformation.dk/eli/ft/202412L00218

- Institut for Menneskerettigheder - høring om PET-loven: https://menneskeret.dk/nyheder/hoering-folketinget-aabner-justeringer-pet-lov
- Reglerne om ransagning findes i retsplejelovens kapitel 73, særligt § 794: https://www.jurabibliotek.ai/retsplejeloven/paragraf/794

B.5 Danske overvågningssager og teleskandaler

Dette er ikke en komplet liste, men viser et mønster i misbrug.

- Version2: Politiet bruger ulovligt indsamlede teledata mere end 11 gange om dagen: https://www.version2.dk/artikel/politiet-bruger-ulovligt-indsamlede-teledata-mere-end-11-gange-om-dagen
- Version2: Teleskandalen - uoverensstemmelser i en tredjedel af undersøgte sager: https://www.version2.dk/artikel/teleskandalen-politiet-fandt-uoverensstemmelser-tredjedel-undersoegte-sager-1088394
- Kristeligt Dagblad: Efterretningstjenester foretager stadig ulovlig overvågning: https://www.kristeligt-dagblad.dk/efterretningstjenester-foretager-stadig-ulovlig-overvaagning
- Tilsyn finder systematiske lovbrud i PET-overvågning: https://www.sn.dk/art1496296/
- Information: PET-overvågning skal undersøges: https://www.information.dk/indland/2011/11/pet-overvaagning-undersoeges
- Version2: POL-INTEL - politifolk har misbrugt digitalt supervåben 30 gange (2022): https://www.version2.dk/artikel/pol-intel-politifolk-har-misbrugt-digitalt-supervaaben-30-gange
- Version2: Tidligere politichef tiltalt for misbrug af it-systemer (2022): https://www.version2.dk/artikel/tidligere-politichef-tiltalt-misbrug-af-it-systemer-til-ulovlig-overvaagning
- Elvir Abaz, Fyns Politi (dom august 2025): 49-årig betjent fra Fyns Politi idømt 30 dages ubetinget fængsel. Tiltalen omfattede 29 punkter om tjenestemisbrug, brud på tavshedspligt, falsk anmeldelse og misbrug af interne systemer. Han slog sager op uden tjenstlig anledning og delte fortrolige oplysninger. Kilde TV2: Fynsk politimand dømt for tjenestemisbrug (2025): https://nyheder.tv2.dk/live/krimi/2025-08-27-fynsk-politimand-doemt-for-tjenestemisbrug
- Andet link DR: Fynsk betjent får fængselsstraf for tjenestemisbrug (2025): https://www.dr.dk/nyheder/indland/fynsk-betjent-faar-faengselsstraf-have-misbrugt-sin-stilling

Se flere eksempler på tab af persondata hos IT-Politisk Forening: Dataskandaler - oversigt over misbrug af persondata: https://itpol.dk/dataskandaler

B.6 Tor chikanesager

Tyske og europæiske sager mod Tor exit-operatører

- EDRi: German police does not understand Tor (2007 - sagen om Alexander Janssen): https://edri.org/our-work/edrigramnumber5-18tor-germany/
- Ars Technica: Tor node operator after run-in with police: ‘‘I can’t do this any more’’ (2007): https://arstechnica.com/news.ars/post/20070917-tor-node-operator-after-run-in-with-police-i-cant-do-this-any-more.html
- The Register: Tor node admin raided by cops - Østrig 2012: https://www.theregister.com/2012/12/10/tor_admin/
- Cybernews: German police raid Tor-linked group - Artikel 5 eV, Essen 2024: https://cybernews.com/privacy/tor-exit-node-operator-raided-germany/
- Tor Project Forum - Gero Kühns indlæg om ransagningen af Artikel 5 eV, 8. september 2024: https://forum.torproject.org/t/tor-relays-artikel-5-e-v-another-police-raid-in-germany-general-assembly-on-sep-21st-2024/14533
- Vice: The People Who Risk Jail to Maintain the Tor Network (baggrundsstory om exit-operatørers vilkår): https://www.vice.com/en/article/the-operators/
- Alexander Janssen i Tyskland blog post: https://itnomad.wordpress.com/2007/09/16/tor-madness-reloaded/

B.7 Internationale links, Privatlivs- og sikkerhedsværktøjer

- Signal (krypteret kommunikation): https://signal.org
- EFF’s Surveillance Self-Defense (SSD): https://ssd.eff.org
- Electronic Frontier Foundation (EFF): https://www.eff.org
- Open Source whistleblower platform https://securedrop.org/
- Cryptome: https://cryptome.org
- Bruce Schneiers Cryptogram: https://www.schneier.com/crypto-gram/
- Four Horsemen of the Infocalypse - Wikipedia: https://en.wikipedia.org/wiki/Four_Horsemen_of_the_Infocalypse
- Edward Snowden - Wikipedia: https://en.wikipedia.org/wiki/Edward_Snowden

- Snowden-afsløringerne - Wikipedia: https://en.wikipedia.org/wiki/Snowden_disclosures
- Snowden om Tor (The Tor Project): https://blog.torproject.org/thank-you-edward-snowden-tor/
- Snowden interview med The Tor Project: https://blog.torproject.org/what-tor-supporter-looks-edward-snowden/
- *Citizenfour* (dokumentarfilm, 2014) - Wikipedia: https://en.wikipedia.org/wiki/Citizenfour
- Laura Poitras - Wikipedia: https://en.wikipedia.org/wiki/Laura_Poitras
- *Snowden* (Oliver Stone, 2016) - spillefilm baseret på begivenhederne
- William ''Bill'' Binney - Wikipedia: https://en.wikipedia.org/wiki/William_Binney_(intelligence_official)
- Wikipedia https://en.wikipedia.org/wiki/Crypto_Wars
- ''The Crypto Wars: Governments Working to Undermine Encryption''. Electronic Frontier Foundation. 2 January 2014
- PGP krypteringssoftware https://en.wikipedia.org/wiki/Pretty_Good_Privacy

En videnskabelig undersøgelse publiceret i Proceedings of the National Academy of Sciences fandt at kun 6,7 % af Tor-brugere dagligt besøgte sider defineret som dark web - og disse sider var ikke nødvendigvis dedikeret til ulovlig aktivitet. Separate opgørelser viser at besøg på dark web kun udgør 1,5 % af den samlede Tor-trafik, og at kun 45 % af websites på dark web hoster ulovligt indhold. - PNAS-studiet (2020): https://www.inverse.com/innovation/a-dark-web-dilemma - https://deepstrike.io/blog/dark-web-statistics-2025 - Big Think-analyse af samme studie: https://bigthink.com/the-present/dark-web-study/

- Let's Encrypt - 10 år: https://letsencrypt.org/2025/12/09/10-years

B.8 Chat Control

Se også https://chatcontrol.dk/da/ som har gjort det meget nemt at forstå

- Patrick Breyer (MEP): End of Chat Control: https://www.patrick-breyer.de/en/end-of-chat-control-eu-parliament-stops-mass-surveillance-in-voting-thriller-paving-the-way-for-genuine-child-protection/
- Tom's Hardware: Chat Control 1.0 sneaks through: https://www.tomshardware.com/tech-industry/cyber-security/chat-control-1-0-sneaks-through-the-eu-parliament-letting-companies-scan-user-data-without-warrants-legal-tactic-used-to-force-a-majority-required-re-vote-on-eve-of-parliament-break

Litteraturliste

Denne liste er nogle af de for mig vigtigste dokumenter omkring masseovervågning, samt to gode bøger om teknologierne.

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. 2015. ‘‘Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications ‡.’’ *Journal of Cybersecurity* 1 (1): 69--79. https://doi.org/10.1093/cybsec/tyv009.

Abelson, Harold, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, et al. 2024. ‘‘Bugs in Our Pockets: The Risks of Client-Side Scanning.’’ *Journal of Cybersecurity* 10 (1): tyad020. https://doi.org/10.1093/cybsec/tyad020.

Aumasson, Jean-Philippe. 2024. *Serious Cryptography: A Practical Introduction to Modern Encryption*. Second Edition.

Singh, Simon. 1999. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*. 1st ed. USA: Doubleday.