POLITIETS
SIKKERHETSTJENESTE

Postboks 4773 Nydalen
0421 OSLO
post@pst.politiet.no
Tlf.nr. 23 30 50 00
Faksnr. 23 30 51 20
Besøksadresse:
Nydalen allé 35

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

Deres ref.: 2016/2699-1
Vår ref.: 16/12123-6
Dato: 20. januar 2017

Innspill fra PST til rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar

Politiets sikkerhetstjeneste (PST) viser til høringsbrev fra Forsvarsdepartementet (FD) angående rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar (DGF). Fristen for å avgi høringsuttalelse var 6. januar d.å. PST ble etter anmodning innvilget utsatt frist til 20. januar s.å.

PST ser det som positivt at spørsmålet knyttet til lovhjemmel for DGF i Norge nå er utredet nøye. Rapporten drøfter grundig behovene for en etablering av DGF og har også særskilt og nødvendig fokus på personvern- og rettssikkerhetsaspektene ved en slik etablering.

DGF vil innebære potensiell tilgang til svært mye informasjon og PST støtter at det må være en forutsetning for en eventuell hjemmel at det både gis en formålsavgrensning og etableres nødvendige godkjenningsordninger, samt etterfølgende kontroll. Vi ser det også som positivt at informasjonsutveksling knyttet til DGF reguleres nøye for å hindre formålsutglidning.

PST merker seg at rapportens redegjørelse for behovet også fremhever PSTs behov for opplysninger innhentet gjennom DGF. Innledningsvis finner vi grunn til å understreke at PST i sin oppgaveløsning selvsagt vil dra fordeler av at Etterretningstjenesten i størst mulig grad gjøres i stand til å løse sin oppgaveportefølje. Det er et nasjonalt ansvar å gjøre landets sikkerhets- og etterretningsorganisasjoner i stand til en optimal løsning av sine oppgaver innenfor de rettssikkerhetsmekanismer staten oppstiller. Når det er sagt, forutsetter PST at den informasjonsutveksling som skjer mellom Etterretningstjenesten og PST skjer innenfor gjeldende rettslige skranker og leser ikke utvalgets rapport dithen at det ønskes etablert ny rett på dette området.

Slik vi ser det, er det særlig to forhold som viser behovet for etablering av DGF;

For det første har trusselbildet endret seg betraktelig de senere årene. Begge scenariene beskrevet i rapporten reflekterer trusselbildet slik PST vurderer det. Vi ser at det er en eskalering av cybertrusler mot Norge og norske interesser. Fremmede tjenester bruker

avanserte datanettverksoperasjoner mot mål innen forsvars- og beredskapssektor samt mot politiske beslutningsprosesser og kritisk infrastruktur. Flere av tjenestene med interesser i Norge har de senere årene brukt store ressurser på å utvikle kapasitet innen digital spionasje og har forsøkt å kompromittere datasystemer hos virksomheter som forvalter grunnleggende nasjonale verdier og store kommersielle interesser.

Videre er terrortrusselen kompleks og til dels uforutsigbar. ISIL har oppfordret sympatisører til å gjennomføre angrep på egen hånd. Et angrep mot Europa kan også være sentralstyrt eller delegert fra ISILs øverste ledelse. Det siste året har det i tillegg vært flere eksempler på at personer har vært sendt med flyktningstrømmen til Europa for å aksjonere. I denne sammenhengen vil DGF, slik PST forstår det, kunne fange opp kommunikasjonen mellom gruppens ledelse i utlandet og støttestrukturer i Norge på et tidlig tidspunkt.

Det er ikke bare trusselbildet som har endret seg, også kommunikasjonsmetoder og bevegelsesmønstre har utviklet seg betraktelig. I følge den svenske FRA-myndigheten går 95 % av all elektronisk kommunikasjon mellom Sverige og utlandet i sjø- og landbaserte kabler. Det er sannsynlig at den overveiende delen av elektronisk kommunikasjon mellom mulige trusselaktører over landegrensene per i dag går i disse kablene. Problemstillingen er også aktuell når det gjelder tidlig deteksjon av mulige cyberangrep.

Manglende hjemmel for DGF, vanskeliggjør Etterretningstjenestens tilgang til hoveddelen av elektronisk kommunikasjon mellom trusselaktører i deres planlegging av terror. PST ser det derfor som viktig for å sikre norske interesser at man tar inn over seg den teknologiske utviklingen og de kommunikasjonsformene som nå foreligger, og at det legges til rette for en klar lovhjemmel. Utvalget skriver i sin rapport at Etterretningstjenesten i dag kun har meget begrenset evne til å kunne fange opp utenlandsk kommunikasjon som kan utgjøre alvorlige sikkerhetsutfordringer for landet og som skjer over Norges landegrenser.

Videre ser vi det som nødvendig å etablere nasjonal kontroll på denne type informasjon.

Mange av våre samarbeidspartnere har allerede i dag en slik tilgang til informasjon som DGF legger opp til. PST kan ved henvendelse til disse motta informasjonen. Dette innebærer imidlertid et forsinkende element i PSTs arbeid med å avdekke en eventuell terrortrussel. I tillegg må vi henvende oss bredt for å få tak i informasjonen. Det er heller ikke gitt at Norge vil bli gitt nødvendig prioritet hos andre tjenester og at disse vil ha som primærfokus å beskytte norske interesser. Dagens trusselbilde tatt i betraktning, bør ikke PST være avhengig av samarbeidspartnere for å fange opp kommunikasjon til og fra Norge.

Hastelementet vil bli ivaretatt i betydelig større grad om den nasjonale etterretningstjenesten settes i stand til en tilsvarende innhenting, og PST får tilgang til denne informasjonen i de tilfellene der dette er relevant for vår oppgaveløsning. Da vil Norge som nasjon gjøres mindre avhengig av våre samarbeidspartnere, hvilket vil sikre nasjonal kontroll over innhentingen, samt at vi i større grad vil være i stand til å agere umiddelbart. I tillegg vil informasjonen være knyttet til nasjonale forhold. Dette er viktige momenter for PST.

Deling av informasjon med PST

I rapportens side 60 andre spalte annet kulepunkt anbefaler utvalget at all overskuddsinformasjon skal slettes og ikke overføres til andre offentlige myndigheter. PST legger til grunn at det som av Etterretningstjenesten ikke oppfattes som

overskuddsinformasjon, kan deles med PST der dette anses relevant og nødvendig for PSTs oppgaveløsning. Dette fremgår for så vidt av rapportens side 61 andre spalte siste avsnitt, og PST oppfatter det derfor slik at Etterretningstjenesten kan dele informasjon med PST etter det ordinære delingsregimet som er gjeldende i dag, slik at vi kan benytte informasjonen som inngangsverdi for egen metodebruk eller etterforskning.

Informasjon innhentet gjennom DGF som bevis i straffesak

Utvalget konkluderer med at informasjon innhentet gjennom DGF ikke skal kunne føres som bevis i straffesak. Slik PST forstår utvalget er dette begrunnet i en formålsavgrensning som innebærer at data samlet inn for et formål ikke skal kunne anvendes for andre formål. Formålet med DGF er å sette Etterretningstjenesten bedre i stand til å innhente etterretninger om utenlandske trusselaktører og relevante utenlandske mål innenfor det de oppgavene som tjenesten er satt til å utføre. Å åpne opp for at informasjon innhentet ved hjelp av DGF skal kunne benyttes som bevis i en straffesak, vil etter utvalgets syn innebære en formålsglidning som vil være problematisk i forhold til de forholdsmessighetsvurderingene som ligger til grunn for en eventuell etablering av DGF.

PST mener det vil være uheldig å lovfeste et slikt forbud for så vidt gjelder bevis knyttet til terrorhandlinger. Det vises først og fremst til statens generelle ansvar for å sikre borgerne, og avvergeplikten lovfestet i straffeloven (2005) § 196, og at et eventuelt bevisforbud kan komme i konflikt med avvergeplikten. Uten anledning til å benytte nødvendig og relevant informasjon kan muligheten for straffeforfølgning som virkemiddel mot terrorhandlinger bli redusert. Dette vil igjen kunne medføre at borgernes forventning om at staten ivaretar deres sikkerhet ikke blir møtt – noe som vil være uheldig for rettsstaten.

Det kan trekkes en parallell til skillet mellom PSTs forebyggende virksomhet og etterforskning, hvor hovedregelen er at informasjon innhentet gjennom bruk av tvangsmidler i forebyggende øyemed, ikke skal kunne benyttes som bevis i en straffesak. Fra dette utgangspunktet er det gjort et unntak i politiloven § 17 f bokstav c) for terrorhandlinger, jf. straffeloven §§ 131, 133 og 134.

I praksis har dette imidlertid ikke kommet på spissen og PST har til nå ikke sett seg nødt til å benytte sensitiv etterretningsinformasjon som bevis i straffesak for eksempelvis for terrorhandlinger. For det tilfellet at informasjon innhentet gjennom DGF kunne utgjøre bevis for en terrorhandling, vil det imidlertid være egnet til å skade tilliten til både Etterretningstjenesten og PST hvis ikke PST skal kunne nyttiggjøre seg dette. Det bør således åpnes for at informasjon om terrorhandlinger også kan benyttes som bevis.

Marie Benedicte Bjørnland