FFI RAPPORT

CYBERSPACE SOM SLAGMARK: Refleksjoner omkring Internett som arena for terrorangrep

JOHANSEN Iver

FFI/RAPPORT-2004/01666

CYBERSPACE SOM SLAGMARK: Refleksjoner omkring Internett som arena for terrorangrep

JOHANSEN Iver

FFI/RAPPORT-2004/01666

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2004/01666	UNCLASSIFIED	35
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFI I/888/044	-	

4) TITLE

CYBERSPACE SOM SLAGMARK: Refleksjoner omkring Internett som arena for terrorangrep

CYBERSPACE AS BATTLEFIELD: Thoughts on the Use of Internet as an Arena for Terror Attack

5) NAMES OF AUTHOR(S) IN FULL (surname first)

JOHANSEN Iver

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Internet	a) Internett
b) Terrorism	b) Terrorisme
c) Scenario	c) Scenario
d) International law	d) Folkerett
e) Computers	e) Datamaskiner

THESAURUS REFERENCE:

8) ABSTRACT

This report outlines a possible disabling attack against the Internet. The attack is described in scenario terms as an attack from a hostile group intent on causing severe damage to modern societies world wide. The main aim of the analysis is to discuss some of the probable consequences on the international political arena should such an attack take place. A main finding is that current international law and international security institutions are largely irrelevant as far as managing threats in cyberspace is concerned. Increased international co-operation and co-ordination is thus called for. However, to the extent that such mechanisms are lacking, resourceful states will most likely concentrate on a unilateral strategy until credible international institutions are in place. Furthermore, the use of digital media and the ability of single individuals or small groups to harm society at large directs defensive measures in new directions. To defend against new threats states therefore tend to coalesce in an attempt to tighten control over individuals – their movements as well as other activities.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
2004-05-26	Jan Erik Torp	Director

ISBN 82-464-0846-1

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

CYBERSPACE SOM SLAGMARK: Refleksjoner omkring Internett som arena for terrorangrep

1 INNLEDNING

Angrepet mot USA 11 september 2001 viste på en dramatisk måte hvilken *kapasitet* og, ikke minst, *vilje* terrorgrupper kan ha til å forårsake enorme ødeleggelser av liv og eiendom. Omfanget av angrepet og de umiddelbare konsekvenser det medførte, oversteg langt all tidligere erfaring fra terroraksjoner, og var på mange måter å sammenligne med regulære krigshandlinger.[1] Nettopp derfor er det ikke overraskende at terrortrusselen i ettertid er blitt omdefinert fra primært å være en intern utfordring til å bli en sikkerhetspolitisk trussel av første rang.

Denne erkjennelsen har skapt en forsterket interesse for terrorisme i allmennhet og i særlig grad for den type aktører som benytter terrorisme som virkemiddel i en ideologisk og religiøst ladet kampanje mot Vesten og Vestens medspillere på globalt plan. Slike intensjoner koblet til en sannsynlig utvikling av disse aktørenes kapasiteter representerer svært problematiske scenarier når en tar i betraktning den sterkt økende sårbarhet som kjennetegner moderne teknologiavhengige samfunn.

1.1 Problemstilling og metode

Denne rapporten[2] tar ikke sikte på en nærmere analyse av terrortrusselen som sådan mot Norge eller andre vestlige samfunn. Den vil heller ikke i noen særlig grad være rettet mot å identifisere sårbarheter eller egnede beskyttelsestiltak. Utgangspunktet for rapporten er i stedet erkjennelsen av at denne trusselen eksisterer, og at den allerede i dag får betydelige samfunnsmessige virkninger. Disse virkningene kan grovt sett grupperes i to hovedkategorier. For det første de *direkte* virkningene av terrorangrep. Disse spenner fra de konkrete fysiske skadevirkninger av angrep til ulike sekundæreffekter som oppstår gjennom individuelle og kollektive tilpasninger til en ny situasjon (endring av reisemønstre, forskyvninger i tilbud og etterspørsel etter varer og tjenester etc). For det andre fører terrortrusselen til en rekke *indirekte* effekter som i hovedsak er knyttet til de virkemidler samfunnet benytter for å beskytte seg mot terrorisme. Disse spenner fra den rent offensive bekjempelse av terrornettverk og deres baser til defensivt orienterte tiltak. Spesielt gjelder dette lovgiving som begrenser individers handlefrihet og åpner for overvåking på områder som tidligere var utenfor myndighetenes kontroll.

---

[1] Beregninger av den totale mengde energi som ble utløst i forbindelse med angrepet på World Trade Center varierer. Den kinetiske energien i begge flyene som ble brukt i angrepet, energiinnholdet i flyenes drivstoff og det energipotensial som ble utløst da bygningene styrtet sammen er beregnet til å tilsvare mellom 0,2 (*The destructive forces unleashed*, BBC news 18.09.01) og 1,9 kilotonn TNT (http//:paulboutin.weblogger.com/2001/09/17).

[2] Rapporten er utarbeidet under prosjekt 888, Terrorbekjempelse og teknologi.

Når terrortrusselen slik sett innebærer et potensial til å gripe inn i nær sagt ethvert samfunnsmessig område, er det rimelig å anta at det på sikt er på det *politiske* felt virkningene av terrorangrep vil kunne bli mest dyptgripende. Internt innen de enkelt land gjelder dette lovgiving som gir terrorgrupper mindre spillerom, men som også endrer maktforhold mellom politisk krefter og som skifter innflytelse mellom myndighetsorganer. På den internasjonale arena får kampen mot terrorisme konsekvenser for hvordan stater knytter seg sammen i nye allianser for felles innsats mot denne trusselen, og for hvordan gamle allianser gis nytt innhold eller mister betydning.

Dette er tendenser som allerede er klart synlige. Problemstillingen for denne rapporten er således hvordan iverksettelse av nye svært omfattende terrorangrep, spesielt på områder hvor moderne samfunn er svært sårbare, kan bidra til å forsterke eller endre disse tendensene. Poenget her er å postulere en utvikling som hittil ikke har manifestert seg, men som bærer i seg muligheter for politiske endringer.

Siden det her er snakk om å studere *fremtidige muligheter* som altså ikke kan studeres med utgangspunkt i foreliggende empiri, står en overfor spesielle analytiske utfordringer. Der en mangler empiriske data, kan imidlertid en beskrivelse av en tenkt fremtidig tilstand eller utvikling danne utgangspunkt for analysen. En slik beskrivelse kan gis form av et *scenario*.

Hva scenariet konkret skal inneholde vil primært måtte styres av formålet med analysen. Dette vil vi komme tilbake til senere. Her er det nok å peke på at vi søker å fokusere mot *usikkerhet*. Dette tilsier at det scenario som legges til grunn for analysen må være slik at konsekvensene av scenariet fortoner seg uklare. På samme måte som angrepet 11 september 2001 førte til konsekvenser ingen på forhånd hadde forutsett, ønsker vi her å bygge på et scenario som kan være egnet til å skape tilsvarende uventede effekter.

Det vi søker er et scenario med potensial til å påføre samfunnet omfattende og langvarige skadevirkninger, men hvor den politiske håndtering er uklar. Det er derfor rimelig å ta utgangspunkt i en utfordring en hittil har hatt begrenset erfaring med, men som i fremtiden står frem som en sentral arena for maktanvendelse. De elektroniske nettverk som binder en økende mengde samfunnsfunksjoner og aktører sammen, er en slik arena. Vi vil derfor basere analysen på et scenario hvor funksjonsdyktigheten til de elektroniske nettverkene svekkes på en kritisk måte som følge av en koordinert angrep av aktører med et erklært ønske om å ramme vestlige samfunn.

Stadig flere av de funksjoner som er nødvendige for at samfunnet skal fungere, baserer seg på utveksling og lagring av informasjon i elektroniske nettverk. Angrep mot informasjons- og kommunikasjonssystemene som styrer vitale samfunnsfunksjoner har hittil i hovedsak vært en arena for isolerte ”hackere” uten mer omfattende politiske ambisjoner for sin virksomhet. Terrorgrupper har derimot inntil i dag utvist en forbløffende tradisjonalisme både mht de mål de angriper og hvilke våpen og metoder de benytter seg av. Bruk av passasjerfly som ”missiler” representerer imidlertid på sitt vis en innovasjon, noe som peker mot en større grad av

oppfinnsomhet i fremtiden. Barrièrene mot en utvikling hvor også det elektroniske rom blir en arena for terrorvirksomhet kan derfor være lettere å bryte enn hva en kanskje kunne forestille seg.

Her står det globale datanettverket vi kaller Internett i en særstilling. Dette nettverket har hittil primært fungert som et *virkemiddel* for å anrette skade ved at det har gitt ulike aktører aksess til de komponenter eller undersystemer som har blitt rammet. Internett representerer imidlertid også i seg selv en sårbar struktur som kan angripes og – i ytterste fall – settes ut av spill. Et mulig scenario for dette vil diskuteres i det følgende.

2 ET SCENARIO FOR CYBER-ANGREP

Internett som globalt datanettverk, står i en særstilling som medium for kommunikasjon mellom individer, bedrifter, offentlige og private institusjoner. Selv om de fleste vitale samfunnsfunksjoner opererer på egne, dedikerte nettverk, blir stadig flere sekundærfunksjoner som f eks bookingsystemene innen luftfarten, prisinformasjon innen verdipapir-, valuta- og kraftmarkedene og informasjonssystemer innen varelogistikk, knyttet direkte til Internett som bærer av kommunikasjon og informasjon. Internett får således en stadig mer sentral rolle i den daglig funksjon for de fleste av verdens samfunn.

2.1 Hvordan virker Internett?

Internett er et system av sammenkoblede datanettverk som gjør det mulig for hvilken som helst datamaskin som er koblet til systemet, å kommunisere med hvilken som helst annen. Internett er altså på den ene siden et *kommunikasjonssystem* som kobler brukere av systemet sammen, og på den andre et *informasjonssystem* som muliggjør lagring og aksess til en formidabel, og stadig økende, mengde digital informasjon rundt om i nettet.

Utviklingen av elektroniske datamaskiner i årene etter Annen verdenskrig førte snart til forsøk på å koble dem sammen i nettverk. Et avgjørende gjennombrudd på veien mot dagens Internett kom på begynnelsen av 1960-tallet med innføringen av *pakkesvitsjing* (packet switching) som metode for å overføre meldinger i et nettverk av datamaskiner. Pakkesvitsjing innebærer at en melding deles opp i et antall ”pakker” som så sendes enkeltvis til mottageren langs ulike veier i nettverket. Hver pakke inneholder informasjon om avsenders og mottagers adresse, meldingens samlede lengde (i antall bytes) og den enkelte pakkes plassering i sekvensen av pakker.

Denne kommunikasjonen er bare mulig gjennom et sett av standarder, prosedyrer og formater som er felles for alle maskinene i nettverket. Disse prosedyrene kalles *protokoller*, og sørger bl a for korrekt sammensetning av meldinger hos mottageren og dessuten for oppsporing av pakker som kan ha gått tapt i nettverket. En sentral funksjon i dette kommunikasjonsnettverket har såkalte *rutere* (routers). Dette er spesialiserte datamaskiner som svitsjer data fra et nettverk til et annet. En ruter er altså typisk tilkoblet flere forskjellige nettverk og fungerer som knutepunkter mellom de ulike nettverkene.

Konseptet med pakkesvitsjing og bruk av dedikerte protokoller for kommunikasjon dannet grunnlaget for etableringen av ARPANET i 1969.[3] Hensikten var i utgangspunktet å bygge opp et militært kommunikasjonssystem som ville kunne fungere på en sikker måte selv om flere av forbindelsene i systemet ble brutt, f eks etter et kjernefysisk angrep. ARPANET demonstrerte fordelene ved en nettverksløsning fremfor alternative konsepter gjennom:

a) *Digitalisering*; ved å gjøre kommunikasjon digital kan den bli feilfri.
b) *Dataprosessering*; ved å inkludere datamaskiner i nettverket kan nettverkets ytelser kontinuerlig forbedres gjennom oppgradering av maskiner og programvare.
c) *Redundans*; nettverket eliminerer avhengighet av én bestemt forbindelse, og kan fungere selv etter omfattende skade.
d) *Effektivitet*; ved at flere enkeltkommunikasjoner kan dele én gitt forbindelse utnyttes nettverkets samlede tilgjengelige båndbredde langt mer effektivt enn ved konvensjonell linjesvitsjing.

ARPANET beveget seg snart ut over det rent militære bruksområdet ved at en rekke sivile brukere – i første rekke universiteter – knyttet seg til nettverket. En milepæl i Internetts utvikling var beslutningen i USA på midten av 1980-tallet om å bygge et eget nettverk for universiteter og forskningsinstitusjoner – NSFNET (National Science Foundation Net) og koble dette til ARPANET. Dette bidro til en radikal utvidelse av både antall brukere og anvendelsesområdet for digital nettverkskommunikasjon. ARPANET ble endelig avviklet innenfor det globale nettverket en i dag kjenner som Internett, i 1990.

En neste milepæl i utviklingen av Internett ble nådd med etableringen av *domenenavn* (Domain Name System/DNS) for å håndtere informasjon om den stadig økende mengde datamaskiner og brukere som etter hvert ble knyttet til systemet.[4] Gjennom systemet med domenenavn er det mulig for enhver Internett-bruker å koble seg til en hvilken som helst adresse innen Internett ved å taste dens domenenavn.

Sentralt i DNS står i dag 13 meget kraftige datamaskiner, såkalte *rottjenere* (root servers), som fungerer som hovedknutepunkter i nettet, og som inneholder informasjon om alle internettadresser og domenenavn.[5] Disse rottjenerne fyller en vital funksjon for kommunikasjonen i Internett ved å knytte spesifikke adresser til korresponderende domenenavn. Dette skjer i praksis ved hjelp av et stort antall spesielle *navnetjenere* (domain name resolvers) som rutinemessig lagrer informasjon om adresser og domenenavn de mottar fra forespørsler til de 13 rottjenerne.

---

[3] Advanced Research Project Agency (ARPA) ble grunnlagt i 1958 under USAs forsvarsdepartement for koordinere militært relatert forskning. (I dag er betegnelsen Defence Advanced Research Project Agency (DARPA).)

[4] DNS er et hierarkisk system. Øverst i systemet er syv generiske "top level domains": .edu, .gov, .mil, .int, .net, .org og .com i tillegg til 244 landspesifikke betegnelser (f eks .no). Lavere nivå domenenavn kan registreres av enkeltpersoner eller organisasjoner for et hvilket som helst formål.

[5] 10 av rottjenerne finnes i USA. I tillegg finnes én hver i Stockholm, London og Tokyo. Sikkerhetsnivået er ulikt. Mens rottjeneren i Stockholm er plassert i et underjordisk anlegg, er det tilsvarende anlegget i London bare beskyttet av piggtråd og sikkerhetsvakter. (Bringing Down the Internet, Newsweek 28 oktober 2003).

De 13 rottjenerne inneholder nøyaktig den samme informasjonen og kan derfor fordele trafikken i Internett mellom seg. Dette betyr at det ikke er nødvendig at alle 13 fungerer kontinuerlig. Selv om én eller noen få maskiner skulle bli satt ut av funksjon, vil ikke dette påvirke den totale kapasitet i nettverket synderlig. DNS er bygd slik at åtte eller flere må svikte før det overhodet begynner å oppstå forsinkelser. Men det er samtidig klart at om alle 13 maskiner skulle bli satt ut av funksjon samtidig, vil all navnebasert *ny* trafikk i Internett umiddelbart bryte sammen. Eksisterende trafikk – dvs der det allerede er opprettet kontakt – vil fortsatt kunne pågå, i det minste i noen dager.

2.2 Hvor avhengige er vi av Internett?

Siden Internett ble etablert, har veksten i antallet tilknyttede datamaskiner vært sterk og jevn. Internett vokser i dag med ca 80% pr år, og forventes å nå igjen verdens telefonnett i omfang i 2006. Internett er altså på rask vei til å bli verdens mest omfattende kommunikasjons-infrastruktur. Dette alene tilsier at verdenssamfunnet allerede på mange felt er sterkt avhengig av et fungerende Internett. Graden av avhengighet varierer imidlertid mellom sektorer, og det er fortsatt slik at vitale samfunnsfunksjoner som krever stor sikkerhet benytter andre IKT-plattformer[6] enn Internett. Vi skal her kort se på noen eksempler.[7]

De fleste teletjenester er ikke avhengige av felles transportnett med andre telenett, men er funksjonelt knyttet til egne tjenestenett (13). Internett er på den annen side i seg selv bærer av teletjenester, eksempelvis e-post, internett-telefoni, betalingstjenester med mer. Dette er bruksområder som øker raskt i omfang. Internett-teknologien har, som vi har sett, en rekke egenskaper som reduserer sårbarhet. Den arkitektur som er bygget opp rundt Internett som teknologi, er imidlertid etablert uten hensyn til sårbarhet, noe vi skal komme nærmere tilbake til i det følgende. Teletjenester basert på Internett som kommunikasjonsplattform er derfor ikke bare fundamentalt avhengige av et fungerende Internett, men også svært sårbare.

Stabil tilgang til elektrisk kraft er et grunnvilkår for moderne, komplekse samfunn. Et sentralt trekk i utviklingen på dette området er en sterkt økende IKT-avhengighet etter hvert som en går over fra betjente anlegg til å overvåke produksjons- og distribusjonssystemene fra et fåtall driftssentraler. Prosesstyring og administrasjon skjer på egne dedikerte nett, som imidlertid – i det minste i teorien – kan aksesseres fra Internett. Dette representerer et potensielt problem all den stund dette gir "hackere" og andre med fiendtlige hensikter en adgang til å angripe kraftsystemene, men som helhet er disse lite avhengige av Internett som kommunikasjonsbærer.[8] En annen sak er imidlertid at dereguleringen av kraftmarkedene har økt

[6] Informasjons- og kommunikasjonsteknologi
[7] Eksemplene er primært hentet fra undersøkelser av hva som er situasjonen i Norge. Konklusjonene kan derfor ikke uten videre gjøres generelt gyldige, men vi vil likevel i denne sammenheng forutsette at forholdene i andre høyt utviklede land ikke er svært forskjellig.
[8] Det store strømutfallet i det nordøstlige USA og Canada i august 2003 kan ha vært forårsaket av angrepet fra det såkalte Blaster-viruset. Dette førte til en degradering av kraftselskapenes kommunikasjonssystemer, noe som gjorde det umulig å avverge overbelastninger i kraftnettet. (Le blackout américain du mois d'août n'aurait eu lieu sans la présence d'un virus, Journaldunet Solutions, 10 september 2003.)

behovet for aktørene i disse markedene til å skaffe seg informasjon om produksjon, forbruk og priser. Dette er informasjon som i betydelig grad kan hentes gjennom bruk av Internett, noe som skaper en mer avgrenset og indirekte avhengighet av Internett innen denne sektoren (12). Dette kan likevel ikke sees som et stort problem på kort sikt.

Innen bank- og finanssektoren har stadig skjerpede lønnsomhetskrav ført til en kraftig effektivisering. Som et ledd i dette er det etablert en rekke banktjenester på Internett. Dette gjelder også for næringslivet generelt, hvor bl a handel og betaling over nettet øker sterkt. Innen offentlig tjenesteyting legges også stadig mer av brukertjenestene til Internett.

Innen industriell virksomhet kan en skille mellom separate prosessnett med høy sikkerhet, som f eks i kraftindustrien, og elektroniske kommunikasjons- og sambandsløsninger gjennom Internett og tradisjonelle telenett. Dette er bl a situasjonen innen den norske olje- og gassvirksomheten (15). Dette tilsier en relativt liten grad av avhengighet av Internett som bærer av informasjon knyttet til produksjonsprosessen. Samtidig spiller Internett en ikke ubetydelig rolle for den øvrige informasjonsflyten. Dette gjør seg ikke minst gjeldende innenfor transportsektoren hvor internettbaserte kommunikasjonsløsninger får en stadig mer sentral plass. Informasjonssystemer for varelogistikk benytter standardiserte formater for booking av oppdrag, styring av vareflyt og lagerhold, overføring av fraktinformasjon, fakturering, fortolling osv. Dette betyr at all vesentlig informasjon som er nødvendig for å bringe en vare fra avsender til mottager legges inn på sentrale datasystemer som kobles opp mot Internett (14 s 23). Dersom Internett skulle slutte å fungere, vil det derfor kunne føre til store forstyrrelser i godstrafikk, og – for den del – i persontrafikk som bruker internettbaserte bookingsystemer. De samfunnsmessige virkningene forsterkes gjennom den økende anvendelse av ”just-in-time”-prinsippet som forhindrer oppbygging av store varelagre.

Noe av det samme gjelder også for flytrafikken hvor logistikkstyringssystemet for flyfrakt bruker Internett for å booke oppdrag og spore varer (16 s 21). I tillegg benyttes Internett i økende grad for booking av personreiser med fly. Konklusjonen er at selv om luftfarten i hovedsak ikke er avhengig av Internett som kommunikasjonsplattform – her benyttes en serie dedikerte nett for alt fra trafikkinformasjon til meteorologiske data – vil et bortfall av internettbasert informasjon på sikt føre til store forstyrrelser i trafikkavviklingen.

Forskning og utdanning var den første ikke-militære samfunnssektor som tok i bruk Internett for formidling av informasjon. I dag er det internasjonale forskersamfunnet i praksis helt avhengig av Internett for lagring og søk etter data, kommunikasjon, publisering (elektronisk i tillegg til eller i stedet for trykte utgaver) osv. Å tenke Internett bort som arbeidsredskap innen denne sektoren uten at det skulle medføre dramatiske konsekvenser, vil derfor i dag i praksis være umulig. På den annen side er dette effekter som for samfunnet som helhet, bare vil vise seg på lengre sikt.

Med den betydning Internett er i ferd med å få som globalt kommunikasjons- og informasjonssystem, vil et neste naturlig spørsmål å stille være hvor sårbart det er. Det kan være

rimelig å dele dette spørsmålet i to. For det første sårbarheten overfor det en kan kalle tilfeldige hendelser. For det andre sårbarheten overfor bevisste og målrettede forsøk på å ramme nettverket.

Internett kan på mange måter betraktes som en organisme i delvis ukontrollert vekst. Dette fører til en utvikling i systemets kompleksitet som vokser raskere enn vår evne til beskytte det og forutse mulige hendelser. En hvilken som helst tilfeldig hendelse kan derfor i og for seg skape store forstyrrelser uten at det verken kan forutses eller forhindres. Her vil vi imidlertid fokusere mot den typen sårbarhet som er forbundet med bevisste angrep mot Internetts funksjonsdyktighet. Dette er for så vidt ikke helt adskilte problemer: Med økende kompleksitet kan selv et begrenset angrep mot en del av nettet under visse betingelser spre seg og få store konsekvenser. Vi skal i det følgende se nærmere på noen aktuelle tekniske muligheter.

2.3 Teknisk scenario

Hvorvidt det er praktisk mulig å ødelegge eller skape betydelige forstyrrelser i Internett kan ikke besvares med et enkelt ja eller nei. Det er ovenfor pekt på at arkitekturen som er bygd opp rundt internetteknologien, er svært sårbar. Det hevdes derfor fra tid til annen at nettet enkelt kan slås ut gjennom spredning av farlige dataprogrammer,[9] men dette er ofte påstander som har sin opprinnelse hos miljøer med økonomiske interesser knyttet til anti-virusindustrien (17). På den annen side er erfaringsmaterialet fra faktiske angrep mot nettet begrenset. Det er derfor vanskelig å vurdere risikoen mer presist.

Like fullt er det i utgangspunktet flere måter hele eller deler av Internett kan angripes på. Vi vil her fokusere mot én slik metode, angrep mot systemets *båndbredde*[10]. Dette vil være en form for såkalt "Denial of Service Attack", eller på norsk, tilgjengelighetsangrep.[11] Hovedpoenget er ikke å fastslå at nettopp denne metoden vil eller kan brukes, men først og fremst peke på muligheter.

2.3.1 Tilgjengelighetsangrep

Begrepet "Denial of Service" (DoS) eller tilgjengelighetsangrep, beskriver en situasjon hvor man søker å hindre normal funksjon av en gitt nettverksressurs, ofte gjennom å begrense dens tilgjengelige båndbredde.[12] Dette kan gjøres på to ulike måter: Enten ved å redusere den samlede båndbredde gjennom fysisk ødeleggelse av maskiner eller kabler, eller ved å legge beslag på mesteparten eller all tilgjengelig båndbredde ved utsendelse av et stort antall uønskede meldinger. Uønsket e-post – spam – er eksempelvis et problem nettopp fordi dette opptar

[9] Viruset "Slammer" spredte seg i 2003 over hele verden på bare 15 minutter. Angrepet ble slått tilbake fordi viruset utnyttet et allerede kjent sikkerhetshull. I en artikkel i Teknisk ukeblad hevdes det at dersom angrepet hadde vært rettet mot et ikke kjent sikkerhetshull, "ville [det] sannsynligvis ha tatt ned hele Internett i løpet av ti til femten minutter". (Terrorfrykt for digital dommedag, Teknisk ukeblad 9 februar 2004).

[10] Båndbredde er et mål for hvor mye informasjon som kan formidles innen et system i løpet av et gitt tidsrom. For digitale systemer uttrykkes dette vanligvis i bit/sekund eller byte/sekund.

[11] Andre metoder for angrep kan være: (i) virusangrep mot navnetjenerne; (ii) angrep mot oppsett av forbindelse mellom maskiner; (iii) angrep mot infrastrukturen (skru av rutere og svitsjer).

[12] Det kan her noteres at "denial of service" kan oppnås ved å angripe andre funksjoner i et system, f eks ved å fylle opp all tilgjengelig lagringskapasitet.

kapasitet og reduserer den tilgjengelige båndbredde for andre aktører.

Selv med relativt beskjeden innsats kan angrep, enten det er av den ene eller de andre typen, lett få store lokale konsekvenser i et nettverk. Det skal imidlertid langt større innsats til for å ramme nettverket som helhet. Når det gjelder Internett er dette nettverket karakterisert av en betydelig robusthet gjennom redundans; husk at Internett-teknologien nettopp ble utviklet for at systemet skulle kunne fungere selv etter omfattende fysisk ødeleggelse.

Nettopp derfor fremstår *fysisk ødeleggelse* ikke som en aktuell hovedstrategi for den eller de som ønsker å ødelegge eller forstyrre funksjonaliteten i Internett, selv om dette i og for seg kan utnyttes som en supplerende strategi.[13] En mer nærliggende strategi kan i stedet være å redusere systemkomponentenes båndbredde ved å generere *overbelastninger* som vil kunne gjøre hele systemet ustabilt eller helt få det til å opphøre å fungere i et gitt tidsrom. Dette kan i prinsippet gjøres fra et hvilket som helst punkt i nettverket. Denne strategien søker å utnytte det faktum at eksempelvis rottjenere og navnetjenere bare kan håndtere en viss mengde trafikk på ethvert tidspunkt basert på gitte begrensninger i minne og båndbredde. Om denne kapasitetsgrensen overskrides vil nye forespørsler bli forkastet. En angriper som ønsker å lamme en gitt tjeneste eller funksjon kan derfor sørge for å belaste denne med uønsket trafikk inntil all tilgjengelig kapasitet er brukt opp.

Nå vil et slikt angrep ikke påføre varig skade på systemet som sådan (noe annet er det selvsagt med eventuelle sekundærkonsekvenser). Kaoset varer bare så lenge angrepet pågår, men dersom angrepet rettes mot vitale ressurser, f eks Internetts 13 rottjenere, kan konsekvensene bli meget betydelige. Denne trusselen kan dessuten synes ytterligere relevant all den stund slike angrep i prinsippet er lette å sett i verk samtidig som beskyttelsesmulighetene er begrensede.

En særegen form for tilgjengelighetsangrep er såkalte *distribuerte* angrep (på engelsk omtales dette som Distributed Denial of Service, eller DDoS). Et slikt angrep kan settes i verk ved at en eller flere angripere bryter seg inn i et stort antall datamaskiner som er knyttet til Internett og installerer et DDoS-program som gjør det mulig å fjernstyre disse som en slags ”slave-maskiner”. Flere tusen maskiner kan på denne måten styres fra ett enkelt punkt og beordres til å generere enorme mengder trafikk i nettverket. Det er altså ikke nødvendig for angriperen å skaffe seg direkte adgang til den maskinen som angripes.

Det er ikke et sentralt poeng å gå detaljert inn på hvordan et slikt angrep kan gjennomføres.[14] Det kan imidlertid fastslås at DDoS-angrep representerer en alvorlig trussel mot

[13] Et spesialtilfelle vil være bruk av elektromagnetisk puls (EMP), som ikke forutsetter et direkte fysisk angrep, men som setter elektronikk ut av spill gjennom å skape sterke elektromagnetiske felt. EMP er bl a én av effektene ved detonasjon av kjernevåpen.

[14] En mulig metode blant flere, er såkalte ”smurf-angrep”. I et smurf-angrep vil en angriper søke å mette systemet med svar på såkalte Internet Control Message Protocol (ICMP)-forespørsler (”ping”). Et ping er et signal i form av en ”pakke” – omtrent én kilobyte – med informasjon om mottager og avsender av pakken, som brukes for å etablere kontakt mellom datamaskiner. Ved å sende slike forespørsler til spesielle ”Internet broadcast”-adresser og samtidig sørge for at avsender-adressen er forfalsket – i stedet oppgis offerets adresse som avsender – kan det genereres enorme mengder trafikk (ping-svar) som i praksis kan fylle all tilgjengelig båndbredde hos offeret.

tilgjengeligheten til sentrale ressurser i Internett. Dette understrekes av at det de siste årene er registrert en rekke mer og mindre omfattende DDoS-angrep. I februar 2000 ble bl a Amazon.com og CNN.com utsatt for et angrep med koordinerte ping mot sentrale servere.[15] 21 oktober 2002 ble det inntil da mest omfattende DDoS-angrep mot rottjenersystemet i Internett gjennomført. Fire eller fem av de 13 rottjenerne klarte imidlertid å motstå angrepet, noe som avverget følbare konsekvenser for trafikken i nettet.[16]

Hvor realistisk det er at et mer systematisk DDoS-angrep kan lamme eller redusere stabiliteten i Internett, er selvsagt vanskelig å si. Det er på den ene siden klart at dette i så fall vil kreve betydelige ressurser og angriperen må lykkes i å stenge ned alle, eller nesten alle rottjenerne, og da helst gjennom angrep som kombinerer ulike metoder: angrep mot navnetjenerne, mot kommunikasjonen mellom maskiner og mot selve infrastrukturen.

På den andre siden er det en rekke indikasjoner på at systemet er svært sårbart. Paul Vixie, styremedlem i Internet Software Consortium (USA), hevder bl a at ”[T]he Internet is very fragile. An attack designed to flood the Web’s master directory servers with traffic is capable of bringing down the Internet.”[17] Peter Neumann, som er tilknyttet SRI International (USA) sier: “The consensus among hackers is that the entire Internet infrastructure can easily be disabled temporarily and – in some cases – (for) a long time”.[18] Også på offisielt hold erkjennes det at den eksplosive veksten i Internetts omfang gjør nettet mer usikkert. USAs regjering fastslår i utkastet til nasjonal strategi for å sikre cyberspace: ”While the Internet has grown enormously and globally, it has also grown increasingly insecure ((10) s 8). Denne erkjennelsen har også ført til at *Internet Corporation for Assigned Names and Numbers* (ICANN)[19] har igangsatt arbeid med å gjøre bl a rottjenersystemet mer robust mot angrep.

2.4 Operativt scenario

2.4.1 Forutsetninger

Diskusjonen ovenfor har primært tatt sikte på å føre belegg for to vesentlige vilkår for det scenario denne studien bygger på. For det første eksistensen av en *trussel* i form av ikke-statlige aktører med motiv og kapasitet til å gjennomføre et omfattende angrep mot vitale digitale kommunikasjons- og informasjonssystemer. For det andre forekomsten av grunnleggende *sårbarheter* knyttet til Internetts arkitektur og funksjonsmåte. Disse to vilkårene utgjør de generelle forutsetninger for scenariet.

I tillegg vil scenariet bygge på følgende spesielle forutsetninger:

---

[15] *Cyber-attacks batter Web heavyweights*, cnn.com, 9 februar 2000.
[16] *Attack on Internet called largest ever*, washingtonpost.com, 22 oktober 2002.
[17] *Experts: Hackers could easily shut down the net*, usatoday.com, 14 november 2002.
[18] *Experts: Cyberspace could be next target*, usatoday.com, 11 november 2001.
[19] ICANN (etableret 1998) er et privat ”non-profit”-foretak med ansvar for å bestyre bl a domenenavn-systemet (DNS) og Internetts rottjenere.

1. *Tidshorisont*:
   Drøftingen ovenfor antyder at de generelle forutsetningene for scenariet allerede eksisterer. Slik sett kan scenariet sies å kunne skje *til enhver tid*.
2. *Aktør*:
   Angriperen oppfattes å være en ikke-statlig aktør som disponerer tilstrekkelige ressurser i form av personell, kompetanse og materiell til å angripe elektroniske nettverk i stor skala.
3. *Angrepsmodus*:
   Angrepet gjennomføres som flere massive og overraskende anslag med sikte på å lamme eller forstyrre digital kommunikasjon i et globalt omfang. Virkningene søkes opprettholdt over så lang tid som mulig. Angriperen benytter seg derfor av en kombinert strategi med både spredning av uønsket programvare og fysisk ødeleggelse av vitale nettverksressurser.
4. *Angrepsobjekt*:
   Angrepet rettes mot Internetts sentrale rottjenere og navnetjenere.
5. *Mål*:
   Angrepet tar sikte på å skape sammenbrudd i vitale samfunnsfunksjoner over store deler av kloden. Hovedmålet er å påføre størst mulig skade på de komplekse og IKT-avhengige samfunnsstrukturene i den vestlige verden.

2.4.2 Hendelsesforløp

Angrepet er grundig forberedt gjennom lengre tid hvor en bl a fra en rekke ”master” datamaskiner har oppnådd illegitim aksess til et stort antall ”slavemaskiner” – *agenter* – hvor det er installert en DDoS programpakke. Angrepet iverksettes på et gitt tidspunkt hvor flere hundre tusen maskiner plutselig begynner å generere enorme mengder trafikk i Internett. Angrepet rettes mot Internetts navnetjenere og rottjenere. I løpet av noen timer er flesteparten av rottjenerne og en betydelig andel av navnetjenerne overbelastet og effektivt lammet. Samtidig ødelegges flere av de dårligst beskyttede rottjenerne i Internett med sprengladninger. Ganske snart oppleves betydelige forsinkelser i trafikken i Internett. For å forhindre reparasjon av skadene forurenses flere av de ødelagte systemkomponentene med miltbrannsporer.

Konsekvensene av angrepet blir raskt følbare og tiltak iverksettes for å bringe Internett tilbake i normal operasjon. Dette lykkes også etter relativt kort tid, og etterforskning settes i gang for å avdekke hvor angrepet har sin årsak. Før det er kommet til noen avklaring på dette området iverksettes et nytt angrep, denne gang med enda mer omfattende virkninger og mer langvarige enn forrige gang. Angrepet varer noen dager. I denne perioden oppleves Internett som svært ustabilt.

Etter denne innledende runden avtar angrepene i intensitet. Like fullt fortsetter mer begrensede angrep jevnlig, noe som skaper et mer vedvarende kaos i nettet. Dette fører til at funksjoner som benytter Internett som kommunikasjonsplattform – e-post, bank- og betalingstjenester, varelogistikk, reiseliv etc – mer eller mindre bryter sammen og aktørene innen disse virksomhetene tvinges til å etablere – i den grad det er mulig – alternative kommunikasjonsløsninger.

Sekundæreffektene for samfunnet er svært omfattende i de periodene angrepene pågår. Selv om de mest vitale samfunnsfunksjoner opprettholdes (kraftproduksjon, teletjenester, helsetjenester etc) skapes det raskt kaos på andre felt. Bl a oppstår raskt akutt pengeknapphet når elektroniske betalingsløsninger slutter å fungere eller blir ustabile. Omfattende forstyrrelser oppstår også i person- og godstrafikken, noe som i neste omgang rammer industri og jordbruk. Vareknapphet fører til at myndighetene enkelte steder innfører rasjoneringsordninger mht de viktigste vareslagene.

Til sammen vedvarer angrepene over 6-8 uker. Det er imidlertid vanskelig å bringe situasjonen tilbake til normaltilstanden før angrepene. Dels er stabiliteten i Internett svekket og dels har et stort antall aktører iverksatt prosedyrer og tekniske tilpasninger som benytter seg av andre plattformer enn Internett, noe som innebærer betydelige omkostninger.

Med utgangspunkt i det beskrevne hendelsesforløp, vil vi i senere kapitler se nærmere på noen mulige konsekvenser. De rent tekniske og sårbarhetsrelaterte virkninger vil imidlertid ikke være et hovedfokus. I stedet vil vekten bli lagt på mulige politiske konsekvenser hendelsene kan utløse.

3 ER CYBER-ANGREP TERRORISME?

Et første spørsmål som fortjener en nærmere drøfting, er i hvilken grad denne formen for angrep i det hele tatt fortjener karakteristikken *terrorisme*. Problemet er jo primært at den gjengse forståelsen av terrorisme – uttalt eller ikke – er nært knyttet til angrep som fører til fysisk ødeleggelse av liv og eiendom, gjerne i spektakulære aksjoner med bred mediadekning. Et cyber-angrep mangler derimot en rekke av disse kjennetegnene. Denne typen angrep har lite av det umiddelbart spektakulære som terroraksjoner tradisjonelt forbindes med, noe som åpenbart skyldes at cyber-space' *immaterielle* karakter gjør at nettopp dette fysiske regimet unndrar seg direkte observasjon. Det kan likevel være nyttig å betrakte dette spørsmålet i lys hva vi vanligvis forstår med terrorismebegrepet. Den definisjon som er lagt til grunn av "Subcommittee on Terrorism and Homeland Security" i USA kan være et godt utgangspunkt:

> "Terrorism is the illegitimate, premeditated use of politically motivated violence or threat of violence by a sub-national group against persons or property with the intent to coerce a government by instilling fear amongst the populace" (1).

Definisjonen peker på at terrorisme må betraktes som et *politisk* virkemiddel, dog illegitimt. Dette innebærer en avgrensning av begrepet til handlinger som utføres for å fremme bestemte politiske målsettinger. Handlinger som utføres på bakgrunn av andre motiver, f eks økonomisk vinning eller ulike idiosynkratiske motiver, faller altså utenom. Videre fokuserer definisjonen på *ikke-statlige aktører* som subjektet for terrorisme. Stater kan for så vidt tenkes å støtte terror-aktører på ulikt vis, men denne støtten vil oftest holdes skjult, eller myndighetene søker å dissosiere seg fra eventuelle terrorhandlinger. I den grad de ikke gjør det, vil handlingen bli et interstatlig anliggende og som sådan ikke være terrorisme. Handlinger der stater er det

handlende subjekt, faller følgelig utenom definisjonen.[20] Denne avgrensningen er analytisk fruktbar fordi den klargjør at terrorgrupper mangler de vesentligste attributter som definerer en stat; territorium, befolkning og anerkjent politisk suverenitet. Dermed blir staters relasjoner til denne typen aktører *asymmetriske* fordi politiske og militære virkemidler som historisk har funnet anvendelse i forholdet mellom stater, bare i begrenset grad vil være relevante (11).

Definisjonen presiserer også terrorgruppers *operasjonsmodus*, nemlig å fremkalle frykt hos en befolkning for derigjennom å legge press på de besluttende myndigheter. Det er altså ikke først og fremst er befolkningens adferd som søkes endret, men snarere regjeringens. Beslutningstagerne skal tvinges til å endre politikk innenfor et gitt saksfelt, enten som følge av press fra befolkningen eller som følge av et ønske om å pasifisere terrorgruppen(e). Slik sett representerer terrorisme en *indirekte strategi* hvor en søker å ramme statens tyngdepunkt – regjeringens handlefrihet – gjennom å påvirke et vitalt støttepunkt for denne, nemlig befolkningens aksept for den politikk som føres.[21]

Denne forståelsen av terrorismebegrepet synes å fange inn de vesentligste sider også ved cyber-terror generelt og vårt scenario mer spesielt. Vi har for det første å gjøre med former for angrep som kan gjennomføres av ikke-statlige aktører. Vi skal ikke her gå langt i å spekulere i hva slags grupper dette kan være. Imidlertid må det være grupper som opererer på basis av en politisk agenda som de søker å fremme ved å anrette størst mulig skade på de mest IKT-avhengige samfunn i verden, hvilket i praksis er landene i Vest-Europa, USA, Japan m fl. Den politiske agenda kan derfor knyttes opp mot en generell kamp mot Vesten og Vestens globale dominans politisk, økonomisk og militært. Denne agendaen gjenfinnes hos grupper som finner sitt grunnlag i en radikal fortolkning av islam (5). Innenfor dette ideologiske universet oppfattes enhver representant for Vesten som en fiende det er legitimt å angripe.[22] Dette bidrar også til å fjerne politiske og moralske barrierer for hvem som kan angripes og med hvilke midler (18).

Et cyber-angrep er, for det andre, et meget presist eksempel på anvendelse av en indirekte strategi. Angriperen søker gjennom dette å påvirke politiske beslutninger, ikke gjennom å angripe eller sikre seg kontroll over det politiske beslutningsapparat direkte (dette må antas å

---

[20] Denne avgrensningen kan likevel kritiseres for å se bort fra tilfeller hvor stater driver "terror" mot egen befolkning. Historiske eksempler er mange og omfatter bl a Stalins politikk innen Sovjetunionen, Kambodsja under Pol Pot og Irak under Saddam Hussein. Den sterke vekt som fra amerikansk side legges på denne avgrensningen kan dessuten tolkes som motivert av ønsket om å unngå at handlinger USA selv eller allierte stater står bak, kan betegnes som terrorisme.

[21] Bombingen av sivile mål under Andre verdenskrig hadde en parallell motivering. Gjengs luftmaktdoktrine før Andre verdenskrig la vekt på å bruke bombefly til å ramme motpartens samfunn for derigjennom å svekke motivasjonen for å fortsette krigen. Betegnelsen "terrorbombing" er da også brukt om denne strategien. Tilsvarende tanker lå bak avskrekkingsdoktrinen mellom supermaktene under Den kalde krigen (jfr begrepet "terrorbalanse"). Den sentrale tanke var å opprettholde en stabil avskrekking ved å sikre den gjensidige evne til å ødelegge motpartens samfunn (Mutual Assured Destruction). Uansett hvor moralsk forkastelig denne praksis har vært og er, vil det i denne sammenheng ikke være formålstjenlig å la vårt terrorbegrep omfatte den. Det avgjørende skillet går altså mellom det som angår forholdet mellom stater (krigføring, avskrekkingsstrategi) og voldsbruk utøvet av aktører som ikke representerer eller handler på vegne av en eller annen stat.

[22] Det mest kjente utsagn om dette er Osama bin Ladens "Erklæring av Jihad mot jøder og korsfarere" fra 23 februar 1998. Her sies det bl a "The ruling to kill Americans and their allies – civilians and military – is an individual duty for every Muslim who can do it in any country in which it is possible to do it …." (jfr 26 s 143).

være utenfor terrorgruppers kapasitet), men ved å skape fryktmotiverte reaksjoner i samfunnet som i neste omgang påvirker myndighetene til endre sin politiske kurs. Dette er selvsagt en svært upresis strategi, hvor det praktiske resultatet kan bli svært forskjellig fra hva som er angriperens mål, men det er i det minste en strategi som lar seg gjennomføre med svært begrenset ressursinnsats. Nettopp i dette forholdet mellom ressursinnsats, strategi og potensielt resultat synes en stå ved et kjernepunkt ved terrorisme som strategi, og dette er like relevant uansett om angrepet skjer innenfor cyber-space eller andre fysiske regimer.

4 STRATEGISKE PROBLEMSTILLINGER

Terrorisme er ovenfor definert som er virkemiddel for å realisere et politisk mål. Slik sett representerer terrorisme en form for krigføring hvor det i første rekke er virkemidlene i seg selv og anvendelsen av dem som skiller denne spesifikke formen fra andre former for krig. Bruk av de globale data-nettverkene som arena for krigføring og terrorisme representerer imidlertid en utvikling som verken er godt forstått på det konseptuelle plan eller har ført til utvikling av effektive mottiltak. Denne erkjennelsen utgjør bakgrunnen for drøftingen i det følgende.

En viktig premiss for en konsekvensanalyse er at et omfattende angrep mot Internett som globalt kommunikasjons- og informasjonssystem, vil få ringvirkninger over svært store områder, om ikke over hele kloden, og påvirke svært mange mennesker. I denne sammenhengen betyr landegrenser svært lite. Denne trusselen er transnasjonal, og virkningene av et slikt angrep vil utgjøre en felles erfaring for mennesker og de politiske myndigheter i en rekke land.

Det er umulig å vite i hvilken grad scenariet som er beskrevet i kapittel 3 representerer en *sannsynlig* fremtidig utvikling. Dette er for så vidt heller ikke et sentralt poeng. Det vesentlige er at scenariet kan oppfattes som mulig, dvs realiserbart, innenfor en ikke svært fjern fremtid. Konsekvensene av et slikt angrep vil dessuten gjøre seg gjeldende på en rekke nivåer: fra det individuelle til det overgripende politiske både på det nasjonale og på det internasjonale nivå. Å drøfte dette problemet i sin fulle bredde vil imidlertid ikke være mulig innen rammen av denne analysen. I stedet vil drøftingen i det følgende fokusere mot følgende problemstilling: I hvilken grad kan det scenariet som er beskrevet gi grunnlag for internasjonal handling, og vil kunnskap om eksistensen og konsekvensene av denne typen trusler kunne få virkninger på det internasjonale politiske og institusjonelle plan?

Før vi går videre i drøftingen kan det imidlertid være nyttig å se nærmere på i hvilken grad angrep mot datasystemer er et egnet virkemiddel for å fremme politiske mål og hvilke begrensninger står angriperen overfor?

4.1 Hva kan motivere dataangrep?

Det synes i utgangspunktet klart at angrep mot elektroniske databaserte systemer innebærer en rekke fordeler for angriperen, spesielt mot en motstander som på de fleste områder er teknologisk og materielt overlegen. Viktige elementer er:

- *Lave kostnader*
  Angrep mot datanettverk krever ingen store investeringer i materiell eller oppbygging av store organisasjonsstrukturer. De vesentligste forutsetninger for å gjennomføre slike angrep er kompetanse, evne til å sette i verk og hemmeligholde planlegging og forberedelser, og tilgang til egnet maskinvare. Sammenlignet med iverksettelse av større konvensjonelle militære operasjoner med sammenlignbare virkninger er kostnadene bagatellmessige.

- *Umiddelbar og overraskende virkning*
  Virkningene av et angrep vil bli følbare i samme øyeblikk som det settes i gang, og det vil komme overraskende på de som rammes. Selv om et omfattende angrep kan kreve nøye planlegging over flere år, vil dette ikke måtte innbære oppbygging av fysiske eller andre strukturer som lett kan oppdages. Etterretning mot denne form for aktører vil formodentlig være ulike mye mer krevende enn etterretning mot aktører med et mer tradisjonelt operasjonsmodus. Det vil således heller ikke være knyttet noen tellende varslingstid til denne typen trusler.

- *Anonymitet*
  Selv etter at et angrep er satt i verk, kan angriperen skjule seg bak et slør av anonymitet. Selv om det mest sannsynlig raskt vil kunne etableres kunnskap om fra hvilke punkter i nettverker angrepet er startet, gir ikke dette i seg selv kunnskap om *hvem* angriperen er. En vil altså mangle et opplagt *mål* en eventuell gjengjeldelse eller defensive tiltak kan rettes mot. Dette er for så vidt ikke noe nytt, men er et fundamentalt problem knyttet til også andre former for asymmetrisk krigføring (gerilja-krig, tradisjonell terrorisme) hvor angriperen søker etter anonymitet i en befolkning. De digitale nettverkene forsterker dette og reduserer mulighetene for å iverksette effektive forsvarstiltak.[23]

- *Global rekkevidde*
  Geografi spiller ingen rolle. Ethvert punkt i nettverket står i forbindelse med ethvert annet, noe som opphever *avstand* som relevant parameter for denne typen trusler.

- *Lav risiko for angriperen*
  Angriperen behøver ikke løpe direkte personlig, fysisk risiko for å gjennomføre et angrep.

- *Tap av menneskeliv kan unngås*
  Angrep mot datanettverk innebærer at angriperen ikke behøver å overstige noen barrière (moralsk eller praktisk) mot å angripe mennesker eller fysiske objekter direkte. Gjennom å operere i et "immaterielt" rom utfordrer denne typen angrep ikke de vanlige tabuer mot å forårsake andre menneskers død.

[23] Asymmetriske utfordringer er svært vanskelige å håndtere nettopp fordi de virkemidler stater rår over ofte er irrelevante overfor aktører som ikke opererer med utgangspunkt i noen fysisk basis som kan angripes, samtidig som statenes komplekse samfunnsstruktur representerer sårbarheter som kan angripes med svært enkle virkemidler.

4.2 Og hva kan hindre det?

På tross av at angrep mot datasystemer representerer åpenbare muligheter, har dette så langt ikke ført til noen omfattende bruk av dette angrepsmediet verken fra terrorgrupper eller andre. Dette kan ha sammenheng med at de fortrinn denne angrepsformen representerer balanseres av en serie like åpenbare ulemper. De viktigste er:

- *Usikkerhet*
  Som det er pekt på tidligere i denne rapporten, har Internett i dag nådd et nivå av kompleksitet som gjør det umulig å ha noen sikker formening om hvilke konsekvenser hendelser ett sted i nettverket vil kunne få for helheten. Denne usikkerheten gjelder også for aktører som søker å påføre nettverket skade. Det er altså ikke mulig å forutsi hvilke effekter et stort angrep – heller ikke et omfattende DDoS-angrep rettet mot Internetts rottjenere – for nettets stabilitet og funksjonalitet som helhet. Denne usikkerheten må antas å representere en vesentlig barrière mot at bl a terrorgrupper skulle prioritere denne typen angrep.

- *Kompetanse*
  Mangel på kompetanse representerer ikke på lang sikt en tilstrekkelig barrière mot omfattende dataangrep. Ikke desto mindre krever et angrep som beskrevet i scenariet, oppbygging av en viss kompetanse og kjennskap til Internetts virkemåte. Denne kompetansen finnes i dag i første rekke i utviklede "vestlige" samfunn. De områder som hittil har vært den primære rekrutteringsmark for anti-vestlig terrorisme, særlig de islamske landene i Nord-Afrika, Midt-Østen og Vest-Asia, ligger derimot på bunnen av alle internasjonale rankinger hva gjelder f eks tilgang til Internett. Mens antall internettbrukere pr 100 innbyggere i USA er ca 50 og i Europa ligger mellom 18 (Spania) og 59 (Island), er tilsvarende tall for arabiske land fra 0,2 (Sudan) til 8,8 (Kuwait). Viktige land som Egypt, Saudi-Arabia og Syria har henholdsvis 0,9, 1,3 og 0,4 internettbrukere pr 100 innbyggere.[24] På den annen side er det også slik, som angrepene 11 september viste, at terrorens utøvere ikke primært rekrutteres fra samfunnets brede lag, men ofte utgjør en intellektuell elite, gjerne med utdannelse fra vestlige læresteder.

- *Gjensidig avhengighet*
  Terrorgrupper bruker Internett aktivt til å spre sitt budskap internasjonalt og til kommunikasjon innen og mellom mer eller mindre fast organisert miljøer. Slik sett etablerer også terrorgrupper selv en betydelig grad av avhengighet av Internett. Et angrep mot Internett vil derfor også ramme dem selv, noe som kan være en avskrekkende faktor for den type angrep som er beskrevet i scenariet, selv om dette ikke nødvendigvis gjelder for andre typer dataangrep.

- *Lite spektakulære virkninger*

[24] UNDP Human Development Indicators 2003. Internet Users (per 100 people), undp.org. De forente arabiske emirater og Bahrain utgjør unntak med 31,5 og 20,3 brukere pr 100.

> Det er ovenfor pekt på at terskelen for angrep mot datasystemer kan være lavere enn for andre typer angrep pga at dette ikke umiddelbart innebærer tap av menneskeliv. Dette argumentet gjelder åpenbart ikke for de former for terrorisme hvor ønsket om å skape store og spektakulære skadevirkninger har forrang. Selvmordsaksjoner, fra den ensomme selvmordsaksjonist til angrepene 11 september, kan være et "case in point". For denne typen aktører fortoner den anonymiserte, immaterielle digitale verden seg neppe som et foretrukket medium for virksomheten.

Drøftingen ovenfor indikerer at angrep mot globale datanettverk – sett fra "avsendersiden" – på tross av en rekke åpenbare attraktive sider, ikke nødvendigvis vil bli sett på som spesielt godt egnet for å fremme en gitt politisk agenda. For ytterligere å belyse dette problemet vil vi i det følgende betrakte spørsmålet fra motsatt side – "mottagersiden" – og vurdere nærmere konsekvenser og mulige tiltak.

5 TILTAK OG VIRKEMIDLER

Beskyttelse mot massive dataangrep forutsetter tiltak på en rekke nivåer; teknisk og operativt, nasjonalt og internasjonalt. Vi vil i denne sammenheng fokusere mot mulige *politiske* konsekvenser knyttet til dette problemkomplekset. For å sette spørsmålet inn i bredere kontekst vil vi imidlertid først berøre noen momenter knyttet til de praktiske konsekvensene av et omfattende tjenesteavbrudd som beskrevet i scenariet.

5.1 Virkninger for samfunnet

Ulike former for uønsket trafikk i Internett er ikke noe ukjent fenomen, og omfatter bl a masseutsendelse av e-post (såkalt "spam"), spredning av virus, innbrudd i datasystemer for å stjele eller ødelegge data etc. Slik virksomhet kan i visse tilfeller påføre bedrifter og enkeltpersoner store omkostninger. Eksempelvis er det beregnet at skadevirkningene etter det såkalte "I-Love-You"-viruset som ble spredd i 2000, medførte kostnader på opp mot 10 milliarder dollar på verdensbasis.[25] Det er samtidig grunn til å tro at kostnadene knyttet til denne typen angrep generelt sett er økende.[26]

Når det gjelder tjeneste-avbrudd av det omfang som scenariet beskriver, finnes det imidlertid ingen empiri som gir grunnlag for å beregne skade og kostnader mer eksakt.[27] Det er heller ikke enkelt å vurdere hvilke umiddelbare effekter dette vil få for den normale operasjon av viktige og mindre viktige samfunnsfunksjoner ut over det som allerede er indikert i scenariet. Konsekvensene kan imidlertid raskt bli store og i store trekk uforutsigbare. Eksempelvis førte

[25] *Love Bug virus costs expected to reach $ 10 billion*, infoworld.com 8 mai 2000
[26] *Virus costs keep rising*, vnunet.com 31 mars 2003
[27] Den erfaring en har om store og vedvarende data-angrep er primært fra øvelser. I USA ble det på 1990-tallet gjennomført flere slike øvelser. I 1995 gjennomført RAND Corporation en øvelse kalt "The Day After" som bygget på et større internasjonalt krise-scenario hvor data-angrep inngikk som ett element i en mer omfattende kampanje. I 1997 gjennomførte Pentagon en øvelse – "Eligible Receiver" – hvor en angriper over en periode på tre måneder systematisk søkte å svekke USAs evne til å føre krig gjennom å angripe militære informasjonssystemer (20).

angrepet mot World Trade Center 11 september 2001 til utfall av tele- og internett-kommunikasjon i New York, Connecticut og Massachusetts. I neste omgang falt hele nettverk ut i Romania, forskningsinstitusjonen CERN i Geneve ble rammet og alle websider med domenenavnet .za (Sør-Afrika) forsvant fra nettet én hel dag pga forstyrrelser i domenenavnsystemet (DNS) (27)! Den direkte årsaken var at sammenbruddet i bygningsstrukturene førte til at en rekke internettrutere og transatlantiske telekabler og andre elektroniske forbindelser ble ødelagt.

For øvrig er kanskje det mest relevante erfaringsmateriale hva gjelder massiv forstyrrelse av samfunnsfunksjoner store strømutfall som rammer store og tett befolkede områder. Eksemplene her er mange. I 1977 ble New York rammet av et strømutfall som varte i 25 timer, og i 1965 mistet 25 millioner mennesker strømmen i det nordøstlige USA.[28] Senest 14 august 2003 ble store deler av det nordøstlige USA og Canada rammet av et nytt strømutfall som medførte kaos i bl a trafikkavvikling, vannforsyning og det meste annet som krever elektrisitet for å fungere.[29] Tilsvarende strømutfall rammet London 28 august 2003 og Danmark og Sør-Sverige 23 september.[30] 28 september ble så å si hele Italia mørklagt etter at kraftnettet ble overbelastet som følge av et linjebrudd på en overføringslinje fra Sveits.[31]

Ved alle disse tilfellene ble strømforsyningen gjenopprettet i løpet av noen timer til ett døgn. Det synes imidlertid klart at mer vedvarende forstyrrelser på dette nivået raskt vil kunne bringe moderne IKT-avhengige samfunn til kollaps.

Avhengigheten av Internett er imidlertid av en helt annen art og langt mindre fundamental enn avhengigheten av elektrisk kraft. Det er derfor ikke mulig å trekke noen direkte sammenligning med de refererte hendelsene. Ikke desto mindre kan det gi grunn til å anta at en mer vedvarende ustabilitet i funksjonaliteten i Internett, som scenariet beskriver, vil kunne få virkninger som på visse områder er like følbare som massive strømutfall.

Studien ”Protecting Critical Infrastructures Against Cyber-Attack” peker på at den type angrep som scenariet beskriver, nettopp utnytter systemets distribuerte, men samtidig tett integrerte arkitektur til å ramme dets mest sårbare punkter. Dersom hyppigheten i angrepene overstiger systemets reparasjonstid kan skaden gjøres mer eller mindre permanent. I en slik situasjon vil brukerne søke etter alternative systemer for å løse viktige funksjoner og oppgaver. Dette vil skape ringvirkninger i samfunnet med vanskelig overskuelige totalvirkninger. Internett som informasjons- og kommunikasjonsinfrastruktur, vil da kunne bryte sammen, ikke først og fremst som følge av de innebygde svakheter i systemet, men fordi brukerne finner andre måter for å tilfredsstille sine behov. En treffende betegnelse på en slik situasjon er uttrykket ”death by a thousand cuts” (24).

---

[28] *Major power outage hits New York, other large cities*, cnn.com 14 august 2003
[29] Ibid.
[30] *Millions without power in Denmark, Sweden*, AP/energycentral.com 23 september 2003. *Rush hour power cut hits London*, cnn.com 28 august 2003.
[31] *Massive power outages sweeps across Italy*, AP/bradenton.com 28 september 2003

5.2 Konseptualisering av trusselen

"Cyber-trusler" av den typen som her er beskrevet, opererer i skjæringspunktet mellom nasjonal og internasjonal politikk. Mens trusselen i sin natur er transnasjonal – dvs uavhengig av landgrenser – er virkemidlene for å motvirke dette i stor grad nasjonale. Dette betyr at statene hver for seg kan iverksette tiltak med sikte på å redusere sårbarhet, endre lovgiving for lettere å kunne rettsforfølge terrorister etc, men dette vil ha begrenset effekt ut over det enkelte lands territorium. Effektiv forebygging og bekjempelse av trusselen forutsetter derfor utstrakt internasjonal koordinering og samarbeid.

Hvordan denne trusselen skal håndteres og hvilke virkemidler som kan tas i bruk, er imidlertid avhengig av en rekke forhold. Et springende punkt er selve definisjonen av problemet. Et første spørsmål en kan stille er følgelig i hvilken grad det er sannsynlig at det beskrevne scenariet vil oppfattes som et *sikkerhetspolitisk* problem av de statene som rammes.

Sikkerhetspolitikken er tradisjonelt oppfattet som den del av forholdet mellom stater – altså internasjonal politikk – som berører statenes *sikkerhet*. Sikkerhet er i denne sammenheng å forstå som knyttet til statens rent fysiske overlevelse (territoriell integritet og beskyttelse av befolkningen) og evnen til å utøve suverenitet (politisk autonomi: evne til å fatte og implementere politiske beslutninger). Sikkerhetspolitikken er derfor primært opptatt av forhold som berører anvendelse av militær makt mellom stater. Anvendelse av tvangsmakt i form av væpnet angrep, militært baserte trusler og press og beskyttelse mot dette, er derfor sentrale anliggender i statenes sikkerhetspolitikk.

Spredning av militære kapasiteter til ulike ikke-statlige aktører og oppkomsten av internasjonal terrorisme[32] har bidratt til å sprenge det statssentrerte fokus for sikkerhetspolitikken. Etter angrepene 11 september 2001 er dessuten terrorisme definert som en førsteordens sikkerhetsutfordring bl a for NATO (gjennom iverksettelsen av kollektive forsvarstiltak ihht Atlanterhavspaktens artikkel 5).

På tross av svært følbare konsekvenser i en rekke land, vil imidlertid det beskrevne angrepet ikke umiddelbart fremstå som en type utfordring man tradisjonelt oppfatter som "sikkerhetspolitisk". Her er det ingen arméer på marsj, enn si krenkelse av territorium. Det er heller ikke direkte fysisk skade i noe tellende omfang og myndighetenes evne til å utøve suveren kontroll over sitt territorium er ikke utfordret på en klar og entydig måte. I tillegg er varigheten av angrepet begrenset, og selv om sekundæreffektene kan være mer langsiktige vil ikke angrepet kunne endre grunntrekkene ved internasjonale maktforhold eller andre aspekter ved den internasjonale status-quo. Det kan altså godt tenkes at angrepet ikke vil oppfattes som et sikkerhetspolitisk anliggende, og at de vesentligste politiske konsekvensene vil være knyttet til den nasjonale arena (lovgiving, sårbarhetsreduserende tiltak etc).

[32] Internasjonal terrorisme kan defineres som grenseoverskridende terrorisme, dvs der et angrep finner sted i et annet land enn der terroraktøren har sitt utgangspunkt, eller der angrepet er rettet mot et annet lands borgere.

En nærmere analyse av dette spørsmålet vil imidlertid raskt kunne lede til motsatt konklusjon. Det globale omfanget av angrepet, og ikke minst potensialet for nye og forsterkede angrep, sannsynliggjør at denne trusselen raskt vil komme opp på den internasjonale dagsorden. Det faktum at angrepet i seg selv ikke fører til tellende tap av menneskeliv, truer den nasjonale suverenitet e l, endrer ikke på dette. Her kan en sammenligning med internasjonal terrorisme synes relevant. Som nevnt anses internasjonal terrorisme i dag for å være en viktig – om ikke den viktigste – trussel mot vestlige lands sikkerhet. Dette kan imidlertid *ikke* skyldes trusselens omfang eller "farlighet" i seg selv. Faktisk er antallet ofre for internasjonal terrorisme svært lavt målt mot de fleste former for organisert voldsutøvelse nasjonalt og internasjonalt. Eksempelvis var det totale antall ofre for internasjonal terrorisme i 1995 ifølge det amerikanske utenriksdepartement ikke mer enn 163.[33] Året før var det tilsvarende tallet 314 og året etter 311. I 1998 førte bl a angrepene mot USAs ambassader i Kenya og Tanzania dette tallet opp i 741(7). I denne sammenheng representerer året 2001, hvor angrepene 11 september alene medførte omkring 3000 drepte, et foreløpig toppunkt. Når internasjonal terrorisme på tross av et i den store sammenheng beskjedent omfang likevel blir tildelt en så sentral rolle i internasjonal politikk, skyldes dette primært denne trusselens *langsiktige* potensial. Her er faren for at transnasjonale terrornettverk av typen Al-Qaida skal få tilgang til (eller utvikle) kjernevåpen en avgjørende faktor.

Legger man et parallelt resonnement til grunn er det således gode grunner for å anta at trusselen om å bli utsatt for et globalt lammende dataangrep vil kunne sees på som en trussel minst på nivå med internasjonal terrorisme for øvrig. I utkastet til nasjonal strategi for "cyberspace" i USA refereres det således eksplisitt til nasjonale "vital interests" i omtalen av denne trusselen. Det fastslås videre at:

> "When a nation, terrorist group or other adversary attacks the United States through cyberspace, the US response need not be limited to criminal prosecution or even to information warfare means. The United States reserves the right to respond in an appropriate manner when its vital interests are threatened by attacks through cyberspace, just as it would with any other kind of aggression" (10 s 80).

Dette sitatet må kunne leses som uttrykk for et ønske om å bevare handlefrihet også i en situasjon hvor et angrep skjer "gjennom cyberspace" (jfr ovenfor). Uten at det spesifiseres nærmere, må en kunne gå ut fra at militære tiltak mot andre stater eller mot individer og grupper i andre land vil kunne inngå i virkemiddelbruken på samme måte som for "enhver annen form for aggresjon" (jfr ovenfor). For USAs del kan en trekke en parallell til angrepene mot Taliban-regimet i Afghanistan etter 11 september, selv om det i dette tilfellet ikke var snakk om noen digital trussel fra Al-Qaida.

I tillegg til at angrep mot datanettverkene i ekstreme tilfeller kan gi grunnlag for ensidige tiltak

[33] Disse tallene omfatter kun det som kan kalles *internasjonal* – altså grenseoverskridende – terrorisme. Derfor er de 168 ofrene for angrepet mot den føderale bygningen i Oklahoma City, som også fant sted i 1995, ikke inkludert. I *nasjonale* konflikter kan dessuten terrorisme, geriljakrig og annen voldsbruk være vanskelig å skille fra hverandre. Uansett fører slike konflikter jevnlig til langt større antall drepte enn internasjonal terrorisme.

av ulik type, inkludert individuelt selvforsvar, vil dette også kunne motivere kollektive tiltak innen rammen av FN eller andre internasjonale institusjoner. Vi vil i det følgende se nærmere på spørsmål knyttet til muligheter og begrensninger for politisk koordinering på den internasjonale arena.

5.3 FN og folkeretten

I den internasjonale kampen mot terror står FN og folkeretten i en særstilling som autoritativt grunnlag for politisk og militær handling. Hovedregelen er her at væpnet angrep mot et annet land er forbudt. Unntakene fra denne regelen er behandlet i FN-charterets kapittel VII. Dette omhandler trusler mot freden, fredsbrudd og angrepshandlinger. I det tilfelle en står overfor et brudd på freden i form av et væpnet angrep kan Sikkerhetsrådet sanksjonere bruk av militær makt fra det internasjonale samfunn for å gjenopprette *status-quo ante*. Dessuten har enhver stat rett til individuelt eller kollektivt selvforsvar. Dette fastslås i artikkel 51 under samme kapittel.

Folkerettens bestemmelser om bruk av væpnet makt behandler primært forholdet mellom stater. Det er langt mindre klart om disse bestemmelsene dekker forholdet mellom private individer og stater. Dette er særlig relevant i forhold til spørsmålet om rett til selvforsvar mot ikke-statlige aktører, f eks terrorgrupper. En mulig tolkning av folkeretten er at retten til selvforsvar bare kan anses som utløst dersom en annen stat kan holdes ansvarlig for angrepet. En slik tolkning representerer åpenbart en begrensning på statenes muligheter til militær maktbruk utenfor egne landgrenser som forsvar mot terrorisme. Folkeretten knytter også retten til selvforsvar spesifikt an til et *væpnet* angrep. Dersom dette ikke har skjedd gjelder heller ikke retten til selvforsvar. Til sist er det et krav at selvforsvarshandlingen skal være proporsjonal med angrepet, dvs at en ikke kan iverksette selvforsvarstiltak av en helt annen art eller i et helt annet omfang (25).

For å kunne utføre selvforsvar mot terrorangrep må altså angrepet både ha et visst omfang (jfr begrepet "væpnet angrep") og en stat må kunne holdes ansvarlig. Etter 11 september 2001 er det imidlertid grunn til å anta at det har skjedd en endring i folkeretten som utvider retten til selvforsvar mot ikke-statlige aktører. Dette er særlig knyttet til de to resolusjonene som ble vedtatt etter angrepene mot USA. Resolusjon 1368 (12 september 2001) klargjør enhver stats rett til individuelt og kollektivt selvforsvar mot terrorisme og retten til å ta i bruk "…all necessary steps …. to combat all forms of terrorism".[34] Resolusjon 1373 (28 september 2001) gir utdypende føringer for den internasjonale innsatsen mot terrorisme. Begge resolusjonene definerer klart terrorisme som trusler mot internasjonal fred og sikkerhet.

Det er imidlertid meget usikkert hvorvidt FN-charteret og Sikkerhetsrådet er relevante instanser i forhold til det scenario denne analysen bygger på. Det springende punkt er hvorvidt angrepet kan defineres som en trussel freden eller en angrepshandling (væpnet angrep). Resolusjon 1368 refererer til "…all forms of terrorism", men det er tvilsomt om denne formuleringen omfatter handlinger som i utgangspunktet ikke innebærer fysiske angrep mot mennesker eller objekter,

[34] NATOs anvendelse av Atlanterhavspaktens artikkel 5 (vedtatt i Det nordatlantiske råd 12 september 2001) etter angrepene mot USA er folkerettslig forankret så vel i FN-charterets kapittel VII, artikkel 51 som i denne resolusjonen i sikkerhetsrådet.

men som bare er rettet mot kommunikasjons- og informasjonssystemer.

Selv om dette hadde vært tilfelle står en overfor det problem at det internasjonale samfunn mangler adekvate virkemidler for å forsvar mot denne typen trusler. FNs kollektive sikkerhetsordninger er i første rekke organisert rundt muligheten til å anvende tvangstiltak, bl a militære, mot aktører som truer den internasjonale fred og sikkerhet. Det fortoner seg imidlertid som temmelig åpenbart at det virkemiddelsett en her rår over har begrenset relevans overfor den trussel scenariet beskriver. Disse begrensningene gjelder også i fullt monn NATOs handlingsmuligheter. I den grad angriperne rår over baser eller annen fysisk infrastruktur som kan angripes, eller om de beskyttes av andre aktører som tvangstiltak kan settes inn overfor (f eks en annen stat), kan militære tiltak ha en viss begrenset rolle. Det scenariet som her er beskrevet, forutsetter imidlertid ingen av disse faktorene; et DDoS-angrep er i sin natur distribuert på en måte som langt på vei gjør fysiske mottiltak irrelevante.

En konklusjon på dette er at det sentrale globale sikkerhetsorgan – FN – i stor grad mangler mulighet for effektiv handling overfor stort anlagte angrep mot verdens informasjons-infrastruktur. Når folkeretten vanskelig kan sees å fange opp denne utfordringen, må den videre bekjempelse av denne spesielle typen terrorisme enten skje med utgangspunkt i de ulike nasjonale lovverk eller gjennom en utvidelse av folkeretten til også å omfatte nasjonal lovgiving. Det siste alternativet synes imidlertid, i det minste innen en overskuelig tidsramme, lite realistisk, selv om hendelser av den typen som er beskrevet i scenariet skulle gi incitamenter i den retning. Når det gjelder det første – utstrakt koordinering av nasjonal rettshåndhevelse – kan det være av interesse å betrakte hvordan oppblomstringen av internasjonal terrorisme har bidratt til dette innenfor EU.

5.4 Bekjempelse av terror i EU

Innen EU er det etablert en rekke ordninger med sikte på å effektivisere rettshåndheving og bekjempelse av terrorisme. I stor grad er imidlertid de ordningene som er etablert rettet mot forhold knyttet til bevegelser av personer og varer. Schengen-avtalen innebærer således en nedbygging av grensekontrollen internt samtidig med en styrket kontroll langs Schengen-områdets yttergrenser.[35] Etableringen av EUROPOL (1995, operativ fra 1999) var i første rekke myntet på bekjempelse av narkotikasmugling. Mer spesifikke tiltak mot internasjonal terrorisme er utferdiget i Gomera-erklæringen (1995) som inneholder bestemmelser om utveksling av informasjon og koordinering av medlemslandenes rettsapparat (19 s 13-14).

Etter 11 september-angrepene er det truffet en rekke nye tiltak. Dette inkluderer en felles definisjon av terrorisme og innføring av en felles arrestordre for å unngå behovet for formelle utleveringsprosedyrer. Utenriksministrene i EU vedtok dessuten allerede 21 september 2001 en handlingsplan hvor et hovedpunkt var å opprette en felles etterforskningsenhet og spesialstyrke (European Counter-Terrorism Task Force) knyttet til EUROPOL. En vedtok også tiltak for å

[35] Schengen-området består i dag av 15 land. Storbritannia og Irland deltar ikke i Schengen-samarbeidet. Norge og Island inngikk avtale med Schengen-landene 19 desember 1996.

begrense finansieringen av terrorvirksomhet, og gjennom "Joint EU US Action Plan" har en etablert et bredt samarbeid med myndighetsorganer i USA (19 s 15-16).

Gjennom slike ordninger er terrorbekjempelse primært plassert innen rammen av sivil myndighetsutøvelse med grunnlag i nasjonale og felles lovbestemmelser. Håndhevelsen styrkes gjennom utstrakt koordinering av tiltak og etablering av fellesorganer.

Terrorismen og kampen mot denne griper imidlertid over det tradisjonelle skillet mellom innenrikspolitikk og utenrikspolitikk. Debatten om dette dreier seg følgelig i vesentlig grad om hvor vidtfavnende tiltakene mot terrorisme skal være, og på hvilken måte militære virkemidler kan spille en rolle. Et "case in point" er eksempelvis etablering av missilforsvar av større regioner, eller ulike former for preventive militære aksjoner utenlands (19 s 22).

Trusler mot informasjons- og kommunikasjonssystemene har imidlertid ingen prominent posisjon, heller ikke innen EUs anti-terrorstrategi. Virkemidlene og tiltakene som det legges opp til er i all hovedsak orientert mot allerede kjente former for terrorisme. Hovedelementene i strategien består dels i å begrense terrorgruppers mulighet til å operere gjennom å hindre deres finansiering og bevegelsesfrihet, dels i forebyggende innsats i konfliktområder. Overfor trusler knyttet til informasjonsnettverkene har imidlertid etter alt å dømme denne typen tiltak begrenset effekt.

6 ET GLOBALT RISIKOSAMFUNN

En hovedkonklusjon fra drøftingen ovenfor er at eksisterende internasjonale institusjoner og samarbeidsordninger bare i begrenset grad er egnet til å forebygge og bekjempe stort anlagte dataangrep. Dette skyldes i hovedsak at de virkemidler en her rår over enten er irrelevante overfor denne spesifikke trusselen (militære), eller har begrenset anvendelsesområde (rettslige). Utvikling av rettshåndhevelsestiltak innen EU representerer imidlertid en tellende utvidelse av virkeområdet for slike tiltak, men i forhold til en trussel som i sitt vesen er global har også dette begrenset effekt.[36]

Når trusselen i sin natur har global rekkevidde, må tiltak for å forebygge og bekjempe denne også kunne anvendes globalt. Vi vil i denne sammenheng se på mulighetene for å få til effektive tiltak på som avhengig av tre grunnforutsetninger:

1. At trusselen oppfattes som reell
2. At trusselen oppfattes som alvorlig (dvs truer vitale interesser)
3. At det er mulig å gjøre noe med den

I tillegg, og spesielt hva gjelder internasjonal handling, må trusselen kunne forstås som *felles*,

[36] En må her huske på at anti-terrorsamarbeidet innen EU hadde sin opprinnelse i behovet for å bekjempe den innenlandske terrorisme med grupper som Rote Armé Fraktion, Brigate Rossa o a på 1970- og 1980-tallet. I forhold til dette representerer internasjonal terrorisme til dels helt andre problemstillinger.

dvs noe alle deler og er like mye utsatt for. Spørsmålet vi i denne sammenheng kan stille oss er i hvilken grad denne formen for ”krigføring” i cyberspace vil kunne være en form for allmennmenneskelig, kollektiv erfaring som vil påvirke den generelle bevissthet om usikkerhet og trusler, og som følge av dette bidrar til å endre politiske realiteter i bestemte retninger.

Det er et gjennomgående trekk ved den utvikling som under tiden går under betegnelsen ”globalisering”, at ikke bare goder av ulikt slag deles og spres til stadig flere, men at også truslene representerer en risiko som ingen kan komme unna, men alle har sin andel av. Den tyske sosiologen Ulrich Beck har begrepsfestet dette skjebnefellesskapet som et globalt ”risiko-samfunn”. Det globale risikosamfunnet har dessuten en *refleksiv* kvalitet: det er nettopp de aktiviteter og strukturer som får samfunnet til å fungere som skaper eller formidler truslene mot samfunnet og dets innbyggere.

Beck hevder at dette risikosamfunnet ”har sitt sentrum i den massemediale offentlighet, i politikken, byråkratiet og økonomien, og ikke nødvendigvis i begivenhetenes sentrum”. Samtidens trusler forsterkes dessuten gjennom ”fiaskoen til institusjonene hvis berettigelse hviler på deres påståtte mestring av faren” (22 s 120). Det er altså ikke nødvendigvis primært hendelsen (f eks et angrep) i seg selv som er problemet, men erkjennelsen av vår manglende evne til å håndtere den. Når vi ikke lenger kan lite på evnen til å mestre faren når den oppstår, er det ikke i første rekke hva som har skjedd, men hva som *kan komme til å skje* som blir utgangspunktet for handling. Trusselscenariene blir slik sett ”the currency of politics” (23 s 328), og det blir, gitt denne logikken, kritisk viktig å hindre truslene i å oppstå ved å komme dem i forkjøpet.

Satt inn i denne rammen er angrepene 11 september 2001 et presist eksempel på utfordringene i det globale risikosamfunnet. Betydningen av 11 september ligger først og fremst i den internasjonale terrorismens *potensial*, ikke i det enkeltstående angrepet. Dette potensialet representerer – særlig om en tenker seg en sammenkobling av terrorister og kjernefysiske våpen – en trussel mot vitale interesser og verdier. En kan si at terrortrusselen er ”sikkerhetisert” (”securitized”) (21). Med dette er internasjonal terrorisme gjort til et anliggende for nasjonale og internasjonale sikkerhetsetablissementer og til objekt for militær innsats, inkludert preventiv bruk av militær makt, for å bekjempe trusler før de kan bli satt ut i livet. Dette skjer uaktet hva som måtte finnes av folkerettslige begrensninger. Terrortrusselen og bekjempelsen av den er i et slikt perspektiv det første skritt på veien mot et post-nasjonalt inter-”nasjonalt” system. Det bør ikke være en alt for dristig forutsigelse at en overgang til et slikt system vil sprenge det normative rammeverk som er etablert for å regulere statenes relasjoner til hverandre.

Betraktet fra denne synsvinkelen tilfredsstiller internasjonal terrorisme de tre forutsetningene: (i) trusselen oppfattes som reell; (ii) den truer vitale interesser og verdier; (iii) bekjempelsen av den er plassert innenfor en sikkerhetspolitisk ramme hvor de viktigste virkemidlene er militære.

Vår avhengighet av den globale informasjons- og kommunikasjonsinfrastrukturen og trusselen om et massivt dataangrep, representerer på mange måter kvintessensen av det globale

risikosamfunnet. Et angrep mot disse systemene bærer i seg muligheten for å berøre langt flere mennesker på langt mer direkte måter enn de fleste andre globale trusler som f eks forurensning eller, som allerede nevnt, mer tradisjonelle former for terrorisme. Behovet for handling er det altså ingen grunn til å stille spørsmål ved. Dilemmaet oppstår imidlertid i spørsmålet om hvordan denne trusselen skal møtes. De kritiske spørsmål er *når* og *på hvilken måte*.

Dersom det globale risikosamfunnets politiske handlingsgrunnlag er knyttet til potensielle trusler mer enn de materialiserte trusler, er det et tankekors at så lite er gjort for å berede grunnen for et globalt forsvar av cyberspace. Virkeliggjøring av trusselen i form av et angrep tilsvarende det beskrevne scenariet, vil imidlertid umiddelbart – dersom en kan støtte seg på erfaringene fra 11 september – skape et akutt behov for å finne virkemidler og metoder for å forhindre nye angrep.

For å lykkes med dette vil det være avgjørende om en finner metoder for å forebygge truslene; når de materialiserer seg er det allerede for sent å unngå skadevirkningene. Å handle preventivt representerer imidlertid åpenbare og vanskelige problemstillinger. En slik strategi stiller bl a svært høye krav til både nasjonal og internasjonal kapasitet til å overvåke og drive etterretning innen cyberspace. Når en tar i betraktning de lave kostnader forbundet med cyberangrep, antallet aktører med kapasitet til å sette dem i verk, mulighetene til å skjule sin identitet og mangelen på pålitelige indikatorer, fortoner dette seg som såpass krevende at dette neppe er en praktisk mulig løsning. I tillegg forutsetter en forkjøpsstrategi evne til å gripe inn med tvangstiltak uten hensyn til landegrenser og nasjonal jurisdiksjon. Som det allerede er pekt på er dette kapasiteter som i stor grad mangler.

Kan cyberangrep avskrekkes? Siden avskrekking hviler på avstraffelse *post-hoc* kan dette synes som mer realiserbart enn å søke å komme en angriperen i forkjøpet. Like fullt vil en effektiv avskrekkingsstrategi være svært krevende å få til. En side ved dette er mulighetene for anonymisering av angriperen, noe som gjør både identifisering og lokalisering vanskelig, og dermed trusselen straff mindre troverdig. Dette fører til at kostnadene ved å iverksette straffen kan bli urimelig høye, noe som ytterligere bidrar til å undregrave strategiens troverdighet. I tillegg må straffen være relevant i forhold angriperens kost-nyttekalkyle; straffen må representere en *reell* kostnad for angriperen. Dersom dette ikke er mulig, vil strategien ha begrenset effekt, og dette er for så vidt et problem som alt i dag er erkjent mht bekjempelsen også av andre former for terrorisme. Til sist forutsetter en troverdig trussel om straff et visst nivå av internasjonal rettshåndhevelse, som i dag i stor grad mangler. De tradisjonelle sikkerhetsmekanismene – primært militære – er som tidligere påpekt, i hovedsak irrelevante overfor distribuerte dataangrep fra ikke-statlige aktører.

Med utgangspunkt i drøftingen overfor kan det argumenteres for at en dramatisk demonstrasjon av trusselen mot globale kommunikasjons- og informasjonsnettverk som beskrevet i scenariet, vil kunne føre til en utvikling i én av to retninger. På den ene siden, etter modell av utviklingen etter 11 september, vil dette kunne utløse en forsterket innsats på det politiske felt for å

forebygge nye trusler gjennom å bekjempe aktørene bak denne formen for terrorisme.[37] En slik utvikling vil imidlertid kunne utløse følgende dilemma: Som Ulrich Beck peker på representerer den nye terrorismen (dette gjelder ikke minst cyber-terrorisme) en form for *individualisering* av krigføringen som skyldes at teknologien gjør det mulig for enkeltindivider å "føre krig" mot stater. Ethvert individ representerer dermed potensielt en trussel, noe som fører til en radikal intensivering av statens kontrolltiltak overfor borgerne. Med dette sprenges en kile mellom staten og samfunnet/borgerne. For å ha effekt må tiltakene dessuten strekkes ut over det enkelte lands grenser. Når regjeringer slik "alliere[r] seg med andre regjeringer mot borgerne", (22 s 132) representerer dette i siste instans en trussel mot de verdier en i første omgang ønsket å beskytte.

Denne utviklingen er allerede i dag klart synlig. Det er således et sentralt trekk ved den globaliserte verden at tradisjonelle borgerlige friheter som ytringsfrihet, personvern og bevegelsesfrihet settes under press gjennom myndighetenes stadig mer påtrengende tiltak for å sortere ut faktiske og mulige terroraktører. Et annet spørsmål er det imidlertid om denne typen intensivert overvåkning og kontroll vil ha effekt overfor trusler som opererer innenfor digitale media. Svaret på dette spørsmålet skal ikke gis her. Imidlertid synes det for det første klart at utfordringene knyttet til å overvåke de globale datanettverkene, og identifisere og varsle trusler synes uoverkommelig store, og for det andre at om en søker å realisere målsettingen om et transparent Internett vil det flytte en rekke grensesteiner mellom det som i dag oppfattes som det offentlige rom og privatsfæren.

Alternativet til en "sikkerhetspolitikk" for cyberspace er imidlertid neppe mer tillokkende. De langsiktige konsekvensene av et ustabilt nettverk vil kunne trekke i retning av at brukerne, ikke som resultat av koordinert beslutninger, men som følge av et stort antall individuelle avveininger av risiko, søker alternativer til Internett som kommunikasjons- og informasjonssystem. Realismen i dette er vanskelig å vurdere, men det synes uansett lite trolig at moderne samfunn vil kunne fungere uten de globale datanettverkene. En mer eller mindre allmenn "flukt" fra Internett vil således kunne få uoverskuelige konsekvenser for utviklingen på så å si alle samfunnsområder.

7 KONKLUSJON

Internett har på mindre enn et tiår ført til revolusjonerende endringer for hvordan mennesker kommuniserer, hvordan informasjon spres, for økonomiske transaksjoner, for hvordan varer og tjenester produseres og dermed for økonomien som helhet. Samtidig er det rimelig å anta at dette bare er begynnelsen på mer omfattende og gjennomgripende samfunnsmessige endringer som følge av fortsatt utvikling av de globale digitale nettverkene. Den videre utvikling på dette feltet vil derfor etter all sannsynlighet også få konsekvenser på det politiske plan, for forholdet mellom myndighetsorganer, for utøvelse av makt innen og mellom land og for hvordan man i

[37] Iverksettelse av sårbarhetsreduserende tiltak vil selvsagt ha en sentral plass. Dette ansvaret vil imidlertid primært ligge på systemeierne, og i mindre grad forutsette politisk inngripen, og faller følgelig i stor grad utenfor denne drøftingen.

det hele tatt konseptualiserer sikkerhet i det som i enkelte sammenhenger kalles *informasjonssamfunnet*.

Denne analysen har tatt utgangspunkt i muligheten for å gjennomføre et – i det minste temporært – lammende angrep mot Internett. Uten at det har vært mulig å beregne virkningene av dette scenariet mer eksakt, synes det like fullt klart at de samlede virkningene i form av forstyrrelser av vitale samfunnsfunksjoner langt vil overskride det en hittil har kunnet iaktta som følge av mer tradisjonelle former for terrorisme. Om en trekker denne sammenligningen ytterligere noen skritt lenger og betrakter de radikale konsekvenser internasjonal terrorisme allerede har fått for internasjonal politikk generelt og rammene for utøvelse av (militær) makt mer spesielt, må det være tillatt å konkludere med at langt mer radikale endringer vil kunne komme som følge av at de globale datanettverkene gjøres til ”slagmark” i stor skala.

Rapporten peker på at dagens regime for opprettholdelse av fred og sikkerhet og for utøvelse av makt – primært folkeretten – i store trekk er irrelevant for å forebygge og å bekjempe den type angrep det her er snakk om. Dette skyldes dels at selve trusselen ikke kan avgrenses til å være rent nasjonal eller internasjonal, men ligger i grenselandet mellom disse to domener, og dels at de tvangsmidler statene besitter, hva enten de er militære eller sivile, er innrettet på helt andre utfordringer enn de som formidles gjennom cyberspace.

Det er følgelig en sentral konklusjon at et angrep av den typen scenariet beskriver, vil kunne representere en sterk impuls til samordning av tiltak mellom land, til koordinering av nasjonale lovverk og evt til etablering av overnasjonale organer for å styrke evnen til å bekjempe de nye truslene. Samtidig – og her kan en trekke på erfaringer fra utviklingen etter 11 september 2001 – vil mangelen på effektive internasjonale regimer for bekjempelse av terror være en sterk driver for at nasjoner med store ressurser vil se det som sin rett å treffe de tiltak – også ensidige – som anses som nødvendige for å sikre sine egne interesser, slik f eks USAs sikkerhetsstrategi for cyberspace indikerer.

I det internasjonale systemet er bruk av militærmakt og krig tradisjonelt sett på som det dominerende sikkerhetsproblem. Folkerettens regler for legitim bruk av makt mellom stater må således sees på som et svar på ønsket om å fange statenes militære potensial inn i et stabiliserende sikkerhetspolitisk regime.

I forhold til tradisjonelle vestlige forestillinger om bruk av makt innen og mellom land representerer imidlertid de nye truslene fra transnasjonale terroraktører helt nye problemstillinger. Dette gjelder i særlig grad når de digitale nettverkene gjøres til arena for angrep og maktutøvelse. Under dette regimet har maktutøvelsen ingen fysisk karakter, og aktørene mangler de sentrale attributter som kjennetegner suverene stater – territorium, befolkning og politiske institusjoner. De metoder, konsepter og rettsregler som er etablert for å håndtere konflikter mellom land mangler derfor i stor grad relevans når en ikke kan peke på en identifiserbar aktør som utøver av (illegitim) vold. Nasjonale myndigheters suverene rett til å håndheve loven innenfor sitt eget territorium kommer også til kort overfor en trussel som i sin

natur er global.

I tillegg åpner den teknologiske utvikling for at enorme skadevirkninger kan forårsakes ved begrenset innsats både materielt og organisasjonsmessig. Det synes f eks klart at det ikke kreves verken uoverstigelig store ressurser eller en stor organisasjon for å iverksette det angrepet som er beskrevet i scenariet. Rapporten peker således på at enkeltindivider – satt på spissen – kan føre krig mot stater. Tiltakene for å beskytte staten og samfunnet blir derfor i større grad rettet mot å føre kontroll med enkeltindivider – en utvikling som allerede er synlig. Trekker en dette ut i sin ytterste konsekvens kan en altså komme i den situasjon at ikke bare enkeltindivider kan føre krig mot stater, men at statene slår seg sammen mot individene. Mye skal imidlertid gå galt før en havner der. Ikke desto mindre stiller muligheten for å gjøre de digitale media til fremtidens slagmark de dilemmaer som reiser seg ved håndteringen av disse truslene i et skarpt relieff.

Litteratur

(1) (2002): Subcommittee on Terrorism and Homeland Security, House Permanent Select Committee on Intelligence, *Counterterrorism Intelligence Capabilities Prior to 9-11*, A Report to the Speaker of the House of Representatives and the Minority Leader, July 2002.

(2) Strindberg Anders (1998): Terrorism in Western Europe In: *FOA Report on Terrorism* (Ed Jervas Gunnar), Defence Research Establishment, Stockholm, FOA, 207-227.

(3) White Jonathan R (1998): Terrorism: An Introduction (second edition), West/Wadsworth Publishing Company, London.

(4) Lia Brynjar, Kjøk Åshild (2001): Islamist Insurgencies, Diasporic Networks and Their Host States: The Case of the Algerian GIA in Europe 1993-2000, FFI/Rapport-2001/03789, ugradert

(5) Ranstorp Magnus (1998): The Inner Logic of Religiously Motivated Terrorism In: *FOA Report on Terrorism* (Ed Jervas Gunnar), Defence Research Establishment, FOA, Stockholm, 21-40.

(6) Hoffman Bruce (1998): Terrorism: Contemporary Trends and Future Prospects In: *FOA Report on Terrorism* (Ed Jervas Gunnar), Defence Research Establishment, FOA, Stockholm, 231-246.

(7) U.S. Department of State: Patterns of Global Terrorism Report.

(8) Kahn Rober E, Vinton G Cerf (1999): What is the Internet (and What Makes it Work)?, *http://www.worldcom.com*.

(9) Tanase Matt (2002): Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks, *http://online.securityfocus.com*.

(10) The President of the USA (2002): The National Strategy to Secure Cyberspace (Draft, September 2002).

(11) Lia Brynjar, Rolf Inge Vogt-Andrésen (2000): Asymmetri, asymmetrisk krigføring og asymmetriske trugsmål: Bruken av asymmetri-omgrepet i tryggingspolitisk og militærteoretisk litteratur, 2000/01718, ugradert

(12) Fridheim Håvard, Janne Hagen, Stein Henriksen (2001): En sårbar kraftforsyning - sluttrapport etter BAS3, FFI/Rapport-2001/02381, ugradert

(13) Hagen Janne M, Nystuen Kjell Olav (1999): Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon, FFI/Rapport-99/00240, ugradert

(14) Rodal Siv Kjersti (2002): Systembeskrivelse av den norske jernbanen, FFI/Rapport-2002/00808, ugradert

(15) Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet,

innstilling fra Sårbarhetsutvalget, NOU 2000:24.

(16) Rodal Gry Hege (2002): Systembeskrivelse av norsk luftfart, FFI/Rapport-2002/01362, ugradert

(17) Hadenius Patric (2003): Internet kan slås ut på 15 minuter, *Forskning och Framsteg* **2/03**, 42-45.

(18) Freedman Lawrence (red) (2002): Superterrorism: policy responses, Blackwell publishing, Oxford, UK.

(19) Knutsen Bjørn Olav, Pernille Rieker (2003): EUs "nye" sikkerhetspolitikk: bekjempelse av terrorisme og internasjonal kriminalitet, FFI/Rapport-2003/01301, ugradert

(20) Adams James (1998): The Next World War: Computers are the Weapons and the Front Line is Everywhere, Simon & Schuster, New York.

(21) Buzan Barry (1997): Rethinking Security After the Cold War, *Cooperation and Conflict* **Vol 32**, No 1, 5-26.

(22) Beck Ulrich (2003): Globalisering og individualisering, bind 3 - Krig og terror, Abstrakt forlag, Oslo.

(23) Rasmussen Mikkel Vedby (2002): A Parallel Globalization of Terror: 9-11, Security and Globalization, *Cooperation and Conflict* **Vol 37**, No 3, 323-349.

(24) Lukasik Stephen J, Seymour E Goodman, David W Longhurst (2003): Protecting Critical Infrastructures Against Cyber-Attack, *Adelphi Papers*, 359.

(25) Hegge Vidar (2002): Rett til sjølvforsvar mot terrorgrupper? Oversyn over enkelte problemstillingar og argument, FFI/Rapport-2002/03524, ugradert

(26) Hegghammer Thomas (2002): Dokumentasjon om Al-Qa'ida - intervjuer, kommunikéer og andre primærkilder 1990-2002, FFI/Rapport-2002/01393, ugradert

(27) Schulzki-Haddouti Christiane (2004): Würmer und Viren im Netz. Gefahren des Cyber-Terrors und seiner Bekämpfung, *Internationale Politik* **59** , 2, 41-48.