Høringssvar fra Norway Chapter of the Internet Society angående rapport om digitalt grenseforsvar (DGF)

Norway Chapter of the Internet Society (ISOC Norge) vil starte med å takke for en grundig og god rapport fra Lysne-II-utvalget. Utvalget tar for seg hvordan man skal kunne bygge opp et digitalt grenseforsvar med gode kontrollorganer og med et fokus på personvern. Det er åpenbart at E-tjenesten har behov for digitale verktøy for å kunne avdekke trusler fra utlandet mot Norge, men ISOC Norge er ikke enig i konklusjonen og støtter ikke innføringen av masseovervåking.

ISOC Norge har valgt å dele opp sine innvendinger i to kategorier;

1. Prinsipielle innvendinger
2. Tekniske innvendinger

1. Prinsipielle innvendinger

ISOC Norge er en del av en organisasjon som jobber for et fritt og åpent Internett. I det ligger ønsket om et Internett hvor man fritt kan kommunisere eller lete frem informasjon uten å frykte for egen rettssikkerhet. Lysne II-utvalget viser til at nedkjølingseffekten ("chilling effect"), vil føre til at befolkningen i økende grad vil vegre seg for ytring eller søk i informasjon. Stadig mer overvåkning utvikler en kultur hvor det å ytre seg ikke er ønskelig, og man blir passiv observatør til hva som skjer rundt seg. Norge som en åpen og demokratisk nasjon bør unngå trenden mot nedkjøling og heller jobbe for at Internettbrukere skal føle seg trygge på sine synspunkter og ytringer.

Utvalget innrømmer at det ikke vil være mulig å verne om grupper med ekstra krav til vern, eksempelvis kommunikasjon mellom journalister og kilder. Masseovervåking vil derfor innebære at også kommunikasjon som har krav på sterkere vern vil bli samlet inn. Kildevern er grunnleggende i et demokratisk samfunn. Det å kunne ytre seg kritisk anonymt, selv med upopulære meninger, er en bærebjelke i et demokratisk samfunn. Dersom DGF, med overlegg, ikke skjermer slik kommunikasjon, vil dette være en trussel mot informasjonssamfunnet som helhet.

Utvalget hevder at den økte bruken av masseovervåking som skjer i verden, ikke er lovstridig. I rapporten står det: "I all hovedsak er det staters syn at bulkaksess vært lovlig og bør fortsette, og at tilgang til store datamengder i seg selv ikke innebærer ulovlig masseovervåkning"(s. 30). Samtidig vises det også til sivile rettssaker som ble opprettet i kjølvannet av Snowden-avsløringene, som indikerer at en slik masseovervåking strider mot allmenn rettsoppfattelse. Norge er et land hvor innbyggere i høy grad har tillit til myndighetene. Ved å innføre DGF vil rettspraksis stride med den allmenne rettsoppfattelsen, og dermed kan det bli et problem med tillit til myndighetene.

Argumentasjonen om at “alle andre gjør det”, holder heller ikke. For å sitere Kirke og fornyingsdepartementets hjemmeside: “*Personvern handler om retten til å få ha ditt privatliv i fred, et grunnleggende prinsipp i en rettsstat”*. I dette betyr det også at enhver person har rett til å ikke frykte for sine handlinger fordi de blir overvåket. Istedenfor masseovervåking bør Norge fokusere på å sikre egen informasjon for å hindre uønsket overvåking fra andre, og samtidig fortsette med fokusert overvåking der man vet det er grunn til det.

Bulkaksess, eller masseovervåking, er uansett hvilken intensjon det implementeres med, ikke noe ISOC Norge støtter. Vi tror heller på å løse Internetts utfordringer med åpenhet og samarbeid rundt problemstillingene, ikke ved bruk av økt overvåkning bak lukkede dører. Erfaringsmessig de siste 30 år viser at det nettopp er åpenheten rundt problemstillinger som har gitt oss den unike plattformen Internett er.

I rapporten kan vi lese at "Nettet benyttes videre til virksomhet som kan utgjøre en ytre trussel mot landet og viktige nasjonale interesser. Trusselbildet er komplekst og dynamisk” (s. 11). Verden har blitt mer global og vi har tilgang til mer informasjon, takket være Internett. Vi undres over hva som oppfattes som mer komplekst? Ofte oppfattes det meste rundt Internett som "komplekst" fordi teknologien er ukjent for mange og forståelsen av hvordan Internett fungerer så lav blant befolkningen generelt at å ha motargumenter mot slike generelle ordlegginger er vanskelig. Og ordlag som "kan utgjøre en ytre trussel" blir vanskelig å argumentere mot. Et åpent og fritt Internett har skapt et utviklings og samarbeidsklima verden aldri før har sett. Internett har også vært en trussel mot totalitære stater som ønsker å ha kontroll på sine innbyggere. Argumentasjonen kan derfor også snus på hodet sett gjennom øyne til befolkningen. Og når det kommer til terrorisme brukes det ofte som den største grunnen til å benytte store ressurser til å overvåke alle. Vi ser ut til å glemme organisasjoner som IRA (Irish Republican Army) fantes lenge før Internett mobiliserte samarbeid av slik art.

2. Tekniske innvendinger

E-tjenesten skal ikke overvåke landets egne innbyggere. Ved å overvåke Internetts linjer inn og ut av landet føles det som en selvmotsigelse at det er E-tjenesten skal overvåke disse linjene. Informasjon ut av landegrensene vil for det meste være kommunikasjon mellom borgere i Norge, enten via tjenester som ligger i utlandet, eller fordi Norge er et land med lange strekninger hvor raskeste veien i nettet går via Sverige, selv om informasjon og mottager står i Norge. For å filtrere bort den store andelen av kommunikasjon mellom norske borgere, blir to metoder nevnt av utvalget; negativ og positiv filtrering. Negativ filtrering innebærer å registrere eksempelvis IP eller andre identifikatorer på borgere, og deretter filtrere bort informasjonen som blir samlet med disse identifikatorene. I seg selv er et slikt register overvåking. Positiv filtrering blir presentert som forhåndsidentifikasjon av objekter som er av interesse, og et direkte overvåking av disse. Med positiv filtrering er det vanskelig å se hvorfor man trenger et digitalt grenseforsvar, og ikke bare gjennomfører aktiv overvåking av de aktuelle objektene. Det er også viktig å legge til at en stor del norske borgere surfer på Internett med en IP-adresse registrert i utlandet. Spesielt når de sitter på jobb i multinasjonale selskap. Hvordan E-tjenesten har tenkt til å filtrere ut denne trafikken stilles det et stort spørsmålstegn ved.

Etter Snowden-avsløringene er det allmenn kjent at stater bedriver stor grad av overvåking på Internett. Det kommer også frem at kjente terrornettverk, som IS, i økende grad bruker krypterte kommunikasjonsmetoder (se for eksempel

http://www.aftenposten.no/verden/Slik-unngar-IS-myndighetenes-overvakning-19540b.html). ISOC Norge ser derfor på en økt masseovervåking som å skyte småspurv med kanoner – til tross for at intensjonen er god, virker det som et stort inngrep og ressursbruk for potensielt lite gevinst.

Cyber-angrep brukes som en årsak til å trenge et digitalt grenseforsvar. Internett har blitt angrepet fra sin spede begynnelse. Vi ser det ikke som E-tjenestens jobb eller kapasitet å løse disse problemstillingene. De har blitt løst på en utmerket måte til nå, av teknologer gjennom uavhengige organisasjoner slik som IETF, uten staters inngripen. Mennesker med dyp teknologiforståelse har hele tiden har gjort Internetts infrastruktur bedre og mer robust for hvert angrep som har kommet. En ny type cyber-angrep er i sin natur ikke noe en kan forutse eller forhindre da den til stadighet tar nye former. Det vil derfor være galt, og naivt å tro at det kan stoppes med masseovervåkning av trafikk.

Det samme gjelder digital spionasje. Her er det helt andre virkemidler for både å sikre infrastruktur av nasjonal interesse enn en generell masseovervåkning som burde være fokuset. Målrettet forsvar mot navngitte trusler er et riktigere fokus slik vi ser det. Digital spionasje er i all hovedsak målrettede angrep/forsøk og kan avdekkes med et tettere samarbeid med de institusjoner, organisasjoner og selskaper man ønsker å beskytte.

Vi stiller oss følgende spørsmål: Vil en slik masseovervåkning virkelig kunne beskytte oss mot det vi tror vi trenger å beskytte oss mot, og med det lage et tryggere samfunn? Vår klare oppfattelse er at det ikke vil gjøre det. Det som argumenteres som farene burde til dels ikke være E-tjenestens arbeid å løse, og det er heller ikke det riktig organ eller metode å bekjempe problemstillinger som cyberangrep eller digital spionasje. Slike angrep kan best bekjempes med åpenhet, åpen deling av informasjon rundt angrep mellom organisasjoner som opplever det, og bedre teknologiske løsninger. Massovervåkning kan muligens i ettertid av en hendelse finne ut hvor et angrep kom fra, men det vil aldri frigjøre oss fra faren, og da er heller ikke midlene som ønskes benyttet i et digitalt grenseforsvar mulig å forsvare slik vi ser det.

Merete Asak og Maja Enes

Norway Chapter of the Internet Society