UNINETT

Deres ref.: Vår ref.: 16/00635-2 Trondheim, 05.01.2017

Forsvarsdepartementet

Høringssvar til Forsvarsdepartementet – Lysne II-utvalgets forslag om etablering av digitalt grenseforsvar (DGF)

Innledning

Kommentarer i UNINETTs høringssvar til Lysne II-utvalgets forslag om innføring av DGF er drøftet med representanter for enkelte av universitetene i Norge: Universitetet i Oslo, Norges teknisk-naturvitenskapelige universitet, Universitetet i Tromsø og Norges miljø- og biovitenskapelige universitet.

Kommentarene i UNINETTs høringssvaret er likevel ikke å anse som de nevnte institusjonenes høringssvar. Disse institusjonene vil eventuelt formidle kommentarer og synspunkter i separate høringssvar.

UNINETT har i dette høringssvaret lagt vekt på å gi generelle kommentarer til Lysne II-utvalgets forslag. UNINETT har derfor ikke spesifikt vurdert betydningen som utvalgets forslag gir i et utdannings- eller forskningspolitisk perspektiv.

Hovedkommentarer

UNINETT mener at Lysne II-utvalget har lagt frem en bred og grundig vurdering av behovet for og argumenter imot etablering av DGF til etterretningsformål. Utvalget presenterer og drøfter en fremtidig løsning for kontroll av grenseoverskridende elektronisk kommunikasjon hvor motstridende hensyn, spesielt etterretningsbehov, personverninteresser og rettssikkerhetsgarantier, blir forsøkt ivaretatt på en balansert måte.

UNINETT er særlig glad for at utvalget legger stor vekt på åpenhet omkring det foreslåtte kontrolltiltaket, og at det inviteres til en bred samfunnsdebatt om de viktige og vanskelige problemstillinger som utvalgets forslag reiser. UNINETT legger spesielt merke til utvalgets grundige drøftelse av de personvernmessige utfordringer som DGF kan tenkes å innebære, og er tilfreds med at disse utfordringene har inntatt en sentral plass i utvalget forslag til utforming av et fremtidig DGF.

Postadresse
UNINETT AS
Postboks 7469 Sluppen
7465 TRONDHEIM

Besøksadresse
Abels gt. 5
7465 TRONDHEIM

Foretaksnr.: 968 100 211
Bankgiro: 4200 40 67953

E-post: postmottak@uninett.no
Tlf.: +47 73 55 79 00
Fax: +47 73 55 79 01

Responsmiljøet ved UNINETT, som monitorerer trafikken i forskningsnettet i Norge og tilbyr analyse- og sikkerhetstjenester til universiteter og høyskoler, har i løpet av de siste årene registrert at uønsket aktivitet i det digitale rom rettet mot norske forsknings- og utdanningsmiljøer har økt i omfang og blitt mer avansert enn tidligere. UNINETT besitter imidlertid ikke detaljert kjennskap til de bakenforliggende årsaker og hvem de ansvarlige trussel-aktørene er. Informasjon fra andre nasjonale responsmiljøer, blant annet NorCERT, og PSTs trusselvurdering for 2016 (side 4, 7, 9 og 22) antyder også at fremmede trussel-aktører trolig har økt sitt fokus på digital etterretningsvirksomhet også innenfor forskningssektoren og høyere utdanning.

UNINETT er derfor i utgangspunktet enig med utvalget i at det er behov for å styrke den nasjonale evnen til å avdekke og håndtere alvorlige eksterne trusler rettet mot norske interesser i det digitale rom, særlig knyttet til større elektroniske angrep eller omfattende elektronisk spionasje utført av fremmede (utenlandske) aktører.

Samtidig deler UNINETT utvalgets bekymringer når det gjelder de potensielle negative konsekvenser knyttet til personvern, tillit og ytringsfrihet som utvikling og etablering av et fremtidig DGF kan medføre. Dette gjelder særlig fire momenter som vies stor oppmerksomhet i utvalgets rapport, i tillegg til betydningen som nye dommer fra EU-domstolen kan tenkes å få for DGF:

1. **Formålsglidning**

Utvalget fremhever at det er avgjørende viktig at DGF ikke anvendes til andre formål enn utenlandsk etterretning. Problemet som utvalget peker på i denne sammenheng er at det kan være fristende å utvide formålsbeskrivelsen etter at kontrolltiltaket er etablert, for eksempel ved at det også gis tillatelse til å anvende innsamlede innholds- eller metadata i etterforskning av alvorlig innenlandsk kriminalitet. Utvalget hevder imidlertid at problemet med formålsglidning kan imøtegås gjennom stram lovregulering, et omfattende godkjennings-, tilsyns- og kontrollregime, samt innebygde tekniske styrings- og kontrollmekanismer (søke- og tilgangsbegrensninger, sporing/logging, osv.). Dersom disse tiltakene blir innført, mener utvalget at det er etablert robuste hindre mot formålsglidning.

UNINETT stiller seg bak de bekymringer som utvalget her gir stemme til, og mener at formålsglidning kan utgjøre en viktig trussel mot kontrolltiltakets integritet og legitimitet. UNINETT mener derfor at det er avgjørende at kontrolltiltakets formål opprettholdes over tid, og at utvalget foreslår hensiktsmessige tiltak for å ivareta dette hensynet. UNINETT ønsker likevel å påpeke at de foreslåtte tiltakene ikke gir noen garantier mot formålsglidning. Dersom det skulle oppstå alvorlige hendelser (for eksempel draps-, overgreps- eller grove narkotikasaker) som får stor medial

Postadresse
UNINETT AS
Postboks 7469 Sluppen
7465 TRONDHEIM

Besøksadresse
Abels gt. 5
7465 TRONDHEIM

Foretaksnr.: 968 100 211
Bankgiro: 4200 40 67953

E-post: postmottak@uninett.no
Tlf.: +47 73 55 79 00
Fax: +47 73 55 79 01

oppmerksomhet, men som faller utenfor virkeområdet for DGF (utenlandsk etterretning), kan det bli vanskelig for nasjonale beslutningstakere å motstå krav fra media, opinionen, aktivistgrupper eller etterforskningsorganer om at DGF også må kunne anvendes til å avdekke og håndtere denne typen hendelser. Kontrolltiltaket er særlig viktig for å hindre formålsglidning i tilfelle DGF ikke gir den forventede etterretningsverdi som følge av teknologidreininger eller en annen teknologibruk enn det Lysne-utvalget har forutsatt, se også senere avsnitt om inngrep i endeutstyr.

Faren for formålsglidning vil også påvirkes av om de foreslåtte domstols- og tilsynsorganer tilføres nødvendig ekspertise og ressurser til å ivareta sine oppgaver på en effektiv måte. Videre er det avgjørende at domstols- og tilsynsorganene opptrer uavhengig overfor E-tjenesten, og at kontakten mellom kontrollorganer og E-tjenesten ikke blir så tett at godkjennings- og tilsynsordninger hovedsakelig ivaretar etterretningsinteresser fremfor samfunnets behov for innsyn i og styring av virksomheten.[1]

Hovedutfordringen, slik UNINETT ser det, er at det kan være problematisk å forskuttere formålsintegriteten til DGF for all fremtid, selv om utvalgets forslag til tiltak for å unngå formålsglidning blir iverksatt. I denne sammenheng blir det viktig med åpenhet omkring prinsippene for informasjonsdelingen mellom EOS-tjenestene slik at integriteten og legitimiteten til et eventuelt DGF-system ikke undergraves av unødig hemmelighold, og at kontrollorganene har nødvendige ressurser og uavhengighet til å utføre sitt oppdrag.

2. Nedkjølingseffekten

Utvalget fremhever at DGF medfører omfattende innsamling av data om befolkningens aktiviteter i det digitale rom. Vissheten om dette kan føre til at enkeltindivider eller grupper blir mer forsiktige med å uttrykke sine meninger eller holdninger i politiske og samfunnsaktuelle spørsmål ved bruk av elektroniske kommunikasjonsverktøy enn hva som ellers ville vært tilfelle. Utvalget mener derfor at DGF kan tenkes å ha negative virkninger på den frie meningsdannelsen i samfunnet.

Også dette er en bekymring som UNINETT deler, selv om forskning indikerer at det er stor grad av usikkerhet knyttet til hvor reell, kraftig og langvarig nedkjølingseffekten faktisk kan sies å være. UNINETT mener likevel at muligheten for at det kan oppstå en nedkjølingseffekt i kjølvannet av DGF gjør det ekstra viktig at formålsglidning forhindres, og at det legges opp til størst mulig åpenhet omkring E-tjenestens innsamling og den videre håndteringen av innholds- og metadata.

[1] Viktigheten av at domstols- og tilsynsorganer ivaretar sine oppgaver på en tilfredsstillende måte, illustreres av oppslag i svenske media. Her hevdes det at kontrollen med Försvarets radioanstalts (FRA) monitorering av internettrafikk har vært til dels mangelfull. Dette hevdes blant annet å ha ført til at avvik, for eksempel at FRA feilaktig har utlevert data til det svenske sikkerhetspolitiet (Säpo), ikke har blitt fulgt godt nok opp. Det stilles også spørsmål ved om informasjonssikkerheten i det svenske grenseforsvarssystemet er tilfredsstillende. Se Dagens Nyheter 11.12.2016, tilgjengelig på http://www.dn.se/nyheter/sverige/facit-inte-ett-enda-larm-efter-atta-ar/ og http://www.dn.se/nyheter/sverige/fras-kansliga-information-kan-hamna-i-fel-hander/.

Postadresse
UNINETT AS
Postboks 7469 Sluppen
7465 TRONDHEIM

Besøksadresse
Abels gt. 5
7465 TRONDHEIM

Foretaksnr.: 968 100 211
Bankgiro: 4200 40 67953

E-post: postmottak@uninett.no
Tlf.: +47 73 55 79 00
Fax: +47 73 55 79 01

Uten at disse hensynene ivaretas er det, etter UNINETTs oppfatning, ikke helt usannsynlig at en eventuell innføring av DGF kan bidra til en viss nedkjøling av den delen av det offentlige (og private) ordskifte som skjer ved hjelp av elektroniske kommunikasjonsverktøy.

3. Inngrep i endeutstyr

Utvalget fremhever at økt elektronisk kontroll som følge av DGF kan føre til mer bruk av kryptografi på endeutstyr. Dette er i så fall en utvikling som, ifølge utvalget, representerer en reell fare for at kontrolltiltaket ikke vil oppnå sin tiltenkte hensikt.

UNINETT deler utvalgets oppfatning om at innføring av DGF kan tenkes å bidra til økt bruk av kryptografi for å beskytte sensitiv kommunikasjon, spesielt dersom befolkningens tillit til DGF svekkes (eller i utgangspunktet er begrenset). Økt bruk av kryptografi kan videre bidra til å svekke den etterretning som gjøres med hjelp av dagens metoder.

Dersom innføring av DGF bidrar til økt anvendelse av kryptografi på endeutstyr, ser UNINETT det ikke som usannsynlig at det vil gi økt legitimitet til forslag om at E-tjenesten, eller andre EOS-tjenester, må kunne gripe inn i endeutstyret for å få tilgang til data som DGF ikke gir tilgang til, eventuelt lede til krav om lovregulering av bruken av kryptografi. Alternativet til dette kan, som utvalget påpeker, være at hensikten med DGF vanskelig lar seg realisere.

Slik UNINETT ser det, vil dette være en utglidning sammenliknet med utvalgets forslag, hvor det blant annet synes å være en forutsetning at kryptografi ikke skal reguleres rettslig (jf. også diskusjon om lovregulering av kryptografi i NOU 2015: 13, Digital sårbarhet). UNINETT kan likevel ikke se at utvalget har diskutert muligheten for økt press på endeutstyr i særlig grad, eller hvilke konsekvenser dette eventuelt kan få for person- og kommunikasjonsvernet.

Tilsvarende kan man se for seg at angripere vil flytte innsatsen mot å kompromittere ressurser på innsiden av DGF, og iverksette angrepene derfra. Uønsket aktivitet fra angriperne, som for eksempel eksfiltrering eller rekognosering, mot norske interesser vil da ikke kunne oppdages av DGF, men foregå på innsiden av grenseforsvaret. Dette er noe som på tross av DGF kan peke i retning av en økt sikkerhetstrussel mot digitale ressurser på norsk jord.

4. DGF sett i lys av nye dommer fra EU-domstolen

UNINETT har merket seg at EU-domstolen nylig har avsagt to dommer vedrørende nasjonal lovgivning som tillater masseregistrering av elektroniske trafikkdata (Sverige og Storbritannia).[2] Særlig interessant i denne sammenheng er at EU-domstolen slår fast at lagring og etterfølgende behandling av trafikkdata som omfatter all elektronisk kommunikasjon i en hel befolkning, og hvor formålet er bekjempelse av alvorlig

[2] Dom 21. desember 2016, Tele2 Sverige AB v. Post- och telestyrelsen, C-203/15; dom 21. desember 2016, Secretary of State for the Home Department v. Watson, Brice and Lewis, C-698/15.

Postadresse
UNINETT AS
Postboks 7469 Sluppen
7465 TRONDHEIM

Besøksadresse
Abels gt. 5
7465 TRONDHEIM

Foretaksnr.: 968 100 211
Bankgiro: 4200 40 67953

E-post: postmottak@uninett.no
Tlf.: +47 73 55 79 00
Fax: +47 73 55 79 01

kriminalitet, går ut over det som er nødvendig i et demokratisk samfunn. Slik masseregistrering er derfor ulovlig.

Norge er på dette området bundet av tilsvarende rettslige prinsipper som gjelder i EU. Spørsmålet UNINETT ønsker å reise er derfor om dommene fra EU-domstolen kan tenkes å få konsekvenser for forslaget om etablering av DGF? Vil utvalgets forslag måtte revideres eller trekkes tilbake sett i lys av de nevnte dommene, eller er formålet med og utformingen av DGF slik at revidering eller tilbaketrekking ikke er påkrevd?

Øvrige kommentarer

I tillegg til momentene som er diskutert ovenfor, vil UNINETT knytte enkelte kommentarer til andre forhold som diskuteres i utvalgets rapport.

For det første fremstår spørsmål om hvilke administrative og økonomiske konsekvenser som utvalgets forslag innebærer som uklare. Utvalget mener riktignok at kostnadene for nett-tilbyderne blir svært begrensede fordi det legges til grunn at staten dekker de kostnader som påløper som følge av tilretteleggingsplikten. Det er imidlertid noe uklart hvor omfattende denne tilretteleggingsplikten eventuelt vil bli og hva den i praksis vil innebære, både på kort og lang sikt. Det fremstår også som uavklart om nettoperatører i statlige sektorer vil få dekket de kostnader som påløper ved innføring og drift av DGF eller om dette bare vil gjelde for private tilbydere.

For det andre ønsker UNINETT å påpeke at stadig flere høykapasitets utenlandslinker, økt bruk av internasjonale skytjenester, løpende nettbasert tjenesteutvikling og tilsvarende endringer i befolkningens bruksmønstre, trolig vil stille svært høye krav til skalering av DGF, både når det kapasitet, det store antallet linker og deres geografiske spredning. Skaleringsproblematikk vil blant annet gjøre seg gjeldende med hensyn til utplassering og oppgradering av sensorteknologi. Også her fremstår det som noe uklart hvor store de fremtidige skaleringskostnadene kan bli, hvem som skal dekke disse kostnadene, spesielt i forhold til nett-tilbydere i statlig sektor, og hvordan ansvarsfordelingen mellom E-tjenesten og nett-tilbyderne er tenkt å være.

For det tredje mener UNINETT at DGF kan bli et viktig angrepsmål og kilde til datalekkasje i seg selv. Tilfredsstillende og kontinuerlig logisk og fysisk sikring av de store mengder innholds- og metadata som samles inn og behandles i DGF fremstår derfor som en svært viktig og ressurskrevende oppgave. Utvalget har kommentert disse utfordringene i sin rapport, men det savnes en nærmere drøftelse av behovet for og problemer knyttet til informasjonssikkerheten i DGF. UNINETT mener at det er svært viktig med tydelighet når ansvaret for informasjonssikkerheten i DGF skal fordeles mellom involverte aktører. Den løpende praktisering av dette ansvaret må også være gjenstand for jevnlige revisjoner, ikke minst på teknisk nivå.

Postadresse
UNINETT AS
Postboks 7469 Sluppen
7465 TRONDHEIM

Besøksadresse
Abels gt. 5
7465 TRONDHEIM

Foretaksnr.: 968 100 211
Bankgiro: 4200 40 67953

E-post: postmottak@uninett.no
Tlf.: +47 73 55 79 00
Fax: +47 73 55 79 01

Til slutt mener UNINETT at innføring og drift av DGF kan tenkes å bidra til en form for «falsk trygghet». Med dette menes at DGF kan føre til at innenlands operatører og eiere av endesystemer opplever at sikkerheten helt eller delvis blir ivaretatt gjennom DGF, slik at det lokale fokuset på sikkerhet svekkes. UNINETT mener at det er svært viktig at en eventuell innføring av DGF ikke fører til slike utilsiktede virkninger mht. det lokale sikkerhetsfokuset og -innsatsen. Samtidig er det viktig at DGF ikke står i veien for eller bremser utviklingen og styrkingen av det tverrsektorielle samarbeidet på sikkerhetsområdet. Her ønsker UNINETT igjen å peke på det paradoksale i at DGF kan bidra til at angripere forsterker fokuset mot kompromittering av potensielle brohoder på innsiden av DGF, der etterretningsmessig interessant kommunikasjon over grensen vil være mindre les- og tolkbar enn i dag.

Hilsen

UNINETT

Petter Kongshaug

Adm. Dir.

Dette dokumentet er elektronisk signert og har derfor ingen håndskreven signatur

Postadresse
UNINETT AS
Postboks 7469 Sluppen
7465 TRONDHEIM

Besøksadresse
Abels gt. 5
7465 TRONDHEIM

Foretaksnr.: 968 100 211
Bankgiro: 4200 40 67953

E-post: postmottak@uninett.no
Tlf.: +47 73 55 79 00
Fax: +47 73 55 79 01