Cecilia Malmström
Tal vid Folk och Försvars rikskonferens
Sälen den 16 januari 2011

DET TALADE ORDET GÄLLER

Cyberhot och EU:s inre säkerhetsstrategi

Mina damer och herrar,

Att åka till Sälen från Bryssel för att sen fortsätta till Strasbourg och EU-parlamentet är inte den enklaste resan, men det var ändå självklart för mig att prioritera den här konferensen. Och det är av två skäl.

För det första är det ett utmärkt tillfälle att träffa gamla och nya vänner för att diskutera säkerhetspolitik. Något som jag aldrig kan få nog av.

Det andra skälet – och här vill jag lovorda Folk och Försvar för sin ständiga förmåga att följa säkerhetspolitiska trender – är det fokus som årets konferens har på cyberbrott och cybersäkerhet.

För mig är detta något av det viktigaste jag har att hantera under min mandatperiod. Men det är ingen isolerad fråga. Som vi alla vet är Internet alltmer en inspirationskälla och arena för både organiserad brottslighet och terrorism.

I dagens Europa, i dagens Sverige, lever vi under ständiga säkerhetshot. Det blev kanske särskilt tydligt i Stockholm i december, med terrorattentatet mitt i julhandeln. Resultatet hade kunnat bli långt mycket värre än det blev, men det visar ändå tyvärr att terrorhotet är verkligt och att terrorister kan slå till också hos oss.

I ljuset av terrordåd uppstår ofta krav på kraftfulla åtgärder. Men ogenomtänkta och framhastade förslag riskerar bara att ge terroristerna ett kvitto på att de uppnått sitt mål: att vi ska styras av rädsla.

Jag är därför glad att Sveriges regering agerat sansat efter december-attacken och undviker drastiska och reaktiva förslag.

Att vi många gånger ändrar policy efter olika dåd är i grunden mänskligt och logiskt, men samtidigt medför det en risk att vi överreagerar och fattar för långtgående beslut utan att tänka över konsekvenserna ordentligt.

Det här är frågor som kräver långsiktigt, strategiskt och kontinuerligt arbete. Förra året lade jag fram flera förslag för att bättre bekämpa och förebygga terrorism på EU-nivå, inklusive för hur vi bättre kan möta radikalisering, och jag kommer att fortsätta arbeta med detta de kommande åren.

Jag ser attentatet i Stockholm som ett av många tecken på att dagens säkerhetshot är ihopkopplade. Radikalisering som leder till terrorattacker sker ofta på Internet. Där utbyts information och inspiration som kan leda till fruktansvärda våldsdåd. Där frodas också organiserad brottslighet.

Dessa kopplingar är viktiga, för bara genom att uppmärksamma dem kan vi bedriva en effektiv säkerhetspolitik.

Inom EU har säkerhetspolitiken alltför länge varit offer för en stuprörsmentalitet, där varje säkerhetshot ansetts isolerat och hanterats för sig. Terrorism är bara ett exempel.

Då det uppdagades sprängämnen i skrivare i flygplan från Jemen i höstas blev det initialt konflikt om det var en transportfråga, en utrikesfråga eller en säkerhetsfråga att hantera. Denna gång undvek vi misstaget och har från EU:s sida tagit fram en gemensam strategi tillsammans.

Ett av de tydligaste argumenten för att vi behöver ett bredare angreppssätt till säkerhetsfrågor är faktiskt just Internet, som är en ny arena för såväl brottslingar som terrorister, och som – om det används i skadligt syfte – också kan leda till stora säkerhetsbrister och humanitära katastrofer.

Det är idag tydligare än någonsin att säkerhetspolitiken måste bli mer mångfacetterad och lämna de traditionella stuprören därhän.

Nyligen presenterade jag därför en ny inre säkerhetsstrategi för Europa, med 41 konkreta åtgärder för de kommande fyra åren och med tydliga riktlinjer för vem som ska göra vad och när.

Åtgärderna har koncentrerats till fem områden där vi ser behov av ökat samarbete inom EU:

- Organiserad brottslighet
- Terrorism
- Krishantering
- Gränssamarbete
- Cyberbrott och cybersäkerhet

Strategin är den första av sitt slag, eftersom den tar ett helhetsgrepp kring säkerhet och lämnar en traditionellt reaktiv hållning inom EU för en mer proaktiv och strategisk europeisk säkerhetspolitik.

* * *

Att cyberbrott och cybersäkerhet skulle vara ett av de fem huvudområdena i strategin var först ingen självklarhet. Men ju längre

arbetet gick kände jag att cyberhotet inte enbart kunde rymmas under organiserad brottslighet. Vi måste fokusera särskilt på cyberfrågorna.

Men att arbeta med dessa frågor är inte enkelt.

Googles VD Erik Schmidt påstås ha sagt att Internet är den första sak mänskligheten har byggt som vi själva inte förstår.

Det är naturligtvis svårt för en politiker att erkänna det – vi vill ju gärna framstå som att vi har svar på allt – men Erik Schmidt sätter fingret på en ödmjukhet jag tror vi måste ha inför internetfrågor.

Internet har förändrat och fortsätter att förändra vår värld. Jag är inte säker på att dagens kompasser leder oss rätt i en ny digital verklighet. Det händer oerhört mycket på detta område hela tiden, och det är till viss del en färd ut i det okända.

Internet kommer att fortsätta öppna upp fantastiska möjligheter, men också ställa krav på att vi politiker hänger med i utvecklingen.

Att arbeta mot cyberbrott innebär att se de dåliga sidorna av Internet. Vi ser just nu en lavinartad trend där allt fler brott sker med hjälp av Internet. Det handlar om allt från att stjäla kontokortsuppgifter eller sjukhusjournaler till en helt ny form av brott där nätet används för

storskaliga attacker och kan slå ut myndigheter, företag eller hela länder.

Och det är inte lite skada man kan göra. De senaste månaderna har väl vi alla försökt följa viruset Stuxnet som attackerat infrastruktur och industri runt om i världen. Inte ens Microsoft trodde ett sådant kraftigt virus var möjligt innan det upptäcktes. Jag har till och med hört experter säga att det känns som något hämtat ur en Hollywood-film.

Vi behöver inte gå längre tillbaka i tiden än till mars 2009 och den attack som involverade 103 länder – flera av dem EU-länder – för att hitta andra oroväckande exempel. Eller för den delen attackerna mot Estland och Georgien 2007 respektive 2008.

Alla dessa attacker måste tas på högsta allvar. Oavsett om det är ett land, den svenska börsen eller ett känsligt patientregister på Karolinska sjukhuset som är målet, så skulle det få stora konsekvenser för våra medborgare.

Den gamla bilden av att det är en sjuttonåring som sitter i källaren hos mamma och pappa och hackar sig in i Pentagons system stämmer helt enkelt inte särskilt bra. Cyberbrott blir istället en allt viktigare verksamhet för den organiserade brottsligheten.

* * *

Tyvärr verkar brott som sker över Internet ofta vara svårare att komma åt än andra brott. Men varför är det så? Det finns flera skäl, men låt mig nämna tre.

För det första måste vi erkänna för oss själva att verktygen för brottsbekämpande arbete måste vässas för att kunna möta de nya cyberhoten. Idag lägger de flesta EU-länder alldeles för små resurser på detta. Det gladde mig därför att statsminister Fredrik Reinfeldt i sin regeringsförklaring i höstas markerade att kampen mot internetbrott ska prioriteras i Sverige.

För det andra ser vi en tendens att de företag som råkar ut för cyberattacker sällan anmäler detta till polisen. Har en kund förlorat pengar i ett kontokortbedrägeri är det ofta lättare att ersätta honom eller henne.

Men då varnas inte andra aktörer och polisen kan inte nysta upp dessa brott. Därigenom underlättar företagen indirekt för den organiserade brottsligheten som får fortsätta att utveckla sin verksamhet – och cyberbrott är nu en av den organiserade brottslighetens främsta inkomstkällor.

Genom att stoppa huvudet i sanden löser vi inga problem. Problemen måste upp till ytan för att kunna bekämpas. Utan ett bra samarbete

mellan företagen och myndigheterna kommer nätbrottslingarna att vinna.

Det för mig till det tredje skälet, som är statistik. Jag är bekymrad över att vi får alldeles för dålig statistik om antalet cyberattacker och därmed får svårt att se större mönster. Vi måste istället göra det lättare för människor att anmäla brott och incidenter på Internet.

* * *

Mina damer och herrar,

Jag får ibland frågan om EU verkligen ska hålla på med den ena eller den andra frågan, och om vi inte ska låta EU-länderna själva hantera de problem vi står inför. Det är viktigt att alltid ställa sig den frågan och resonera över det eventuella europeiska mervärdet att ta sig an en fråga på EU-nivå. Men jag tror att få människor kan förneka att mot något så gränsöverskridande som cyberbrott måste vi jobba tillsammans.

En person kan sitta vid en dator Nederländerna och använda infekterade datorer – eller zombies som jag förstår att detta kallas i IT-kretsar – i nästan hela Europa för att genomföra en attack mot en brittisk bank.

Då är en rimlig fråga vad EU gör för att komma tillrätta med dessa problem?

Jag skulle vilja svara trefaldigt:

1. Lagstiftning
2. Praktiskt samarbete inom EU
3. Samarbete med andra likasinnade partners

Förra året, under mitt första år som EU-kommissionär, lade jag fram ett **lagförslag** som handlar om att bekämpa storskaliga IT-attacker. Jag vill att:

- Det blir förbjudet att tillverka, äga eller sälja så kallade botnets.
- Straffskalorna för sådana här brott skärps. Detta är inte enbart för att ge en signal om brottens allvarliga karaktär. Det handlar lika mycket om att högre straffskalor ger myndigheter större resurser att hantera dessa brott.
- De nationella polismyndigheterna blir snabbare på att hjälpa varandra över gränserna.

Lagstiftning är förstås en förutsättning för att kunna bekämpa brott på EU-nivå, men i lika hög grad handlar det om att främja det **praktiska samarbetet**. Och det är just det som är utgångspunkten i den inre säkerhetsstrategin.

EU:s polismyndighet EUROPOL ska utveckla sin förmåga att hantera cyberbrott. För närvarande koordinerar de flera brottsutredningar, och det är ett utmärkt exempel på europeiskt samarbete.

Men jag skulle gärna gå längre och se att man på EUROPOL skapar ett cyberbrottcenter som ska fungera både operativt och analytiskt. Ett sådant center skulle kunna bli en viktig komponent i Europas arbete mot cyberbrottsligheten. Det skulle arbeta nära såväl internationella partners som EU:s myndighet för informationssäkerhet, ENISA.

Nu fungerar ENISA för all del ännu inte helt tillfredsställande. Men i september la EU-kommissionen ett förslag om att stärka ENISA genom att ge dem mer resurser och öka befogenheterna. Ett stärkt ENISA är viktigt för att öka informationssäkerheten i Europa.

Tidigare fanns det till exempel inget samarbete mellan ENISA och EUROPOL. Detta ändrar vi nu.

Men även om vi kan göra en del från EU:s sida ligger huvudansvaret hos varje enskild regering. Nationella polis- och åklagarmyndigheter måste utveckla sina kunskaper och förmåga att snabbt kunna genomföra brottsutredningar.

Det finns ytterligare en viktig grupp av aktörer som vi inte får glömma: företagen. Nationella regeringar och EU:s institutioner kan inte göra allt själva. Företagen har stor kunskap om hur de försvarar sina system och vilken säkerhet kunderna behöver. Min slutsats är att vi behöver arbeta mer med branschföretagen för att hitta långsiktiga lösningar.

Jag vill därför uppmuntra företagen att fortsätta arbeta för ökad säkerhet. Precis som vi införde bilbälte för att öka säkerheten i bilen skulle vi kanske kunna få företagen att utveckla virtuella bilbälten för alla som har en dator.

För låt oss inte glömma att även om många av oss vet hur vi skyddar våra datorer, så måste även våra föräldrar och mor- och farföräldrar känna sig lika trygga med att betala en räkning över internet som med att gå till banken.

Och så den tredje komponenten. Vi behöver bli bättre på att **samarbeta internationellt**. Helt enkelt eftersom globala utmaningar kräver globala lösningar.

EU-samarbete är viktigt men ensamma kan vi inte lösa alla problem. Vid toppmötet mellan EU och USA i november upprättade vi en arbetsgrupp för att gemensamt se hur vi kan bli bättre på att möta

cyberhotet. Arbetsgruppen lanserade jag i Washington strax innan jul tillsammans med min amerikanska kollega Janet Napolitano.

Vi ska presentera konkreta resultat inom ett år. Detta handlar om allt från att förbereda gemensamma cyberövningar till krafttag för att möta cyberkriminaliteten. Detta kommer att ställa höga krav på oss. Men jag är övertygad om att vi kommer leverera.

Men EU måste också samarbeta bättre med Nato.

På cyberområdet har det fram till nu inte funnits en dialog mellan EU och Nato. Jag beklagar detta. Inträffar en attack kommer vi i många fall inte omedelbart veta om det är ett land, en terroristorganisation eller organiserad brottslighet som ligger bakom – det finns många aktörer som kan ha ett intresse av att orsaka samma skada.

Cyberhotet är både civilt och militärt och jag har därför tagit initiativ till en dialog med Nato om hur vi kan samordna oss bättre.

Nato tar just nu fram en övergripande policy om cyberförsvar. Den ska vara klar i juni detta år. Även om vi delvis fokuserar på olika saker, givet de olika uppgifter EU och Nato har, finns det tydliga gemensamma intressen.

Att skydda kritisk infrastruktur är till exempel en viktig del av det civila krisförebyggande arbete vi gör inom EU, men också en viktig försvarspolitisk insats som har direkt relevans för Nato.

Jag kommer därför aktivt verka för en nära dialog mellan EU och Nato de kommande månaderna.

* * *

Låt mig slutligen återvända till Googles VD Erik Schmidt, som menar att internet är det första mänskligheten har byggt som vi inte själva förstår. Men det var faktiskt bara halva citatet. Han fortsatte:

"Det är det största experimentet i anarki vi gjort".

Det är möjligt att han har rätt. Sant är att internet är ett fantastiskt frihetsprojekt. Men även frihet förutsätter vissa regler.

Och arbetet med cyberfrågor innebär svåra avvägningar. Jag såg att jag i en IT-tidning fick en guldvåg i julklapp. Den skulle vara till för att väga alla mina framtida ord om nätintegritet.

Detta är belysande för att frågorna om personlig integritet fått stor vikt i diskussionerna om utvecklingen av Internet. Jag välkomnar detta, som liberal är jag den första att framhålla den personliga integriteten.

Men vi måste vara medvetna om att vi står inför svåra avvägningar och att många Internetfrågor i stor utsträckning är ny mark, som Schmidt framhåller.

Vi måste både värna den personliga integriteten och beivra brott och bekämpa övergrepp, och detta ställer oss inför ständiga frågor om vad som proportionerligt. Men jag tror att det är viktigt att komma ihåg att det som är ett brott i övriga samhället också är brottsligt på Internet.

* * *

Mina damer och herrar,

Det jag vill uppnå är ett Internet som är säkert. Ett Internet som ska kunna användas tryggt av alla. Det innebär att vi måste ta ett gemensamt ansvar för nätet och inte låta den organiserade brottsligheten – eller terrorister för den delen – få fritt spelrum.

Bara om vi litar på att våra kontokortsnummer inte kapas vågar vi betala över Internet.

Bara om vi har säkra system vågar vi digitalisera allt mer av myndigheters och företags arbete.

Och bara genom samverkan inom EU men även med USA och Nato kan vi bygga långsiktiga lösningar för att möta det växande cyberhotet.

Detta kommer jag att arbeta för de kommande fyra åren. Men vi måste jobba tillsammans. Bara genom samarbete kan vi få ett säkrare Internet och därigenom ett säkrare samhälle.

Tack.