FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--0830--SE

ISSN 1650-1942

Josefin Grennert och Magdalena Tham Lindell

Cyberterrorism

Öppnar IT nya möjligheter för terrorism?

Avdelningen för Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT

FOI-R--0626--SE
ISSN 1650-1942

Josefin Grennert och Magdalena Tham Lindell

Cyberterrorism

Öppnar IT nya möjligheter för terrorism?

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI	FOI-R--0626--SE	Användarrapport
	Forskningsområde	
	Försvars- och säkerhetspolitik	
	Månad, år	**Projektnummer**
	1002	A1154
	Verksamhetsgren	
	Forskning för regeringens behov	
	Delområde	
	Teknik, industri och politik	

Författare/redaktör	Projektledare
Josefin Grennert	Josefin Grennert
Magdalena Tham Lindell	**Godkänd av**
	Eva Mittermaier
	Uppdragsgivare/kundbeteckning
	Försvarsdepartementet
	Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel

Cyberterrorism: Öppnar IT nya möjligheter för terrorism?

Sammanfattning (högst 200 ord)

Syftet med rapporten är att klargöra vad cyberterrorism är samt att utröna huruvida ett sådant hot föreligger mot vårt samhälle eller har potentialen att utvecklas på sikt. I rapporten förs en definitionsdiskussion och en definition av cyberterrorism föreslås. Sammanslagningen av ”cyber” med ”terrorism” ger vid handen att begreppet innebär ett nytt medel för terrorism samt att det är skilt från andra typer av databrottslighet vilka inte är att klassa som terrorism.

Det är mer sannolikt att cyberterrorism växer fram som ett komplement till, snarare än ersättning av, konventionella angrepp. Det är tänkbart att cyberterrorism skulle kunna användas i anslutning till konventionella angrepp i syfte att förstärka våldsverkan och fördröja samhällets återhämtning.

Sveriges utsatthet för terrorism förefaller idag vara liten. Hotbilden kan dock snabbt komma att förändras och faktorer som kan påverka är internationella insatser, deltagande i kampen mot internationell terrorism eller en starkare integrering inom EU genom vilken Sverige kan få del i andra länders säkerhetsproblematik.

Möjligheterna att idag utföra cyberterrorism i Sverige bedöms som små. Det är av säkerhetspolitisk betydelse att sårbarheten i den kritiska tekniska infrastrukturen hålls så låg som möjligt och att sårbarheter inte byggs in i systemen.

Nyckelord

Informationsteknik, IT-hot, Informationsoperationer, Informationskrigföring, Terrorism, Cyberterrorism

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** s. 42
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization FOI – Swedish Defence Research Agency	**Report number, ISRN** FOI-R--0626--SE	**Report type** User report
	Research area code Defence and security policy	
	Month year 1002	**Project no.** A1154
	Customers code Research for the Government	
	Sub area code	

Author/s (editor/s) Josefin Grennert och Magdalena Tham Lindell	**Project manager** Josefin Grennert
	Approved by Eva Mittermaier
	Sponsoring agency Department of Defence
	Scientifically and technically responsible

Report title (In translation)

Cyberterrorism: Does IT open new possibilities for terrorism?

Abstract (not more than 200 words)

The purpose of the report is to clarify what cyber terrorism is and to determine if there is such a threat against our society or if one could develop over time. A definition of cyber terrorism is suggested. The connection between "cyber" and "terrorism" suggests that the word implies a new means for terrorism and also that it is separated from other forms of computer crime that can not be classified as terrorism.

It is more likely that cyber terrorism develops as a complement to, rather than replacement of, conventional attacks. It is likely that cyber terrorism could be used in connection with conventional attacks as a means to enhance violence and to delay the recovery of the society. The likelihood of terrorist attacks in Sweden is low. This, however, can change rapidly and factors that may influence this development are international military efforts, participation or statements in the fight against international terrorism, and a stronger integration within the EU through which Sweden may get part of the security problems of other countries.

The possibilities to carry out cyber terrorism in Sweden are seen as small. It is of relevance to national security that the vulnerability in the critical technical infrastructures is kept to a minimum and that new vulnerabilities are not built in to the systems.

Keywords

Information technology, IT-related threats, Information operations, Information warfare, Terrorism, Cyber terrorism

Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** p. 42
	Price acc. to pricelist

SAMMANFATTNING

Begreppet ”cyberterrorism” har förekommit frekvent i medierna och har även i ökande omfattning nämnts i forskningssammanhang. Det är svårt att få en klar bild av vad begreppet står för då det har getts en rad olika betydelser. Denna begreppsmässiga förvirring i kombination med den entusiasm med vilken ordet har använts, kan till viss del förklara de skillnader i allvarlighetsgrad hotet tillskrivits.

I föreliggande rapport har ambitionen varit att föra en grundlig definitionsdiskussion för att utröna vad begreppet cyberterrorism betecknar. Först efter detta, när den definition som kommer att användas i rapporten är vald, förs en diskussion om cyberterrorism som potentiellt hot. *Syftet med rapporten har sålunda varit att klargöra vad cyberterrorism är samt att utröna huruvida ett sådant hot föreligger mot vårt samhälle eller har potential att utvecklas på sikt.*

Den definition av cyberterrorism som föreslås och används i rapporten lyder:

> Cyberterrorism är politiskt betingade angrepp utförda med hjälp av datorer och telekommunikation, riktade mot teknisk infrastruktur, som resulterar i våld mot för samhället kritiska funktioner, i syfte att påverka samhället eller ett lands politik utan hänsyn till om oskyldiga drabbas.

Cyberterrorism konstateras vara en typ av informationsoperation. När cyberterrorism inträffar under kris eller krig är det en form av informationskrigföring.

Vi vet att IT idag är ett viktigt verktyg för kommunikation inom terroristnätverk, inte minst för internationellt etablerade organisationer. Det som är av intresse för rapporten är om IT även kan användas som vapen i genomförandet av terroristangrepp. Vi har idag inte sett några exempel på genomförd cyberterrorism. Trots detta är det uppenbart att IT öppnar nya möjligheter till att åsamka samhället skada.

Argument som talar för användandet av IT som vapen är bland annat dess omfattande räckvidd som innebär att angriparen kan befinna sig på stort avstånd från måltavlan.

För den angripne är dessutom skyddet av kritiska system förenat med stora kostnader och svårigheter. Något som däremot kan tala mot framväxt av renodlad cyberterrorism är svårigheterna att framgångsrikt angripa kritisk infrastruktur med IT-medel. Dessutom är det i många fall tekniskt enklare att genomföra angrepp med konventionella vapen.

Störst potential för cyberterrorism ser vi som ett medel att förstärka våld och fördröja samhällets återhämtning efter ett angrepp. Det är idag svårt att se hur IT skulle kunna generera tillräckligt våld för att användas som ensamt vapen vid terroristangrepp. Ett argument som stärker detta är svårigheterna att vid IT-angrepp orsaka direkt våld mot människor. Om en konventionell terroristattack kombineras med IT-angrepp mot kritisk infrastruktur, till exempel för kommunikation, el- och vattenförsörjning, kan detta öka den fysiska skadan och lidandet för de angripna och samtidigt kraftigt fördröja samhällets återhämtning.

För att IT skall kunna användas som verkningsfullt medel för terrorister krävs teknisk kompetens och kännedom om de system som skall angripas. I rapporten nämns tre scenarier för hur kompetensuppbyggnaden kan ske. Befintliga grupper kan tillägna sig ny kunskap. De kan också tänkas ta in expertis utifrån. Ett tredje alternativ är att helt nya grupper växer fram. Huruvida potentiella terrorister är under utbildning eller om tillräcklig kapacitet finns samlad hos en aktör redan idag, vet vi inte.

När det gäller den svenska hotbilden bedöms risken för terrorism över huvud taget som liten. Denna bild kan dock snabbt förändras. Politiska faktorer som bedöms kunna påverka detta är bland andra ett svenskt deltagande i internationella operationer och ställningstagande i den internationella kampen mot terrorismen. Den geografiska obundenhet som är en egenskap hos cyberterrorismen, och IT-hot i allmänhet, gör den till ett lämpligt vapen mot länder som betraktas som fiender.

En utveckling mot en tydlig gemensam utrikespolitik inom EU skulle också kunna påverka Sverige genom att vi får del av andra länders säkerhetsproblematik. Som en

del av en kollektiv utrikespolitik och som potentiell deltagare i gemensamma militära insatser utanför unionens gränser, kan det inte uteslutas att andra EU-länders säkerhetsproblematik kan innebära ett ökat hot mot Sverige. En stark union med en tydlig gemensam utrikespolitik kan dessutom i sig uppfattas som ett provocerande koncentrat av politisk, ekonomisk och militär makt på det sätt USA ofta uppfattas idag.

Ett viktigt inslag i bedömningen av hotbilden är den tekniska infrastrukturens sårbarhet för attacker. För att göra en bedömning av denna skulle en grundlig analys av den svenska infrastrukturen behöva göras. Det finns en stark koppling mellan den nationella säkerheten och IT-säkerheten i de kritiska infrastrukturerna. De tekniska styr- och reglersystem som tas fram och används för drift av de olika infrastrukturerna beställs, tillverkas och drivs i stor utsträckning av privat sektor. Det är av säkerhetspolitisk betydelse att dessa från början får en inbyggd säkerhet, eftersom det är både komplicerat och dyrt att säkra system i efterhand.

1 BAKGRUND

Cyberterrorism är ett begrepp som använts flitigt av media och forskningsrelaterade organisationer den senaste tiden, starkt aktualiserat av de diskussioner om framtida hot och risker som följt i spåren av terroristattackerna mot USA den 11 september 2001.[1] Åsikterna om cyberterrorismens betydelse som hot mot samhället går dock vitt isär. Ett typiskt exempel på hur begreppet tolkas stod att läsa i Aftonbladet den 12 oktober 2001:

> ”Ett knapptryck räcker! En cyberterrorist kan sitta var som helst på jorden och med ett tryck på tangentbordet slå ut hela samhällen i andra delar av världen”.[2]

Artikeln innehåller emellertid ingen beskrivning av hur detta tekniskt skulle möjliggöras eller vilka intressen som skulle kunna ligga bakom. Å andra sidan finns det de som anser att cyberterrorism är en ren överdrift och en hotbild skapad ur starka intressen. Att cyberterrorism utmålas som ett stort hot sägs gynna försvarssektorn som söker nya hotbilder för att berättiga sin existens och dimensionering samt de företag inom näringslivet som utvecklar säkerhetslösningar för datasystem.[3]

Det är dock långt ifrån säkert att de som i olika sammanhang har beskrivit cyberterrorism låter ordet beteckna samma typ av företeelse, vilket till viss del kan förklara skillnader i den allvarlighetsgrad hotet tillskrivs. Ordet definieras sällan och verkar antas ha en vedertagen eller intuitiv betydelse.

Vi har konstaterat att en systematisk och analytisk genomgång av begreppet och vad det skulle kunna innebära saknas. Definitionsdebatten kring IT-hotets olika aspekter har redan pågått under flera år och det är tveksamt om ett nytt begrepp bidrar till ökad

---

[1] Begreppet har bland annat diskuterats på den ledande konferensen på området, InfowarCon, 2001 och 2002. Se www.infowarcon.com .

[2] Sture Olsson, ”Cyberterrorister – nästa stora hot”, Aftonbladet, 12 oktober 2001.

[3] The Ottawa Citizen, Cyber News, *Hacktivism is OK, Professor says: Cyberterrorism Fears Overblown, Expert tells Ottawa Conference*, 29 mars 2001.

klarhet. Om cyberterrorism används som benämning på företeelser som redan har ett annat namn bidrar inte begreppet till ökad förståelse eller kunskap om IT-hot. Den enda grunden för att använda ordet ”cyberterrorism” vore att det faktiskt betecknar något nytt och specifikt.

1.1 Motiv till rapporten

Rapporten är skriven inom ramen för det av Försvarsdepartementet beställda projektet ”Säkerhet i nätverkssamhället” (SINS). Ett brett fokus är anlagt i projektet för att förse beställaren med aktuellt underlag i IT-relaterade policyfrågor. Syftet med projektet är att fånga upp aktuella trender och större händelser som har eller kan komma att få säkerhetspolitisk bäring samt att analysera dessa.

Cyberterrorism är ett begrepp som används i USA men som nu även börjar vinna mark i Sverige. Vi anser att det är av största vikt att analysera begreppets konceptuella innebörd och hur detta fenomen kan yttra sig. För att kunna bedöma hotets betydelse måste enighet råda om begreppets innebörd. Motivet till studien är sålunda att ge en avvägd bild av vad cyberterrorism innebär och i vilken utsträckning det kräver särskilda åtgärder.

1.2 Syfte och frågeställningar

Syftet med rapporten är att klargöra vad cyberterrorism är, samt att utröna huruvida ett sådant hot föreligger mot vårt samhälle eller har potential att utvecklas på sikt. Rapporten omfattar såväl en analys av begreppet som en diskussion kring hur cyberterrorism skulle kunna växa fram i praktiken. Frågor som behandlas i rapporten är hur en definition skulle kunna se ut och vad som talar för respektive mot terroristers användande av IT vid genomförandet av terroristangrepp. Vi berör också vad som kan åstadkommas med IT som vapen och hur den potentielle aktören skulle kunna tillägna sig adekvat kompetens för cyberterrorism.

1.3 Metod och material

Rapporten utgör en kvalitativ analys av cyberterrorism. Materialet till rapporten är huvudsakligen skriftligt, i form av artiklar och rapporter samt material från Internet. Även om media har bevakats så är merparten av materialet hämtad från källor som bedöms ha auktoritet på området, såsom försvarsrelaterade myndigheter och forskningsorganisationer. Eftersom begreppet ursprungligen kommer från USA och det också är där diskussionen förts längst, är det naturligt att merparten av källorna är amerikanska. För den tekniska bedömningen av hotets karaktär har vi genomfört intervjuer med forskare från institutionen för Systemanalys och IT-säkerhet, FOI.

1.4 Läsanvisningar

I **kapitel 2** föreslår vi hur en definition av cyberterrorism skulle kunna se ut. Resonemanget bygger på en diskussion om innebörden av såväl ”cyber” som ”terrorism”. En definitionsdiskussion är, förutom en nödvändig förutsättning för tolkning av fenomenets förekomst i samtid, första steget i ett resonemang om dess framtid. Den föreslagna definitionen av cyberterrorism är utgångspunkt för rapporten. I kapitlet relaterar vi även begreppet till andra näraliggande begrepp då detta är av relevans för förståelsen.

I **kapitel 3** analyserar vi den tekniska utvecklingens möjligheter och begränsningar för cyberterrorism. Informationstekniken har i grunden förändrat vårt sätt att kommunicera – så även för terrorister. Frågan är om informationsteknik också kan användas som faktiskt medel vid utförandet av terroristangrepp och vad som i så fall kan åstadkommas. Om mer konventionella vapen som bomber ger avsedd verkan, varför skulle då terrorister välja att använda IT? Finns det fördelar med cyberterrorism i jämförelse med konventionell terrorism? I kapitlet diskuteras IT som ensamt vapen och IT i kombination med konventionella vapen.

Kapitel 4 handlar om aktören. För att cyberterrorism ska utgöra ett hot måste det förutom en teknisk möjlighet och en samhällelig sårbarhet även finnas individer med

drivkraft att använda sig av tekniken i utförandet av terroristangrepp. Därför är aktören central. På grund av den starka koppling till terrorism som ligger i begreppet är det rimligt att ponera att eventuella framtida aktörer eller aktörstyper kommer att vara besläktade med befintliga terroristgrupper eller med en utveckling av dessa. I kapitlet diskuterar vi tre utvecklingsscenarier för hur aktör och kompetens skulle kunna mötas.

I **kapitel 5** diskuteras huruvida cyberterrorism kan utgöra ett hot mot Sverige. Det hot cyberterrorism skulle kunna utgöra mot det svenska samhället är avhängigt möjligheter det rent tekniskt finns att skada eller allvarligt störa samhället med IT-vapen. Skyddet av kritiska infrastrukturer är därför avgörande för vår sårbarhet för IT-angrepp och sålunda för cyberterrorism. Eventuella angripare kan, på grund av informationsteknikens gränsöverskridande karaktär, vara baserade såväl inom Sverige som i vilket annat land som helst. Risken för angrepp är emellertid relaterad till den generella hotbild som finns mot Sverige och inte enbart till de tekniska möjligheterna.

2 BEGREPPET CYBERTERRORISM

Begreppet cyberterrorism har sitt ursprung i USA. Det myntades 1982 av Barry Collin, Institute for Security and Intelligence i Kalifornien, och betecknade en förening mellan cybernetik[4] och terrorism.[5] I praktiken innebär detta en sammansmältning av terrorism och användning av datorer och telekommunikation. Denna tidiga definition ger dock ingen beskrivning av hur cyberterrorism faktiskt skulle manifestera sig utan pekar endast på cyberspace[6] som ny arena för terrorister. Mest frekvent används begreppet cyberterrorism i ursprungslandet USA.

Som nämns i inledningen definieras cyberterrorism sällan, utan verkar antas ha en vedertagen betydelse. Eftersom begreppet har börjat användas innan det har tillskrivits en faktisk innebörd är det svårt att kritiskt granska begreppet. Begreppet cyberterrorism förekommer idag, trots bristande definitionsgrund, i en mängd olika fora, i såväl officiella dokument, media som forskningsrapporter. En genomgång av tillgängligt material ger en bild av ett omoget begrepp som ges flera olika betydelser – många talar om det, långt ifrån alla är överens om vad det är.

2.1 Rapportens definition av cyberterrorism

För att cyberterrorism som begrepp ska ha någon egentlig innebörd måste vi kunna skilja det från andra typer av missbruk av datorer som till exempel databrottslighet, ekonomiskt spionage eller informationskrigföring. Vi måste också kunna skilja det från andra typer av terrorism. Utifrån de definitioner av cyberterrorism vi tagit del av[7]

---

[4] Cybernetik är föregångare till det som idag kallas artificiell intelligens. Källa: Begreppet ”cybernetik” i Nationalencyklopedin, http://www.ne.se/jsp/search/article.jsp?i_art_id=148888 (30 september 2002).

[5] William L. Tafoya, 2002, Cyberterrorism: Is Your IT Safe?”, sid. 12, http://www.itforum2002.com/repositories/files/Bill%20Tafoya%Presentation.pdf (8 oktober 2002).

[6] Se avsnitt 2.2 för definition av begreppen ”cyber” och ”cyberspace”.

[7] Den definition av cyberterrorism som vi anser ligga närmast vårt resonemang är NIPC:s definition: *”Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a*

och det resonemang vi för, kommer följande definition av cyberterrorism att användas i föreliggande rapport:

> Cyberterrorism är politiskt betingade angrepp utförda med hjälp av datorer och telekommunikation, riktade mot teknisk infrastruktur, som resulterar i våld mot för samhället kritiska funktioner, i syfte att påverka samhället eller ett lands politik utan hänsyn till om oskyldiga drabbas.

I detta kapitel kommer vi att redogöra för hur vi har tagit fram rapportens definition av cyberterrorism. Detta gör vi genom att relatera begreppet till definitioner av begreppen ”cyber” och ”terrorism”. Vidare kommer vi att motivera definitionens olika kriterier och kommentera begreppets förhållande till de centrala begreppen informationsoperationer och informationskrigföring.

2.2 Definition av ”cyber”

Termen cybernetik, föregångaren till det som idag kallas artificiell intelligens, kan härledas till 1948 och den amerikanske matematikern Norbert Wiener.[8] Begreppet cyberspace myntades 1984 av författaren William Gibson i hans science fictionroman Neuromancer. Cyberspace definieras på svenska som det ”konstgjorda, datorskapade rummet eller det elektroniska universum, som man befinner sig i när man kommunicerar via dator”.[9] Det kan också beskrivas som en icke-fysisk terräng bestående av datorsystem. Onlinesystem skapar ett cyberspace, i vilket människor till exempel kan kommunicera eller söka information. Till skillnad från den fysiska världen, kräver inte utforskning av cyberspace någon fysisk aktivitet, förutom tryckandet på knappar eller flyttandet av en datormus.[10] ”Cyber” är på så sätt ett prefix

---

particular political, social or ideological agenda”. Källa: Linda Garrison och Martin Grand (red.), ”Cyberterrorism: An Evolving Concept” NIPC Highlights, sid.1, nr. 06-01, 15 juni 2001, National Infrastructure Protection Center, Analysis and Information Sharing Unit.

[8] Begreppet “cybernetik” i Nationalencyklopedin, http://www.ne.se/jsp/search/article.jsp?i_art_id=148885, 2002-10-28

[9] Begreppet ”cyberspace” i IT-ordlistan, 2001.

[10] Se ”Webopedia”, http://aol.pcwebopedia.com/TERM/c/cyberspace.html (10 oktober 2002).

använt i ord som betecknar företeelser i cyberspace. I praktiken förutsätter ”cyber” en användning av IT-relaterade medel såsom datorteknik och telekommunikation.

2.3 Definition av ”terrorism”

Eftersom cyberterrorism är sammansatt av begreppen ”cyber” och ”terrorism” är det i sammanhanget relevant att fundera på vad som vanligen betecknar terrorism. Definitionerna av terrorism är många och vi har inte ambitionen att skapa ordning bland dessa. För att visa på denna definitionssvårighet går Alex Schmid i boken ”Political Terrorism” igenom etthundra definitioner av terrorism. Han drar slutsatsen att ”terrorism” är ett abstrakt begrepp utan egentlig kärna och att en ensam definition inte kan täcka alla de betydelser ordet kan ges.[11]

Även om det långt ifrån råder konsensus om hur terrorism ska definieras, eller kanske just därför, är det viktigt att slå fast vilken definition vi kommer att utgå ifrån i den här rapporten. Nationalencyklopedins definition är kortfattad och tydlig och därför en bra utgångspunkt för vår definitionsdiskussion:

> Våldshandlingar som är politiskt betingade och syftar till att påverka samhället eller ett lands politik utan hänsyn till om oskyldiga drabbas.[12]

Begreppet ”politiskt betingade” anser vi även omfatta religiöst motiverat våld, då detta också syftar till att styra eller påverka utvecklingen i samhället.

2.4 Beståndsdelarna i definitionen av cyberterrorism

Med utgångspunkt i begreppen ”cyber” och ”terrorism”, kommer vi att redogöra för de resonemang som ligger bakom rapportens definition av cyberterrorism. Vi kommer att

---

[11] Alex Schmid och Albert J. Jongman, 1988, ”Political terrorism”.

[12] Begreppet ”terrorism” i Nationalencyklopedin, www.ne.se/jsp/search/article.jsp?i_art_id=326201, (30 september 2002).

utgå ifrån definitionens olika komponenter: medel, måltavla, våldsrekvisit och motiv. Vi kommer även att kommentera aktören.

2.4.1 Medel

Sammankopplingen av ”cyber” och ”terrorism” i begreppet cyberterrorism antyder att cyberrelaterade medel är ett nytt vapen i terroristens arsenal. En intuitiv tolkning av cyberterrorism borde därför vara att det betecknar terrorism där attacker genomförs med hjälp av IT-relaterade medel. Exempel på så kallade IT-relaterade medel är virus, trojaner, logiska bomber och distribuerade överbelastningsattacker.

Konventionella terroristattacker mot kritisk infrastruktur kan självfallet påverka denna allvarligt men är inte cyberterrorism. Detta då angreppet inte utnyttjar datorteknik eller telekommunikation och sålunda inte kan betraktas som en företeelse i cyberspace. Användningen av IT som vapen är det som motiverar prefixet ”cyber” i cyberterrorism. Av den anledningen innehåller rapportens definition kravet på att cyberterrorism är ”angrepp utförda med hjälp av datorer och telekommunikation”.

2.4.2 Måltavla

Den direkta måltavlan för cyberterrorism är datorer eller datarelaterad utrustning. Måltavlan kan vara såväl mjuk- och hårdvara som nätverk och information. Användandet av IT-vapen implicerar att även måltavlan måste vara IT-relaterad för att vara åtkomlig för angrepp. Utifrån detta har måltavlan i definitionen specificerats till ”teknisk infrastruktur”.

2.4.3 Våldsrekvisit

För att ett angrepp skall klassificeras som terrorism kräver definitionen att det är en ”våldshandling”[13]. I rapportens definition av cyberterrorism innebär våld att ett

[13] Se definition under 2.3.

angrepp ”resulterar i våld mot för samhället kritiska funktioner”. Effekten av ett angrepp brukar inte anges i definitioner av terrorism men sett till vapnets karaktär finner vi det vara en rimlig tolkning att ett elektroniskt angrepp kan anses vara en ”våldshandling” om effekten är våld. Cyberterrorism skulle kunna innebära direkt åverkan på datorrelaterad utrustning och indirekt våld mot människor. En vidare diskussion om våld och cyberterrorism förs i kapitel 3.

2.4.4 Motiv

Motivet i definitionen, att handlingarna är ”politiskt betingade” och syftar till ”att påverka samhället eller ett lands politik utan hänsyn till om oskyldiga drabbas”, är hämtat från definitionen av terrorism[14]. Att skapa rädsla och kaos och därigenom påverka en regering att genomföra politiska, sociala eller ideologiska förändringar är en motivbeskrivning som är central för begreppet terrorism.

Att motivet för terrorism är uppfyllt är viktigt. Om tankarna förs till hackare eller organiserade brottslingar, som kan skapa stora störningar men som saknar terroristens motiv, riskeras en urvattning av terrorismbegreppet. Stöld av information, intrång i datorer och nätverk samt distribuerade överbelastningsattacker är kriminella handlingar men dessa kan inte sägas vara exempel på terrorism. Skillnaden mellan cyberterrorism och kriminellt användande av datorer är densamma som skillnaden mellan konventionell terrorism och kriminalitet, det vill säga det bakomliggande motivet.

2.4.5 Aktör

I definitionen av cyberterrorism specificeras inte vem som är aktören eftersom det finns både nationell terrorism, internationell terrorism och statsterrorism[15]. Terrorism

---

[14] Se definition under 2.3.

[15] Begreppet ”terrorism” i Nationalencyklopedin, www.ne.se/jsp/search/article.jsp?i_art_id=326201, (30 september 2002).

kan således utföras av både individer, icke-statliga organisationer och stater. Därmed finns det ingen anledning att omnämna aktörstyper i definitionen.

2.6 En typ av informationsoperation

När vi nu har formulerat rapportens definition av cyberterrorism är det viktigt att sätta denna i sitt begreppsliga sammanhang. Informationsoperationer och informationskrigföring är idag vedertagna begrepp och det är av vikt att nya begrepp ställs i relation till dessa. I den år 2001 publicerade rapporten från Sårbarhets- och säkerhetsutredningen definieras informationsoperationer som det:

> ”övergripande begreppet, omfattande samlade och samordnade åtgärder i fred, kris och krig till stöd för ekonomiska, politiska eller militära mål i syfte att påverka eller utnyttja en motståndares eller annan aktörs information och informationssystem och samtidigt skydda egen information och egna informationssystem”.[16]

Informationskrigföring beskrivs av Försvarsmakten som:

> ”informationsoperation som genomförs under kris och krig för att främja eller uppnå särskilda politiska eller militära mål gentemot en eller flera motståndare”.[17]

Informationsoperationer är enligt ovanstående definitioner det överordnade begreppet. Informationsoperationer och informationskrigföring skiljs i definitionerna åt genom att informationsoperationer är det samlade begreppet för operationer över hela spektrumet fred – kris – krig, medan informationskrigföring är begränsat till kris och krig, det vill säga dessa operationer är del av krigföring. Denna skillnad är dock svår att se när det gäller terrorism. Det finns ingen anledning att tro att inte cyberterrorism skulle kunna förekomma över hela spannet fred, kris och krig.

---

[16] SOU 2001:41,” Säkerhet i en ny tid”, Sårbarhets- och säkerhetsutredningen, sid. 189.

[17] Försvarsmakten, *Nomen FM*, november 1999, remissutgåva.

Detta innebär att cyberterrorism är en typ av informationsoperation och att cyberterrorism som utförs under kris och krig är en typ av informationskrigföring.

3 ÖPPNAR IT NYA MÖJLIGHETER FÖR TERRORISM?

3.1 Teknisk utveckling

Det vi vet om terroristers användning av IT idag är att informationstekniken är ett viktigt verktyg för kommunikation inom terroristnätverk, inte minst för de organisationer som är internationellt etablerade. Ett exempel på detta är al-Qaidas förmodade användning av Internet för att försöka omgruppera sig under 2002 efter USA:s omfattande strider mot organisationen i Afghanistan.[18]

För att skapa publicitet och sprida propaganda är IT ett viktigt verktyg. I kombination med andra medier kan information snabbt, effektivt och utan större kostnad spridas till en stor mängd människor över hela världen och där avsändaren har direkt kontroll över budskapet. Därför kan IT förväntas vara ett passande instrument för informationsspridning även för terrorister.[19] Det kan konstateras att beroendet av den informationstekniska infrastrukturen för kommunikation och styrning gäller terrorister såväl som andra grupper i samhället.

Det finns i diskussioner om cyberterrorism en benägenhet att klassificera all IT-relaterad verksamhet som utförs av terrorister som cyberterrorism. Tillskrivs begreppet cyberterrorism en sådan vidd, förlorar ”terrorism” i sammanhanget sin betydelse. Att skicka e-post, köpa flygbiljetter eller hyra bilar över Internet är i sig lagligt oavsett vem som gör det.

Det som är intressant från vår utgångspunkt är om informationstekniken kan användas som ett vapen för terrorism. Vi har idag inte sett några exempel på genomförd cyberterrorism och inte heller funnit ett enda exempel på faktisk cyberterrorism i tillgängligt material. Däremot finns det ett antal exempel på elektroniska angrepp som

[18] James Risen och David Johnston, “Intercepted Al Qaeda E-Mail Is Said to Hint at Regrouping”, The New York Times, www.nytimes.com, 6 mars 2002.

har tolkats som *försök* till cyberterrorism[20]. Gemensamt för alla dessa exempel är emellertid att de inte har lyckats. Trots bristen på faktiska exempel på cyberterrorism som uppfyller rapportens definition, är det uppenbart att informationstekniken öppnar nya möjligheter för att åsamka samhället skada.

I följande kapitel kommer vi därför att diskutera vad som talar för respektive emot användande av IT-relaterade vapen i syfte att utöva terrorism och vad som skulle kunna åstadkommas genom cyberterrorism.

3.1.1 Relativa fördelar med cyberterrorism

Det finns flera egenskaper hos informationstekniken som skulle kunna tala för en ökad användning i just terrorismsyfte. Argument som ofta förs fram är att det är kostsamt att skydda nätverk samtidigt som attacker mot desamma är förhållandevis billiga att genomföra.[21] Anskaffandet av den utrustning som en potentiell cyberterrorist behöver ha tillgång till kräver mindre ekonomiska resurser än anskaffandet av konventionella vapen. Utrustningen är vidare lätt att smuggla och angrepp är ofta mycket svåra att spåra. Måltavlor för attack kan sökas och studeras på Internet för att identifiera och kartlägga svaga punkter.[22]

En fördel med användningen av IT som vapen för terrorister är även att attacker kan genomföras på mycket stort avstånd från måltavlan. Möjligheten att befinna sig långt från måltavlan i kombination med svårigheten att spåra och upptäcka angriparen,

---

[19] Michele Zanini och Sean J. A. Edwards, "The Networking of Terror in the Information Age", i John Arquilla och David Ronfeldt, 2001,"Networks and Netwars: The Future of Terror, Crime and Militancy", sid. 41.

[20] Ett exempel på detta är de allvarliga angrepp mot elkraftförsörjningen i Kalifornien som genomfördes 25 april - 11 maj 2001. Enligt FBI var angriparna inte långt ifrån att lyckas kontrollera distributionen av elkraft efter att ha kartlagt sårbarheter i systemet i syfte att identifiera dess mest kritiska komponenter. Inledningsvis ansågs angreppen ha kinesiskt ursprung men detta har inte kunnat bekräftas. Källa: Delete, nyhetsbrev från Försvarshögskolan, nr. 12, 2001.

[21] Se t.ex. Yael Shahar, "Information Warfare: The Perfect Terrorist Weapon", The International Policy Institute for Counter-Terrorism, 26 februari 1997.

[22] Andrew Koch, Space Imaging gets .5m Go Ahead, Jane´s Defence Weekly, 10 januari 2001.

minskar drastiskt det personliga risktagandet för angriparen i jämförelse med konventionell terrorism. Användning av elektroniska medel för att slå ut ett mål innebär dessutom att förövaren inte behöver hantera explosiva vapen.[23] Med ett lägre risktagande och därmed en lägre tröskel för medverkan, skulle nya aktörer kunna attraheras att utföra dåd och rekryteringsbasen därmed potentiellt kunna breddas för terroristorganisationer.

3.1.2 Relativa nackdelar med cyberterrorism

Terrorister har konstaterats vara operationellt konservativa i sitt val av metoder.[24] För att säkra en terroroperations framgång är det mindre riskabelt att använda sig av väl beprövade metoder än att prioritera ett nydanande i angreppssättet.[25] Detta, i kombination med att anammandet av tekniken kan innebära kostnader och risker innan önskad effekt uppnås, innebär att ny teknik har svårt att få ett omedelbart genomslag. Risker med IT-användning i dessa sammanhang kan bland annat vara att nya verktyg för attacker blir verkningslösa på kort tid så snart de blivit kända eller sårbarheten upptäckts.[26]

Terrorister som vill öka sin offensiva förmåga till informationsoperationer måste kontinuerligt hålla sig uppdaterade om nya tekniker och inte minst de säkerhetslösningar som finns tillgängliga hos såväl systemadministratörer som brottsbekämpande myndigheter. Detta innebär osäkerhet för operationer som planeras över lång tid. Kampen om vem som är bäst uppdaterad och utrustad skulle dessutom

---

[23] Michele Zanini och Sean J. A. Edwards, "The Networking of Terror in the Information Age", i John Arquilla och David Ronfeldt, 2001, "Networks and Netwars: The Future of Terror, Crime and Militancy", sid. 45.

[24] Bruce Hoffman, "Terrorism, Trends and Prospects" i Lesser, et al., "Countering the New Terrorism", sid. 39.

[25] Dorothy E. Denning, "Cyberterrorism", Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 23 maj 2000; Hoffman, Roy och Benjamin, 2000, "America and the New Terrorism: An Exchange".

[26] Caroline Benner, "The Phantom Cyber-threat", Salon, 4 april 2001.

kräva kontinuerligt arbete och uppmärksamhet och ta resurser från kanske redan ansträngda organisationer.[27]

Många tekniska system är komplexa vilket kan innebära svårigheter att över huvudtaget attackera exempelvis kritisk infrastruktur på ett framgångsrikt sätt.[28] I de flesta tänkbara scenarier är en terroristattack tekniskt enklare att genomföra och effekten säkrare, om angreppet utförs konventionellt istället för elektroniskt. Det är exempelvis lättare att avlägsna en meter järnvägsräls, vilket skulle få ödesdigra konsekvenser, än det är att elektroniskt påverka tågens system för styrning.[29] Det kan vidare vara svårare än vid en konventionell attack att kontrollera effekterna för att garantera att tillräcklig skadenivå uppnås.[30] Datorangrepp är till exempel bara effektiva en kort tid eftersom brister i system kan rättas till när de har identifierats.[31]

Med ökad kompetens och erfarenhet torde problemen för terrorister att framgångsrikt angripa kritisk infrastruktur kunna minska. På samma sätt kan risktagandet förknippat med att utnyttja ny teknik utgöra en övergående svårighet för dem.

3.2 Vad som kan åstadkommas med cyberterrorism

Utvecklingen av informationstekniken öppnar för nya angreppsmetoder. Kan man med

---

[27] Martin Libicki, James Mulvenon och Zalmay Khalilzad, opublicerad RAND-forskning, citerad i John Arquilla och David Ronfeldt, 2001, ”Networks and Netwars: The Future of Terror, Crime and Militancy”, sid. 46.

[28] T.ex. Svenska Kraftnät använder för driftsövervakning och styrning av sina nät ett helt separat system som de bedömer måste angripas fysiskt för att man ska kunna åstadkomma skada på det. Slutna system torde utgöra, om än inte oöverstigliga, problem för cyberterrorister som söker påverka med hjälp av IT-medel. Se Josefin Grennert, ”En strategisk allians?: Förutsättningar för samarbete mellan privat och offentlig sektor för hantering av IT-hot”, sid. 18-25 för utvalda infrastrukturers säkerhetssituation.

[29] Intervju med David Lindahl, Arne Vidström och Mikael Wedlin, FOI, Linköping, 6 maj 2002.

[30] Dorothy E. Denning, “Cyberterrorism”, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 23 maj 2000.

[31] Intervju med David Lindahl, Arne Vidström och Mikael Wedlin, FOI, Linköping, 6 maj 2002.

IT-relaterade medel uppnå samma effekter som med konventionella vapen? Resultatet av ett terroristangrepp behöver inte nödvändigtvis vara permanent fysisk förstörelse utan man kan föreställa sig att cyberterrorism tar sig andra uttryck.

3.2.1 Som ensamt vapen

Enligt rapportens definition skall cyberterrorism resultera i ”våld mot för samhället kritiska funktioner”. Angrepp kan riktas mot samhällets kritiska infrastruktur, till exempel el-, tele- och vattensystem. Sett till systemens komplexitet är det sannolikt att ett angrepp föregås av en omfattande kartläggning av de tekniska systemen och kritiska noderna. Om angreppen riktas samtidigt mot ett flertal kritiska infrastrukturer kan man föreställa sig att detta medför allvarliga konsekvenser för samhället. Cyberterrorism tycks sålunda kunna ge upphov till våld mot kritiska funktioner.

Det har dock diskuterats huruvida en aktör med hjälp av IT kan orsaka avbrott i den tekniska infrastrukturen som kan innebära fara för människoliv.[32] Om detta är möjligt är det sannolikt att denna typ av terrorism skulle få psykologiska effekter liknande de som uppstår i samband med konventionella terroristdåd. Idag är det dock inte tekniskt möjligt att enbart genom IT-angrepp förmå exempelvis flygplan att störta, tåg att krocka eller Internet att helt stängas av.[33] För att IT-angrepp skulle kunna leda till fara för människoliv skulle det krävas att flera kritiska funktioner angreps och slogs ut samtidigt. Störningarna skulle också behöva pågå under en längre tid och eventuella dödsfall skulle inte vara en direkt konsekvens av IT-angreppet utan en sekundäreffekt som konsekvens av störningar i de angripna funktionerna.[34] Enligt detta resonemang ter sig inte *direkt* våld mot människor vara möjligt att uppnå med cyberterrorism.

---

[32] Michele Zanini och Sean J. A. Edwards, ”The Networking of Terror in the Information Age”, sid. 45, samt intervju med David Lindahl, Arne Vidström och Mikael Wedlin, FOI, Linköping, 6 maj 2002.

[33] Intervju med David Lindahl, Arne Vidström och Mikael Wedlin, FOI, Linköping, 6 maj 2002.

[34] Ibid.

3.2.2 I kombination med konventionella vapen

För terrorister kan det finnas fördelar med att utnyttja informationsteknik som del av ett större angrepp med inslag av både konventionell terrorism och cyberterrorism. IT-angrepp skulle då användas som ett verkningsfullt komplement till konventionell terrorism. Exempel på en sådan kombinationsattack kan vara att kommunikationsinfrastrukturen angrips i samband med en konventionell attack, till exempel ett omfattande bombdåd. Ett stort antal datorer kan i förväg infekteras för att vid en given tidpunkt gång på gång ringa upp larmnummer och på så sätt slå ut larmvägarna. Det skulle dock inte vara möjligt att slå ut alla media samtidigt. Det hade till exempel inte varit möjligt att hindra all kommunikation på Manhattan den 11 september 2001.[35]

Om en konventionell terroristattack kombineras med IT-angrepp mot kritisk infrastruktur, till exempel för kommunikation, el- och vattenförsörjning, kan detta öka både den fysiska skadan och lidandet för de angripna och dessutom kraftigt fördröja samhällets återhämtning. Störst potential för cyberterrorism ser vi därför som ett medel att förstärka våld. Mest sannolikt tycks det oss att cyberterrorism inlemmas som ett komplement i terroristers vapenarsenal eftersom cyberterrorism inte kan ge upphov till direkt våld mot människor såsom konventionell terrorism.

[35] Ibid.

4 POTENTIELLA CYBERTERRORISTER

Huruvida det idag finns aktörer med både kapaciteten och motivet att utöva cyberterrorism är svårt att svara på. Kraven på utbildning för att hantera den nya tekniken kan eventuellt förklara varför ingen omfattande cyberterrorism ännu har förekommit. Det utesluter dock inte att potentiella terrorister är under utbildning eller att kapaciteten och motivet finns samlade hos en aktör redan idag.

Framväxten av cyberterrorister kan tänkas ske på olika sätt. Existerande terroristgrupperingar kan tillägna sig ny kunskap eller ta in expertis utifrån. En tredje möjlighet är att helt nya typer av grupper växer fram.

4.1 Terrorister som skaffar sig ny kompetens

Cyberterrorister skulle kunna utvecklas genom att befintliga terroristgrupper skaffar sig ny kompetens och kapacitet för IT-angrepp. Det finns en möjlighet att nu befintliga terroristgrupper skulle påbörja, eller kanske redan har påbörjat, kunskapsuppbyggnad för cyberterrorism.

I och med attentaten mot USA den 11 september 2001 har verksamma terrorister bevisat att de är fullt kapabla att genomföra mycket avancerade terroristoperationer ifråga om långsiktig planering och utbildning.[36] Attackerna med hjälp av kapade flygplan krävde att medlemmar av terroristnätverket genomgick flygutbildning inför uppdragen. Med en sådan kapacitet för komplexa operationer ter det sig givet att samma organisation, eller liknande grupper, skulle vara förmögen att lägga ner samma möda på att tillskansa sig IT-kompetens och planera cyberattacker om terroristerna önskade utnyttja informationsteknik i kommande operationer.

[36] Magnus Norell, 2001, ”Terrorns anatomi” i ”Snabbstudie av terrorattacken mot WTC/Pentagon 11 september 2001 och dess konsekvenser”, sid. 6.

4.2 Befintliga grupper som får extern hjälp

En annan möjlighet är att ta in utomstående expertis men detta skulle utsätta ett terroristnätverk för säkerhetsrisker. En väg till ökad förmåga som nämnts är att de ökade kontakterna mellan terroristnätverk och organiserad brottslighet kan förse de förstnämnda med ny teknisk kompetens[37].

4.3 Nya typer av grupper

Ett tredje utvecklingsscenario är framväxten av nya grupper som påskyndar utvecklingen mot utnyttjande av IT för angrepp. Den tekniska kompetensen skulle då vara central i organisationen som till och med skulle kunna ses som ett slags ”joint venture” mellan hackare och terrorister. Zanini och Edwards beskriver en sådan hybridgrupps verksamhet:

> ”Like hackers they would undertake most of their attacks in cyberspace. Like terrorists, they would seek to strike targets by both disruptive and destructive means to further a political or religious agenda”.[38]

Hybridgrupper som kombinerar terroristens drivkrafter med hackarens teknikkunskap har potentialen att bli mycket verkningsfulla i cyberterrorismsammanhang. Det som sannolikt ska till för att cyberterrorism ska bli ett utbrett hot är framväxten av en ny generations terrorister för vilka användandet av datorer ter sig naturligt.

---

[37] CSIS, *Terrorism*, Global Organized Crime Project, Task Force Activity, Center for Strategic and International Studies, www.csis.org/goc/taskterr.html.

[38] Michele Zanini och Sean J. A. Edwards, “The Networking of Terror in the Information Age”, sid. 51.

5 CYBERTERRORISM – ETT HOT MOT SVERIGE?

5.1 Den svenska hotbilden

I Försvarsmaktens strategiska omvärldsbedömande för 2001-2006 bedöms terroristhotet mot Sverige som ytterst litet. Samtidigt konstateras det att denna hotbild snabbt kan förändras.[39]

En sådan förändring skulle kunna komma till stånd genom att Sverige exempelvis fortsätter eller ökar sitt deltagande i internationella operationer i utlandet. Deltagande i internationell krishantering kan öka risken för Sverige att bli måltavla för terroristhot eftersom Sverige blir en aktör i konfliktområdet. Om Sverige uppfattas som fiende öppnar elektroniska attacker nya möjligheter för angrepp över stora geografiska avstånd. En aktör skulle kunna angripa det svenska samhället utan att fysiskt behöva befinna sig inom rikets gränser eller ha tillgång till lika stora resurser som konventionella angrepp skulle kräva.

Under de närmaste åren ser Försvarsmakten en möjlighet att Sverige kan komma att göra insatser till stöd för den internationella bekämpning av terrorism som USA initierat.[40] Ett svenskt samarbete med USA eller andra länder vars politik och agerande uppfattas som ytterst provocerande i vissa delar av världen, kan också komma att öka hotbilden mot Sverige. Sverige blir i ett sådant samarbete en part i konflikten mellan i första hand USA och terroristorganisationer i världen. Genom en sådan exponering kan hotet mot Sverige förhöjas.

Om EU:s utrikespolitiska samarbete utvecklas mot en mer sammanhållen och gemensam utrikespolitik för hela unionen kan även detta komma att påverka Sveriges hotbild. Sverige har exempelvis inga spända relationer till forna kolonier såsom flera västeuropeiska stater har. Som en del av en kollektiv utrikespolitik och potentiell

[39] Försvarsmaktens strategiska omvärldsbedömande 2001-2006, sid. 4.

[40] Ibid, sid. 2 och 15.

deltagare i gemensamma militära insatser utanför unionens gränser, kan det inte uteslutas att andra EU-länders säkerhetsproblematik kan innebära en ökad hotbild för Sverige. En stark union med en tydlig gemensam utrikespolitik kan dessutom i sig uppfattas som ett provocerande koncentrat av politisk, ekonomisk och militär makt på det sätt USA ofta uppfattas idag.

För både inhemska och globala intresseorganisationer och nätverk som inte är främmande för att använda sig av våld, kan cyberterrorism vara ett kraftfullt vapen. Det elektroniska angreppet innebär inte bara att angriparna kan befinna sig långt ifrån måltavlan utan också att angrepp kan samordnas mellan olika individer eller grupper som befinner sig långt ifrån varandra. Tröskeln kan dessutom vara lägre för att använda cyberterrorism än för konventionell terrorism med till exempel sprängladdningar.

5.2 Svensk sårbarhet för cyberterrorism

Hoten mot IT-system bedöms öka under de närmaste åren och samhällets växande beroende av informationsinfrastrukturen gör gränsdragningen mellan säkerhetspolitik och IT-säkerhetsfrågor allt svårare.[41] Som konstaterats i en FOI-rapport från 2001, öppnar användningen av informationsteknik möjligheter för fler aktörer med mindre resurser att genomföra angrepp över stora avstånd vilket breddar aktörsbilden.[42]

Idag kan möjligheterna att utföra cyberterrorism i Sverige dock anses som små. Detta beror på att denna typ av angrepp kräver stora resurser och att sårbarheten för riktigt allvarliga elektroniska angrepp mot den kritiska infrastrukturen kan anses som låg. Det är emellertid systemdesignen som är avgörande. Om ett säkerhetstänkande finns med från början då system utvecklas kan ett starkt skydd uppnås. En oroande utveckling är dock att det finns indikationer på att nya system som byggs standardiseras för att styras

[41] Ibid, sid. 2.

[42] Josefin Grennert & Magdalena Tham, 2001, ”Att påverka konflikter med IT-vapen. Icke-statliga aktörers möjligheter till inverkan på konfliktförlopp”, FOI-R—0263—SE.

via Internet. Detta för att möjliggöra för personal att gå in och sköta underhåll även på stort fysiskt avstånd från installationerna. Risken är att kraven på tillgänglighet på sikt skapar en sårbarhet för cyberterrorism. [43]

Även om möjligheterna för cyberterrorism mot Sverige idag är ringa, är det viktigt att påpeka att detta gäller terroristdåd. Andra typer av IT-hot är fortfarande högst aktuella och kan bland annat orsaka omfattande ekonomiska skador för privatpersoner och företag, utan att det för den skull kan benämnas som cyberterrorism.

Vi kan konstatera att en detaljerad analys av den svenska hotbilden för cyberterrorism kräver en noggrann kartläggning av den tekniska infrastrukturen och inte minst de sekundära effekter som en attack mot den skulle kunna orsaka i samhället. Utveckling av å ena sidan vapenteknik på IT-sidan och å andra sidan säkerhetslösningar för att stävja dessa, kommer att påverka framväxten av cyberterrorism. Det bildliga nät som säkerhetslösningar utgör kan sannolikt hindra de extraordinära effekter som terroristen eftersträvar. Det potentiella hotet från cyberterrorism liksom hoten från organiserad brottslighet och hacking, måste dock finnas i åtanke när datorsystem för den kritiska infrastrukturen konstrueras och utvecklas.

[43] Intervju med David Lindahl, Arne Vidström och Mikael Wedlin, FOI, Linköping, 6 maj 2002.

6 AVSLUTANDE RESONEMANG

Som de resonemang som förs i texten anger, är det en mängd kriterier som ska vara uppfyllda för att cyberterrorism som sådan ska kunna utgöra ett egentligt hot. Enkelt uttryckt måste kapacitet hos en aktör med ett visst motiv, sammanfalla med en sårbarhet hos måltavlan. Saknas någon komponent, sårbarheten hos måltavlan, kapaciteten eller motivet hos aktören, finns inget aktuellt hot.

Cyberterrorism utgör sålunda ett starkt villkorat hot som inte är omedelbart utan snarare en potentiell del av en framtida verklighet. För att förhindra framväxten av cyberterrorism måste vi redan idag arbeta för att säkra våra samhällsnödvändiga system. Det faktum att känsliga system i stor utsträckning inte är uppkopplade mot Internet idag, försvårar för cyberterroristen.

Det är oerhört viktigt för framtiden att inte ökad sårbarhet för elektroniska angrepp skapas i nya tekniska system. Det främsta sättet att förhindra framväxten av cyberterrorism är att agera proaktivt och att tänka långsiktigt vad gäller säkerhet i kritiska system. Staten måste också beakta länken mellan IT-säkerhet och säkerhetspolitik. Sammanlänkningen av system och de potentiella sårbarheterna i den kritiska infrastrukturen innebär att den nationella säkerheten även är beroende av privat ägda system. IT-säkerheten är sålunda inte en fråga enbart för systemägaren.

En invändning mot IT som medel i terroristaktioner är bristen på direkt våld mot människor, i synnerhet i ljuset av den rådande utvecklingen i världen mot allt blodigare terrorism. Det senaste decenniet har antalet terroristdåd minskat i jämförelse med 1980-talet men antalet offer har samtidigt ökat. Terrorismen har således utvecklats mot ett alltmer dödligt våld.[44] Ett eventuellt IT-angrepp mot teknisk infrastruktur kan inte vara dödligt i sig. Möjligen kan konsekvenserna av det, i ett andra steg, innebära fara för människoliv. Detta är en viktig skillnad då det vid IT-

[44] Magnus Norell, 2001, ”Terrorns anatomi” i ”Snabbstudie av terrorattacken mot WTC/Pentagon 11 september 2001 och dess konsekvenser”, sid. 6.

angrepp, mot till exempel en blodbank, ges utrymme att avvärja angreppet efter det att det är avfyrat. Denna möjlighet finns inte på samma sätt när exempelvis en bomb redan detonerat. För att man i realtid skall kunna avvärja ett IT-angrepp krävs givetvis mänsklig eller teknisk kontroll och säkerhetsrutiner.

Det är teoretiskt möjligt att IT-angrepp i framtiden skulle kunna innebära direkt våld mot människor men detta är avhängigt dels en teknisk utveckling där fler kritiska system styrs utan mänsklig kontroll, dels att dessa byggs utan backup-möjligheter eller andra tekniska säkerhetslösningar. Om människor inte allvarligt skadas eller dödas genom cyberterrorism blir dramatiken och den känslomässiga effekten på samhället betydligt mindre än vid konventionella dåd.[45] Cyberterrorism kan tänkas ha svårt att konkurrera med konventionella terroristangrepp eftersom det hittills har varit det grova våldet och de mänskliga offren som gett terrorism så stort utrymme i massmedia och genomslag i samhället. Denna bristande psykologiska effekt på offer och omvärld talar emot en omfattande användning av informationstekniken i syfte att sprida skräck och förvirring i ett angripet samhälle.

En relevant fråga för framtida studier är dock huruvida det kan vara en fördel med attacker med stora känningar för samhället fast med liten eller ingen fysisk skada av människor. Blodiga attacker riskerar att väcka avsky snarare än beundran hos människor som kanske i stort delar terroristernas övergripande målsättning som till exempel självständighet. Cyberterrorism skulle på så sätt kunna innebära att grupper kan få genomslag utan att förlora stöd för sin sak i de egna kretsarna.[46] Det kan inte uteslutas att nya grupper växer fram som följer en annan strategi och använder andra metoder än de terroristgrupper som är kända idag. Grupper som använder sig av mindre våldsamma metoder för påtryckning skulle, på grund av en lägre tröskel för deltagande eller sympatier, potentiellt kunna rekrytera ett större antal anhängare.

---

[45] Dorothy E. Denning, "Cyberterrorism", Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 23 maj 2000.

[46] Michele Zanini och Sean J. A. Edwards, "The Networking of Terror in the Information Age", sid. 45.

Mest sannolikt i framtiden är, enligt vår uppfattning, cyberterrorism som förstärkning av våld. Terrorister som använder sig av informationsteknik kan öka angreppens effektivitet och genomslag i samhället. Att kombinera konventionell terrorism med cyberterrorism skulle vara i linje med strategin att slå mot människan där hon känner sig som säkrast. På så sätt orsakar terroristangreppet störst förvirring och trauma, något som bland annat utnyttjats av självmordsbombare[47]. Terroristgruppers anskaffande av offensiv förmåga till informationsoperationer är i det ljuset ett potentiellt stort hot mot det moderna samhället.[48]

[47] Yael Shahar, "Information Warfare: The Perfect Terrorist Weapon", The International Policy Institute for Counter-Terrorism, 26 februari 1997.

[48] John Arquilla och David Ronfeldt, "Cyberwar is Coming", Comparative Strategy, vol. 12, nr. 2 Summer 1993, sid. 141-165.

LITTERATURFÖRTECKNING

Arquilla, John och David, F. Ronfeldt, 1993, *Cyberwar is coming*, Comparative Strategy, Vol. 12, nr. 2, Summer 1993.

Arquilla, John och Ronfeldt, David, 2001, *Networks and Netwars: The Future of Terror, Crime and Militancy*, RAND 2001.

Benner, Caroline, *The Phantom Cyber-Threat*, Salon, www.salon.com , 4 april 2001.

CSIS, *Terrorism*, Global Organized Crime Project, Task Force Activity, Center for Strategic and International Studies, www.csis.org/goc/taskterr.html

Delete, nyhetsbrev från Försvarshögskolan, nr. 12, 2001.

Denning, E. Dorothy, *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, 23 maj 2000.

Försvarsmakten, *Försvarsmaktens strategiska omvärldsbedömande 2001-2006*, 2002.

Försvarsmakten, *Nomen FM*, november 1999, remissutgåva.

Garrison, Linda and Grand, Martin (red.), *Cyberterrorism: An Evolving Concept*, NIPC Highlights, nr. 06-01, 15 juni 2001, www.nipc.gov.

Grennert, Josefin, 2001, *En strategisk allians? Förutsättningar för samarbete mellan privat och offentlig sektor för hantering av IT-hot*, FOI-R—0076—SE.

Grennert, Josefin och Tham, Magdalena, 2001, *Att påverka konflikter med IT-vapen. Icke-statliga aktörers möjligheter till inverkan på konfliktförlopp*, FOI-R—0263—SE.

Hoffman, Bruce; Roy, Olivier och Benjamin, Daniel, 2000, *America and the New Terrorism: An Exchange*, Survival, Vol. 42, nr. 2, Summer 2000.

Hoffman, Bruce, *Terrorism, Trends and Prospects*, i Lesser, Ian O.; Hoffman, Bruce; Arquilla, John, Ronfeldt, David Zanini, Michele och Jenkins, Brian, 1999, *Countering the New Terrorism*, Santa Monica, Calif.: RAND, MR-989-AF.

Koch, Andrew, 2001, *Space Imaging Gets .5m Go Ahead*, Jane's Defence Weekly, 10 januari 2001.

Norell, Magnus, 2001, *Terrorns anatomi* i *Snabbstudie av terrorattacken mot WTC/Pentagon 11 september 2001 och dess konsekvenser*, FOI Memo 01-3102.

Olsson, Sture, *Cyberterrorister – nästa stora hot*, Aftonbladet, 12 oktober 2001.

The Ottawa Citizen, Cyber News, *Hacktivism is OK, Professor says: Cyberterrorism Fears Overblown, Expert tells Ottawa Conference*, 29 mars 2001.

Risen, James och Johnston, David, *Intercepted Al Qaeda E-mail is said to hint at Regrouping,* The New York Times, www.nytimes.com, 6 mars 2002.

Schmid, Alex och Jongman, J. Albert, 1988, *Political Terrorism*, Rev. Edition, Transaction Publishers.

Shahar, Yael, *Information Warfare: The Perfect Terrorist Weapon*, The International Institute for Counter-Terrorism, 26 februari 1997, www.ict.org.il/articles/infowar.htm.

Tafoya, William L., 2002, Cyberterrorism: Is Your IT Safe?", sid. 12, http://www.itforum2002.com/repositories/files/Bill%20Tafoya%Presentation.pdf.

Zanini, Michele och Edwards, J. A., *The Networking of Terror in the Information Age*, i Arquilla, John och Ronfeldt, David, (eds.), 2001, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND

Offentligt tryck

SOU 2001:41, *Säkerhet i en ny tid*, Sårbarhets- och säkerhetsutredningen.

Uppslagsverk

IT-ordlistan, STF Ingenjörsutbildning AB, 2001.
Nationalencyklopedin online, 2002.
Webopedia, http://aol.pcwebopedia.com

Webbresurser

Center for Strategic and International Studies	www.csis.org
InfowarCon	www.infowarcon.com
IT Forum 2002	www.itforum2002.com
Nationalencyklopedin	www.ne.se
National Infrastructure Protection Center	www.nipc.gov
New York Times	www.nytimes.com
Salon	www.salon.com
Webopedia	http://aol.pcwebopedia.com

Intervjuer

David Lindahl, Arne Widström och Mikael Wedlin, Institutionen för Systemanalys och IT-säkerhet, Totalförsvarets forskningsinstitut (FOI), Linköping, 6 maj 2002.

AKRONYMLISTA

CSIS	Center for Strategic and International Studies
EU	Europeiska unionen
FBI	Federal Bureau of Investigation
IT	Informationsteknik
NIPC	National Infrastructure Protection Center