FRAMTIDSUTSKOTTETS UTLÅTANDE 1/2013 rd

Statsrådets utredning om statsrådets principbeslut om en strategi för cybersäkerhet en i Finland

Till utrikesutskottet

INLEDNING

Remiss

Utrikesutskottet remitterade den 8 februari 2013 statsrådets utredning om statsrådets principbeslut om en strategi för cybersäkerheten i Finland (USP 2/2013 rd) till framtidsutskottet för eventuella åtgärder.

Sakkunniga

Utskottet har hört

- säkerhetsdirektör Timo Härkönen, statsrådets kansli
- generalsekreterare Aapo Cederberg, försvarsministeriet
- specialsakkunnig Yrjö Benson, finansministeriet
- verkställande direktör Ilkka Kananen, Försörjningsberedskapscentralen
- professor Aki-Mauri Huhtinen, Försvarshögskolan
- professor Rauno Kuusisto, försvarsmakten
- överinspektör Pertti Haaksluoto, skyddspolisen
- expert Hannu Kauppinen
- forskningschef Mikko Hyppönen, F-Secure Abp
- direktör Reima Päivinen, Fingrid Abp
- Head of Corporate Security Juha Härkönen, Fortum Abp
- expertchef Jussi Snellman, OP-Pohjola-gruppen
- direktör Timo Heimo, Kesko Livs Ab
- Director of Cyber Security, Doctor of Military Science Jarno Limnéll, Stonesoft Corporation
- ledande expert Mika Linna, Finansbranschens Centralförbund.

UTSKOTTETS ÖVERVÄGANDEN

Motivering

Strategin för cybersäkerheten i Finland

Strategin för cybersäkerheten i Finland är relativt lyckad, anser framtidsutskottet. Den identifierar de största förändringarna i cybermiljön och visionen går i rätt riktning.

Målet med strategin är att öka aktörernas gemensamma kunskaper om cybersäkerheten, starta samhällsomfattande säkerhets- och planeringsåtgärder, förbättra förmågan att skydda livsviktiga samhällsfunktioner, stärka trovärdigheten i vår försvarsförmåga och göra vår cybermiljö till en nationell konkurrensfördel.

Det är ingen lätt uppgift att omsätta visionen i vår multipolära och snabbt föränderliga globala omvärld. Det krävs samarbete. Ingen av de många involverade kan ensam ha kontroll över hela den cyberfysiska världen. Också allmänhetens kompetens och attityder spelar en stor roll för att upprätthålla och förbättra cybersäkerheten.

Hoten är många och därför svåra att förutse: tekniska fel, olyckor, skadegörelse, brottslighet, terrorism, spionage och rentav cyberkrig. Beroende på definition har garderingen mot cyberhot också kopplingar till elektronisk krigföring, informationskrig, psykologisk påverkan, försök att påverka nyckelpersoner, strategisk kommunikation, vilseledning, informationssäkerhet och ryktesspridning.

Det krävs god samordning och bra anvisningar för att man ska kunna gardera sig för och bekämpa cyberhot och återhämta sig från regelrätta anfall. I vissa fall kan både samordning och anvisningar bli ett nytt hot eftersom redan fritt tillgängliga telefonnummer kan avslöja den organisatoriska hierarkin hos säkerhetsmyndigheterna.

Det är hotbilderna som dominerar strategin, men samtidigt erbjuder cybermiljön en chans att satsa på hållbar utveckling. I bästa fall kan ett gott renommé och trovärdighet i cybersäkerhetsfrågor också vara till nytta för annan produktion och export i en värld som blir allt mer multipolär och inriktad på blockbildning.

Följaktligen fokuserar utskottet på följande teman:

1. Samarbete mellan offentlig och privat sektor
2. Internationellt samarbete
3. Allmänhetens roll för cybersäkerheten
4. Större kompetens i cyberfrågor
5. Kristålighet
6. Möjligheter att utnyttja cybermiljön affärsmässigt.

Utgångspunkter

Strategin innehåller en vision, en handlingsmodell och strategiska riktlinjer för cybersäkerheten. Fokus läggs på ledarskap och nationell samordning av cybersäkerheten. I år kommer dessutom ett nationellt verkställighetsprogram att läggas upp. Det ska innehålla de åtgärder som förvaltningsområdena och aktörerna är skyldiga att förbereda.

Vidare ska det avsättas ett tilläggsanslag för att bygga upp och driva ett cybersäkerhetscenter. Hur stort anslaget kommer att vara planeras in i den gemensamma genomförandeplanen. Centret ska vara i funktion dygnet runt sju dagar i veckan (24/7). Enligt en preliminär bedömning kräver det en extra resurs på ungefär tio årsverken och cirka en miljon euro.

> Framtidsutskottet anser att det brådskar med verkställighetsprogrammet för strategin, anser utskottet som ställer sig bakom förslaget att inrätta ett cybersäkerhetscenter. Centret måste få adekvata anslag.

Funktionssäkra datanät är nödvändiga för att det moderna informationssamhället ska fungera. Följaktligen är cyberhot mot kritiska företag och kritisk produktion en stor risk.

Skadegörelse, brottslighet, underrättelse och operationer på nätet har ökat i hög grad. Aldrig tidigare har det funnits så många sabotageprogram som nu. År 2010 utsattes förvaltningen och näringslivet i Finland för drygt två miljoner försök att utnyttja eller göra intrång i sårbara datasystem.

Många cyberhot (exempelvis virus, bedrägerier, identitetsstölder och överbelastningsattacker) är välkända och det finns metoder för att bekämpa dem. På senare år har det dock förekommit skräddarsydda och mycket professionellt utförda attacker mot öppna nät, och det har varit mycket svårt att komma åt dem. Statliga aktörer har varit involverade i attackerna som också riktats mot industri- och fastighetsautomation och datoriserade styrprocesser. Man räknar med att problemen kommer att öka i framtiden eftersom allt fler apparater är kopplade till nätet och därmed är potentiella föremål för cyberattacker.

Merparten av attackerna med sabotageprogram har ekonomisk vinning som mål. Virusen

sänder e-post, fiskar lösenord, kreditkortsnummer och personuppgifter, gör decentraliserade överbelastningsattacker eller stjäl information. För den stora allmänheten är keylogger det största problemet. Keyloggern registrerar alla tangenttryckningar på den kapade datorn och skickar informationen vidare. Då hamnar lösenord och e-post i fel händer. Det största problemet är dock personuppgifter och kreditkortsnummer som man skriver in när man handlar på nätet. I Finland begås det hela tiden bedrägerier med kreditkortsnummer som någon kommit över via sabotageprogram. Konsumenterna förlorar omkring 85 miljarder euro per år på grund av cyberbrottsligheten.

Flame (2012) och Red October (2013) är de mest kända spionprogrammen. De registrerar och sparar det som görs på datorn och stjäl filer. Programmen kan stjäla filer och e-post, avlyssna samtal på Skype och överlag registrera allt som görs på datorn. De kan spridas i USB-minnen och slutna lokala nätverk. Dessutom kan de också drabba smarttelefoner. I fjol avslöjades det att utländska journalister i Peking var utsatta för cyberspionage i stor skala.

I detta läge är påtryckning och cyberkonflikt mer sannolika hotbilder än fullskaligt cyberkrig. Och hotbilden är inte bara en teoretisk konstruktion eftersom alla nationella och internationella konflikter på senare tid utan undantag också har haft en cyberkoppling. Exempelvis samtidigt med kravallerna på grund av soldatstatyn i Estland 2007 skedde det en cyberattack som lamslog en rad viktiga informationssystem i landet. Attackerna pågick i mer än två veckor och riktade sig mot bland annat dagstidningar, banker och statliga webbplatser. Det handlade om överbelastningsattacker som inte avsåg att göra intrång i servrar utan att bara överbelasta dem för att de skulle bli otillgängliga. För att klara av attackerna såg sig Estland tvunget att stänga den internationella internetåtkomsten. Efter angreppen på Estland måste också Finland försvara sig mot cyberangrepp. Hos oss riktades angreppen mot bland annat Rundradion, FNB, Eniro och Suomi24.fi.

Också danska webbsidor attackerades flitigt från arabländerna i samband med Mohammedkarikatyren 2005. Den dag Irakkriget startade 2003 infekterades amerikanska och brittiska webbplatser med slagord mot alliansen. Redan under Kosovokrisen (slutet av 1990-talet) förekom det enstaka nätattacker utförda av privatpersoner.

Cyberkrig kan föras via sociala medier. Det var fallet 2011 i Nordafrika och Ryssland, och nyligen också i samband med Gazakrisen. I sociala medier och överlag i medievärlden är det inte bara fakta som spelar en roll. Det är också av vikt vilken roll fakta får i samspelet människor emellan. Största delen av informationen på internet rör sig utan någon som helst integrations- eller ursprungskontroll. Därför är det lätt att manipulera information till stora massor på internet utan att någon lägger märke till det. Folks åsikter polariseras och blir extrema när normala åsikter försvinner.

Rysslands koncept för cyberförsvar innefattar tanken att ha cybersäkerhetsstyrkor också på andra staters territorium, om det behövs. US Cyber Command samordnar den amerikanska kapaciteten och beredskapen för att säkerställa att USA och de allierade har handlingsfrihet i cyberrymden och fråntar motståndarna samma rätt. USA har uppskattningsvis 10 000 cybersoldater. Kinas cyberförsvarsstrategi bygger på att sätta in krigföring och datanätsoperationer samtidigt mot motståndarens vitala informationssystem. Enligt strategin ska dessa medel sättas in i början av en konflikt, eventuellt också i förebyggande syfte. Målet är att genomföra angrepp som lamslår ledningssystem samtidigt som man tillgriper missiler, luftattacker och tillslag från specialstyrkor mot fysiska objekt och anordningar. Kina beräknas ha upp till 160 000 cybersoldater.

> Framtidsutskottet anser att de ökande cyberhoten inte minskar risken för traditionella fysiska angrepp. Cybervapen kan också utnyttjas för att förbereda fysiska angrepp och den strategiska infrastrukturen kan trots cybervapnen fortfarande mejas ner med fysiska angrepp. Därför bör strategin för cybersäkerheten också ta fasta på att skydda informationssystem

och annan strategisk infrastruktur mot fysiska angrepp.

Till exempel kärnvapen har blivit mer användbara i takt med cyberdimensionens frammarsch. En smutsig bomb genererad av kärnvapen kan lamslå hela cyberdimensionen i tid och rum genom att använda elektromagnetisk puls.

Samarbete mellan offentlig och privat sektor

Begreppsapparaten inom cybermiljön är fortfarande splittrad och bristfällig. Aktörerna är många och därför har förmågan att upptäcka, kontrollera och reagera på datasäkerhetsincidenter ojämn kvalitet och varierar mellan olika sektorer. Därför måste processer, ansvarsfördelning och direktiv för ledning och utredning av en cyberkris förtydligas och tränas.

> Framtidsutskottet ställer sig bakom de mål för att förbättra den nationella samordningen och lägesbilden av cyberhotet som ingår i strategin för cybersäkerheten.

För att lägesbilden och samarbetet mellan myndigheterna ska kunna förbättras krävs det, enligt de sakkunniga, att distributionen av konfidentiell information preciseras och lagstiftningen ändras på vissa punkter.

> Framtidsutskottet anser att det snabbt bör utredas vilka lagändringar det behövs för att samordna cybersäkerheten och upprätthålla lägesbilden.

Ett cyberhot som verkställs kan ha omfattande konsekvenser för våra livsviktiga verksamheter. Det så kallade femminuterskriget brukar ges som exempel på hot:

1. Den första minuten stoppas transaktionerna mellan bankerna.
2. Den andra minuten stoppas största delen av kollektivtrafiken och en stor del av privatbilismen.
3. Den tredje minuten skapas det oordning i logistiksystemen för livsmedelstransporter.
4. Den fjärde minuten stoppas eller bromsas de viktigaste dataförbindelserna.
5. Den femte minuten instabiliseras stamnätet för elöverföring och genereras en global black-out.

Till en början ansågs detta hypotetiska scenario inte särskilt sannolikt av experterna. Trots det kom hackare, sannolikt från Östeuropa, åt 150 000 datorer i Nederländerna 2012 och stal 750 GB information om infrastrukturen i livsviktiga samhällsfunktioner. Dataintrånget berörde tusentals organisationer, bland annat inom ministerier, regionförvaltning, sjukhus och vattenförsörjning. Hela landet hade sannolikt kunnat lamslås med de stulna uppgifterna. Sedan dess har man haft en allvarligare inställning till ett sammanhållet cyberhot (scenarier som femminuterskriget).

Ett annat mycket uppmärksammat fall är Stuxnet (2010), som enligt vissa bedömningar hade sitt ursprung i väst. Stuxnet är ett målsökande cybervapen som i hög grad lyckades bromsa upp Irans urananrikningsprogram. Det spreds inte via datanätet utan sabotageprogrammet togs in i det slutna systemet med USB-minne. En ny approach var att anfallet genomfördes med ett programmerbart kretskort för industriautomation.

Fallet visade hur effektivt ett cybervapen kan vara. Den eftersträvade effekten nåddes med en hundadel av priset för ett militärt angrepp - och utan mänskliga offer. Därför anses Stuxnet ha startat en ny cyberera, där vi kommer ifrån hackerattacker, men i stället går mot välorganiserade och avancerade operationer som kräver stora kunskaper om industriautomation och där stater eller stora organisationer är involverade. Det finns miljoner liknande kretskort av olika märken och i de mest skilda anläggningar i varje land, också i vapensystem, och kretskorten har dålig intern datasäkerhet. Strategisk infrastruktur, exempelvis energiverk, men också datasystem inom offentlig förvaltning använder programvara som är flera decennier gamla. Ju äldre ett system är desto mer mottagligt för cyberhot är det eftersom skyddsnivån ursprungligen lagts fast enligt säkerhetskraven när det konstruerades.

> Framtidsutskottet anser att den offentliga förvaltningen och andra med relevans för försörjningsberedskapen så snabbt som möjligt bör uppdatera programvaran och informationssäkerheten för sina datasystem.

De sakkunniga anser att strategin för cybersäkerheten i mycket hög grad tar hänsyn till viktiga behov och utvecklingskrav inom offentlig sektor. En stor del av den samhällsviktiga kritiska infrastrukturen ligger emellertid på privata aktörers ansvar. Detta framhålls också i strategin. Därför krävs det nära samverkan och informationsutbyte mellan privat och offentlig sektor för att strategin ska kunna genomföras med goda resultat.

Vitala funktioner för den samlade säkerheten är bland annat ledning av staten, internationell verksamhet, Finlands försvarsförmåga, inre säkerhet, fungerande ekonomi och infrastruktur, befolkningens försörjning och funktionsförmåga samt mental kristålighet. Erfarenheterna från Estland 2007 visade att en attack mot offentliga informationssystem inte lamslår ett helt folk. Risken är betydligt större när andra informationssystem och energisystem slås ut.

> Framtidsutskottet understryker att privat sektor och strategisk infrastruktur intar en framträdande roll för att utveckla cybersäkerheten. Målet bör vara att offentlig och privat sektor etablerar bättre samarbete för att bekämpa cyberhot. Övningar är ett sätt att förbättra samarbetet mellan aktörer inom många områden.

I exempelvis Estland finns Kyberkaitse som med jämna mellanrum övar cyberattacker mot kritisk infrastruktur. Dessa trupper har också varit med vid Natos cyberövningar, där Finland hade en aktiv roll 2012. Estland inrättade Kyberkaitse efter att ha återhämtat sig från cyberattacken 2007. Senare startade Nato ett centrum för cyberförsvar (CCD COE) i Tallinn. Finland har goda relationer med centret och både Finland och Sverige har inbjudits att bli associerade medlemmar.

Hotbilderna inom handel och industri lyfter fram störningar i logistik, informationssystem och energiproduktion. Störningar kan bero på bland annat skadegörelse, brottslighet, olyckor, tekniska fel och extrema naturfenomen. Företrädare för handel och industri anser att beredskapen för cyberrisker inom privat sektor och strategisk infrastruktur bör integreras i de normala beredskapsåtgärderna, eftersom samma metoder tillämpas vid ett flertal olika störningar. Cyberattacker, vattenskador, bränder eller exempelvis stormar har samma konsekvenser för data- och energinätet. Därför bör beredskapsåtgärderna inför cyberhot ingå i företagens normala varningssystem. Det är komplicerat, medför extra arbete och orsakar onödiga kostnader att bygga särskilda varningssystem.

> Framtidsutskottet anser att åtgärder inför cyberrisker måste övas och utvecklas inom ramen för den normala riskberedskapen.

Vardagens informationssamhälle är en viktig utvecklingstrend i den framtida cyberfysiska miljön. Det betyder att fler och fler apparater och produkter har smarta egenskaper och att de kan avläsas beröringsfritt eller kopplade till nätet på något annat sätt. Stuxnet (2010), Flame (2012) och Red October (2013) är exempel på sabotageprogram som är inriktade på denna nya infrastruktur och omvärld. De kan finnas i slutna lokala nätverk, kretskort inom industrin och i anläggningar, men också i smarttelefoner. Här är datasäkerheten inte på samma höga nivå som i datorer. Problem kan uppstå med juridiken och användningen kring material på nätet. Vilket lands lagstiftning ska tillämpas på globala webbtjänster och molntjänster?

> Framtidsutskottet understryker att Finland måste undersöka och utreda noga vilka cyberrisker och cybermöjligheter som är förknippade med vardagens informationssamhälle.

Internationellt samarbete

Cybermiljön är global. Därför går det inte att få kontroll över riskerna eller att gripa tag i möjligheterna bara på nationell nivå. Den cyberfysiska miljön blir ännu mer komplicerad om varje land satsar på egna säkerhetslösningar.

Inom bland annat elnät och banksystem behövs det internationellt samarbete. I Finland går 75 procent av elektriciteten via Fingridnät som har direkt kontakt med Ryssland, Sverige, Norge och Estland. Vårt elnät kan påverkas från utlandet och det kan utsättas för attacker när någon försöker komma åt energinätet i något annat land, exempelvis Ryssland eller Estland.

Modern banking bygger på helt och hållet automatiserad hantering av elektroniska data. Därför är fungerande informationssystem A och O för alla vitala bankfunktioner. Efter övergången till det enhetliga betalningssystemet i euro (SEPA) är en betydande del av systemen för betalningar mellan bankgrupperna allmäneuropeiska, till exempel clearingtjänsten EBA clearing och Europeiska centralbankens system Target2 för överföring av marginaler mellan banker.

En attack mot banksystemet i Finland behöver alltså inte rikta sig mot Finland, utan mot bankernas gemensamma servicecentrum någon annanstans i Europa eller rentav på någon annan kontinent.

> Framtidsutskottet anser att den internationella cybersäkerheten måste förbättras i samarbete med internationella nätverk. Det går inte att få kontroll över hot bara med nationella åtgärder.

Auktoritativa samarbetspartner är exempelvis Natos centrum för cyberförsvar (CCD COE) i Tallinn och European Network and Information Security Agency (ENISA).

Allmänhetens roll för cybersäkerheten

Informations- och kommunikationstekniken har utvecklats snabbt och e-tjänster finns tillgängliga på terminaler oberoende av tid och rum. I ett modernt informationssamhälle hör allsidig bearbetning och diversifierat utnyttjande av data som allmänheten och näringslivet behöver till de viktigaste framgångsfaktorerna. Smarttelefonerna och trådlösa nättjänster har gett upphov till det som kallas sakernas Internet, en omvärld där saker och apparater kan ha kontakt med varandra och med databaser och molntjänster. Fler och fler funktioner är automatiserade. Det handlar inte bara om tekniska omställningar, utan också om sociala och kulturella förändringar som får genomslag i människors och organisationers strukturer, handlingsmodeller, levnadsvanor och värderingar.

Den cyberfysiska miljön är inte begränsad till någon bestämd teknik eller vara den virtuella omvärlden. Den handlar inte bara om säkerheten för förvaltningens och den strategiska infrastrukturens informationssystem. Vi har att göra med kulturella och sociala fenomen i det moderna informationssamhället och de är djupt förankrade i människors individuella livsstil. Allt detta är svårt att kontrollera med politiska medel. Den cyberfysiska miljön kan bara till viss del regleras av den offentliga förvaltningen.

> Framtidsutskottet understryker att cybersäkerhet framför allt ska ses som ett samhälleligt, kulturellt och socialt fenomen, och inte bara som en teknisk lösning.

Allmänheten spelar en stor roll för cybersäkerheten. Så är exempelvis största delen av all e-post skräppost och största delen av skräpposten kommer via infekterade datorer. Också största delen av sabotageprogrammen är riktade mot allmänheten och de är ute efter ekonomiska fördelar antingen genom bedrägeri eller stöld av lösenord. Därför har människor attityder, vanor och medvetenhet stor betydelse för hur cybersäkerheten ser hemma och på jobbet. Att uppdatera antivirusprogram, tänka på hur man använder USB-minnen och vara på sin vakt med internet och e-post spelar en stor roll för cybersäkerheten i vardagen.

I mars 2013 gjordes den största överbelastningsattacken hittills mot tjänstetillhandahållaren Cloud Fares server Spam Hous. Cloud Fare är specialiserat på spamfilter. Attacken utnyttjade namnservern Resolver som används av före-

tag och operatörer. Över hundra finländska servrar involverades i attacken. Men kärnan i spridningen av spam och överbelastningsattacken bestod av flera miljoner infekterade hemdatorer.

> Framtidsutskottet anser att allmänheten måste engageras i arbetet för att förbättra cybersäkerheten och att cybersäkerhet måste bli en färdighet som alla behärskar i vardagens moderna informationssamhälle.

Större kompetens i cyberfrågor

Strategin understryker vikten av organisering, anpassning till situationen, nya förmågor, förståelse för vad den nya miljön innebär och anpassning av beslutsmaskineriet till den nya miljön. Allt detta samarbete och uppdatering av lägesbilden kräver att aktörer inom många områden får råd och utbildning.

Det behövs högkvalitativ teknik och kompetens om programvara. För att få den kompetensen behövs det satsningar på utbildning, forskning och utveckling. Även om strategin just nu inte så mycket går in på sociala och kulturella modeller och strukturer, kommer det i framtiden för cybersäkerheten att behövas många personer som inte har teknisk utbildning.

A och O är att öka kompetensen om cybersäkerhet på alla nivåer i företag och organisationer, från ledningen till verkstadsgolvet, och bland den stora allmänheten.

> Framtidsutskottet understryker att det också behövs satsningar på forskning, utbildning och produktutveckling för att kunna genomföra strategin för cybersäkerheten.

Ett bra exempel på forskning och utbildning i cyberfrågor är det brett upplagda utbildningsprogrammet i informationssäkerhet inom program- och datatrafikteknik som Jyväskylä universitet startade redan 2011.

Kristålighet

Risken är störst vid utlagda verksamheter. Vapenmakterna i västvärlden är kapabla att skydda och säkra sitt eget ledningssystem, men strategiska partner och underleverantörer av teknik och underhåll till vapensystemen är ett problem.

Så krävs det styrning av miljontals datorer och miljontals uppdateringar av program för att det högteknologiska flygplanet F-35 ska fungera. Hur kan man försäkra sig om att programvaran inte har bakdörrar och att det inte sker dominoeffekter? Att styra planet är som att använda en iPad. Därför behöver den som gör en attack inte förstå sig på hela systemet. Det räcker med att veta hur man stör systemet.

Det går inte längre att kontrollera vare sig interna cyberhot i det civila samhället eller internationella cyberhot med hjälp av lagstiftning. Risker kan inte motverkas fullt ut. Vi måste acceptera att cyberhot redan nu är potentiella risker i vitala samhällsfunktioner. Om de blir verklighet är det allra viktigaste att snabbt återställa de livsviktiga samhällsfunktionerna eller så måste det finnas reservsystem.

> Framtidsutskottet anser att Finland bör räkna med att det kommer att krävas kristålighet i cyberfrågor, att vi måste lära oss återhämta oss från störningar och att våra vitala funktioner måste ha kapacitet att klara av mycket olika och tidsmässigt varierande störningar i cybersäkerheten.

Det är ett kompetensbehov som genomsyrar hela samhället. Hur ska vi återhämta oss och klara oss, om vi av en eller annan orsak måste vara utan vatten, el, ljus, pengar, mat från butiken, kollektivtrafik, bränsle, mediciner och annat?

Affärsmöjligheter i anslutning till cybermiljön

Som ett litet, kompetent och samarbetsvilligt land har Finland utmärkta förutsättningar att bli en föregångare i cybersäkerhet. Vi har en stark kompetensplattform och långa traditioner av intensivt och förtroendefullt samarbete mellan dels privat och offentlig sektor, dels förvalt-

ningsområdena. Vår infrastruktur och förvaltning är stabila.

Cybermiljön är alltså inte bara hot. Den är också en möjlighet och en resurs. En säker cybermiljö stimulerar den ekonomiska aktiviteten. Cybersäkerheten i sig är en ny och växande affärsgren. En säker omvärld gör dessutom Finland mer attraktivt för internationella investeringar.

I cybervärlden är inte storlek och massa några dominerande konkurrensfaktorer. I stället bygger framgång i allt högre grad på kompetens. Supermakterna dominerar inte cybermiljön helt och hållet trots att de har stora resurser att röra sig med. Också små länder som Finland kan skaffa sig kompetens på hög nivå och utvecklas inom många sektorer av cybersäkerheten.

I ett land med gott skydd mot cyberhot är det säkert att placera sin produktion. En intressant möjlighet erbjuder sabotageprogram och bakdörrar som Stuxnet och den misstänksamhet de väcker. Man kan nämligen fråga sig om köparna av civil och militär utrustning i framtiden kommer att lita på att den inte har dolda egenskaper. En sådan global atmosfär av misstro kan vara till fördel för ett litet och erkänt neutralt och öppet land som Finland med stabil förvaltning. Alla kan lita på våra varor.

De största möjligheterna att utnyttja den cyberfysiska miljön ekonomiskt handlar om hur cybersäkerheten kan bli ett mervärde i den strategiska infrastrukturen och därmed i företagens omvärld, och i all teknik som tillverkas i Finland. Cybersäkerheten kan bli en stor exportprodukt.

Strategin går inte i tillräckligt hög grad in på möjligheterna med den cyberfysiska miljön.

> Framtidsutskottet föreslår att berörda aktörer, privata och offentliga, i nästa steg utarbetar en cyberstrategi som också tar fasta på möjligheterna.

Ställningstagande

Framtidsutskottet anför

> *att utrikesutskottet bör beakta det som sägs ovan.*

Helsingfors den 3 april 2013

I den avgörande behandlingen deltog

ordf. Päivi Lipponen /sd
vordf. Oras Tynkkynen /gröna
medl. Mikko Alatalo /cent
Olli Immonen /saf (delvis)
Harri Jaskari /saml
Kalle Jokinen /saml
Mikael Jungner /sd
Markus Mustajärvi /vg
Jaana Pelkonen /saml (delvis)
Juha Sipilä /cent
Stefan Wallin /sv (delvis)
Sinuhe Wallinheimo /saml
Ville Vähämäki /saf
ers. Jouko Jääskeläinen /kd
Mika Niikko /saf.

Sekreterare var

utskottsråd Paula Tiihonen
ständig expert Olli Hietanen.