Terrorgrupper og kommunikasjon

Af Thomas Hegghammer, forsker, Forsvarets forskningsinstitutt, Norge

Forskningsprosjektet "Terrorisme og asymmetrisk krigføring" (TERRA)

Dette bakgrunnsdokumentet er laget for Det danske folketings rettsutvalg i forbindelse med den åpne høringen om terrorbekjempelse den 10. mai 2006. Dokumentet vil presentere betraktninger om terrorgruppers bruk av kommunikasjonsmidler, og vil inngå i en debatt om hvilke midler og metoder politi og etterretning skal ha tilgang til i sitt antiterrorarbeid. Spørsmålet om hvordan terrorister kommuniserer har særskilt relevans i dag fordi de siste årenes store terroraksjoner i Europa har endret trusselbildet og fordi teknologiutviklingen har introdusert en rekke nye kommunikasjonsmidler som mobiltelefoner og Internett.

Forfatteren er tilknyttet det norske Forsvarets forskningsinstitutt (FFI), en etat underlagt Forsvarsdepartementet og bemannet av sivilt ansatte forskere. Samfunnsvitere ved FFI har forsket på terrorisme siden 1999 gjennom en serie prosjekter kjent som TERRA-prosjektene. Dagens TERRA-prosjekt fokuserer på transnasjonale radikale islamistbevegelser, og drives av fire fulltidsforskere under ledelse av Dr. Brynjar Lia. Prosjektet driver akademisk virksomhet og har ingen direkte beskjeftigelse med politi- eller etterretningsarbeid. Forskningen er basert utelukkende på ugraderte kilder og publiseres offentlig (se www.ffi.no/TERRA). FFIs terrorismeforskningsmiljø er internasjonalt anerkjent, særlig for sin forskning på radikal islamisme på Internett (Lia and Hegghammer 2004; Lia 2005).

Innledningsvis er det viktig å understreke to viktige begrensninger i FFI-miljøets kompetanse. For det første har vi lite kunnskap om den taktiske dimensjonen i politiets antiterrorarbeid. Vi er ikke involvert i etterforskninger eller etterretningsarbeid på noe nivå, så vår kjennskap til terroristers kommunikasjonsmønstre er ikke spesielt detaljert. For det andre driver vi først og fremst med sosiologisk og historisk informerte analyser av terroraktørene, ikke med utvikling av teknologi eller antiterrormetoder.

Jeg skal derfor vike litt fra de spesifikke spørsmålene jeg er bedt om å besvare, og komme med noen relaterte betraktninger basert på FFIs forskning. Jeg vil frembringe tre hovedpoenger. For det første: Begrepet "terrorist" rommer et bredt spekter aktører med svært ulike kommunikasjonsmønstre, noe som utgjør en stor juridisk og etterretningsmessig utfordring. For det andre: Internett har åpnet enorme nye kommunikasjons- og propagandamuligheter for radikale aktører, men sosial kontakt og interaksjon er fortsatt svært viktig både i radikaliseringsprosessen og i den operasjonelle fasen. For det tredje: Avansert kommunikasjons- og overvåkningsteknologi tidligere forbeholdt stater blir gradvis mer tilgjengelig på det private markedet.

Ulike "terrorister" – ulike kommunikasjonsmønstre

De største problemene for tenkningen rundt terroristers bruk av kommunikasjon knytter seg til selve begrepet "terrorist". For det første rommer begrepet terrorist et bredt spekter aktører med ofte svært forskjellige funksjoner. For det andre finnes det svært mange ulike grader involvering i terrorismeaktiviteter. Disse ulike funksjonene og involveringsgradene medfører svært forskjellige kommunikasjonsmønstre og –behov. Enkelte kommunikasjonsmidler vil være viktigere enn andre på de ulike stadiene eller områdene av den radikale politiske virksomheten. Disse ulikhetene må tas i betrakting ved utforming av antiterrorpolitikk.

Den ideologiske orienteringen til en terroristgruppe legger svært viktige føringer for gruppens atferd. For eksempel har høyrekstreme terrorister helt andre mål, handlingsmønstre og intern kultur enn venstreekstreme grupper. Man kan derfor anta at ulike terroristgrupper også har ulike kommunikasjonsmønstre. De tre viktigste variablene som avgjør kommunikasjonsmønsteret er 1) graden av internasjonale koplinger, 2) typen foretrukne aksjonsformer og 3) de generelle sosialiseringsmønstrene. Disse vil variere sterkt mellom høyre- og venstreekstremister, etnisk-separatistiske terrorister, ensaksgrupper (f eks militante abortmotstandere), og militante islamister. Det er også nyttig å skille mellom tre ulike hovedtyper islamistgrupper: sosio-revolusjonære islamister (som kjemper om statsmakt mot et lokalt regime), nasjonalistisk-separatistiske islamister (som kjemper om et spesifikt territorium mot en okkupasjonsmakt eller en sentralregjering), og globale jihadister (som kjemper mot USA og vesten).
Videre er slik at det løse begrepet "terrorismevirksomhet" er i realiteten et variert sett av aktiviteter som spenner fra rekruttering og pengeinnsamling til anskaffelse av sprengstoff og utførelse av en aksjon. I et militant miljø vil ulike personer derfor har ulike roller og funksjoner. De mest kritiske - og mest illegale - funksjonene vil være best skjermet og vanskeligst å oppdage. Selv i den helt spisse enden av en terroraksjon, altså den operative cellen, er det klart definerte roller og funksjoner. FFI-forskeren Petter Nesser har identifisert generiske rollemønstre i terrorceller i Europa (Nesser 2006). Nesser beskriver fire hovedtyper roller:

- The "Entrepreneur" – drives av ideologi/politikk, karismatisk, kommuniserer med ledere på høyere nivå
- The "Protegé" – drives av ideologi/politikk, entreprenørens høyre hånd, har ofte tekniske kunnskaper
- The "Misfits" – drives av personlige problemer/sosial eksklusjon, har gjerne en kriminell fortid, utfører farlige oppdrag som f eks å skaffe sprengstoff
- The "Drifters" – påvirket av venner, utfører ulike funksjoner.

Dette betyr at kommunikasjonsmønsteret og -behovet i militante miljøer vil variere mye fra miljø til miljø og fra person til person, noe som igjen har konsekvenser for effektiviteten av de ulike antiterrormidler som staten måtte disponere.

En ytterligere utfordring er at det finnes ulike grader av involvering i terrorisme, samt at personer beveger seg gradvis inn i terrorvirksomhet. De fleste som utfører terrorhandlinger har imidlertid gått gjennom en prosess med flere faser:

- *Åpningsfasen* – når en persons reseptivitet for propaganda og rekruttering øker, ofte som resultat av en gradvis økende sosial eller politisk frustrasjon, eller en endring i livssituasjonen (personlig krise, overgang fra skole til arbeidsmarked etc)
- *Radikaliseringsfasen* – når en persons politiske standpunkter blir mer ekstreme, ofte gjennom eksponering for propaganda og gruppedynamikker
- *Rekrutteringsfasen* – når en person utvikler personlige relasjoner med individer og miljøer involvert i planlegging av eller støtte til terrorisme. Man kan skille mellom "top-down", "bottom-up" og "horisontal" rekruttering.
- *Organisasjonsfasen* – når en person er direkte involvert i planlegging av eller støtte til terrorisme. Graden av formell organisering trenger ikke være spesielt høy.
- *Den operative fasen* – når en person har en nøkkelrolle i koordineringen eller utførelsen av en terroraksjon

Det må understrekes at dette kun er analytiske kategorier. Ikke alle individer går gjennom samtlige faser; Ofte flyter fasene over i hverandre.
Denne nyanseringen er relevant fordi kommunikasjonsmønsteret endrer seg og blir mer skjermet jo nærmere utøvelsesfasen en person befinner seg. For eksempel vil en person i radikaliseringsfasen vil ofte

tilbringe mye tid på Internett og vil skrive fritt om sine gradvis mer radikale politiske synspunkter. Derimot vil en person i organisasjonsfasen være svært varsom i sin bruk av internett og andre elektroniske kommunikasjonsmidler, og vil foretrekke fysiske møter i private leiligheter.
Det sentrale dilemmaet her er at den fasen hvor internettovervåkning er mest fruktbar (radikaliseringsfasen) er også den juridisk mest problematiske, ettersom personene det dreier seg om ikke har gjort noe straffbart. Når personene beveger seg mot terrorvirksomhet, blir de lettere (juridisk sett) å overvåke, men de reduserer samtidig sin eksponering på internett og telefon.

Radikale islamisters bruk av Internett

Radikale islamistgrupper har brukt Internett siden midten av 1990-tallet, men de siste fem årene har omfanget av denne bruken vokst eksponensielt. Denne veksten kan forklares av tre strukturelle faktorer: økningen i Internettets båndbredde og bruksområder, den økte tilgangen på IT og Internett i Den muslimske verden, samt jihadistenes tap i 2001 av et fysisk møtested i al-Qaidas treningsleirer i Afghanistan. I dag er Internett en helt sentral dimensjon av fenomenet militant islamisme. Internett utgjør en global, rask og billig kommunikasjonsplattform som egner seg spesielt godt for den såkalte globale jihadistbevegelsen
Før terrorangrepene 11. september 2001 ble Internett brukt mer direkte og åpenlyst til terrorismerelatert virksomhet som pengeinnsamling og rekruttering. Idag har antiterrortiltak og økt overvåkning gjort det vanskeligere å bruke Internett til denne typen virksomhet. Det er bred enighet i terrorismeforskningsmiljøer at Internett brukes primært til propaganda- og informasjonrelatert virksomhet, og i mindre grad til taktisk kommunikasjon eller planlegging av terroraksjoner (Lia 2005). Mye tyder på at militante islamister har gått bort fra å bruke epost i operasjonell sammenheng, sannsynligvis som en konsekvens av negative erfaringer med overvåkning og arrestasjoner.
Internetts nytte for militante islamister kan deles opp i primære og sekundære funksjoner:
Primære funksjoner:

- Kanal for distribusjon av informasjon fra aktive militante og radikale religiøse lærde til sympatisører og potensielle rekrutter
- Møtested for religiøs, politisk og strategisk debatt mellom sympatisører
- Bibliotek for radikal ideologisk litteratur og audiovisuelt materiale
- Database for teknisk-taktisk informasjon om terrorisme- og geriljavirksomhet

Sekundære funksjoner:

- Kilde til informasjon om "fienden"
- Plattform for cyberterrorisme eller "e-jihad"

Som sagt er det vanskelig for forskere som baserer seg på åpne kilder å bedømme i hvilken grad Internett fortsatt brukes av terrorister som kommunikasjonsmiddel i operasjonelle sammenhenger. Det har tidvis kommet spekulasjoner om at Internett rommer visse smutthull som muliggjør taktisk kommunikasjon.
En ofte nevnt utfordring er såkalt Internett-basert telefoni eller IP-telefoni, som sies å være langt vanskeligere å overvåke enn analog telefontrafikk, fordi IP-telefoni innebærer en form for kryptering.
En annen spekulasjon knytter seg til bruken av steganografi, som innebærer å inkorporere hemmelige meldinger i bilde- eller lydfiler. Slike filer kan deretter legges ut på tilsynelatende urelaterte internettsider for så å lastes ned og dekodes av mottaker. Etter det vi kjenner til, finnes det ikke tilstrekkelig grunnlag i åpne kilder for å hevde at på at steganografi brukes i utstrakt grad av militante islamister. Det finnes imidlertid mange indikasjoner på at noen grupper har eksperimentert med krypteringsprogrammer. For eksempel la en irakisk motstandsgruppe ut et krypteringsprogram til nedlastning på sine hjemmesider i 2003.
Man har også sett bruk av helt enkle koder i forbindelse med fildistribuering på diskusjonsforumer. For eksempel legger man ut to bruddstykker av en link, sammen med en gåte (f eks "det motsatte av svart") skrevet på arabisk. Den smarte leser vil da sette ordet "white" med latinske bokstaver mellom de to halvdelene og får dermed en fungerende link. Dette trikset ble sannsynligvis utviklet for å lure dataprogrammer som automatisk ødelegger eksterne linker fra slike nettsteder.

En annet smutthull som har vært utnyttet i operasjonell sammenheng er det som kalles "virtual dead drop". Det innebærer at man bruker "kladd/utkast"-folderen i en epostkonto (Hotmail, Yahoo e.l.) til å legge igjen meldinger til andre personer som kjenner passordet til den samme kontoen. På den måten blir meldingen aldri egentlig sendt som epost, men innholdet er tilgjengelig for andre med passord. Denne metoden skal blant annet ha blitt brukt av personene som gjennomførte Madrid-aksjonen 11. mars 2004. Denne typen kommunikasjon er antakeligvis langt vanskeligere å spore. Et "virtual dead drop" innebærer imidlertid kommunikasjon mellom en datamaskin og en server, og skal således ikke være teoretisk umulig å spore.
Internetts åpenbart sentrale rolle i indoktrinering og radikalisering av militante islamister har fått mange til å beskrive Cyberspace som jihadistenes nye Afghanistan, dvs et møtested hvor rekrutter fra hele verden kan bygge nettverk, radikaliseres og opplæres. Selv om dette til en viss grad er riktig, er det viktig å understreke at virtuell sosialisering og opplæring ikke kan erstatte menneskelig kontakt og fysisk trening. Menneskelig kontakt er fortsatt en svært viktig faktor i radikaliseringsprosessen. Fysisk trening, våpenerfaring og eksponering for vold er fortsatt helt sentralt i operasjonaliseringen av motiverte rekrutter.

Privatisering av kommunikasjons- og overvåkningsteknologi

Den raske utviklingen innen IT og teknologi har ikke bare bidratt til å introdusere banebrytende nye teknologier, men har også utvidet tilgangen til eksisterende kommunikasjonsutstyr. Avansert kommunikasjons- og overvåkningsteknologi som tidligere var forbehold politi og etterretningstjenester, er nå i økende grad tilgjengelig på det åpne og det svarte marked (Lia 2005). Butikker som den norske *Spyshop* selger sofistikert utstyr for ulike typer avlytting og overvåkning. Faktisk er det slik at private aktører idag har tilgang på utstyr som politi i mange land ikke kan bruke (av juridiske eller budsjettmessige grunner). Denne typen utstyr brukes allerede av privatetterforskere og vinningskriminelle.

Denne utviklingen har utvilsomt potensiale til å øke terrorgruppers kapasitet til rekognosering, intern kommunikasjon og kontraetterretning. Foreløpig er det relativt få indikasjoner i åpne kilder på at terrorgrupper i Europa har benyttet slikt utstyr i spesielt stort omfang. Man har funnet nattkikkerter og annet avansert militært utstyr hos terrorgrupper i områder utenfor Europa, som for eksempel i Irak og Saudi Arabia, men vi vet lite om bruken av denne typen utstyr blant terrorgrupper i Europa.

Teknologiutviklingens påvirkning på maktforholdet mellom statlige og ikke-statlige aktører er en velkjent dynamikk i historievitenskapene. I perioder har teknologi gitt stater mye makt, i andre perioder har utviklingen forskjøvet maktforholdet i de ikke-statlige aktørers favør. Utviklingen av Internett og IP-telefoni samt demokratiseringen av avansert overvåkningsteknologi kan sees på som deler av en slik maktforskyvning. Mye tyder på at denne generelle utviklingen vil fortsette på kort og middels lang sikt. Dette innebærer store utfordringer for bekjempelsen av terrorisme.

Lia, B. (2005). "Al-Qaeda online: understanding jihadist internet infrastructure." Jane's Intelligence Review **17**(12).

Lia, B. (2005). Globalisation and the future of terrorism : patterns and predictions. London ; New York, Routledge.

Lia, B. and T. Hegghammer (2004). "Jihadi Strategic Studies: The Alleged Policy Study Preceding the Madrid Bombings." Studies in Conflict and Terrorism **27**(5): 355-375.

Nesser, P. (2006). Profiles of Jihadist Terrorists in Europe. A Future for the Young, Options for Helping Middle Eastern Youth Escape the Trap of Radicalization. C. Bernard. Washington DC, RAND**:** 31-49.