SÄRTRYCK UR STRATEGISK UTBLICK 7

Internet som militär arena

En utmaning i totalförsvaret

Mikael Wedlin och Erik Westring

Beroendet av internet för samhällsviktig verksamhet ökar idag oerhört snabbt, nya tjänster utvecklas hela tiden och ersätter gamla sätt att kommunicera. Detta har också ökat internets betydelse ur försvarssynpunkt. Inhämtning av underrättelser, påverkansoperationer samt dolda militära operationer är områden där vi har kunnat se internet användas som ett nytt militärt verktyg även i fredstid. Det digitala slagfältet är därför av stor betydelse i utvecklingen av det nya totalförsvaret och Sverige behöver därför följa med i utvecklingen, tekniskt, organisatoriskt och legalt.

Att internet kan fungera som en arena även för militär verksamhet är inte någon ny tanke. När FOI började studera IT-krigföring under andra halvan av 90-talet utgick forskningen från att detta var krigföringens framtid; kanoner och krut tillhörde historien. Speciellt oroväckande var den digitala påverkan eller utslagning av vår kritiska infrastruktur som förväntades kunna ske. Nu när internetoperationer börjat bli verklighet i pågående konflikter kan vi bättre avgöra vad som utgör en realistisk framtid. Att internet skulle få en stor del i vårt dagliga liv gissade vi rätt på, det finns idag ingen del av vårt dagliga liv som inte berörs av internetkopplade system. Internetarenans påverkan på nutida konflikter har dock inte skapat det totala digitala angrepp som slagit ut hela samhällen som tidigare befarats. Istället har vi kunnat se att det har varit i fasen före själva konflikten som användningen av internet varit som störst.

Även om vi nu börjar förstå mekanismerna för krigföring på internet så är det oerhört svårt att förutse den framtida utvecklingen. Den första svenska internetbanken startade redan 1996 men det är först under de senaste fem till tio åren som utvecklingen lett till att internet de facto blivit den främsta kommunikationsvägen för bankärenden. Nästan alla de tjänster som vi idag betraktar som självklara som Google, Facebook och Youtube har skapats under de senaste 20 åren. Vad vi med god sannolikhet kan förutspå är att internet fortsätter vara en betydande infrastruktur i alla samhällssektorer och att dess betydelse också förmodligen kommer att öka. Man skulle till och med kunna gå så långt som att påstå att internet på sikt kommer att medföra större förändringar i vår livsstil än vad den industriella revolutionen gjorde under 1800-talet.

De militära utmaningarna

Internet har framför allt fyra egenskaper som skapar försvars- och säkerhetspolitiska utmaningar och särskilda militära problem:

Eftersom det med relativt enkla medel går att dölja sin sanna identitet på internet kan operationer på internet lätt förnekas. På internet är det svårt att vara säker på att någon verkligen är den personen som den utger sig för att vara. Rättslig legitimering av militär intervention gäller bara om man kan associera en militär statsaktör till det som sker; något som i grunden kan vara svårt på internet. Ur ett militärt perspektiv är detta till fördel för den som vill agera i det dolda och till nackdel för den som ska försvara sig.

Genom internet kan operationer med militära syften genomföras även på stort avstånd. Internet är en domän helt utan nationsgränser och ”förflyttning” är i princip omedelbar och utan avstånd. Detta gör att operationer på internet kan ske varifrån som helst och i princip helt utan risk för egen personal. Gränslösheten innebär också ett oklart juridiskt och folkrättsligt läge. Använder jag annans territorium om min skadliga kod placeras på mejlservers i tredje land?

Infrastrukturen för den digitala militära arenan delas även med civila. Tidigare har militära och civila hot varit väl åtskilda. Speciellt i Sverige har vi av tradition vinnlagt oss om en extra tydlig åtskillnad. På internet flyter dock de militära och civila hoten in i varandra. Detta är särskilt så eftersom det kan vara svårt att avgöra en attacks ursprung, syfte och mål: om samtliga banker i ett land plötsligt får sina webbportaler utslagna samtidigt kan antagonisten vara en annan stat som utför en krigshandling, eller några enskilda tonåringar utan något annat syfte än att provocera. Generellt är sådana händelser svåra att värdera och analysera. Detta gör det också komplicerat att avgöra

FOI Memo 6171
Godkänd av: Lena Bartholdson

Särtryck ur Strategisk utblick 7
November 2017

vilka lagar som gäller vid IT-angrepp, eller om det ens finns några. I stort sett alla konflikter runt mellanöstern har följts av intrång i webservrar. Är detta en del av de militära operationerna? Vem kan ställas till svars? Spelar det någon roll om avsändaren är militär? Sveriges största utmaning här är att fördela uppgifterna mellan Försvarsmakten och det civila försvaret.

Internet öppnar upp kostnadseffektiva möjligheter som möjliggör för asymmetrisk krigföring. Angrepp över internet är ofta till sin natur asymmetriska; även små, monetärt resurssvaga organisationer eller individer kan utföra aktioner över internet. Förmågan att genomföra internetattacker byggs till stor del upp av ren kunskap och det räcker med enstaka individer med rätt kompetens för att störa även relativt stora system. För att generera större störningar eller långsiktig skada behöver dock även angrepp över internet större resurser, både i form av underrättelseförmåga och gott om tid.

Ett tydligt exempel på detta är *Stuxnet*, angreppet på Irans nukleära program med hjälp av ett datorvirus mot anrikningsanläggningen för uran i Natanz. Genom att plantera in ett virus i styrsystemen fick man ett antal av deras centrifuger att gå sönder och inte producera något uran. Även om denna skadliga kod var ett av de mer avancerade som setts då det hittades, och var hopsatt av ett flertal olika typer av kod från flera olika programmerare, så kan man tänka sig att det skulle kunna ha skrivits av en enda enskild person med tillräckligt mycket kunskap och tid. För att skapa en framgångsrik skadlig kod av den här riktade typen behövs dock också ingående kunskaper om Irans nukleära program, detaljerade ritningar och tillgång till både den hårdvara och mjukvara man vill kunna angripa och de frekvensomformare som styr dessa. Det sistnämnda är nödvändigt för att kunna utveckla den skadliga kod som förstör centrifugen utan att de inbyggda skydden slår till. Tillgång till denna typ av resurser är det idag bara stater som har.

Även om internet möjliggör asymmetrisk krigföring är det osannolikt att någon med små resurser kan åstadkomma mer än mindre störningar. För att slå mot hela samhällssektorer krävs en mycket kvalificerad motståndare.

INTERNET SOM MILITÄRT MEDEL

Traditionella militära medel genererar oftast en större och mer förutsägbar effekt än ett cyberangrepp. Man kan som exempel på detta betrakta angreppet mot Ukrainas elförsörjning julen 2015. Angreppet var planerat åtminstone sex månader i förväg och åstadkom en störning med ett kortare avbrott där de första abonnenterna började återfå strömmen redan efter tre timmar. Traditionell bekämpning av Ukrainas elförsörjning hade rimligen gett mer permanenta skador, dessutom på ett mer förutsägbart sätt. Militära angrepp för att slå ut infrastruktur kommer sannolikt därför bara att vara ett komplement till traditionella förmågor.

Vi har dock framför allt kunnat se tre områden där internet är en intressant arena för militära operationer:

För underrättelseinhämtning. Internet torde vara varje underrättelseorganisations dröm. All information finns samlad på ett ställe, relativt enkelt åtkomlig i ett format som är möjligt att bearbeta maskinellt. Det är uppenbart att detta redan pågår i stor skala och att stora resurser allokeras för informationsinhämtning. Ett nästan övertydligt exempel på detta är de avslöjanden som Snowden gjorde för ett par år sedan. Det finns också ett flertal publicerade exempel på illegal övervakning av organisationer och individer av den kinesiska staten.

Som en plattform och medel för påverkansoperationer. Internet har förändrat våra medievanor och metoder för nyhetsinhämtning på ett fundamentalt sätt. Till skillnad från tidigare kan idag vem som helst på ett enkelt sätt vara producent av information och att identifiera avsändaren är näst intill omöjligt. Falsk information med syfte att påverka sprids med epidemisk effektivitet. Informationsflödet ökar lavinartat och aktörer i vårt närområde upprustar målinriktat på internet för att använda dessa nya digitala medier för sina geopolitiska syften. Ett oroväckande exempel är den påverkan som presidentvalet i USA utsattes för. Det är mycket troligt att framtida europeiska val kommer att utsättas för samma typ av påverkan. Exemplet med Ukrainas elförsörjning kan också betraktas som en påverkansoperation, vars syfte troligen snarare var att ingjuta osäkerhet hos befolkningen än att uppfylla något traditionellt militärt mål. Internet har således öppnat upp för nya effektivare metoder och verktyg inom påverkansoperationer och det finns all anledning att anta att omfattningen kommer att fortsätta öka.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick

Dolda operationer vid skymningsläge/gråzon. Förnekbarheten i internetbaserade operationer kan särskilt utnyttjas i de lägen man vill genomföra militära operationer utan att de uppfattas som krigshandlingar. Aktioner på internet har därför en särskild betydelse i krigsförberedande åtgärder och i så kallad förbekämpning. Det tidigare nämnda exemplet med *Stuxnet* faller typiskt in under den här kategorin. Det var en extremt avancerad och osäker operation, men vi kan anta att avsändaren inte ville eskalera motsättningen till öppen konflikt.

Sammanfattningsvis kan vi konstatera att internet som militärt medel framförallt kommer att beröra oss i fredstid.

Internationell utblick

Flera stater har numera öppet deklarerat att de förfogar över en militär internetförmåga, vilket styrker antagandet att internet kommer att vara en naturlig del av framtida militära konflikter. Ryssland har till exempel bara de senaste åren vid flera tillfällen blivit anklagade för att ha använt dataintrång som konfliktmetod. Stuxnetoperationen genomfördes sannolikt av USA och Israel, även om ingen av dem har erkänt detta. Även Iran och Kina, bland andra, har förekommit i intrångsrapporter där det är rimligt att anta att en statsaktör låg bakom intrånget.

De senaste åren har det uppdagats att stater är mycket intresserade av information avseende andra länders infrastruktur. Det finns ett antal rapporter från amerikanska myndigheter som konstaterar spår av att främmande stater har kartlagt infrastrukturen i USA. Även FRA rapporterar om 10 000 ”cyberaktiviteter” riktade mot Sverige varje månad. Enligt FRA är den övervägande delen av dessa rent spionerі och försök att komma över information, men man har också identifierat åtminstone ett försök att kartlägga svensk infrastruktur.

Efter att Estland var hårt ansatt av IT-attacker under våren 2007 bildade man något som närmast är att likna vid ett digitalt hemvärn, ”Estonian Cyber Defence League”. Syftet med detta har varit att stärka samhällets förmåga att hantera cyberangrepp samt att främja privat-offentlig samverkan.

Var står Sverige idag?

Sverige har en förhållandevis god datormognad och har arbetat aktivt med att förstärka den allmänna IT-säkerhetsnivån under de senaste 10 åren. I internationell jämförelse av risker kopplade till IT-hot ligger Sverige därför relativt bra till. Vår kritiska infrastruktur är dock inte byggd för att kunna stå emot attacker från någon med en stats resurser, varken i cyberrymden eller i den vanliga världen. Där har vi mycket kvar att göra. FOI:s IT-säkerhetsarbete har främst syftat till att höja medvetandet och att införa skydd mot de enklaste typerna av angrepp. IT-säkerhet har dock varit ett litet forskningsområde i förhållande till hur snabbt området utvecklas. Det är en utmaning att få med säkerhetsaspekterna i den snabba utvecklingen. Det finns ett stort behov av mer kvalificerad forskning.

Förändringar i omvärldsläget de senaste åren har gjort att Sverige har börjat återuppbygga det civila försvaret och totalförsvarstanken har fått ny aktualitet. De samhällsförändringar kopplade till internet som har skett sedan Sverige senast hade en totalförsvarsorganisation ställer krav på att det nya totalförsvaret även omfattar ett försvar mot digitala hot.

Rollerna för hantering av de digitala hoten behöver klaras ut och nödvändig samverkan mellan myndigheter och andra aktörer behöver utvecklas. Vems uppgift är det att släcka bränder på internet? Om militärflyg från andra länder kränker Sveriges gränser skickar Försvarsmakten ut eget flyg för att avvisa detta. Om ett tyskt godståg med kemikalier spårar ut utanför Stenungssund är det polisen och brandkåren som hanterar detta. I internetvärlden är det annorlunda, inte minst på grund av att de civila och militära hoten flyter in i varandra.

Sveriges motståndskraft mot digitala hot kommer att vara beroende av att alla i samhället samverkar. Samverkan finns redan mellan försvarsmyndigheterna och inom krishanteringssystemet. Denna samverkan behöver utvecklas ytterligare. Här måste det till en tydligare samverkan mellan polisiära och militära myndigheter och möjligheterna utökas för Försvarsmakten att stödja Polisen. Försvarsmakten är rimligtvis ansvarig för att motverka militära attacker även via internet. Dessutom måste civila leverantörer av samhällskritiska funktioner, så som mobiloperatörer eller banker, involveras i planering och hantering av hoten. Här finns en stor

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick

utmaning för det nya totalförsvaret.

Påverkansoperationer på internet utgör ett uppenbart hot mot vår demokrati och våra politiska processer. En självklarhet under uppbyggnaden av totalförsvaret är att vi bygger kompetens samt utvecklar teknik för att förstå även dessa angrepp, så att vi effektivt kan motverka också denna typ av subtil krigföring.

För att hantera de digitala hoten behövs regleringar nationellt och internationellt. Det är dock en utmaning att reglera ett så snabbt föränderligt område. Samtidigt är det viktigt att värna om öppenheten på internet. Sverige har en roll i att stå för en öppenhet som samtidigt möjliggör ansvarsutkrävande. På samma sätt som att vi har en brandkår som rycker ut vid bränder som den enskilda inte klarar att släcka själv, borde vi kanske vid större påfrestningar ha en styrka av frivilliga IT-tekniker som redan är samövade och förberedda att agera i en krissituation på ett sätt som en enskild systemägare ensam har svårt att göra.

Behöver kanske Sverige, i likhet med Estland, ett digitalt hemvärn?

Strategisk utblick 7 **finns att ladda ner från www.foi.se/om-foi/strategisk-utblick**

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
www.foi.se/om-foi/strategisk-utblick