DET NASJONALE STATSADVOKATEMBETET

FOR BEKJEMPELSE AV ORGANISERT OG ANNEN ALVORLIG KRIMINALITET

Forsvarsdepartementet
Postboks 8126 Dep
0032 Oslo

Deres referanse	*Vår referanse*	*Dato*
2010/00794-1/FD I /OFD	61/10-2/IMS	23.06.10

Høring – Nasjonal strategi for cybersikkerhet

1. Innledning

Det vises til høringsbrev av 30. mars 2010 fra Forsvarsdepartementet med forslag til strategi for cybersikkerhet. Saken kom inn til Det nasjonale statsadvokatembetet (NAST) torsdag 17. juni. Med frist til 25. juni har det ikke vært mulig å innhente statistikk og eldre dokumentasjon av interesse for saken. Etter anmodning fra riksadvokaten avgir NAST uttalelse direkte til Forsvarsdepartementet, med kopi til Justisdepartementet (Politiavdelingen) og riksadvokaten.

2. Støtte til NSMs initiativ

NSM har tatt et viktig initiativ ved å legge frem forslag til en nasjonal strategi for cybersikkerhet, som NAST støtter. Det er dessverre slik at nå, ca 10 år etter at det ble truffet politiske beslutninger om en strategisk satsing på en koordinert innsats mot trusler via elektronisk nettverk, er innsatsen hos de ansvarlige organer fremdeles ukoordinert. I et rettshåndhevelsesperspektiv kan det konstateres at effektive samarbeidsrutiner for varsling og anmeldelse fremdeles mangler, noe som leder til at det i årenes løp bare har vært et fåtall straffesaker om dataangrep. Dette til tross for at mørketallene er store. Med så lavt reaksjonsnivå oppnås ingen allmennpreventiv virkning, fordi lovbryterens risiko for å bli holdt ansvarlig åpenbart er meget lav. Et tettere samarbeid innrettet på å nå felles mål mellom organene, er påkrevet for å kunne gi en troverdig respons med allmennpreventiv effekt på området.

Utviklingen i Norge har gått i retning av at trafikkdata fra ISPer lagres i stadig kortere tid. Etter dagens regler lagres dette nå kun i 21 dager. Denne lagringstiden er helt uforenlig med troverdig bekjempelse av cyberkriminalitet. Behovet for lengre lagring er spilt inn i gjeldende høring om

Postadresse: Postboks 8044 Dep 0030 OSLO
Kontoradresse: Brynsalléen 4 0667 OSLO
Telefon: 23 17 42 00
Telefax: 23 17 42 10

implementering av EUs datalagringsdirektiv. Dersom direktivet (eller lignende regler) ikke vedtas i Norge er det etter NASTs oppfatning et bevisst valg om at etterforsking på dette området skal nedprioriteres. De vurderinger som skal gjøres om nasjonal strategi for cybersikkerhet må derfor ses i sammenheng med de vurderinger som gjøres rundt implementering av datalagringsdirektivet.

NAST fremhever på denne bakgrunn betydningen av - og gir sin fulle tilslutning til - strategiens hovedmål nr. 1, nemlig "å etablere en felles situasjonsoversikt og forståelse". Situasjonsforståelsen må imidlertid forankres *på ledernivå* i hver enkelt organisasjon. Med et blikk på politiets lave innsats de siste 5 år (se pkt. 6), er det klart utilstrekkelig alene å utpeke personer nedover i organisasjonen med ansvar for håndteringen av saker, fordi en effektiv innsats forutsetter støtte fra ledelsen gjennom tydelige prioriteringer.

3. Politiets og påtalemyndighetens rolle

Politiets og påtalemyndighetens rolle på området er å etterforske, påtaleavgjøre og iretteføre saker. Aktiviteten er rettslig styrt og av reaktiv karakter, dvs. at den iverksettes etter at en straffbar handling har skjedd. Sett fra politiets side er det derfor klart at strategien for cybersikkerhet bør ha en "defensiv innretting" slik det står i strategien pkt. 2 s. 13. I pkt. 2.5 om etterforsking og bekjempelse av "IKT-hendelser" står det imidlertid i tiltakspunkt nr. 20 (s. 21) om "Offensive kapasiteter" som gjelder militær innsats på området. "Offensive tiltak" mot gjerningsmenn er også nevnt i kulepunkt 4 på s. 20.

Spenningsforholdet mellom defensiv og offensiv innsats illustrerer behovet for "en felles situasjonsoversikt og forståelse" som nevnt. NAST understreker imidlertid at til tross for at politiets innsats som utgangspunkt er reaktiv, finnes et visst rom for en mer proaktiv innsats, blant annet i form av infiltrasjon på nett mv. Forslag til eventuelle nye retningslinjer om dette er under utarbeidelse hos NAST. Dialog med kompetansen ved et cybersenter om aktuell metodebruk, er åpenbart hensiktsmessig for å kunne gjøre retningslinjene så relevante som mulig. Dermed lettes også samarbeidsmulighetene, fordi det åpnes for at polititjenestemenn under påtalemessig styring kan yte bidrag til cybersenteret med tanke på å fange opp saker.
I forhold til tiltakspunkt nr. 20 om "Offensive kapasiteter", tillater NAST seg å påpeke at i fredstid er de aktuelle "IKT-hendelsene" å anse som kriminelle handlinger som rammes av straffeloven. De senere år er det gjort atskillig arbeid nasjonalt og internasjonalt for å styrke og

harmonisere lovverket. I Norge forbedres situasjonen ytterligere når straffeloven 2005 settes i kraft.

Det er neppe treffende å ta som utgangspunkt at "cyberspace er uregulert i sin natur", slik det står i strategidokumentet s. 20. Utfordringene knytter seg til å etablere *effektive samarbeidsrutiner* mellom ansvarlige organer nasjonalt, og tilsvarende i forhold til internasjonale samarbeidspartnere, fordi man jevnlig er avhengig av opplysninger fra utlandet for å oppklare sakene. Dette bør være cybersenterets hovedfokus. NAST antar at cybersenteret ved å virke som drivkraft for skjerpet bevissthet og koordinert innsats, kan bidra til å realisere dette.

4. Volum – og relevante mål for virksomheten

Som ledd i begrunnelsen for opprettelse av cybersenteret anføres det at "få trusselaktører er dømt for planleggingen eller gjennomføringen av alvorlige IKT-hendelser i Norge" (pkt. 2.5 s. 20, status kulepunkt nr. 3).

Til dette er å kommentere at som hovedregel er planlegging av straffbare forhold *ikke* straffbart. Selv om enkelte lovbestemmelser riktignok rammer det å "inngå forbund" om en alvorlig straffbar handling, antar NAST at cybersenteret i første omgang bør konsentrere seg om å få opp responsen på dataangrep som faktisk begås.[1]

I den forbindelse er det viktig å oppstille *relevante mål* for politiets virksomhet og fokusere på betydningen av de internasjonale samarbeidsrelasjonene. Ikke sjelden spores en "IKT-hendelse" mot norsk virksomhet tilbake til oppkobling via en utenlandsk ekomtilbyder, og politiet er følgelig avhengig av å få innhentet logginformasjon fra denne for å kunne gå videre i etterforskingen. (Denne avhengigheten av trafikkdata en årsak til behovet for datalagring, se pkt. 2). Opplysningene er ofte taushetsbelagt og rettsanmodning må benyttes for å få dem utlevert. Det kan også være aktuelt med bruk av sikringspålegg i denne situasjonen. Det er påtalemyndigheten som har kompetanse til å fremsette rettsanmodning, og handlingen kan anses som et påtalemessig etterforskingsskritt som forutsetter at sak er åpnet, jf. strpl. § 224. Det er adgang til å fremsette forespørsel på forhånd direkte til tilbyder, om vedkommende har slike data

[1] Blant forbundsreglene er strl. 1902 § 147 a siste, jf. første ledd, jf. § 151 b første og tredje ledd relevant for "cyberterror". Utenfor terrorbestemmelsene har man for eksempel strl. § 159, jf. § 159 b. Lignende bestemmelser finnes med tanke på statsspionasje, mens lovverket mot industrispionasje er langt svakere.

lagret hos seg, dvs. før bruk av rettsanmodningen, men politiet får ikke opplyst hva dataene viser. Slik innledende sondering er imidlertid ikke å anse som etterforsking.[2]

Tilbakemeldingen på rettsanmodningen kan være at opplysningene peker mot en gjerningsperson i Norge, hvoretter strafforfølgningen fortsatt er en sak for norsk politi. Minst like sannsynlig er det at opplysningene peker videre til utenlandske aktører. Da må saken sendes utenlandsk påtalemyndighet med anmodning om overtakelse av straffesak med strafforfølgning og pådømmelse i utlandet.

"IKT-hendelsenes" internasjonale karakter innebærer at målet på god straffesakshåndtering ikke kan være antallet positive påtalevedtak/pådømmelser i Norge. Målsettingen bør være *å få opp volumet* totalt sett, hvor de saker som sendes utlandet telles med på lik linje med de som pådømmes i Norge. Mange tiltak må settes inn for å øke volumet. Det handler om effektiv rapportering/anmeldelse fra cybersenteret, så vel som forenklete inntaksprosedyrer hos politiet. Funksjonen bør fortsatt være sentralisert hos Kripos som er blitt tilført ressurser i form av utstyr og kompetanse nettopp med tanke på å håndtere denne sakstypen (se pkt. 6).

Økt volum er viktig også med tanke på den internasjonale innsatsen mot "IKT-hendelser". Med hyppigere kontakt dokumenteres behovet for prioritering av andre lands saker på dette området, og mer effektive og praktiske samarbeidsformer utvikles. Selv om bruk av rettsanmodning tradisjonelt anses som et tungvint verktøy, bør det brukes rutinemessig og bidra til å synliggjøre den norske prioriteringen av innsatsen mot cyberkriminalitet.

Tilsvarende bør norsk politi rutinemessig ta inn og følge opp sporingsforespørsler fra utlandet. Også denne aktiviteten må telles med ved fastsettelse av virksomhetsmål. Sporingsforespørslene fra utlandet kan også tenkes å utgjøre nyttig informasjon for cybersenteret om trusselaktører. Det er derfor behov for å se på om de straffeprosessuelle taushetsreglene er hensiktsmessige for informasjonsdeling.

Bruk av rettsanmodninger og hyppig kontakt med utenlandske samarbeidspartnere er også viktig i lys av de begrensninger som jurisdiksjonsregler setter for "offensiv" atferd av myndighetsorganer på nettet. Selv om norske myndigheter etter sin egen fortolkning av reglene kan mene å holde seg

innenfor disse grensene, er det velkjent at andre land kan ha annet syn på saken. Det beste grunnlaget for å utvikle den rettslige og praktiske tilnærmingen på dette området er å få opp saksvolumet for å ha et erfaringsgrunnlag å vise til i drøftelser med utenlandske samarbeidspartnere.

5. Et internasjonalt cyberpoliti?

NAST synes forslaget til strategi for cybersikkerhet langt på vei har dekket de viktigste temaene. NAST vil imidlertid påpeke behovet for en strategisk bevisstgjøring i forhold til spørsmålet om det er ønskelig med et overnasjonalt cyberpoliti, med spisskompetanse og sofistikerte tekniske ressurser. Forslag om etablering av en slik internasjonal ressurs fremsettes iblant i internasjonale fora, og Norge bør avklare et prinsipielt syn på spørsmålet. Det bør derfor inngå som et nytt kulepunkt blant strategiens hovedmål. Det står om å gi sin tilslutning til en samarbeidslinje mellom likeverdige partnere i strafforfølgningen av cyberkriminalitet, eller å støtte en annen form for overnasjonal ressurs hvor man har mindre kontroll med fullmakter og metodebruk, men som til gjengjeld kan operere mer effektivt på egen hånd.

6. Økonomiske og administrative konsekvenser

Det er spesielt anmodet om å kommentere de økonomiske og administrative konsekvenser ved strategiforslaget.

NAST begrenser seg til kort å kommentere konsekvenser for Kripos og statsadvokatembetet. For så vidt gjelder Kripos bør det bringes i erindring at Politiets datakrimsenter i sin tid ble bygget opp nettopp med tanke på å inneha spisskompetanse til å håndtere denne type saker. Etter innlemmelsen i Kripos fra årsskiftet 2004/2005 har virksomheten fokusert mer på bistand til etterforsking av organisert og annen alvorlig kriminalitet enn på etterforsking av egne saker, mye på grunn av de kriminelles økte bruk av teknologi. Etterforskingskapasiteten i dag er således mindre enn det behovet som vil foreligge dersom forslagene skal følges opp på en forsvarlig måte. Det vil derfor være nødvendig å tilføre ressurser på etterforskingssiden hvis man fremover ønsker også å opprettholde den helt nødvendige bistandskapasiteten.

NAST antar at det og er behov for å se på statsadvokatens rolle i forhold til håndtering av sakstypen. Dersom volumet øker, øker behovet for å ha en dedikert statsadvokatstilling på

---

[2] Se riksadvokatens rundskriv "Etterforsking" (Del II-3/1999) pkt. 4, om den nedre terskel for etterforsking.

området, noe som hittil ikke har vært tilfelle. Sakene vil kunne være prinsipielle, så statsadvokaten bør ha kunnskaper på feltet. Med økt volum antas det å være behov for å opprette et permanent statsadvokatembete med slikt ansvar.

Med hilsen

Siri S. Frigaard
førstestatsadvokat

Inger Marie Sunde
førstestatsadvokat

Gjenpart: Justisdepartementet, Politiavdelingen (ref. 201005069/THN)
Riksadvokaten (ref. Ra 10-309 KHK/jaa 763)