Høringssvar - Digitalt grenseforsvar (DGF) Lysne II-utvalget

Undertegnede jobber til daglig med sikring av samfunnskritisk infrastruktur og har erfaring fra ulike sektorer som forsvar, finans, industri og helse. Synspunktene i dette høringssvaret er mine personlige meninger og de har ingen forbindelser med min nåværende (eller tidligere arbeidsgivere) eller utdanningsinstitusjoner.

Innledningsvis vil jeg si at rapporten på en god måte belyser mange av de utfordingene man står ovenfor når det gjelder å sikre det norske samfunnet mot digitale trusler, men konklusjonene synes noe forhastet å konkludere postivt til innføring av DGF gitt de utfordringer rapporten faktisk peker på.

Merknader som følger:

Mandatet og utvalget (1.1 mv.)

"Forsvarsministeren nedsetter et utvalg for å utrede sentrale problemstillinger knyttet til Etterretningstjenestens mulige tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge (digitalt grenseforsvar).

Bruken av det nøytrale ordet 'elektronisk informasjon' og DGF fjerner mye av personvernaspektet i de sentrale problemstillingene som ønskes utredet. SIGINT i tradisjonell forstand forsøker å skaffe seg tilgang til fiendens kommunikasjon, men dette utgjør bare en liten brøkdel av informasjonen som kommuniseres i de fiberoptiske kablene og som i økende grad er personopplysninger. EU sin personvernforordning har som målsetting å åpne det digitale indre marked og 'elektronisk informasjon' vil derfor etterhvert omfatte stadig mer sensitive personopplysninger som f.eks helseopplysninger. Stadig mer økende bruk av skytjenester forsterker også dette. Det er uheldig for den brede offentlige debatten man har ønsket seg at man innledningsvis ikke benytter mer presise begreper som gjør at man forstår at man her snakker om bulk datainnsamling. Utvalget kunne også gjerne vært forsterket med personer som har erfaring med myndigheters overvåkning og med ofre for terror/cyberangrep.

4.5 Om kryptering

Det kommer ikke helt klart fram at det i tillegg til sterk kryptografi også eksisisterer en krypteringsalgoritme som er matematisk perfekt - 'One time pad' [1]. Denne er av mange kryptoeksperter ansett som praktisk ubrukelig da krypteringsnøkler må være helt tilfeldig generert, like lange som klarteksten og kun benyttes én gang. Nøkkelutveksling er også ansett som en stor utfordring, men algoritmen ble likevel benyttet under den kalde krigen for å sikre kommunikasjon og har nylig også gjenoppstått i moderne kvantekryptografiske protokoller.

En god del trusselaktører f.eks terrorister har imidlertid ikke behov for en nøkkelutveksling i industriell skala som Public Key Infrastructure (PKI) gir - her kan det være veldig få parter som kommuniserer, eller celler som kun kommuniserer med andre predefinerte celler.

Scenarie – to terrorister utveksler i skjul et par micro-SD kort med 'one time-pad'. De er nå istand til å utveksle på en kryptografisk og matematisk perfekt sikker måte en informasjonsmengde tilsvarende kapasitet på kortet uten at DGF operatører hverken nå eller i framtiden kan finne ut av innholdet.

[1] Matematisk bevis for at 'One time pad' er teoretisk perfekt er kjent fra kryptografien og finnes I "Communication Theory of Secrecy Systems" Claude Shannon 1949

Det kreves tilgang til nøkkel og denne må da framskaffes på annen måte f.eks via kleptografiske bakdører i enhetene eller andre sårbarheter i disse – avlytting av selve kommunikasjon er nytteløst. Metadata med IP adresser vil også være svært vanskelig tilgjenglig hvis de også benytter seg av anonymiseringsverktøy som f.eks Tor[2], se også [3] for referanse.

9.2 Et mulig DGF-system med kontrollmekanismer

For å forhindre manipulering av logger så bør disse sikres med f.eks block chain teknologi (benyttes i Bitcoin). Det er heller ikke tilstrekkelig å kun sikre applikasjonsloggene til operatørene, også selve operativsystem og databaseloggene må sikres og gjennomgås tilsvarende som operatørenes applikasjonslogger. Lagringssystemet er også en potensiell utfording med tredjeparts tilgang til servere og disksystemer for vedlikehold. Bakdører kan også være implentert i maskinvare til infrastruktur allerede ved leveranse av nettverksutstyr, servere og lagringsenheter/disker til DGF[4].

DGF og risiko for tillitskapitalen i det norske samfunnet

Rockeartisten Roger Waters besøkte Oslo Spektrum for noen år side og sang følgende: 'Mother should I trust the government?' – på scenen lyste med meterhøy rød skrift 'No Fucking Way'. Han tilføyde imidlertid: "However, when I sing that line in Norway, the audiences always look puzzeled. Maybe because they have a trustworthy government?

Statlige institusjoner, herunder Forsvaret nyter relativt stor tillit i befolkningen, men den oppbygde 'tillitskapitalen' kan utsettes for risiko gjennom bulk innsamling av data. Historien har tidligere vist at ulovligheter begås ref. Lund kommisjonen og overvåkning av venstresiden i Norge. Det er derfor stor risiko for at ulovligheter begås hvis de antar at sjansen for å bli oppdaget er liten, ref avsløringer rundt ulovlig bruk hos NSA ansatte som overvåket ektefeller og kjærester5. NRK radio meldte på nyhetene 06.01.17 om at politiets tillit i befolkningen var synkende i befolkningen generelt og på Vestlandet spesielt.

DGF vil innebære opprettelse av ny sårbar infrastruktur

Gitt datamengden som et tenkt DGF vil inneholde, så vil dette være et attraktiv mål i seg selv for en rekke trusselaktører og risiko knyttet til dette bør utredes nærmere. Data i DGF må raskt kunne tilintetgjøres ved en okkupasjon eller ved et statskupp.

Med vennlig hilsen

Sjur Hartveit

[2] 'Why Tor Stinks' http://securityaffairs.co/wordpress/18397/hacking/tor-anonymity-tor-stinks.html
[3] https://www.schneier.com/blog/archives/2015/11/paris_terrorist.html
[4] https://techcrunch.com/2014/05/12/nsa-allegedly-intercepts-shipments-of-servers-to-install-spying-backdoors/
[5] http://www.pcworld.com/article/2050100/nsa-admits-employees-spied-on-loved-ones.html