



Socialdemokraterna

“Datorer är dagens missiler”

En rapport om förbättrad Informationssäkerhet



“We don't know when or if a cyber attack rises to the level of an armed attack”

Professor Daniel Ryan, National Defence University

Genom historien har ny teknik påverkat krigskonsten, ibland drastiskt. Några exempel är införandet av vagnen, krutet, flygmaskinen, radarn och nukleär fission. Vår tids tekniksprång heter informationsteknologi. Datorer och Internet har i grunden förändrat vår vardag, i de flesta avseenden på ett positivt sätt, men människor världen över är nu också beroende av att systemen fungerar. Det gäller även den militära förmågan. Teknikutvecklingen har fört med sig att också krigföring, såväl i det abstrakta som fysiska territoriet, i grunden har förändrats.

Idag finns möjligheten att skicka fjärrstyrda förarlösa farkoster runt om i världen för att samla in information eller attackera mål. Militärt hemligt material om Afghanistan kunde lagras på en liten plastskiva för att sedan spridas över hela världen på Wikileaks.

Samtidigt innebär redan dagens informationsteknologi att cyberspace blivit en ny arena för krigföring, men allvarligt nog saknar våra demokratiska stater tillräcklig kraft och förmåga att effektivt omsätta den insikten i konkret handling. Vi måste idag kunna ge svar på frågan; vad ett storskaligt angrepp mot digitala medier, banker eller avancerade sjukvårdssystem skulle innebära? Och framför allt; vi måste nu vara beredda att fullt ta konsekvenserna av att vi lever i ett digitalt beroende samhälle.

Vi måste inse att det är sårbarheten i vårt högteknologiska samhälle som är den främsta och säkerhetspolitiska utmaningen. Idag är kapade datorer de nya missilerna och inplanterade virus en ny tids biologiska stridsmedel. Samtidigt är det inte i första hand det fysiska territoriet som är hotat, utan funktioner och värden som vi delar med andra människor världen över. På detta slagfält har nationsgränser upphört att existera och angriparen kan vara såväl en stat som en organisation, ett företag eller en enskild individ.

Historien om den trojanska hästen är ett mytologiskt exempel på krigslist. Nu finns verkliga moderna trojanska hästar i vår tids krigskonst. Ett exempel på det är Stuxnet, den farliga datorprogramvara vilken har identifierats som ett IT-vapen med en komplexitet och precision utan tidigare motstycke.



Stuxnet är en datamask vilken upptäcktes i juli 2010 och som är specialiserad på att slå ut utvalda mål utan att märkas på sin spridningsväg genom nätet. Masken inte bara anfaller och utspionerar system för övervakning och styrning av industriprocesser – den manipulerar också systemen som den attackerar. Enligt Siemens, vars system masken attackerat, hade masken i slutet av september 2010 infiltrerat fjorton industrianläggningar. Iranska myndigheter räknar med att masken finns i cirka 30 000 datorer i landet, inklusive datorer som styr kärnkraftverk. Vem eller vad som ligger bakom Stuxnet vet ingen, men fackexperter menar att på grund av maskens komplexitet är det troligare att en stat än privatpersoner ligger bakom. Exemplet understryker att IT-angrepp i dag inte bara handlar om ekonomisk brottslighet, kreditkortbedrägeri och liknande utan att en cyberattack också kan innebära risker som ett havererat kärnkraftverk och därmed hot mot människors liv och hälsa.

Ett lokalt exempel på en cyberattack som nyligen skedde men som fick begränsad medial uppmärksamhet, var hackerattacken i Motala mot bostadsbolaget Platens datasystem som skedde i mitten av december 2010. Vad som skett upptäcktes först när de 700 hyresgästerna, ett äldreboende och ett köpcentrum blev av med värmen och människor började frysa. Någon hade lyckats ta sig in i bostadsstiftelsens datasystem och därefter lyckats påverka elva värmecentraler. Det går bara att spekulera i konsekvenserna om detta skett samordnat och i betydligt större skala mot en stads hela vatten-, el-, och värmesystem under några kalla dagar i december. Det visar på innebörden av och allvarligheten i de nya hoten och på hur sårbart vårt samhälle är.

Vi minns alla hur hårt vårt grannland Estland drabbades år 2007 av en samlad attack från utländska datorer mot centrala samhällsorgan i samband med en känslig konflikt kring ett sovjetiskt krigsminne.

Det är dessa nya digitala hotbilder som vi både civilt och militärt måste rusta samhället för. Vi behöver i högre grad inrikta försvaret av Sverige mot att möta dessa nya hot, parallellt med att det militära försvaret utvecklar sin förmåga att möta militära maktmedel.

Hemdatoren tar oss ut i världen på samma sätt som rörelsefriheten ökade när bilen blev tillgänglig för vanliga människor. Vi tycker det är självklart med trafikregler, bilbesiktningar och bestämmelser om säkrare bilar. Vem skulle t.ex. idag köpa en ny bil utan krockkudde? Det borde vara lika självklart att enskilda datorer designas så att de inte kan kapas och användas i en botnet attack. För det handlar inte bara om att enskilda användare måste lära sig att inte klicka på roliga och lockande, men ack så farliga länkar. Vi borde kunna åstadkomma en hel del genom att sätta press på hård- och mjukvarutillverkare. Enkla, små åtgärder, som att alla bilar måste utrustas med bilbälte, som sammantaget blir oerhört betydelsefullt om det alla gör det.



Ett gott exempel på vad staten kan göra är skriften ”Protecting Yourself Online – What Everyone Needs to Know” framtagen av Australiens regering. Där finns bland annat information om hur man säkerhetsanpassar sin dator och hur man agerar utifrån ett säkerhetstänkande på Internet.

Politiskt är vi överens om att Sverige ska vara en världsledande IT-nation. Nu måste vi vidga ambitionen till att vara ledande även när det gäller IT-säkerhet. Det handlar om att skydda vårt sårbara samhälle, och i förlängningen att skapa förutsättningar för en stabil ekonomi. Det krävs ett digitalt försvar av vårt digitala territorium, i den mån som det är möjligt att avgränsa.

Det här kräver ett nytänkande, eftersom IT-säkerhet berör så många frågor i samhället: försvar, energi, transporter och kommunikationer, finansmarknad. Konsekvenserna kan bli förödande, om el, kärnkraft, vattenförsörjning eller våra ekonomiska system angrips. Det är den nya digitala hotbilden. För att nå ovanstående mål behövs en politisk diskussion och utveckling av lagstiftningen om hur vi skyddar vårt samhälle. Lagstödet för skydd av vårt territorium är väl utvecklat, men det är svårt att tillämpa dessa förordningar även på informationsarenan. Det är politikens uppgift att inte stanna vid detta faktum. Det är nödvändigt att utveckla lagstiftningen för att försvara även IT-samhället mot angrepp och kränkningar.

Den förra S-regeringen gav för budgetåret 2006 PTS i uppdrag att lämna förslag på en strategi för ett säkrare Internet. Uppdraget redovisades i juli 2006 och i december samma år klubbades strategin av den då nytilträdde regeringen. Det har gått många år sedan dess om man ser i förhållande till teknikutvecklingen. Regeringen måste kontinuerligt uppdatera de statliga strategierna för informationssäkerhet så att dessa ligger i framkant och inte i bakvattnet i förhållande till den tekniska utvecklingen.

Det krävs en bättre samordning av skyddsåtgärderna och ett tydliggörande av ansvarsförhållandena på informationssäkerhetsområdet. Den senaste utredningen om informationssäkerhet pekade särskilt ut den stelbenta myndighetsstrukturen i det svenska underrättelsesamhället som ett betydande problem. Det är djupt problematiskt att frågan fortfarande är obesvarad om vilken myndighet som har ansvaret för att koordinera skyddsåtgärder om Sverige utsätts för en större cyberattack.

En förutsättning för att det ska fungera på myndighetsnivån är att det tydliggörs var inom regeringskansliet som ansvaret ytterst ligger för dessa frågor. Alla departement är berörda, men flera tunga fackdepartement är i högsta grad involverade. Det säger sig självt att det krävs ett tydligt mandat och resurser för att samordna Försvars-, utrikes-, justitie-, närings- och finansdepartementens informationssäkerhetsarbete.



Det handlar inte om att någon ska ta över andras ansvar, men de olika, ibland motstridiga, perspektiven på informationssäkerhet måste hållas samman. Samordning bygger på frivillighet och ömsesidiga intressen, men inte sällan uppstår motstridiga intressen eller rent av utpräglade särintressen varför starkare styrmedel än dagens måste tillföras.

I Sverige har vi haft en lång tradition av vad som kallats ett ”folkförsvaret” och ett medborgerligt engagemang och deltagandet i skyddet av vårt eget land. Det har tjänat två syften, dels att stärka försvarsförmågan, men också som ett starkt demokratiskt inslag i samhällsbygget. Detta är värt att bygga vidare på även i den nya tiden och för att hantera dagens och morgondagens relevanta hot.

Den orimliga elitisering av Försvarsmakten som regeringen nu driver igenom leder obönhörligen till ett litet yrkesförsvaret, till professionen i huvudsak avskilt från samhället i övrigt. Det militära försvaret av Sverige och vår gemensamma krishantering blir snabbt en angelägenhet och uppgift för bara några få anställda. Det kommer att leda till ett sämre skydd av landet. Men den frågan om FM:s personalförsörjning och de frivilliga organisationernas roll avhandlas på annan plats, inte i denna rapport.

Idén om ”folkförsvaret” måste dock vara utgångspunkten också för det digitala it-försvaret. Föreningen mellan experter, företag, myndigheter, enskilda och organiserade medborgare är det som bäst kan bygga vår nya försvarsförmåga.

IT-försvaret måste därför även utvecklas underifrån och fungera lokalt. Det som inträffar och som kan nå nivå av nationell kris kommer att ske lokalt på många platser, i hem och på arbetsplatser.

Den lägesbild som beskrivs ovan gör det angeläget att riksdagen är pådrivande för att förmå regeringen att vidta ett antal angelägna åtgärder. Det behövs en sammanhållen bred och tvärasektoriell strategi från individnivå- till nationell och internationell nivå.

INDIVIDEN

- Det är angeläget att öka enskilda medborgares kunskaper om vår sårbarhet och de hot som kan riktas mot oss, inte bara som kunder och konsumenter, utan som land. Låt ”Om kriget kommer” återuppstå med kunskap och råd till allmänheten för att stärka robustheten i våra system och hur vi ska agera när det oväntade inträffar. Allt fler söker idag viktig information via Internet. Var finns denna information idag om en cyberattack slår ut våra digitala system?
- Vi vill ha en översyn av hur informationskanalerna till allmänheten ska kunna säkras nationellt, i händelse av en större attack mot Internet.



- Identifiera nyckelpersoner i myndigheter och företag och organisera dem, som en del av ett nationellt it-försvar, med förberedda uppgifter och rutiner, som vi tidigare gjorde med krigsplacering, men idag på ett nytt slagfält, mot en betydligt mer mångfacetterad hotbild.

NATIONELLT

- Sverige ska vara en världsledande IT-nation – och i det begreppet ingår även att vara ledande när det gäller IT-säkerhet. Utan IT-säkerhet så skyddar vi inte samhället. Då hotas stabiliteten i vår ekonomi. Vi behöver därför ett effektivt digitalt försvar av vårt digitala territorium.
- Den politiska samordningen av IT-säkerhetsarbetet måste ske i statsrådsberedningen eller genom att tydligt peka ut ett ansvarigt statsråd/departement för detta, inte endast som en sidouppgift i en stor departementsportfölj. Alternativt att inrätta ett särskilt IT-säkdepartement.
- Regeringen måste omgående tydliggöra vilket departement/statsråd som har det yttersta ansvaret i händelse av en större incident på IT-säkerhetsområdet. En tydlig och väl känd ansvarsfördelning är en förutsättning för en effektiv krishantering i händelse av en större IT-störning.
- Vi vill att regeringen med tydlighet ger en myndighet i ansvar, exempelvis MSB, för att utveckla en kommunikations- och informationsstruktur för de delar av samhället som rör viktiga samhällsfunktioner. En sådan informationsstruktur skulle kunna användas för kriskommunikation inom områdena skydd mot olyckor, krisberedskap och civilt försvar.
- Vi vill se en tydlig struktur på nationell nivå för samverkan på IT-säkerhetsområdet mellan offentliga och privata aktörer. För att kunna hantera allvarliga IT-incidenter behövs en stark samverkan mellan privata och offentliga organisationer. Det kräver ett organ där berörda organisationer kan utbyta information på ett förtroendefullt sätt. Detta organ måste inkludera organisationer i alla delar av samhället där behoven finns. Ett nära operativt samarbete är nödvändigt för att klara de snabba insatser som kan krävas vid en allvarlig IT-incident.



- Lagstiftningen måste utvecklas så att den digitala hotbilden täcks in. Det behövs en politisk diskussion och utveckling av lagstiftningen om hur vi skyddar vårt samhälle på området IT-säkerhet. Lagstödet för de tre traditionella försvarsgrenarna finns i IKFN-förordningen. Dock finns det flera exempel på att det är svårt att tillämpa denna förordning även på ett fjärde område, informationsarenan. Framförallt därför att alla områden i samhället berörs. Det handlar om försvar, samhällets transporter och kommunikationer, finansmarknaden och så vidare. Därför behöver frågan om skydd mot cyberattacker utvecklas på andra juridiska grunder än via IKFN-mandat. Konsekvenserna kan dock bli lika förödande om el, kärnkraft, vattenförsörjning eller våra ekonomiska system angrips som att vi utsätts för ett militärt intrång. En statlig utredning ska se över det befintliga regelverket för både civila och militära myndigheter och se hur detta kan utvecklas för att ta ett bättre samlat grepp kring frågan.
- De statliga strategierna för IT-säkerhet måste uppdateras årligen. Detta för att den ska ligga i framkant och inte, som idag i bakvattnet i förhållande till den tekniska utvecklingen. Det kontinuerliga målet för en aktuell IT-strategi måste vara att strategiska samhällsfunktioner ska vara säkrade.
- Det behövs bättre samordning av skyddsåtgärderna och ett tydliggörande av ansvarsförhållandena på informations- och säkerhetsområdet på myndighetsnivå. Den senaste utredningen om informationssäkerhet pekade särskilt ut den stelbenta myndighetsstrukturen i det svenska underrättelsesamhället som ett betydande problem. Det är djupt problematiskt att frågan fortfarande är obesvarad om vilken myndighet som har ansvaret och kan koordinera skyddsåtgärder om Sverige utsätts för en större cyberattack. Vi föreslår att MSB får en sådan tydligt definierad uppgift. Den svenska CERTen STIC har nu vid årskiftet flyttats från PTS till MSB och det är ett viktigt första steg. Men deras mandat måste klargöras ytterligare tvärsektorielt och mellan myndigheter som har olika ansvarsområden.
- Vi vill se en politisk utredning som förutsättningslöst granskar behov, villkor, regler, förmågor och ansvar för egna offensiva kapaciteter.
- Vi vill ha en offentlig innovationsupphandling som driver fram ny teknik/metoder och som stärker svenska leverantörer av IT-säkerhet. I höstas kom en utredning som syftade till att ge myndigheter verktyg att genom funktionsupphandling, utifrån ett beskrivet problem/behov, öka efterfrågan på innovationer.



GLOBALT

- Folkkrätten måste även på den digitala arenan med högsta prioritet, juridiskt klarlägga vad en digital kränkning innebär och vad som är ett reellt digitalt angrepp? Hur bevisar man vem som har utfört attacken och vem bär ansvaret för bevisbördan? Vilka passiva och aktiva digitala motmedel ska vara tillåtna att ta till, och vem ska ha rätten att utföra dem? Vad är rimligt eller proportionerligt? Det finns många luckor och frågetecken i FN-stadgan som försvårar eller förhindrar ett effektivt försvar mot de digitala hoten. Vi efterfrågar här ett svenskt initiativ i frågan.
- Vårt ”digitala territorium” är förstås inte begränsat till vår traditionella territorialgräns. Sverige ingår i ett större digitalt globalt och europeiskt sammanhang. En viktig del av det arbetet med förbättrad IT-säkerhet behöver därför vara att aktivt och snabbare driva den europeiska agendan och samarbetet framåt. Insatser för att göra EU till en gemensam digital ekonomi med möjligheter att handla och verka på nätet oberoende av nationsgränser måste kopplas till gemensamma insatser för förbättrad IT-säkerhet i hela EU-området.
- Sverige behöver öka delaktigheten i internationella cybersäkerhetsövningar för att förbättra förmågan till ”cyber incident response”, öka samverkan mellan offentlig och privat sektor, stärka samverkan mellan de regionala, nationella och internationella nivåerna. I september förra året deltog Sverige för första gången, tillsammans med 11 andra nationer, i den internationella cybersäkerhetsövningen Cyber Storm III. Det var ett steg i rätt riktning. Vi vill betona vikten av globala cybersäkerhetsövningar, och välkomnar den första paneuropeiska övning, den så kallade [Cyber Europe 2010](#) som EUs ’IT-säkerhetsmyndighet’ ENISA nyligen genomförde, med bland andra PTS som deltagare för Sverige. Den 20 januari kommer EU och USA att mötas för att diskutera erfarenheter mer inom detta område, och för att planera för en gemensam, synkroniserad transatlantiska cybersäkerhetsövning under 2012 eller 2013 i syfte att öka det globala säkerhetsarbetet. Det är viktigt att Sverige engagerar sig i och driver på detta arbete.
- Vi vill ge i uppdrag åt MSB att vidareutveckla Computer Emergency Response Teams – en så kallad digital brandkår. En sådan funktion kan fördjupa utbytet av viktig information med andra EU-länder.



AVSLUTNING

Vi är vana att se effekterna av krig, terror och kriminalitet med våra ögon. Vi har referensramar och kan med dem bedöma allvaret i det som sker. Traditionellt är försvaret ett säkerhetspolitiskt instrument för att kunna möta andra nationers angrepp och vi är vana vid att ha mycket långa förvarningstider innan krig och konflikter bryter ut.

Med it-hoten är allt detta nu historia.

Generellt sett vet vi inte vad som sker, varför det sker, vilken omfattningen är eller vem som är aktören. Det mesta sker i det fördolda. Endast få mer omfattande exempel ges medial uppmärksamhet. Angriparen behöver inte vara en stat, angreppet kan ske på stort geografiskt avstånd, angriparen kan välja att vara dold och angreppet kan ske helt utan förvarning. Vi talar om angrepp som sker på tusendelar av en sekund.

Det är en helt ny säkerhetspolitisk karta, men fortfarande är det för många som orienterar efter den gamla kartan. Det gamla och det kända styr i stor omfattning den politiska debatten och resursfördelningen.

Just därför är det viktigt att politiken kraftsamlar för att öka våra länders och medborgares skydd. För överskådlig tid är informationssäkerhet en central del av försvaret av vårt land och vårt lands funktionalitet. Det är inget litet lyxproblem för några få särskilt it-intresserade, det är en nationell angelägenhet, med stark internationell dimension.

Som vi pekat på i denna rapport sker en hel del insatser i privata företag, på regerings- och myndighetsnivå samt internationellt. Men för länge har frågan getts för låg prioritet. Insatserna spretar, ansvarsförhållanden och regelverk är oklara och än så länge saknas helt det medborgerliga perspektivet och ansvaret.

Med vår rapport vill vi lämna ett bidrag till debatten om förbättrad och stärkt informationssäkerhet. Rapporten gör inte anspråk på att vara heltäckande, men vi vill särskilt uppmärksamma att insatser måste göras på alla tre nivåer; individ – nationellt och internationellt.

