FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--0263--SE
december 2001
ISSN 1650-1942
Användarrapport

Josefin Grennert och Magdalena Tham

Att påverka konflikter med IT-vapen

Icke-statliga aktörers möjligheter till inverkan på konfliktförlopp

Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Försvarsanalys
172 90 Stockholm

FOI-R--0263--SE
December 2001
ISSN 1650-1942
Användarrapport

Josefin Grennert och Magdalena Tham

Att påverka konflikter med IT-vapen

Ickestatliga aktörers möjligheter till inverkan på konfliktförlopp

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI Försvarsanalys 172 90 Stockholm	FOI-R--0263--SE	Användarrapport
	Forskningsområde 1. Försvar- och säkerhetspolitik	
	Månad, år december 2001	**Projektnummer** A1154
	Verksamhetsgren 1. Forskning för regeringens behov	
	Delområde 11 Försvarsforskning för regeringens behov	
Författare/redaktör Josefin Grennert Magdalena Tham	**Projektledare** Josefin Grennert	
	Godkänd av Jan-Erik Svensson	
	Tekniskt och/eller vetenskapligt ansvarig	

Rapportens titel

Att påverka konflikter med IT-vapen: Icke-statliga aktörers möjligheter till inverkan på konfliktförlopp

Sammanfattning (högst 200 ord)

I rapporten analyseras icke-statliga aktörers utnyttjande av informationsteknik under pågående konflikt, i vilken minst en part är en stat. Huvudfrågan som ställs i rapporten är: Vilka säkerhetspolitiska konsekvenser kan det få för förloppet i en konflikt där minst en stat är inblandad, att andra aktörer än stater på eget bevåg lägger sig i storpolitiska skeenden med hjälp av informationsteknologi?

Tidigare studier visar att konventionella konflikter i allt större utsträckning följs av cyberattacker. Anhängare till parterna i en konflikt kan vilja visa sitt stöd och gör det med de medel de har tillgång till. Hittills har cyberattacker mest utgjort ett irritationsmoment och även om stora värden, i termer av pengar och arbete, har krävts så har ingen människa varit allvarligt hotad. Det finns dock en potential för att dessa attacker skall bli långt mer förödande till exempel om de samordnas och riktas mot länders kritiska infrastruktur. På sikt kan IT-angrepp även påverka staters förmåga att hantera sin säkerhetspolitik.

I rapporten presenteras och analyseras ett flertal exempel på politiskt motiverade systemintrång där icke-statliga aktörers aktioner med hjälp av IT, löper parallellt med statligt agerande i en konflikt. Det mest aktuella exemplet är den ökade cyberaktivitet som följde direkt på terrorattentaten mot USA i september 2001. Andra fall som studeras är Kina och USA under spionplansincidenten 2001, Israel och Palestina under intifadan 2000-2001 samt NATO-länderna och Serbien under Kosovo-konflikten 1999.

Nyckelord

IT-hot, konflikter, hacktivism, cyberterrorism

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 47
Distribution enligt missiv	**Pris: Enligt prislista** **Sekretess**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	FOI-R--0263--SE	User report
	Research area code 1. Defence and Security Policy	
	Month year December 2001	**Project no.** A1154
	Customers code 1. Research for the Government	
	Sub area code 11 Defence Research for the Government	

Author/s (editor/s)	Project manager
Josefin Grennert Magdalena Tham	Josefin Grennert
	Approved by Jan-Erik Svensson
	Scientifically and technically responsible

Report title (In translation)

Influencing conflicts with IT-weapons: The possibility of non-state actors influencing the course of a conflict

Abstract (not more than 200 words)

In this report the use of information technology by non-state actors during an on-going conflict in which at least one part is a state, is analysed. The main question posed is: What security policy related consequenses on the course of a conflict in which at least one part is a state, can follow if other actors than states, on their own initiative, interfere in high politics situations by using information technology?

Recent research show that conventional conflicts increasingly are followed by cyber attacks. Adherents of the parties in a conflict may want to show support and do so by using the means available to them. Up to date, cyber attacks have in large been a source of irritation and even if the cost has been high, in terms of money and work, human lives have never been in danger. However, if attacks are coordinated and directed at critical infrastructures there is a potential for them to become far more devastating. In the long run IT-attacks may even have an influence on a state´s ability to deal with security policy.

In the report a number of examples of politically motivated system break-ins are presented, in which non-state actors use IT-weapons, in parallel to state actions in conflicts. One recent example is the increasing cyber activity that followed on the terrorist attack against the U.S. in September 2001. Other studied cases are China and USA during the spy plane incident 2001, Israel and Palestine during 2000-2001 and the NATO-countries and Serbia during the Kosovo conflict in 1999.

Keywords

IT-threats, conflicts, hacktivism, cyber terrorism

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 47
	Price acc. to pricelist
	Security classification

FÖRORD

Totalförsvarets forskningsinstitut bedriver studier om IT-hot ur ett nationellt och internationellt säkerhetsperspektiv. Föreliggande rapport är producerad inom ramen för projektet "Säkerhet i nätverkssamhället", SINS, som startades år 2000.

Tidigare rapporter som producerats inom projektet har fokuserat på staten som policyskapare och central aktör för hanteringen av IT-relaterade hot och näringslivet som primus motor för teknikutvecklingen. Under de senaste åren har icke-statliga aktörers användning av IT i politiskt syfte ökat. Konventionella konflikter följs i allt större utsträckning av cyberattacker utförda av icke-statliga aktörer.

Aktörsutvecklingen motiverar studiet av angreppens förekomst i samband med konflikter och de konsekvenser angreppen kan få för ett konfliktförlopp. IT-angrepp utförda av icke-statliga aktörer är ett inslag i konflikter som statliga beslutsfattare måste räkna med.

Eva Mittermaier, FOI, har granskat rapporten vid ett särskilt granskningsseminarium.

Stockholm i december 2001
Josefin Grennert

SAMMANFATTNING

Med en intrikat informationsinfrastruktur där flera av våra samhällsnödvändiga funktioner är elektroniskt styrda och där systemen dessutom i stor utsträckning hänger samman, följer naturligt att vi är mer sårbara för angrepp med elektroniska medel. Den globala spridningen av informationsteknik innebär att en potentiell antagonist inte fysiskt behöver vara i målets närområde. Teknikens ökade tillgänglighet innebär också att allt fler aktörer med skiftande syften har möjlighet att använda sig av IT som vapen.

I rapporten analyseras icke-statliga aktörers utnyttjande av informationsteknik under pågående konflikt, i vilken minst en part är en stat. Huvudfrågan som ställs i rapporten är: Vilka säkerhetspolitiska konsekvenser kan det få för förloppet i en konflikt där minst en stat är inblandad, att andra aktörer än stater på eget bevåg lägger sig i storpolitiska skeenden med hjälp av informationsteknik?

Hittills har cyberattacker mest utgjort ett irritationsmoment och även om stora värden, i termer av pengar och arbete, har krävts så har ingen människa varit allvarligt hotad. Det finns dock en potential för att dessa attacker skall bli långt mer förödande till exempel om de samordnas och riktas mot länders kritiska infrastruktur. En framgångsrik elektronisk attack skulle exempelvis kunna orsaka avbrott i vatten- och elförsörjningen, störa flygledningsfunktioner eller orsaka ekonomiskt kaos genom att hindra ekonomiska transaktioner.

I rapporten studeras ett flertal exempel på politiskt motiverade systemintrång där icke-statliga aktörers aktioner med hjälp av IT löper parallellt med statligt agerande i en konflikt. Det mest aktuella exemplet är den ökade cyberaktivitet som följde direkt på terrorattentaten mot USA i september 2001. Vidare studeras Kina och USA under spionplansincidenten 2001, Israel och Palestina under intifadan 2000-2001 samt NATO-länderna och Serbien under Kosovo-konflikten 1999.

Det faktum att icke-statliga aktörer agerar under konflikt kan på sikt utmana den monopolställning som staten har haft som säkerhetslokus och ensam auktoritet vad gäller underrättelseinhämtning, policyskapande och implementerande av politiska beslut. Det skall dock noteras att de icke-statliga aktörer som avses, IT-aktörer, resursmässigt är underlägsna, och beroende av, staten.

1 IT SOM VAPEN

1.1 Det sårbara informationssamhället

Allt fler funktioner i samhället blir datoriserade. I takt med ökade krav på snabbt tillgänglig information har den tekniska utvecklingen bidragit till användarvänlig och billig teknik. Därigenom blir de positiva effekterna av informationsrevolutionen kännbara på alla nivåer i samhället – för såväl myndigheter och företag som privatpersoner. Ökad tillgänglighet till information är tveklöst en av de positiva effekter som IT[1] har bidragit till. Både möjligheten att ta del av information och att sprida sina åsikter är en viktig del av det demokratiska samhället, vilken nu underlättas genom ökad användning av IT.

Genomslaget av IT har varit mest påtagligt i västvärlden där teknikutvecklingen har varit som snabbast. För mindre tekniskt utvecklade länder kan IT vara ett sätt att komma ikapp med relativt sett mindre resurser än vad som skulle krävas för att få de gamla systemen att fungera. I vissa länder kan det till och med vara lättare att kommunicera med hjälp av ny teknik som exempelvis e-post, jämfört med telefon.[2]

Att samhällets ökade användning och beroende av IT även har skapat nya typer av sårbarheter är ingen nyhet.[3] Med en intrikat informationsinfrastruktur där flera av våra samhällsnödvändiga funktioner är datakontrollerade och där systemen dessutom i stor utsträckning hänger samman, följer naturligt att vi är mer sårbara för angrepp med elektroniska medel. En framgångsrik logisk attack skulle till exempel kunna orsaka avbrott i elförsörjningen, störa flygledningsfunktioner eller orsaka ekonomiskt kaos genom att hindra ekonomiska transaktioner. Skulle kritiska datornätverk slås ut får ansvariga myndigheter svårt att upprätthålla sin verksamhet. Avsaknaden av fungerande datornätverk skulle kunna förhindra eller försvåra genomförandet av uppgifter genom till exempel avbrott i kommunikation och informationsöverföring

[1] IT står för "informationsteknik". I rapporten kommer genomgående förkortningen att användas.
[2] Ambassadör J. Stapleton Roy, Charles Smith och John A. Wiant, "Bits, Bytes and Cyber-Diplomacy". Framförande på konferensen Infowar Con 2001, Washington D.C., 6 september 2001.

mellan myndigheter. Om flera kritiska funktioner drabbas samtidigt blir verkningarna naturligtvis än mer kännbara än om systemen störs vid olika tillfällen.

Det är idag ett välkänt faktum att den globala spridningen av tekniken innebär att en potentiell antagonist inte fysiskt behöver vara i målets närområde. Ett angrepp kan komma från en annan del av världen likväl som från byggnaden bredvid. Tillgängligheten till den teknik som krävs för att genomföra angrepp bidrar till att allt fler aktörer med skiftande syften har tillgång till den.

Det förefaller svårt, för att inte säga omöjligt, att under en längre tid kontrollera en stat enbart genom elektronisk manipulering av dess infrastruktur. Det hot som IT-vapen[4] utgör ligger inte heller häri utan snarare i det att tekniken ger en god möjlighet att störa ett land och göra det mer känsligt för ett konventionellt anfall. Under en pågående konflikt, då läget mellan parterna är extra sårbart, kan ett IT-angrepp sålunda få ökad genomslagskraft.

1.2 Användning av IT under konflikt

Omedelbart efter terrorattacken mot USA i september 2001 började det spridas rykten på Internet om vedergällning från pro-amerikanska hackare. Vissa attacker har genomförts, bland annat mot muslimska webbsidor, även om man inte har kunnat tala om en samlad nätattack. Pro-muslimska hackare har vedergällt de amerikanska attackerna.[5]

Det är således inte enbart stater som har möjlighet att agera i konfliktsituationer. Andra, icke-statliga aktörer kan utnyttja det sårbara läge parterna i en konflikt befinner sig i. Tidigare studier visar att konventionella konflikter i allt större utsträckning följs

[3] DS 2001:14, "Gränslösa sårbarheter – gemensam säkerhet", sid. 113; SOU 2001:41, "Säkerhet i en ny tid", Sårbarhets- och säkerhetsutredningen, sid. 187.
[4] Med IT-vapen avses i rapporten informationstekniska medel då de används i syfte att åsamka skada.
[5] Se avsnitt 2.1.

av cyberattacker.[6] Anhängare till parterna i en konflikt kan vilja visa sitt stöd och gör det med de medel de har tillgång till. Detta har vi sett flera exempel på efter terrorattackerna mot USA i september 2001 men även tidigare, under andra konflikter.[7] Hittills har cyberattacker mest utgjort ett irritationsmoment och även om stora värden, i termer av pengar och arbete, har krävts så har ingen människa varit allvarligt hotad. Det finns dock en potential för att dessa attacker skall bli långt mer förödande till exempel om de samordnas och riktas mot länders kritiska infrastruktur.[8]

I rapporten analyseras icke-statliga gruppers utnyttjande av informationsteknik under pågående konflikt, i vilken minst en part är en stat. Huvudfrågan som ställs i rapporten är: Vilka säkerhetspolitiska konsekvenser kan det få för förloppet i en konflikt där minst en stat är inblandad, att andra aktörer än stater på eget bevåg lägger sig i storpolitiska skeenden med hjälp av informationsteknik? Rapporten kommer däremot inte att analysera initierandet av konflikt med hjälp av IT-vapen eller staters officiella användning av dessa i en konfliktsituation.

I kapitel två presenteras fyra exempel på konflikter där icke-statliga aktörer har använt IT för att påverka konfliktförloppet. Motiven som kan ligga bakom IT-angrepp och aktörernas politiska insikt diskuteras i kapitel tre. I kapitel fyra förs ett teoretiskt resonemang om vilka de säkerhetspolitiska konsekvenserna kan bli för staten i fråga om autonomi och handlingsutrymme. I det avslutande kapitlet sammanfattas de trender som identifieras i rapporten och en potentiell utveckling av dessa diskuteras. Rapporten avslutas med förslag på hanteringsåtgärder.

De källor som använts är alla av öppen karaktär. Det är värt att notera att ytterligare material om incidenterna kan finnas i hemlig form. Andra källor, till exempel från andra länder än de vi använt finns sannolikt också att tillgå om man vill gräva ännu djupare i de presenterade incidenterna.

---

[6] Michael A. Vatis, 2001, "Cyber Attacks During the War on Terrorism: A Predictive Analysis", The Institute for Security Technology Studies at Dartmouth College.
[7] Se kapitel 2.
[8] Michael A. Vatis, "Cyber Attacks During the War on Terrorism: A Predictive Analysis", passim.

1.3 Användning av IT-vapen i politiskt syfte

Under slutet av 90-talet ökade användningen av IT i politiskt syfte markant. Den första mer datoriserade aktivismen ägde rum i mitten av 1980-talet då bland annat fredsaktivister utnyttjade den nya tekniken för att kommunicera över nationsgränserna. Nästa steg som följde var en intensifierad kommunikation som syftade till att ge upphov till faktiskt politiskt agerande och inte bara till informationsutbyte. De former av nätaktivism som dominerar är elektronisk civil olydnad, som lånat taktik och terminologi från traditionell civil olydnad, och politiserad hacking. Elektronisk civil olydnad sker främst i form av massaktioner som organiseras av nätverk och organisationer som sällan är anonyma. De politiserade hackarna agerar däremot oftare individuellt, vanligtvis under pseudonymer och ibland olagligt.[9]

Medan aktivisterna bakom elektronisk civil olydnad har sin bakgrund i politiska rörelser har de politiserade hackarna sin bakgrund i hacking. Båda fenomenen brukar betecknas som "hacktivism". Som benämningen ger vid handen avses en sammansmältning av politisk aktivism med hacking[10]. Hacktivism är hacking med politiska syften där budskapet är det viktiga snarare än teknikanvändningen i sig. IT ses i sammanhanget som ett verktyg.[11] Utvecklingen är sannolikt en logisk följd av den nya teknikens tillgänglighet.

Ett exempel på en grupp som utnyttjat IT för att nå sitt mål är EZLN (Zapatista National Liberation Army) som via Internet har skapat ett informationsnätverk med över etthundra stödjande noder runt om i världen som länkar samman ytterligare individer. Nätverket möjliggör direkt kommunikation med omvärlden utan att informationen behöver passera media som potentiellt hindrar eller förvanskar

---

[9] Wray, Stefan. "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics", A paper for the World Wide Web and Contemporary Cultural Theory Conference, Drake University, november 1998; www.nyu.edu/projects/wray/wwwhack.html.

[10] Hacking står för operationer som på okonventionella och ofta illegala sätt inbegriper datorer, oftast med hjälp av mjukvara (Dorothy E. Denning, 2000, "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foregn Policy, sid. 12). Utförarna kommer vi i rapporten att benämna "hackare", vilket är en översättning av engelskans "hacker" som börjar få genomslag i Sverige.

[11] "The Golden Age of Hacktivism", www.wired.com, 22 september 1998.

budskapet.[12] IT ger sålunda en god möjlighet att föra fram ett budskap via icke-officiella kanaler och ändå få gehör i officiella sammanhang. Hackingincidenter rapporteras ofta i media vilket innebär att man lätt kan få uppmärksamhet såväl för vad man gjort som för varför. [13]

Även om de elektroniska attacker vi hittills har sett inte har varit av den allvarlighetsgraden att liv har hotats så kan hacktivism sägas utgöra ett hot mot utrikespolitiskt agerande och diplomatiska förhandlingar. Dorothy E. Denning, professor i datorvetenskap på Georgetown University, Washington D.C., USA, för resonemanget så långt som att hon hävdar att hacktivistattacker kan störa statens diplomatiska förehavanden. Detta skulle ske genom att ambassaders datorer saboteras eller genom att information, till exempel om förhandlingsstrategier, publiceras eller överlämnas till andra länder.[14]

En anledning till att diplomatiska förhandlingar kan störas av cyberattacker är att det kan vara svårt för motparten att avgöra vad som är sanktionerat av staten och vad som är attacker iscensatta av oberoende hackare. Det finns ingen öppen information som talar för att stater har utnyttjat hackare under konflikter även om det har funnits misstankar om att så har varit fallet.

Spridningen av tekniken medför att kriminella organisationer och extremiströrelser har tillgång till Internet som kommunikationsmedel.[15] Jeffrey A. Hunker, dekan vid Heinz School of Public Policy and Management, Carnegie Mellon University och före detta chef för skydd av kritisk infrastruktur vid National Security Council, menar att:

---

[12] Dorothy E. Denning, 2000, "Aktivism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", sid. 12.
[13] Ibid. sid. 11.
[14] Dorothy E. Denning, 2000, "Hacktivism: An Emerging Threat to Diplomacy", AFSA, American Foreign Service Association, sid. 1-2.
[15] Se t.ex. AgIW (numera AgIO), 1998, "Rapport nr. 2: Åtgärder och skydd mot informationskrigföring – förslag till ansvarsfördelning mm.", sid. 16 och Dorothy E. Denning, 2000, "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", sid. 6.

"...there are clearly transnational groups that are incredibly capable of executing sophisticated operations and are enormously creative and innovative. We are sitting on a cyber time bomb".[16]

Samma medel som används av hackare och numera även hacktivister kan potentiellt komma att utnyttjas även av terrorister. Det finns idag terroristgrupper som har tillgång till IT.[17] Mark Pollitt, FBI, USA, beskriver cyberterrorism som:
"the premeditated, politically motivated attack against information, computer systems, computer programs and data, wich result in violence against noncombatant targets by subnational groups or clandestine agents".[18]

Det som skiljer det vi ser exempel på idag, hacktivism, från cyberterrorism är densamma som mellan aktivism och terrorism. Det som kan komma att förena dem är att de verktyg som hacktivister använder och som terrorister förutspås använda i framtiden, är hård- och mjukvara och att attackerna riktas mot datornätverk och elektronisk infrastruktur. Genom att sätta ordet "cyber" framför "terrorism" har man skapat ett begrepp som innebär uppfyllandet av samma mål men med andra medel.[19]

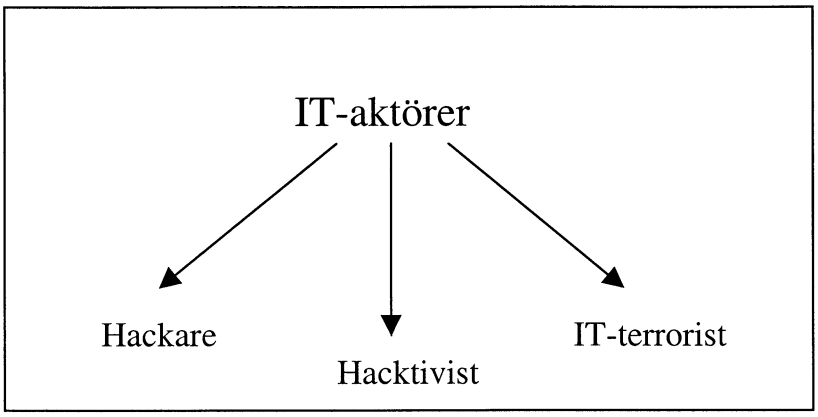
Aktörsdefinitioner som används i rapporten:

- IT-aktör – agerar med hjälp av IT (övergripande begrepp)
- Hackare – gör olovliga datorintrång
- Hacktivist – hackar i politiskt syfte
- IT-terrorist (cyberterrorist) – utövar terrorism med hjälp av IT

Begreppens inbördes relation framgår av figur 1.

---

[16] Jeffrey A. Hunker, i John Schwartz, "USA: Avoiding a Digital Pearl Harbour", The New York Times News Service, 4 oktober 2001.
[17] Clark L. Staten, "Testimony before the Subcommittee on Technology, Terrorism and Government Information: Foreign Terrorism in the United States: Five Years After the Word Trade Center", U.S. Senate Judiciary Committee, 24 februari 1998.
[18] Mark M. Pollitt, "Cyberterrorism – Fact or Fancy?". Proceedings of the 20th National Information Systems Security Conference, oktober 1997, sid. 285-289.



Figur 1. Använda begrepps inbördes relation.

1.4 Urval av fall

Följderna av terrorattacken mot USA ges förhållandevis stort utrymme i analysen då händelsen har gett upphov till en konflikt som pågår i skrivande stund. Det finns dock andra fall vilka även de belyses. Det urval av fall som vi utgår ifrån grundar sig på kriterierna att det rör sig om politiskt motiverade systemintrång, att aktionerna tidsmässigt löper parallellt med statligt agerande i en konflikt där minst en av parterna utgörs av en stat och att aktionerna inte har uppgetts vara statligt sanktionerade.

De exempel som vi funnit uppfyller dessa krav och som vi kommer att använda för att stödja våra resonemang är:

- USA – Afghanistan under terroristbekämpningen 2001
- Kina – USA under spionplansincidenten 2001
- Israel – Palestina under intifadan 2000-2001
- NATO-länderna – Serbien under Kosovo-konflikten 1999

[19] Alex Turkington i Woo Siew Chin, "Malaysia: Insight into Cyberterrorism", New Straits Times, 3 oktober

2001.

2 HUR AGERAR HACKTIVISTER?

Logiska angrepp utförda av hacktivister som på olika sätt söker delta i eller påverka en konflikt- eller krissituation[20] har de senaste åren ökat i antal och omfång. Politiska motståndare har utpekas både inom och utom hacktivisternas ursprungsland. Attacker har även riktats mot den stat eller aktör hacktivisterna själva sympatiserar med i syfte att påverka dess agerande. Vi kommer här att redogöra för fyra exempel på hur icke-statliga aktörer med hjälp av informationsteknik har agerat under konflikter med minst en statlig part: USA och Afghanistan ifråga om skydd av terrorister 2001, Kina och USA under spionplansincidenten 2001, Israel och Palestina under intifadan 2000-2001 samt NATO-länderna och Serbien under Kosovo-kriget 1999.

2.1 USA och Afghanistan 2001

Med anledning av terrorattackerna mot USA den 11 september 2001 förväntades en våg av politiskt motiverade angrepp av individer och nätverk som i sympati med USA skulle attackera de aktörer eller stater de uppfattat som ansvariga för dåden. NIPC, det nationella centret för skydd av infrastruktur placerat inom FBI, uppmanade därför tidigt hacktivister att avstå från privata motangrepp eftersom detta skulle vara att göra USA en otjänst.[21] Under de första veckorna efter terrorangreppen, då USA avvaktade med öppna militära aktioner, genomfördes trots detta hundratals angrepp mot måltavlor i Mellanöstern.[22]

Under den tid som förflutit sedan USA i början av oktober 2001 inledde en väpnad konflikt med talibanregimen i Afghanistan, synes emellertid hacktivistangreppen ha avtagit. Detta skulle kunna förklaras antingen med att hacktivisternas mål var uppfyllt

---

[20] För begreppet *konflikt* har vi använt definitionen "upplevt skiljaktiga intressen, eller en uppfattning att parternas nuvarande aspirationer inte kan uppnås samtidigt" (Jeffrey Z. Rubin et al, 1994, *Social Conflict. Escalation, Stalemate and Settlement*); för begreppet *kris* har vi tillämpat de tre grundläggande kriterier som skall vara uppfyllda för att en kris skall råda: "viktiga värden står på spel, osäkerhet råder och tidspress föreligger" (M. Breacher och J. Willenfeldt, 1989, "*Crisis, Conflict and Instability*", sid. 5.)

[21] "FBI: Beware 'patriot' hackers", MSNBC, www.msnbc.com 18 september 2001.

[22] "Computer Pros Launch Hack Attack on Mideast", AntiOnline, www.antionline.com, 19 september 2001.

sedan USA intervenerat, eller att massmedias intresse för att rapportera hacktivistincidenter mattades av betydligt sedan konventionell krigföring inletts.

2.1.1 Angrepp mot webbplatser

Med hänvisning till att USA inte agerat tillräckligt kraftfullt gentemot terrorismen under dagarna som följde terrorattentaten, inledde grupper av hacktivister ett eget svar på aktionerna. I första hand initierade man angrepp mot webbplatser tillhörande regeringar och företag i Mellanöstern. Enligt uppgift rörde det sig om upp till 300 angripna webbplatser under de första dagarna. Innehåll förändrades på webbplatser bland annat tillhörande Irans inrikesdepartement, Irans största universitet och palestinska Internetoperatörer.[23]

Tre dagar efter terrorangreppen mot New York och Washington dirigerades trafiken till runt 10.000 webbplatser om så att besökarna istället möttes av en protest mot att utnyttja religion för att rättfärdiga våldshandlingar.[24] Gamla virus döptes om till namn med koppling till terroristangreppen[25] och nya virus och maskar distribuerades efter händelserna.[26]

Dagen efter attacken mot USA kungjorde Dispatchers, ett nätverk av omkring 300 hackare från ett femtontal länder, att de redan inlett nätverksoperationer mot Internetoperatörer och Internetinfrastruktur. De förvarnade också om att över 1000 datorer från vilka de kan utföra sina attacker, stod under deras kontroll.[27] Sedan misstankar riktats mot Usama bin Ladins organisation med bas i Afghanistan utsattes webbplatsen www.afghangovernment.org för massiva distribuerade överbelastnings-

---

[23] "Hackare attackerade offer istället för fiender", Computer Sweden, www.computersweden.se 18 september 2001.
[24] "Hackare på krigsstigen efter tisdagens terrordåd", Computer Sweden, www.computersweden.se, 17 september 2001.
[25] För exempel på maskar se t.ex. "Bin Ladin-mask siktar in sig på ICQ-användare", Computer Sweden, Computer Sweden, www.computersweden.se, oktober 2001; "Buggig mjältbrandsmask har svårt att föröka sig", Computer Sweden, www.computersweden.se, 18 oktober 2001.
[26] "Experts warn of more cyber attacks", MSNBC, www.msnbc.com, 27 september 2001.
[27] National Infrastructure Protection Center, "Potential Distributed Denial of Service (DDoS) Attacks", Advisory 01-021, NIPC, www.nipc.gov, 17 september 2001.

attacker[28], så kallade DDoS-attacker. Webbplatsen tillhör emellertid den regering som störtades 1996 och som förväxlats med talibanregimen.[29] Grannlandet Pakistans officiella webbplats utsattes också för DDoS-attacker.[30]

2.1.2 Angrepp mot infrastruktur

Hackare har hävdat att de på eget initiativ tömt bankkonton med kopplingar till Usama bin Ladin. De påstår sig även ha angripit telenät för att omöjliggöra kommunikation mellan Usama bin Ladin i Afghanistan och terrorister i andra delar av världen.[31]

2.1.3 Insamling av underrättelser

En brittisk hackargrupp kallad YIHAT[32] hävdar att de gjort elektroniska intrång i den sudanesiska banken AlShamal Islamic Bank. Via en säkerhetslucka i en brandvägg skulle gruppen ha tagit fram information om konton med koppling till den misstänkte terrorledaren Usama bin Ladin och hans organisation al-Qaida. Denna information sägs ha vidarebefordrats till FBI som varken bekräftar eller dementerar huruvida de tagit emot några sådana underrättelser.[33] Samma grupp uppger också att de tagit sig in i systemen hos Arab National Bank i Saudiarabien, men där inte funnit någon information om de misstänkta terroristerna.[34] Även pakistanska hacktivister har hävdat att de fått tillgång till konfidentiell information om USA som de skulle vidarebefordra till al-Qaida om inte USA uppfyllde vissa villkor. Kraven omfattade bland annat ett tillbakadragande av amerikanska trupper från Saudiarabien och ett slut på bombningarna av Afghanistan.[35]

---

[28] Distribuerade överbelastningsattacker, så kallade Denial of Service-attacker, syftar till att förhindra leverans av information. Detta kan ske till exempel genom att en webbplats överbelastas tills dess att datorn kraschar eller fungerar mycket långsamt. DDoS-attacker innebär ofta att en webbplats temporärt måste tas bort från Internet tills dess att angreppen upphört.

[29] "FBI: Beware 'patriot' hackers", MSNBC, www.msnbc.com, 18 september 2001.

[30] Anne Saita, "Hacktivists Eyeing U.S., Arab Cyberstrikes", Security Wire Digest, Vol. 3, No 71, 17 september 2001.

[31] Inlägg på MSNBC, www.msnbc.com, "Discussion Boards" i ämnet "Hacking the talibans' network", 1 oktober 2001.

[32] Young Intelligent Hackers Against Terror

[33] "Hackare är bin Laden på spåren", Computer Sweden, www.computersweden.se, 28 september 2001.

[34] "Hacking for the Cause", ABC News, www.abcnews.com, 15 oktober 2001.

[35] "Pakistani Hackers Deface U.S. Site with Ultimatum", AntiOnline, www.antionline.com, 18 oktober 2001.

2.2 Kina och USA 2001

Den 1 april 2001 kolliderade ett amerikanskt signalspaningsplan med ett kinesiskt stridsflygplan i internationellt luftrum utanför Kinas kust. Den kinesiske piloten omkom och det amerikanska planet tvingades nödlanda på kinesiskt territorium. Kina höll kvar planets besättning i elva dygn och krävde formella amerikanska ursäkter, något USA vägrade i avsaknad av en utredning av händelsen. Kina uttryckte också stor irritation över USA:s regelbundna och nästan dagliga flygningar utmed den kinesiska kusten, vilket den kinesiska regeringen protesterat mot redan tidigare[36]. Förutom att USA riktade skarp kritik mot att Kina höll kvar besättningen och flygplanet, kritiserades också Kinas "aggressiva flygningar". Enligt USA hade kinesiska flyg vid upprepade tillfällen flugit inom ett par meters avstånd från amerikanska spaningsplan i internationellt luftrum.[37]

Det spända politiska läge som uppstod mellan USA och Kina löstes genom diplomatiska förhandlingar och besättningen, samt senare även själva flygplanet, återlämnades till USA. Till följd av kollisionen mellan planen den 1 april inleddes omedelbart ett "nätkrig" mellan kinesiska och amerikanska hacktivister. Fram till den 9 maj då angreppen avbröts skedde uppskattningsvis 14.000 samordnade angrepp mot båda länders statliga institutioner och företag.[38]

2.2.1 Angrepp mot webbplatser

Enligt uppgifter från NIPC slogs amerikanska webbplatser ut genom distribuerade överbelastningsattacker och innehåll förändrades på webbplatser till pro-kinesiska eller anti-amerikanska budskap. Bland de institutioner vars webbplatser angreps fanns Vita huset, det amerikanska flygvapnet och USA:s energidepartement.[39] Den 30 april iscensatte kinesiska hackare även ett samordnat angrepp mot statliga och kommersiella

---

[36] "China's ambassador talks about the surveillance plane standoff", Public Broadcasting Service, www.pbs.org/newshour/bb/asia/jan-june01/chinaamb4-4.html, 4 april 2001.
[37] "The U.S. Deputy Secretary of State details the diplomatic story of the U.S.-China spy plane standoff", PBS, www.pbs.org/newshour/bb/asia/jan-june01/armitage4-13.html, 13 april 2001.
[38] NIPC, "Increased Internet Attacks Against US Web Sites and Mail Servers Possible in Early May", Advisory 01-009, NIPC, www.nipc.gov, 21 april 2001.
[39] Michael A. Vatis, 2001, "Cyber Attacks During the War on Terrorism: A Predictive Analysis", The Institute for Security Technology Studies at Dartmouth College, sid. 8.

amerikanska webbplatser. Ett virus som installerade DDoS-verktyg på datorer sades också vara av kinesisk härkomst. Amerikanska hacktivister genomförde på likartat sätt hundratals angrepp mot statliga kinesiska webbplatser.[40] Informationen från Kina om vilka IT-attacker landet utsattes för är emellertid mycket knapphändiga.

2.2.2 Angrepp mot infrastruktur

Allvarliga angrepp mot elkraftförsörjningen i Kalifornien genomfördes mellan den 25 april och 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. Angreppen ansågs ha kinesiskt ursprung men det är obekräftat huruvida dessa angrepp hade något politiskt samröre med spionplansincidenten eller med de nätangrepp som i övrigt följde på denna.[41]

2.2.3 Tidigare angrepp

Kinesiska hacktivister angrep även USA 1999 sedan USA bombat den kinesiska ambassaden i Jugoslaviens huvudstad Belgrad, vilket dödade tre kineser i byggnaden[42]. USA framförde ursäkter för händelsen som de uppgav vara ett misstag. Även den gången angreps bland annat Vita huset och energidepartementets webbplatser men i jämförelse med angreppen 2001 var detta relativt oorganiserat och begränsat både i intensitet och i tid.[43]

2.3 Israel och Palestina 2000-2001

Sedan fredssamtalen under hösten 2000 gått i stå och en ny intifada utropats, inleddes även en så kallad inter-fada, ett "nätkrig" mellan palestinier och israeler. Denna våg av nätangrepp inleddes den 6 oktober 2000 sedan motståndsrörelsen Hizbollah kidnappat fyra israeliska soldater i syfte att utväxla dem mot libanesiska fångar i israeliska

---

[40] NIPC, "Increased Internet Attacks Against US Web Sites and Mail Servers Possible in Early May", Advisory 01-009, NIPC, www.nipc.gov, 21 april 2001.
[41] Delete, nyhetsbrev från Försvarshögskolan, nr. 12, 2001.
[42] "Hackers protest embassy bombing", ZDNET, www.zdnet.com, 9 maj 1999.
[43] National Infrastructure Protection Center, "Cyber Protests: The Threat to the U.S. Information Infrastructure", oktober 2001, sid. 3, NIPC, www.nipc.gov.

fängelser. Det första angreppet riktades därför mot Hizbollahs webbplats.[44] Under det dryga år som gått sedan dess har den elektroniska konflikten följt samma eskalerings- och deeskaleringsmönster som konflikten mellan Palestina och Israel i övrigt: med ökade politiska spänningar och våldsyttringar i regionen har också de logiska angreppen intensifierats.[45]

Palestinska hackare presenterade en strategi för angrepp mot Israel i fyra steg. Den första fasen var inriktad på statliga webbplatser, därefter riktade man sig mot centrala finansiella institutioner. Fas tre fokuserade på kommunikations-infrastruktur, medan den sista och fjärde fasen uppgavs bestå i en ytterligare eskalering, bland annat i form av angrepp mot måltavlor i andra länder.[46]

2.3.1 Angrepp mot webbplatser

Israeliska och palestinska hacktivister har angripit politiska, akademiska och privata företags webbplatser.[47] Dessa angrepp har omfattat både massiva distribuerade överbelastningsattacker, förändring av innehåll på webbplatser, systemintrång och försök att få full behörighet och därmed full tillgång till datorsystem.[48] I Israel har bland annat parlamentet, försvarsmakten, utrikesdepartementet, riksbanken, börsen i Tel Aviv och universitet attackerats. På den palestinska sidan har den palestinska nationella myndigheten, motståndsrörelsen Hizbollah och Politics Forum of Albawaba, ett nätforum för debatter mellan israeler och palestinier, utgjort måltavlor.[49]

2.3.2 Angrepp mot infrastruktur

Angrepp mot AIPAC, en pro-israelisk lobbyorganisation i USA, uppges ha resulterat i tillgång till kreditkortsnummer och medlemsregister.[50] AIPAC tillbakavisar dock att de

---

[44] "Palestinian Crackers Share Bugs", WIRED, www.wired.com, 2 december 2000.
[45] "Israel Discusses the Inter-fada", WIRED, www.wired.com, 12 januari 2001.
[46] Michael A. Vatis, 2001, "Cyber Attacks During the War on Terrorism: A Predictive Analysis", The Institute for Security Technology Studies at Dartmouth College, sid. 7.
[47] "Israel Discusses the Inter-fada", WIRED, www.wired.com, 12 januari 2001.
[48] "Palestinian Crackers Share Bugs", WIRED, www.wired.com, 2 december 2000.
[49] Fadi Salem och Fawaz Jarrah, "Israeli Palestinian Clashes Spur Hacking Attacks", Dabbagh Information Technology, www.dit.net/itnews/newsoct2000/63.html, 18 oktober 2000.
[50] "Hackers target U.S. Pro-Israel Site", AP Washington, 4 november 2000.

utsatts för angrepp av palestinska hackare över huvudtaget.[51] Däremot är det bekräftat att Internetleverantörer och telekommunikationsföretag angripits.[52]

2.4 NATO-länderna och Serbien 1999

Under slutet av 1990-talet ledde motsättningar mellan olika befolkningsgrupper i provinsen Kosovo i Serbien till att en väpnad konflikt bröt ut. Sedan Serbien/Jugoslavien i början av 1999 vägrat skriva under det fredsavtal som utarbetats av det internationella samfundet, gjorde försvarsalliansen NATO verklighet av de hot man uttalat mot landets ledning. Detta innebar att NATO ingrep militärt i konflikten, i första hand genom bombningar riktade mot mål i Kosovo och andra delar av den jugoslaviska federationen.

2.4.1 Angrepp mot webbplatser

Sedan NATO övergått till krigshandlingar angreps försvarsalliansens servrar av serbiska hackare genom distribuerade överbelastningsattacker. Officiella webbplatser i NATO-länder angreps också, virus spreds genom e-post och allt från små företag till centrala politiska och militära institutioner drabbades av e-postbombning.[53] I sympati med Serbien deltog också individer från andra stater i aktionerna, bland annat från Ryssland. Officiella amerikanska webbplatser angreps även av inhemska hacktivistgrupper som protesterade mot NATO:s krigföring.[54] Information på Jugoslaviens officiella webbplatser förvanskades till NATO:s fördel av amerikanska och europeiska hacktivister och innehållet på NATO-fientliga webbplatser ersattes med NATO-propaganda.[55]

---

[51] Cheryl Greenberg, AIPAC Web Site Coordinator, e-brev till Magdalena Tham, 22 oktober 2001.
[52] Michael A. Vatis, 2001, "Cyber Attacks During the War on Terrorism: A Predictive Analysis", The Institute for Security Technology Studies at Dartmouth College, sid. 7.
[53] "War on the Web: Serb hackers blitz sites", Arkansas Democrat-Gazette, www.ardemgaz.com, 12 april 1999.
[54] Denning, Dorothy E., 2000, "Hacktivism: An Emerging Threat to Diplomacy", sid. 2, American Foreign Service Association (AFSA).
[55] "Kosovo cyber-war intensifies", Network World Fusion, www.nwfusion.com, 12 maj 1999; samt AntiOnline, www.antionline.com/archives/pages/www.pentagon.co.uk, 12 januari 2001.

2.5 Slutsatser utifrån studerade fall

Det stora flertalet av de angrepp vi känner till har syftat till att temporärt störa datorsystem, exempelvis genom DDoS-attacker som överbelastar systemet, att förändra webbplatsers innehåll för att demonstrera en åsikt eller sprida desinformation samt omdirigering av trafik till annan webbplats. Den här typen av aktioner kan snarast jämföras med demonstrationer eller vandalisering som om än kostsamt, tidsödande och störande för de drabbade inte kan betecknas som ett direkt hot mot den nationella säkerheten. Angrepp har emellertid även gjorts mot telesystem, elkraftförsörjning och banksystem och att aktioner även syftat till inhämtning av underrättelser.

2.5.1 Hacktivisternas motiv och måltavlor

Motiven bakom aktionerna kan sammanfattas i tre huvudmotiv. I samtliga omnämnda fall sker angreppen som ett slags protest mot den part som åsamkat fysisk skada. I fråga om Israel/Palestina och NATO/Serbien var motiven förutom detta även att hjälpa den sida i konflikten hacktivisten sympatiserar med. Aktörernas ambition är i detta fall att utgöra en komponent i den konventionella krigföring som pågår mellan parterna. När det gäller terroristangreppen mot USA 2001 ser vi dessutom en tredje typ av motiv, ett agerande som syftar till att i första hand hjälpa den part hacktivisten sympatiserar med men som också har det tydliga syftet att iscensätta motangrepp på egen hand i frånvaro av statligt agerande. Detta gällde under de första veckorna efter attackerna mot New York och Washington då USA avvaktade med krigshandlingar.

Måltavlorna hacktivisterna har inriktat sig på i de beskrivna fallen kan delas upp i två kategorier, dels angrepp mot direkt involverade institutioner i konflikten, dels måltavlor med högt symbolvärde. Måltavlor som faller inom den förstnämnda kategorin är Hizbollah som angreps i oktober 2000 sedan organisationen kidnappat israeliska soldater, det amerikanska flygvapnet som angreps av kineser sedan dess spionplan kolliderat med ett kinesiskt stridsflygplan 2000 och NATO vars servrar attackerades under Kosovo-kriget 1999 sedan alliansen fällt bomber över Serbien.

Oavsett konfliktfrågans karaktär kan vi också konstatera att involverade staters officiella webbplatser alltid utgör måltavlor på grund av sitt höga symbolvärde. Det innebär att webbplatser för regering, parlament, departement och myndigheter alltid kan räknas som potentiella måltavlor för angrepp av hacktivister. Även universitet och privata företag har i våra exempel tydligtvis tilldelats en representativ funktion för sitt land och därmed utgjort symboliska måltavlor för protester mot staten i fråga. I de fall ett ömsesidigt ”nätkrig” brutit ut mellan hacktivister har även Internetleverantörer angripits i syfte att påverka motståndarens möjligheter till angrepp. Sammanfattningsvis har kända hacktivistangrepp omfattat de flesta samhällssektorer: politiska, akademiska och finansiella institutioner samt privata företag.

2.5.2 När angrepp kan förväntas

Utifrån våra exempel kan vi konstatera två tidpunkter under en kris eller konflikt då man kan räkna med angrepp av hacktivister. För det första sker angrepp som omedelbara reaktioner på fysiska angrepp eller incidenter som ger upphov till ett krisläge. Detta gäller för terrorangreppen mot USA, för spionplansincidenten, för de havererade fredsförhandlingarna mellan israeler och palestinier, liksom för NATO:s bombningar av Serbien och för bombningen av den kinesiska ambassaden i Belgrad. Under intensiva, uppmärksammade men tidsbegränsade konflikter, såsom spionplansincidenten, pågår hacktivisternas angrepp under hela den akuta krisfasen då allmänhetens engagemang och massmedias bevakning är som störst.

I mer långvariga konflikter där intensiteten i fientligheterna mellan parterna varierar, äger inte heller de elektroniska angreppen rum med samma intensitet. Vårt andra konstaterande om när under en konflikt hacktivister agerar, är därmed att angrepp sker när en pågående konflikt eskalerar. Det tydligaste exemplet på detta är konflikten mellan Israel och Palestina där omfattande logiska angrepp följer på utbrott av våld mellan parterna.

2.5.3 Aktörernas politiska insikt

Kunskaperna om de mål hacktivisterna riktar in sig på tycks i vissa fall ha varit bristfälliga. Som nämnts ovan attackerade USA-sympatiserande hacktivister den afghanska regering som gick i exil 1996, istället för talibanregimen. Hacktivistgrupper hotade vidare i september 2001 med att förstöra tillgången till Internet i Afghanistan, en aktion vars betydelse starkt kan ifrågasättas då landets tekniska infrastruktur efter decennier av krig och inbördesstrider i princip är obefintlig. Större delen av landet saknar exempelvis tillgång till telekommunikationer och en mycket liten andel av befolkningen är läskunnig.

Hacktivisterna riktade också i det här fallet in sig på måltavlor som ofta i andra sammanhang pekats ut som amerikanska fiender, såsom Iran och palestinska grupperingar, eftersom USA anser dem skydda eller understödja terrorism. Detta trots att de just i denna konflikt ställt sig bakom USA och inga officiella amerikanska anklagelser har riktats mot Iran eller Palestina. De aktioner vi sett med anknytning till terrordåden mot USA tycks därmed kraftigt ha dominerats av hacktivister med teknisk kompetens och med engagemang i konflikten men med begränsad politisk insikt.

2.5.4 Konsekvenser av hacktivism

Vilka aktioner som verkligen genomförts, i vilken omfattning och vilka effekter som uppnåtts är svårt att avgöra eftersom många uppgifter är svåra att verifiera. Hacktivisterna har intresse av att överdriva sina framgångar av statusskäl samtidigt som angripna stater, organisationer och företag har ett intresse av att tona ner incidenter då allvarliga konsekvenser skulle avslöja säkerhetsbrister eller kunna inspirera till nya angrepp.

Slutsatser som drogs vid Ben Gurion-universitetet i Israel under ett akademiskt seminarium om nätangrepp, var att den elektroniska konflikten inte ersatte intresset för konventionell krigföring utan snarare bidrog till att föra samman fler människor med samma mål och intressen. Detta, menade man, skulle kunna inspirera och motivera till

ökad konflikt på marken, snarare än att utgöra ett substitut för det fysiska våldet.[56] Även aktivister som motsätter sig våldsanvändning uppfattar att politiska aktioner genomförs, och i ökad utsträckning kommer att genomföras, i två sfärer:

"*One is on the ground, in the streets, in offices, in universities, in factories - in real spaces. The other is on the Net, in what the Pentagon now calls 'battlespace'. And we support the development and practice of joint virtual-real actions of resistance.*"[57]

[56] "Israel Discusses the Inter-fada", WIRED, www.wired.com, 12 januari 2001.
[57] Electronic Disturbance Theater, "Infowar: Call for FloodNet Action for Peace in the Middle East", Ars Electronical Center, www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00633.html, 18 december 1998.

3 MOTIV

3.1 Att delta i eller påverka konfliktförloppet

Utifrån våra exempel i kapitel 2 drog vi slutsatsen att tre olika typer av motiv kunde skönjas bakom hacktivisters agerande i de aktuella fallen. Dessa var att protestera mot en parts agerande i den pågående konflikten, att hjälpa part samt att agera i brist på tillfredställande agerande från part i konflikten. Samtliga tre motiv klassificerar vi som politiska motiv vars huvudsyfte är att delta i eller påverka konfliktförloppet.

Politiska motiv syftar till att antingen hjälpa någon av de officiella parterna i konflikten med de medel man förfogar över, att motarbeta eller förhindra agerande av part eller att på annat sätt påverka parterna och därmed konfliktdynamiken. Med sådana motiv anser vi att hacktivistens ambition är att utgöra en part i konflikten, att ur någon aspekt komplettera de officiella parternas eget agerande. Detta sagt utan att på något sätt jämställa hacktivistens egna insatser med krigföring eller med kapaciteten för detta hos en stat.

Mycket av den hacktivism vi sett hittills har varit demonstrationer av stöd för en parts sak eller agerande eller av missnöje med att en part exempelvis inte agerar kraftfullt nog, vid rätt tillfälle, med rätt medel eller mot rätt måltavla. Vi har också sett agerande som syftat till att demonstrera den principiella uppfattningen att staten inte har monopol på agerande i krig:
"We do not believe that only nation-states have the legitimate authority to engage in war and agression. And we see cyberspace as a means for non-state political actors to enter present and future arenas of conflict, and to do so across international borders"[58]

Dagens hacktivisters möjligheter att direkt inverka på en stats politik, exempelvis genom att utöva utpressning, måste anses ytterst begränsade. Den direkta måltavlan för

[58] Electronic Disturbance Theater, "Infowar: Call for FloodNet Action for Peace in the Middle East", Ars Electronical Center, www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00633.html, 18 december 1998.

den här typen av demonstrationer är därför i första hand den allmänna opinionen. Om den nationella eller internationella opinionen förändras, kan det sedan i sin tur påverka konfliktparternas eller andra aktörers policy och därigenom agerande, i den pågående konflikten. Många aktioner kan också tolkas som uttryck för ett behov av att avreagera sig mer än att söka uppnå konkreta policyförändringar.

3.2 Gynna icke-politiska intressen

Den andra kategorin av motiv har vi benämnt icke-politiska. Spänningar och konflikter mellan stater och andra internationella aktörer kan utnyttjas för att tillgodose andra intressen än att påverka konflikten i sig. I konflikter finns till exempel alltid ekonomiska intressen som kan gynnas av att konflikten utvecklas i en viss riktning. Ett rimligt antagande är att hackarverksamhet då kan syfta till att skapa kaos, rikta statens uppmärksamhet mot ett visst område eller söka påverka parterna i konflikten, inte av intresse för den politiska frågan utan i syfte att indirekt gynna privata intressen. Det som synes vara politisk aktivism på nätet kan också ha som enda syfte att uppnå status inom en grupp. Den typ av IT-aktörer vars huvudmotiv och drivkraft är att uppnå berömmelse och väcka uppmärksamhet bör emellertid benämnas hackare och inte hacktivister.

Att skilja på politiska och ideologiska motiv å ena sidan och icke-politiska motiv å andra sidan har relevans för den aktör som söker påverka hacktivisternas eller hackarnas agerande. Om den största drivkraften är berömmelse kommer intensiteten i hackarangreppen inte nödvändigtvis att följa utvecklingen av konflikten utan snarare medias intresse för att rapportera hackarincidenter. Motivationen hos dessa grupper kan också förutsättas variera. Under en utdragen konflikt utan brett uppmärksammade faser av eskalering kommer sannolikt hackarangreppen att avta i större utsträckning än angreppen från starkt politiskt motiverade hacktivister. Det är dock viktigt att understryka att ett agerande kan leda till säkerhetspolitiska konsekvenser även om motiven i första hand inte är politiska.

3.3 Dolda motiv

Det kan inte uteslutas att det finns hacktivister som agerar på andra aktörers uppdrag men som utger sig för att agera på eget initiativ. Ett flertal stater har idag kapacitet för informationskrigföring och kan använda informationsoperationer som inslag i sin krigföring. Flera stater, däribland Sverige[59], vill använda sig av hackares kompetens för att göra intrångstester i förebyggande syfte. Betydligt mer kontroversiellt skulle det emellertid vara om det visade sig att stater inofficiellt anlitar icke-statliga aktörer för att utföra systemintrång, men att dessa angrepp kamoufleras som spontana attacker av enskilda individer som står utanför statens kontroll. I ett sådant läge, där det kan tänkas att staten ifråga officiellt dementerar inblandning i incidenterna, blir det snart mycket svårt för den attackerade parten att urskilja vem som egentligen är angripare.

Om misstankar uppstår om att "hacktivister" i själva verket utgör en del av en stats strategi blir hacktivister generellt legitima måltavlor i konflikten. Med mer sofistikerade hacktivistangrepp mot kritisk infrastruktur blir det svårare att skilja politisk nätaktivism från statlig informationskrigföring. Detta kan leda till komplikationer för verkliga hacktivister och till säkerhetspolitiska konsekvenser för stater. Bristande förtroende för vilka aktioner som verkligen är statligt sanktionerade eller inte, skulle kunna leda till att alla allvarliga angrepp över nätet under en konfliktsituation betraktas som en del av de officiella parternas krigföring.

[59] "Försvarsminister vill ha statliga hackare", Computer Sweden, www.computersweden.se, 4 oktober 2001.

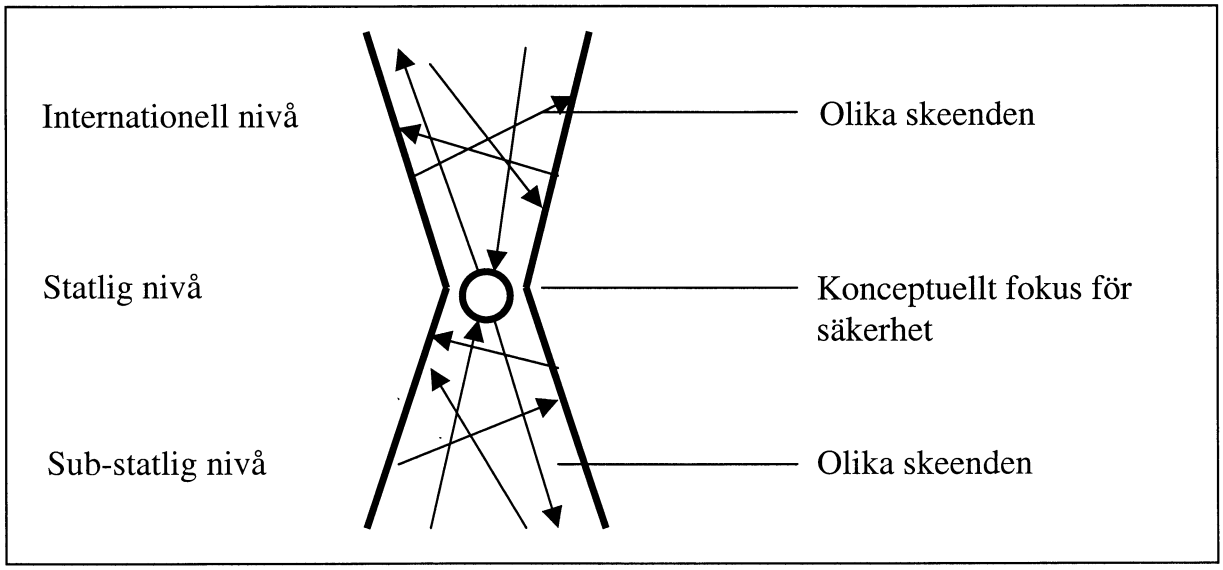
4 KONSEKVENSER AV HACKTIVISM UNDER KONFLIKT

4.1 Säkerhetspolitiska konsekvenser

Förutom de direkta konsekvenser ett allvarligt IT-angrepp kan få för en stat i form av störd infrastruktur, saboterade webbsidor och datanätverk, så kan det på sikt få säkerhetspolitiska konsekvenser. Det faktum att icke-statliga aktörer kan delta i en konflikt, utan att de officiella parterna kan påverka dem i någon större utsträckning, är en verklighet som har potentialen att utmana det statliga våldsmonopolet och den statliga autonomin.

Säkerhetspolitik är schematiskt uttryckt de beslut, framarbetade av regering och riksdag, som ligger till grund för statens säkerhetsarbete, det vill säga de åtgärder staten vidtar för att skydda sin suveränitet och därmed sin autonomi. Staten reagerar på nationella och internationella skeenden av betydelse för rikets säkerhet och säkerhetspolitiken formas i enlighet med den uppfattade hotbilden och statens målsättningar. Om skeendena får inverkan på de säkerhetspolitiska beslut som fattas och följaktligen på statens agerande, har händelserna fått säkerhetspolitiska konsekvenser för staten. Staten, med sina resurser i form av lagstiftningsmonopol, ekonomiska medel, myndighetsstruktur och inte minst tillgång till militära medel, genomför åtgärder i enlighet med politiska beslut. Detta kan uttryckas som att staten är uppsamlare av nationella och internationella skeenden, den policyskapande auktoriteten såväl som implementerare av fattade beslut. Statens funktion som konceptuellt säkerhetslokus illustreras i Ole Wævers timglasmodell[60] (figur 2).

[60] Ole Wæver, 1989, "Security, the speech act: analyzing the politics of a word", sid. 35-6.



Figur 2. Ole Wævers timglasmodell av säkerhet.

4.1.2 Ett utmanat säkerhetslokus

Vi har hävdat att spridning av informationsteknik har bidragit till att allt fler aktörer, från individer till nätverk och organiserade grupper, har givits en historiskt oöverträffad möjlighet att föra fram sitt budskap. Transnationella flöden var tidigare i stor utsträckning beroende av byråkratiska organisationer såsom till exempel multinationella företag eller statliga organ, eftersom det var dessa som hade tillräckliga resurser att skapa kommunikationsinfrastruktur. Idag är tekniken både betydligt billigare och mer lättillgänglig vilket har fått till följd att även löst sammansatta nätverk och till och med individer kan nå in i stater med ett budskap utan att behöva ta hänsyn till geografiska gränsdragningar eller statens agenda.[61]

Tekniken innebär sålunda ökade möjligheter att göra sin röst hörd och att förmedla sitt budskap till omvärlden. Man kan också på ett behändigare sätt än tidigare föra samman de som är av samma åsikt och värva likasinnade. Det finns, enkelt uttryckt, fler kanaler in och ut ur ett land och det är inte nödvändigt att gå via staten – gränskontroller är inte möjliga i den logiska sfären. Baksidan av denna utveckling är att ett samhälle som är beroende av fungerande datornätverk för att klara viktiga

[61] Robert O. Keohane och Joseph Nye, 2001, "Power and Independence", sid. 217ff.

samhällsfunktioner, inte bara är ett effektivt och informationstätt organisationssystem utan även ett mycket sårbart sådant.[62]

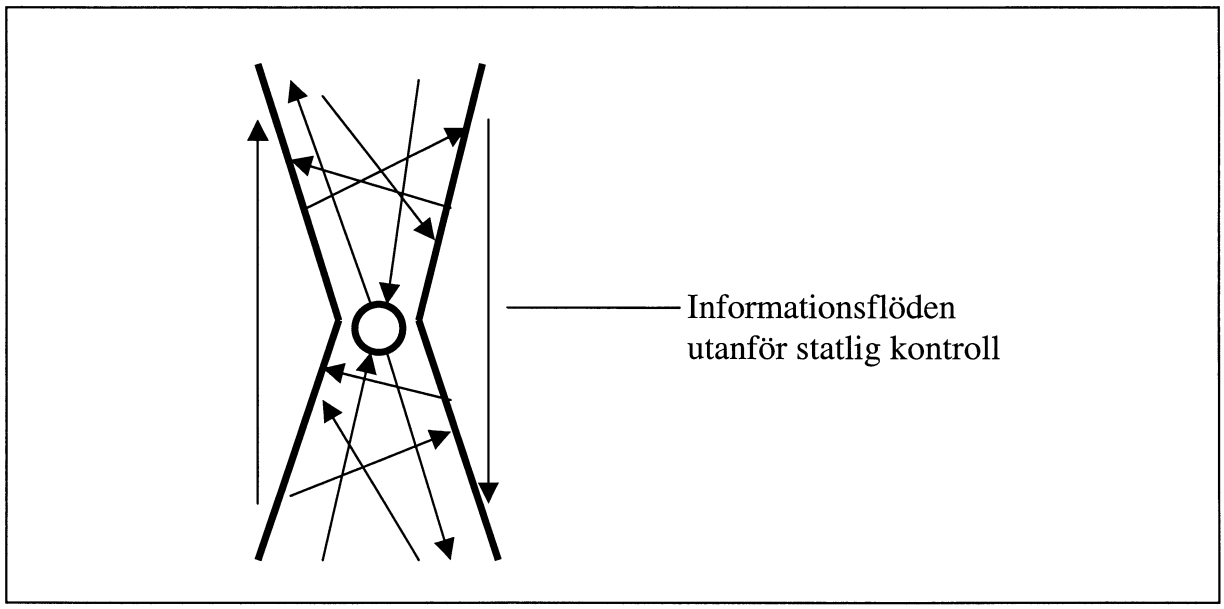
Att andra aktörer försöker påverka den statliga agendan även i fråga om säkerhetspolitik, är inget nytt fenomen. Med den nya tekniken har dessa aktörer större möjligheter att faktiskt agera utifrån sin egen agenda och att delta i en internationell konflikt. Det vapen man använder, IT, har samma räckvidd som datasystemet vilket i princip är globalt. Aktörerna är därmed inte territoriellt bundna. Det är också svårare för en stat att upptäcka och kontrollera vem som har tillgång till IT-vapen jämfört med innehav av konventionella vapen. Det är svårt att i efterhand utröna vem som kan ha haft tillräcklig kompetens för att genomföra angrepp och under vilken jurisdiktion denne lyder.

Användningen av IT som vapen vållar staten bekymmer eftersom det egentligen rör sig om illegalt användande av teknik som det moderna samhället är beroende av. Man kan tala om "dual use"[63] i ny bemärkelse – samma teknik som är skapad för att effektivisera samhället och underlätta kommunikation och informationsöverföring används även till krigföring eller störning. Restriktioner av ägande, utvecklande och utnyttjande är därför inte möjliga i samma utsträckning som när det gäller konventionella vapen eftersom IT i sig inte är ett vapen. Inga stater vill sätta käppar i hjulet för sin egen teknikutveckling. Som exempel kan nämnas att Ryssland 1998 lämnade in ett resolutionsförslag till FN, i vilket IT-operationer definierades som informationskrigföring och jämställdes med massförstörelsevapen. Följaktligen ville man reglera den tekniska utveckling i resten av världen som möjliggjorde framställandet av IT-vapen. Inga andra länder anammade definitionen.[64]

Den monopolställning som staten har haft som säkerhetslokus och ensam auktoritet vad gäller underrättelseinhämtning, policyskapande och implementerande av politiska beslut, utmanas av att icke-statliga aktörer finner medel att utföra dessa uppgifter

[62] SOU 2001:41, "Säkerhet i en ny tid", Sårbarhets- och säkerhetsutredningen, sid. 187.
[63] "Dual use" tolkas vanligtvis som att privat och militär sektor drar nytta av samma tekniska utveckling.
[64] Josefin Grennert, "Internationell hantering av IT-hot. Är FN rätt forum?", sid. 6 och 9ff.

enligt sin egen agenda. IT möjliggör för andra aktörer än stater att reagera och agera på inre och yttre skeenden. Teknikens gränslöshet och sträckning är av betydelse för kontakt mellan likasinnade såväl som för aktioner eller angrepp. Dessa aktörer kan ha en egen handlingsplan och potentiellt även en egen underrättelsetjänst i form av nationella och internationella nätverk, där informationen inte har passerat statliga filter. Hacktivisterna skapar utifrån sin världsbild sin egen policy. Tekniken skapar kanaler för kommunikation och även angrepp som möjliggör kringgående av staten (se figur 3).



Figur 3. Informationsflöden utanför statlig kontroll.

Resursmässigt är hacktivisterna underlägsna staten. Med IT-vapen kan man störa andra datorer, nätverk eller ett helt samhälle men inte överta territorium eller slutgiltigt betvinga en annan stat. Genom att tidsmässigt låta IT-angrepp löpa parallellt med en konflikt där minst en part är en stat ökar man genomslagskraften. Därför kan man säga att det finns andra aktörer än stater, till exempel hacktivister, som inte är beroende av staten för vare sig uppsamling av inre och yttre skeenden, policyskapandet eller implementerandet av åtgärder för att nå sina mål. Staten används som territoriell bas och, när IT-angrepp sammanfaller med en konflikt, som resursförstärkare.

4.1.3 Statligt handlingsutrymme

Staten har våldsmonopol såväl inåt gentemot den egna befolkningen som utåt. Detta innebär att staten ensam har rätten att förklara och föra krig. Som en konsekvens härav är det staten som enligt gällande folkrättsliga regler stipulerar vad som är att betrakta som anledning till krigsförklaring, hur förklaringen skall gå till, vilka villkor som skall ställas på motparten eller hur en eventuell vedergällning skall genomföras. I det fall att andra aktörer än staten har förmåga att på ett inflytelserikt sätt agera mot en annan stat eller annan aktör får staten se sitt monopol utmanat. Om hacktivister agerar parallellt med staten i en konflikt utan att agerandet är sanktionerat av någon stat kan staten inte till fullo sägas kunna kontrollera konfliktförloppet. I sin yttersta form innebär denna inblandning av icke-statliga aktörer att staten inte ensam råder över krigsförklaring och krigföring.

Hacktivisters agerande under pågående konflikt kan av motparten komma att betraktas som sanktionerat av en av de officiella parterna. Detta kan uppfattas som en provokation och skapa svårigheter för diplomatiska förhandlingar. Även i det fall det står klart att IT-angreppen inte är statligt sanktionerade kan de få konsekvenser för konfliktförloppet. Oförmåga att kontrollera hacktivisterna kan generera ytterligare animositet mellan parterna och förvärra ett redan spänt läge. För stater är detta ett svårlöst problem. Möjligheten att agera anonymt över nätet gör det svårt att spåra och hindra hacktivister. Anonymiteten bidrar till osäkerhet i fråga om aktörens hemvist och därmed under vilken jurisdiktion denne lyder och potentiellt även det bakomliggande syftet med angrepp.

4.2 Pro-aktivt agerande

Hacktivisters agerande kan påverka en stats långsiktiga säkerhetspolitiska agenda. Angrepp kan till exempel driva fram förändringar i lagstiftningen inom IT-området vilka i praktiken kan begränsa friheten att publicera material och möjligheten att vara anonym på nätet. Detta sker i så fall med motiveringen att det minskar riskerna för

sabotage och angrepp via nätet bland annat genom att brottsutredande myndigheter får större möjligheter att spåra misstänkta på nätet.

Det efterarbete som skedde och fortfarande pågår i kölvattnet av terrorattackerna mot USA i september 2001 är ett aktuellt exempel. Attackerna har bidragit till att aktualisera frågorna om vad som kan åstadkommas via nätet och vilka typer av aktörer som skulle kunna tänkas ligga bakom. Såväl länder som organisationer har reagerat och rustar nu för att i framtiden kunna klara av att bemöta angrepp via datornätverk.

De åtgärder som kan vara aktuella för att förhindra hacktivism är desamma som för att bekämpa cyberkriminalitet i allmänhet och potentiellt även cyberterrorism. Samma metoder och verktyg används vid angrepp och det är i huvudsak det bakomliggande syftet som skiljer de olika grupperna åt. Det har länge ansetts vara en ovedersäglig sanning att det inte är möjligt att skapa ett fullständigt vattentätt tekniskt skydd mot elektroniska angrepp över nätet. Istället försöker man nu anpassa gällande lagstiftning för att kriminalisera angreppen och öka möjligheterna för brottsutredande myndigheter att arbeta proaktivt, det vill säga för att förebygga angrepp.

4.2.1 Legal anpassning

USA:s justitieminister John Aschcroft lade den 24 september 2001 fram ett lagförslag, Mobilization Against Terrorism Act, genom vilket brottsbekämpande myndigheter skall ges större möjlighet till avlyssning av kommunikation över Internet. Kriminella handlingar över nätet skall enligt förslaget kunna straffas med högst livstids fängelse.[65] Detta förslag gav upphov till högljudda klagomål från bland annat medborgarrättsorganisationer som menade att förslaget innebar att så gott som alla databrott betraktas som potentiell terrorism.[66] Ett nytt förslag, "Patriot", lades därefter fram inför representanthuset. Patriot, som står för "Provide Appropriate Tools Required to Intercept and Obstruct Terrorism", innebär även det möjligheten att databrottslighet ska kunna bestraffas med livstids fängelse men då måste tilltaget vara

[65] USA:s justitiedepartement, september 2001, http://usdoj.gov/opa/pr/2001/September/492ag.htm.
[66] "Revamped Anti-terrorism Act Removes Low-level Crackers", Cryptome, http://cryptome.org/patriot.htm (10 oktober 2001).

utfört för att påverka eller ha inflytande över myndighetsutövande genom hot eller tvång; eller hämnas myndighetsutövande.[67] USA Patriot Act skrevs under av president Bush den 26 oktober efter att en stor majoritet i representanthuset röstat för förslaget.[68]

En åtgärd, vars omfattning styrs av rådande lagstiftning, för att identifiera hacktivister är infiltrering i nätverk och organisationer där de misstänks verka. Eftersom det tidigare i de flesta länder har funnits begränsningar gällande spårning av brottslingar via nätet och framförallt att spåra över statsgränser, har en möjlighet för brottsutredande myndigheter varit att utge sig för att vara hackare eller hacktivister. Ett framgångsrikt fall är FBI:s och det amerikanska försvarsdepartementets gemensamma 18 månader långa operation som startades under Kosovo-konflikten 1999 för att identifiera serbiska hackare som gjort sig skyldiga till angrepp på amerikanska webbservrar. Sex kriminalutredare från FBI och Pentagon angrep under täckmantel statliga webbservrar och fick resultaten publicerade på Attrition.org, en webbsida där lyckade hack arkiveras. Detta, i kombination med deltagande på chat-sidor, gav goda kontakter i hackervärlden.[69] Metoden att infiltrera hackargrupperingar sägs ha haft stor betydelse för FBI:s möjligheter att spåra hackare, särskilt vad gäller de som befinner sig utanför amerikanskt territorium.[70]

EU:s justitieministrar beslutade den 27 september 2001 att permanent inrätta det juridiska samarbetet "Eurojust". Beslutet att formalisera Eurojust som tidigare enbart existerat som ett provisoriskt organ sägs ha direkt koppling till terroristattackerna i USA. Organet skall fungera som ett nätverk av EU-medlemmarnas justitieministrar för att öka det juridiska samarbetet kring bland annat terrorism och cyberkriminalitet.[71]

Det är intressant att notera att man både i USA och inom EU nämner cybersäkerhet som del av bekämpning av terrorism. Det kan ses som ett tecken på att man är

[67] 107th Senate, first session, http://cryptome.org/patriot.htm.
[68] "Bush signs antiterrorism bill into law", CNN, http://cnn.com, 28 oktober 2001.
[69] "FBI operation penetrates hacker underground", Computer World, www.computerworld.se, 11 september 2001.
[70] Ibid.

medveten om att tekniken som möjliggör allvarliga attacker finns och att välorganiserade grupperingar har tillgång till den. Det förefaller också troligt att man ser cyberattacker som en möjlig del av framtida konflikter.

[71] Delete, nyhetsbrev från Försvarshögskolan, nr. 14, september 2001, sid. 4 samt Euractive, www.euractive.com/cgi-bin/eurb/cgint.exe/134689-323?1100=1&204&OIDN=1502308&-home=home.

5 UTVECKLING OCH HANTERING

Vi har i rapporten presenterat exempel på konflikter där icke-statliga aktörer har nyttjat IT-medel för att söka påverka konfliktförlopp. Denna typ av inblandning kommer med största sannolikhet att finnas med som en given komponent i framtida konflikter. Tekniken som behövs för att genomföra angrepp på datorsystem, militära eller civila, existerar och som exemplen visar har olika grupper, såväl hacktivister med uttalade politiska mål som hackare, tillgång till tekniken. Även om attackerna hittills har skett på en relativt låg nivå med begränsade konsekvenser för de officiella parterna i konflikten, finns det inga indikationer på annat än att angreppen har potential att öka såväl i frekvens som i sofistikeringsgrad. Relevant teknik och politiska grupperingar har mötts men för att kunna utnyttja tekniken på ett effektivare sätt krävs djupare kunskap om hur man hanterar den. För att utgöra ett reellt hot behöver potentiella användare också ha tillgång till underrättelser för att identifiera kritiska noder i datornätverk och infrastruktur att slå mot. Det är därför naturligt att vänta sig en viss ställtid innan hacktivistgrupperingar kan utnyttja tekniken till dess fulla potential.

Vilken grad av beredskap en stat skall ha för IT-attacker utförda av icke-statliga aktörer under konflikt, bör baseras på en avvägning mellan vad som idag och framöver är tekniskt möjligt och vad som är troligt givet statens säkerhetssituation. Staten bör dock göra bedömningen baserad på tillgänglig information om, i detta fall, IT-hot snarare än att konstatera att det hittills inte har utgjort något problem. Det är i sammanhanget viktigt att notera att eftersom användningen av IT-vapen inte är territoriellt bundet, det vill säga såväl förövare som måltavla kan befinna sig var som helst inom det globala datornätverket, finns det heller ingen definitiv fysisk front. Andra länder än de som är direkt involverade i den aktuella konflikten kan, till exempel vid tydlig partiskhet, bli föremål för angrepp. Riskerna för en militär konflikt i det nordiska området bedöms i Försvarsmaktens strategiska omvärldsbedömande 2001-2006 vara fortsatt mycket små. Hotet mot IT-system bedöms dock successivt öka

under perioden såväl i Sverige som i samband med Sveriges internationella verksamhet.[72]

5.1 Möjliga utvecklingsvägar

Vi har i den här rapporten diskuterat vilka säkerhetspolitiska konsekvenser hacktivism skulle kunna medföra. En möjlig framtida utveckling är rimligen även att användningen av hacktivism mattas av. Andra metoder att påverka konfliktdynamik kan visa sig mer framgångsrika, i synnerhet om pågående konflikter endast involverar parter som inte är nåbara elektroniskt. Det finns också en risk för en avtrubbningseffekt om hacktivism används för ofta. Möjligheten att mobilisera omvärlden och skapa opinion genom hacktivistverktyg kan minska om aktionerna är många och effekterna små.

Som vi nämnt tidigare kan informationsteknik användas till att föra samman likasinnade och på det sättet stimulera till ökad våldsanvändning på marken. Men IT kan också medföra att aktivister som inte använder sig av våld får ökade möjligheter att delta i konflikter och göra sin röst hörd vilket skulle kunna betyda ett uppsving för fredlig politisk aktivism. På samma sätt som vi menar att informationskrigföring inte helt kommer att ersätta konventionell krigföring, anser vi självfallet inte heller att hacktivism kommer att utgöra den enda formen för att uttrycka politiskt engagemang. Det viktiga här är att det är troligt att fler politiska grupperingar tar till sig hacktivism som medel att synas och höras och att hacktivism blir en naturlig del av aktivism.

Hacktivistgruppen Electronic Disturbance Theater som bedrivit åtskilliga politiska kampanjer över nätet, föredrar kombinerade så kallade ”virtual-real”-aktioner där hacktivism äger rum samtidigt som aktioner på marken. När kapacitet eller tid saknas för att organisera kombinerade aktioner använder sig gruppen enbart av hacktivism i form av till exempel elektroniska blockader av staters officiella hemsidor. Den här typen av elektroniska aktioner betraktas som direkta motsvarigheter till fysiska

[72] Försvarsmakten, Högkvarteret, *Försvarsmaktens strategiska omvärldsbedömande 2001-2006*, sid. 7 och 13.

blockader och demonstrationer och gruppen använder samma terminologi för aktioner i båda sfärerna.[73]

5.2 Samhällets sårbarhet för IT-attacker

En förutsättning för ökad användning av hacktivism är att samhällens sårbarhet för denna typ av angrepp kvarstår eller ökar, bland annat genom att globaliseringen av användningen av informationsteknik fortsätter. En teknisk utveckling som möjliggör mer sofistikerade angreppsmetoder som gör IT-vapnen, i form av bland annat virus, mer kontrollerbara och precisa stimulerar också sannolikt till en ökad användning. Ett samhälle som är beroende av datorsystem för att upprätthålla regeringsfunktioner och en rad andra samhällsnödvändiga funktioner är sannolikt inte primärt hotade av tonåringar med datorkunskap. Det man bör ha beredskap mot är snarare samordnade attacker utförda av tekniskt sofistikerade grupper. Om samordnade attacker utförs när ett land befinner sig i en nationell kris, kan det leda till svåra konsekvenser för staten.[74]

Som rapporten har visat kan attacker riktas mot såväl privata och statliga informationssystem som teknisk infrastruktur. Vår bedömning är att hacktivism skulle ha störst direkta effekter på samhället i det fall framgångsrika angrepp genomförs mot den kritiska infrastrukturen. Samordnade hacktivistangrepp med förbättrade verktyg riktade mot samhällets kritiska infrastruktur skulle kunna medföra betydligt allvarligare konsekvenser än vad vi hittills upplevt. En tänkbar utveckling är att existerande grupper tar till våldsammare metoder, alternativt att grupperingar som redan idag använder sig av våld tillägnar sig ökad kompetens att använda sig av informationsteknik.

Lawrence Gershwin, underrättelseofficer och teknisk specialist hos CIA, USA, har gjort bedömningen att endast stater kommer att inneha kapacitet för angrepp mot

[73] Electronic Disturbance Theater, "Infowar: Call for FloodNet Action for Peace in the Middle East", Ars Electronical Center, www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00633.html , 18 december 1998.
[74] Richard Clarke, USA:s nationelle cybersäkerhetsrådgivare, i Shawna McAlearney, "Cyberspace braces for escalation and war", Security Wire Digest, Vol. 3, nr. 89, november 2001.

kritisk infrastruktur under de närmaste fem till tio åren.[75] Om så är fallet är den troliga utvecklingen att hacktivism under de närmaste åren fortsätter att främst bestå av vandalisering av webbplatser och liknande störande mer än förstörande angrepp.

Det mest sannolika är att hacktivism under de närmaste åren kommer att förekomma som omedelbara reaktioner på politiska beslut eller extrema händelser samt under krissituationer då hacktivister ges massmedialt utrymme. Massmedias intresse för hacktivistincidenter har tydligtvis varit som störst då öppna våldsamheter inte inträffat mellan parterna och då hacktivistangreppen utgör de tydligaste aktionerna i konflikten. Om hacktivism skall kunna hävda sig under väpnade konflikter eller krig måste dock sannolikt tyngre taktik utvecklas i riktning mot cyberterrorism. Uteblir en sådan utveckling kan hacktivistangrepp komma att bli begränsade till akuta kriser samt utgöra en naturlig form för aktivister att uttrycka och demonstrera sina åsikter i kombination med traditionella politiska aktioner på marken.

5.3 Åtgärdsförslag

De senaste åren har produktionen av tekniska säkerhetslösningar såsom antivirusprogram ökat dramatiskt. Det är dock viktigt att vara medveten om att tekniska säkerhetslösningar enbart kan skydda mot redan kända säkerhetsrisker. Sårbarheter i datorsystem kan bero på fel eller säkerhetsbrister i hård- och mjukvara såväl som i felaktigt eller obetänksamt användande av datorer. Såväl medvetenhet om korrekt användande som mänsklig övervakning av nät är nödvändigt för att uppnå system som är så motståndskraftiga mot angrepp som möjligt. Elektronisk säkerhet är komplicerad att uppnå, inte minst då man inte kan stänga alla vägar in i ett land om en IT-attack inträffar.

I Sverige föreslog Post- och telestyrelsen år 2000 att
"regeringen utreder och om så behövs utarbetar förslag till de författningsändringar som behövs för att underlätta brottsutredningar vid dataintrång"[76].

[75] "U.S.: Fear Countries, Not Hackers", WIRED, www.wired.com , 22 juni 2001.

I USA har man efter terrorattackerna gjort lagändringar som innebär just detta. Andra pro-aktiva åtgärder kan omfatta utbildandet av IT-specialister inom försvaret och fortsatt arbete med säkring av kritisk infrastruktur. Det kanske viktigaste åtgärdsförslaget är att skapa medvetenhet om att icke-statliga aktörers inblandning i konflikter med IT-vapen är en del av framtida konflikter oavsett om de innebär ett störningsmoment eller reell fara för en stat.

[76] Post- och telestyrelsen, 2000, "Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering", sid. 9.

LITTERATURFÖRTECKNING

AgIW, 1998, *Rapport nr. 2: Åtgärder och skydd mot informationskrigföring – förslag till ansvarsfördelning mm.*

Breacher, M. och Willenfeldt, J., 1989, *Crisis, Conflict and Instability*, Oxford: Pergamon Press.

Chin, Woo Siew, *Malaysia: Insight into Cyberterrorism*, New Straits Times, 3 oktober 2001.

Delete, nr. 12 och 14, 2001. (Nyhetsbrev som ges ut i samverkan mellan Försvarshögskolan och Överstyrelsen för civil beredskap).

Denning, Dorothy E., 2000, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.* (http://www.afsa.org/fsj/sept00/Denning.html).

Denning, Dorothy E., 2000, *Hacktivism: An Emerging Threat to Diplomacy*, AFSA, American Foreign Service Association.

Försvarsmakten, Högkvarteret, *Försvarsmaktens strategiska omvärldsbedömande 2001-2006*, 01 600:72003.

Grennert, Josefin, 2000, *Internationell hantering av IT-hot. Är FN rätt forum?*, FOA-R—00-01578-170—SE.

Hackers target U.S. Pro-Israel Site, AP Washington, 4 november 2000.

Keohane, Robert O. och Nye, Joseph, 2001, *Power and Independence*, Third Edition, Longman: New York.

McAlearney, Shawna, *Cyberspace braces for escalation and war*, Security Wire Digest, Vol. 3, nr. 89, november 2001.

National Infrastructure Protection Center, *Increased Internet Attacks Against US Web Sites and Mail Servers Possible in Early May*, Advisory 01-009, 21 april 2001.

National Infrastructure Protection Center, *Potential Distributed Denial of Service (DDoS) Attacks*, Advisory 01-021, 17 september 2001.

Pescatore, John, Government Computer News, 25 september 2001.

Pollitt, Mark M., *Cyberterrorism – Fact or Fancy?*, Proceedings of the 20th National Information Systems Security Conferens, oktober 1997.

Post- och telestyrelsen, 2000, *Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering*.

Rubin, Jeffrey Z., Pruitt, Dean G. och Kim, Sung Hee, 1994, *Social Conflict. Escalation, Stalemate and Settlement*, New York: Random House.

Saita, Anne, *Hacktivists Eyeing U.S., Arab Cyberstrikes*, Security Wire Digest, Vol. 3, No 71, 17 september 2001.

Schwartz, John, *USA: Avoiding a Digital Pearl Harbour*, New York Times News Service, 4 oktober 2001.

Staten, Clark L. *Foreign Terrorism in the United States: Five years After the World Trade Center*, U.S. Senate Judiciary Committee, 24 februari 1998.

Vatis, Michael A., 2001, *Cyber Attacks During the Fight Against Terrorism: A Predictive Analysis*, Institute for Security Technology Studies at Dartmouth College.

Wæver, Ole, 1989, *Security, the speech act: analyzing the politics of a word*, second draft, Köpenhamn: Centre for Peace and Conflict Research.

Wray, Stefan, 1998, *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics*, A paper for the World Wide Web and Contemporary Cultural Theory Conference, Drake University. (www.nyu.edu/projects/wray/wwwhack.html).

Offentligt tryck

DS 2001:14, *Gränslösa sårbarheter – gemensam säkerhet.*

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

Webbresurser

ABC News	www.abcnews.com
AntiOnline	www.antionline.com
Arkansas Democrat-Gazette	www.ardemgaz.com
Ars Electonica	www.aec.at
Cincinatti Post	www.cincypost.com
Computer Sweden	www.computersweden.se
Computer World	www.computerworld.se
CNN fyi	http://fyi.cnn.com
Cryptome	http://cryptome.org
Dabbagh Information Technology	www.dit.net
EurActive	www.euractive.com
The Hacktivist	www.thehacktivist.com
InfoWorld	www.infoworld.com
Institute for Security Technology Studies	www.ists.dartmouth.edu
National Center for Policy Analysis	www.ncpa.org
National Infrastructure Protection Center	www.nipc.gov
Network World Fusion	www.nwfusion.com

New York University	www.nyu.edu
PBS	www.pbs.org
United States Department of Justice	www.usdoj.gov
Wired News	www.wired.com
ZNet	www.zdnet.com

Övriga källor

Greenberg, Cheryl, AIPAC Web Site Coordinator, e-brev till Magdalena Tham, 22 oktober 2001.

Stapleton, L., Smith, Charles och Wiant, John A., *Bits, Bytes and Cyber Diplomacy*. Framförande på konferensen Infowar Con 2001, Washington D.C., 6 september 2001.

AKRONYMLISTA

AIPAC	American Israel Public Affairs Committee
CIA	Central Intelligence Agency
DoS	Denial of Service
EU	Europeiska unionen
EZLN	Zapatista National Liberation Army
FBI	Federal Bureau of Investigation
FN	Förenta nationerna
IT	Informationsteknik
NATO	North Atlantic Treaty Organisation
NIPC	National Infrastructure Protection Center
PATRIOT	Provide Appropriate Tools Required to Intercept and Obstruct Terrorism
YIHAT	Young Intelligent Hackers Against Terror