Forsvarsdepartementet

Vår ref: PAL Oslo 6. januar 2017

Høring om digitalt grenseforsvar

Tekna er landets største forening for akademikere. Vi har ca. 72 000 medlemmer med høyere grads universitets- og høgskoleutdanning innen teknisk-naturvitenskapelige fag.

Nedenfor følger våre kommentarer til Lysne II-utvalgets rapport om Digitalt grenseforsvar (DGF).

Formålet med DGF - teknologisk mulighetsrom og begrensninger ikke godt beskrevet
Utvalget tolker mandatet sitt til at: «… Verken mandatet, tiden til rådighet eller utvalgets sammensetning har tilsagt at utvalget skal utrede konkrete tekniske løsninger for etablering og innfasing av et eventuelt DGF i Norge». Tekna mener det er avgjørende å legge til grunn kunnskap om teknologiske muligheter og utviklingstrekk for å kunne vurdere DGF. Tekna mener det er svært vanskelig å gjøre prinsipielle avveininger med utgangspunkt i teknologiuavhengighet. Tekna mener at teknologien og teknologiske forhold i seg selv er rammesettende. Vi har eksempelvis merket oss at det ikke er gjort forsøk på å regne på norsk trafikk-mengde nå og i framtiden, noe som er sentralt. Dette er overraskende.

Utviklingen mot mer kryptering av kommunikasjonen innebærer at analyse og tolkning av data blir vanskeligere. Dette gir risiko for formålsglidning. På sikt vil det være nødvendig med svært inngripende metoder. Tekna mener at de sterke teknologiske driverne som trekker i retning av et overvåkningsregime ikke er godt nok belyst og vurdert.

Det er velkjent at det internasjonale leverandørmarkedet for avlyttings- og overvåkingssystemer er stort og omfattende med mange tilbud og løsninger. Dette er ikke drøftet i rapporten. Rapporten burde videre belyst den tekniske forskjellen mellom overvåkingssystemer anvendt i mer autoritære regimer og demokratier. En eventuell implementering av et DGF bør ha innebygde sikringstiltak som gjør at ingen kan anvende systemet mot egne innbyggere om det skulle oppstå en ekstrem situasjon.

Vi mener også at tittelen kan gi feil assosiasjoner til de konkrete forslagene i rapporten. Rapportens tittel gir inntrykk av at Norge kan etablere et *digitalt forsvar* hvor uønskede elementer kan stoppes ved grensen. Tekna mener et riktigere språklig bilde vil være *digital grenseovervåking*.

Tekniske løsninger for overvåkning og organisatorisk kontroll
Utvalgets løsningsskisse viser tre datalager:

1) Et masseovervåkingslager, hvor all trafikk skal tappes og lagres. Bruk begrenses organisatorisk til 14 dager, men E-tjenesten vil lagre dataene for å kunne se tilbake hvis det oppstår konkrete hendelser.
2) Et metadatalager, som har likhetstrekk med datalagringsdirektivet som ble skissert få år tilbake, men som ble forkastet av EU-domstolen. Lagringstid er foreslått til 18 måneder, lenger tid enn det som ble foreslått for datalagringsdirektivet i Stortinget.
3) Et innholdsdatalager, som inneholder all kommunikasjon av utvalgte personer. Dette synes å være tilsvarende den avlytting som allerede skjer i dag av Telenor og andre. Her forutsetter utvalget en organisatorisk kontroll ved EOS-utvalget, som må «forstå tekniske detaljer knyttet til søk og filtrering".

Utvalget foreslår et omfattende kontrollregime for disse datalagrene.

Vi har i dag mangel på spesialistkompetanse innenfor IKT i Norge, og Tekna stiller spørsmål ved om vi har tilstrekkelig kapasitet til å etablere et slikt kontrollregime ved en eventuell innføring av DGF i Norge. Det vil kreve teknisk kompetanse, tilsynskompetanse og domstolkompetanse. EOS-utvalget må også besettes slik at det har forutsetninger for å forstå de teknologiske sidene av et slikt kontrollregime. Disse sidene ved innføring av digital grenseovervåking har ikke utvalget vurdert godt nok og bør utredes nærmere. Kompetanse må bygges underveis i prosessen. Det å legge til rette for læring bør være en av hovedprosessene i både etableringen og operasjonen av ett eventuelt DGF.

Forutsetningen om et kompetent kontrollutvalg viste seg gjennom Snowden-avsløringene å ikke holde i USA. Amerikanske politikerne hadde ikke nødvendig bakgrunn og kunnskap for å forstå de tekniske implikasjoner av NSA-briefingene. Denne saken er et eksempel på at informasjon fra verdens strengest bevoktede system i NSA og CIA kan *hackes.*

Kryptering – muligheter for å omgå sikkerhetssystemene
Rapporten omtaler teknikker for å gjøre data vanskelig tilgjengelige for en overvåker, at disse teknikkene er sterke og blir stadig sterkere, og at nytten av DGF dermed blir mindre. Utvalget fremhever at nytten fortsatt vil være stor, og at DGF vil være «nødvendig».

Tekna mener verdien av datafangsten, dersom dataene er krypterte, burde ha vært drøftet grundigere i rapporten.

Kryptering er svært utbredt i dag. Om tre år antas det at 60 % av trafikken er kryptert. Frem til kjernen av en kommunikasjonsstrøm vil det være flere lag med kryptering. Fenomener som burde vært omtalt er symmetrisk og asymmetriske kryptering, steganografi, *Løk-ruting* av IP pakker, og *blockchains*. Uten en viss forståelse av mulighetene og begrensningene som disse teknologiene gir, vil en diskusjon rundt verdien av DGF versus ulempen ved inngripen i personvern være mangelfull.

Mulighetene til å omgå de foreslåtte sikkerhetssystemene ved kryptering er store. Det antydes i rapporten at det vil være nødvendig å få tilgang til visse typer ukryptert trafikk (linknivå). Dette vil imidlertid ikke virke for ende-til-ende kryptert trafikk som benytter IP-anonymiseringstjenester. En logisk glidning vil være at man i framtiden vil ønske ytterligere tilgang til ukryptert materiale nærmere sluttbrukerne. Denne problematikken blir skissert, men ikke tilstrekkelig problematisert.

Kobling av flere typer data for automatiserte statistiske analyser
Ut fra utvalgets beskrivelse gis det inntrykk av at analysen av dataene vil gjøres av mennesker som observerer og vurderer dataene. Dette er imidlertid ikke mulig med større datamengder. Det må lages statistiske modeller som tolker innsamlede data, og deretter generere signaler for forskjellige slags kategoriseringer og vurderinger ut fra disse modellene. Informasjon innsamlet gjennom DGF vil videre kunne settes i sammenheng med andre data og dermed gi innsikter som går utover det som de umiddelbare innsamlede data gir. Utvalget gir her en for enkel beskrivelse. Analysearbeidet som må gjøres for å foredle råmaterialet fra DGF blir beskrevet overfladisk.

Dette er ikke en ny tanke. Etterretningsorganisasjonen Nation Security Agency (NSA) sitt Stellar Wind system er ifølge beskrivelser gitt av varsleren William Binney konstruert for å samle inn data om personer fra mange kilder, som så kobles sammen for å danne et bilde av personers aktiviteter og samvirke over tid. I næringslivet bruker man i dag systemer for målretting av reklame, slik som Telenor-eide Tapad. Disse systemene bruker flere åpne og mindre åpne kilder som settes sammen i en statistisk modell. En teleoperatør vil for eksempel i enkelte land med mindre streng personvernlovgivning enn i Norge kunne bruke trafikkdata fra telenettet for å oppdage hvilke telefontyper samtalepartnere har og kan lage en modell for markedsføring mot den enkelte. Teleoperatører i andre land har ikke lov til å bruke trafikkdata på denne måten men nesten alle steder er det tillatt å bruke demografiske data basert på bl.a. postnummer, alder og kjønn på abonnenten. Avhengig av hvor mye data man kan bruke, vil modellene kunne gi mer eller mindre pålitelige signaler.

Det er naturlig å tenke seg at et eventuelt DGF vil ha et grensesnitt som ligner på dette: De hemmelige dataene innhentet fra det digitale grenseforsvarets databaser legges på toppen av en database av mindre hemmelige data, og det er så denne totale datamengden tolkninger gjøres ut fra. Dette er en naturlig framskriving av teknologibruk som er vanlig i næringslivet i dag, og det er sannsynlig at slik teknologibruk vil være mer vanlig i den fremtiden hvor digitalt grenseforsvar evt. blir en realitet. Vi mener dette burde ha vært grundigere drøftet i rapporten, spesielt problemstillingene rundt de etiske sidene ved kobling av data og hvilke restriksjoner som eventuelt skal gjelde.

Analyse med kunstig intelligens og maskinlæring ikke behandlet i rapporten
Det er rimelig å anta at alle innsamlede data i et DGF vil bli gjort tilgjengelig for forskjellige typer maskinlæringsprogrammer. Det er derfor helt realistisk at mange funn vil gjøres av det man i dag kan kalle *kunstig intelligens*, i beste fall i samarbeid med mennesker. I virkeligheten vil nok

menneskenes rolle være svært liten hva arbeidsmengde angår, og muligens også hva angår konklusjoner og begrunnelser for disse. Dette er noe det sies lite om i rapporten, og er en svakhet i framstillingen.

Uklart kostnadsbilde for innføring av DGF
Tekna støtter FFI's uttalelse når det gjelder teknologiske behov og kostnader for tilretteleggelse hos norske ekomleverandører. Eksempler kan være fysisk lokalisering av komponenter, ekomleverandørens bistand til dekryptering, samt krav til båndbredde, prosesseringskraft og lagring. Et viktig spørsmål er hvem som skal betale for utvikling, investering og drift av slikt utstyr. Et DGF vil involvere mange parter som kan tenkes å måtte bidra, blant andre forsvarets etterretning, de kommersielle teleoperatørene, PST, og ulike kontrollinstanser.

Tapte økonomiske muligheter
I et kort avsnitt diskuterer rapporten økonomiske konsekvenser av å innføre DGF (side 68 venstre spalte). Med henvisning til en finsk rapport blir dette ansett som av liten betydning. Dette virker lettvint. Det er godt kjent at NSA sin massive dataovervåkning har ført til redusert vekst for USA-baserte skytjenester, og en oppblomstring av EU-baserte skytjenester. Denne signifikante effekten av massiv dataovervåkning, og hva DGF derfor kan bety for norsk næringsutvikling, blir ikke utdypet av utvalget. Tekna ser dette som en stor mangel ved rapporten, spesielt i den omstillingssituasjonen det norske samfunnet er i.

DGF – en sårbar infrastruktur i seg selv
Rapporten går i liten grad inn på sårbarhetene tilrettelegging for DGF kan ha. Rett nok blir faren for misbruk av dataene nevnt (side 36), men rapporten nøyer seg med summarisk å peke på myndighetene, E-tjenesten selv og enkeltindivider i E-tjenesten. Faren ved «uvedkommende interessenter» – som kan ha betydelig kompetanse og kapasitet – blir ikke diskutert. Mange av disse vil se den foreslåtte metadatasamlingen i regi av DGF som en svært nyttig kilde for planlegging av både cyber- og hybrid kriminalitet og -angrep. Slike interessenter kan utnytte, inkludert manipulere, både de innsamlede data og infrastrukturen for innsamling av slike data, uten nødvendigvis å bli oppdaget. Tekna ser disse faremomentene som grovt undervurdert av utvalget.

Sikring av hvor data lagres bør drøftes grundigere. Hvilken organisasjon som står for lagring er viktig. Tekna tar som en selvfølge at norsk-innhentede data vil bli lagret og behandlet i Norge. Vi ser imidlertid at glidning pga. konkurranseutsetting kan tenkes å skje. Påtrykk for konkurranseutsetting, også for datalagring, kommer av ulike grunner. Det er allerede kjent at data som blir sky-lagret ofte havner på servere utenfor landet, og at manglende kapasitet og kompetanse i Norge brukes som argument for bruk av tjenester i andre land.

Andre lands juridiske skranker for et norsk DGF
Trenden nå er at en stadig større andel av individ- og massekommunikasjon går gjennom «digitale nettverksmedia». Både metadata og innholdsdata blir dermed lukket for innsyn for DGF. Slike media er for en stor del under utenlandsk kontroll. Trafikken, selv mellom norske aktører, blir

grensekryssende, men tilgang til slike data vil ofte kreve domstolkjennelser i utlandet. I mange tilfeller vil den norske tjenesteproduksjonen foregå og ha et regionalt hovedkontor i et EU-land, men i flere tilfelle i andre land. Mest aktuelle er for tiden USA, India, Japan, Kina, og Korea. Tekna skulle gjerne sett en dypere diskusjon av hva dette vil bety for DGF.

Internasjonalt samarbeid gir innsikt, oversikt og tillit
Internasjonalt samarbeid kommer ikke klart nok frem i rapporten. Det nevnes at det vil være positivt for både norsk sikkerhetspoliti og etterretning med DGF med hensyn på internasjonalt samarbeid. Internett er i dag i stor grad uregulert. Dette skyldes at teknologisk utvikling går mye raskere enn juridiske avklaringer, og at internett i sin natur er internasjonalt og ikke kan begrenses av enkelte lands grenser og innenfor demokratiske prinsipper. Internasjonale samarbeid er eneste mulighet for demokratiske reguleringer som har praktisk betydning.

Norge må påvirke i de internasjonale fora der reguleringer utformes. I tillegg bør internasjonalt samarbeid for å forbedre prosesser diskuteres. At Norge jobber tett med internasjonale partnere bidrar i forhold til den kompetanse og forståelse som skal til for om mulig en gang i fremtiden få bedre regulering av internett.

Kontrollmekanismer kan ikke fullverdig løse de moralske og etiske problemstillingene overvåkning gir. Derfor mener vi transparens bør drøftes grundigere. Innsikt og oversikt kan være ekstra viktig både som iboende kontrollmekanisme mot misbruk og for innbyggernes tillit til systemet. Data som utveksles med andre lands myndigheter må også selvsagt underlegges kontrollmekanismer.

Oppsummering
Tekna mener behandlingen av premissene for overvåkning er mangelfulle, herunder både metoder for å omgå DGF og nytten av det. Dette gjør at forholdsmessighetsvurderingen i rapporten også blir mangelfull. Rapportens vurderinger om formålsglidning virker vel funderte, men grunnlaget de bygger på er spinkelt beskrevet. Dette gjør det enklere å presse på for en mandat- og formålsglidning i fremtiden.

Utvalgets konklusjon, om at et digitalt grenseforsvar vil «…virke modererende på det samlede nasjonale overvåkingstrykket....» mener vi ikke er godt nok fundert. På sikt vil det være nødvendig med svært inngripende metoder selv for å få til et minimum av innsyn i, og analyse av, data, jf. eksempelvis utviklingen med kryptert datatrafikk. Denne problemstillingen er ikke godt nok drøftet i rapporten. Tekna mener det finnes sterke teknologiske drivere som vil gi glidning mot et overvåkningsregime i Norge. Tekna mener at dette ikke er godt nok behandlet i rapporten. Ved en eventuell etablering av et DGF må det etableres en demokratisk og kompetent kontroll. EOS og domstolene må også besitte tilstrekkelig kompetanse. Tekna mener rapporten fra Lysne II-utvalget ikke utgjør et tilstrekkelig kunnskapsgrunnlag for å ta stilling til DGF.

Med vennlig hilsen
Tekna – Teknisk-naturvitenskaplig forening

Ivar Horneland Kristensen
Generalsekretær