Tal vid konferensen Internetdagarna i Stockholm den 26 oktober

CHECK AGAINST DELIVERY / DET TALADE ORDET GÄLLER

Hur skyddar vi Europa mot det ökande cyberhotet?

Mina damer och herrar,

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 vi måste ha inför Internetfrågor.

Som EU-kommissionär arbetar jag mot den organiserade och gränsöverskridande brottsligheten, som trafficking, drogsmuggling och illegal vapenhandel. Det innebär också att jag fått möjligheten att ta mig an Internetbrottslighet inom EU.

I detta arbete tar jag med mig den ödmjukhet Schmidt påminner oss om. Internet har förändrat och fortsätter att förändra vår värld. Jag är inte säker att dagens kompasser leder oss rätt i en ny digital verklighet. Det händer oerhört mycket på detta område, och det är till viss del en färd ut i det okända. Internet kommer att fortsätta att öppna upp fantastiska möjligheter, men också ställa krav på att vi politiker hänger med i utvecklingen. Just därför vill jag tacka .SE för att ha blivit inbjuden hit idag.

* * *

Att arbeta mot cyberbrott innebär att man bara ser de dåliga sidorna av Internet. Men det är nog så viktigt att vi också tar oss an Internets skuggsida. Vi ser just nu en lavinartad trend där allt fler brott sker med hjälp av Internet. Det handlar om allt från att stjäla kontokortsuppgifter till en helt ny form av brott där nätet används för storskaliga attacker.

Och det är inte lite skada man kan göra. De senaste månaderna har väl vi alla försökt följa viruset Stuxnet. Ett virus som inte ens Microsoft trodde 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 – inklusive flera från EU – för att hitta andra oroväckande exempel. Eller för den delen attackerna mot Estland och Litauen 2007 respektive 2008.

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

Om man tar in allt detta blir det svårt att inte sätta cyberfrågorna högt på dagordningen.

* * *

Den gamla bilden om att det är en femtonåring 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.

Också för terroristorganisationer erbjuder Internet oanade möjligheter. Det handlar om allt från att förmedla budskap och att uppvigla människor till att genomföra terroristattacker via nätet.

Det är faktiskt så illa att vi ligger steget efter den organiserade brottsligheten och andra negativa krafter. 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 cyberbrotten. Alldeles för små resurser läggs idag inom de flesta EU-länder på detta. Det gladde mig därför att statsminister Reinfeldt i sin

regeringsförklaring markerade att kampen mot Internetbrott ska prioriteras i Sverige.

För det andra så ser vi en tendens att de företag – men även statliga institutioner – 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. Internetbrott är nu en av den organiserade brottslighetens främsta inkomstkällor.

Här ligger också en förståelig problematik i att om vi är ärliga med de hot Internet står inför så blir folk oroliga och vågar kanske inte riktigt lita på den digitala världen. Men genom att stoppa huvudet i sanden löser vi inga problem. Problemen måste upp till ytan för att kunna

bekämpas. Utan att bra samarbete mellan företagen och myndigheterna kommer cyberbrottslingarna att vinna.

Det för mig till det tredje skälet, som är statistik. Det bekymrar mig att vi får alldeles för dålig statistik om antalet cyberattacker. Detta gör att vi får svårt att se större mönster. Därför är det viktigt att diskutera hur vi möjliggör för människor att anmäla brott och incidenter på Internet på ett enklare sätt än idag.

* * *

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. 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, 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?

Allra viktigast är att vi gör samarbete mellan brottsbekämpande myndigheter möjligt. För detta behövs gemensam lagstiftning. Därför presenterade jag för några veckor sedan ett lagförslag som handlar om att bekämpa storskaliga IT-attacker. Förslaget innehåller framför allt:

- Att det blir förbjudet att tillverka, inneha eller sälja så kallade botnets.
- Att 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.

- Att polismyndigheterna blir snabbare med att hjälpa andra EU-länder i brottsbekämpning.

Dessutom ska EU:s polismyndighet EUROPOL utveckla sin förmåga att hantera cyberbrott. För närvarande finns flera brottsutredningar som koordineras därifrån. Jag tycker att detta är ett utmärkt exempel på europeiskt samarbete.

Men jag skulle gärna gå längre och se att man på EUROPOL skapar ett cyberbrottcenter. Centret bör ha både en operativ och en analytisk förmåga. 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 för några veckor sedan lade vi i kommissionen ett förslag om att stärka ENISA – både för att ge mer resurser och öka befogenheterna.

Tidigare fanns det till exempel inget samarbete mellan ENISA och EUROPOL. Detta ändrar vi nu. Ett stärkt ENISA är viktigt för att öka informationssäkerheten i Europa.

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.

Men det finns en ytterligare viktig aktör som vi inte får glömma: företagen. Nationella regeringar och EU kan inte göra allt själva. Min slutsats är att vi behöver arbeta mer med branschföretagen för att hitta långsiktiga lösningar. Varför är då det så viktigt?

Företagen har stor kunskap om hur man försvarar sina system och vilken säkerhet kunderna behöver. Som jag nämnde tidigare har även god insikt i de hot och attacker som genomförts.

Jag skulle även vilja uppmuntra företagen att fortsätta arbeta för säkerhetslösningar. 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 er vet hur man skyddar sin dator, så måste även våra mor- och farföräldrar känna sig lika trygga med att betala en räkning över Internet som med att gå till banken.

Idag är det oftast den enskilde medborgaren som får betala priset när systemet inte fungerar. Det kan handla om allt från en infekterad dator som blir långsam eller måste bytas ut till att vi ständigt behöver köpa nya säkerhetsuppdateringar.

* * *

Mina damer och herrar,

Om några veckor kommer jag att presentera en inre säkerhetsstrategi för EU. Där har cyberbrott en självklar plats. Jag ser det som min uppgift som EU-kommissionär att sätta in cyberbrottsligheten i ett större sammanhang så att det blir tydligt vilka skador den kan leda till.

Denna säkerhetsstrategi innehåller konkreta förslag på vad som måste ske de kommande fyra åren. Och här har jag valt att lyfta fram cyberbrott och cybersäkerhet som en av de fem riktigt stora utmaningarna.

Detta är mitt försök att skapa den politiska dynamik och uppmärksamhet cyberbrott och cybersäkerhet förtjänar. Jag var inne på det i min inledning: Cyberbrott måste bli en lika naturlig del av vårt arbete mot organiserad brottslighet som trafficking, drogsmuggling eller illegal vapenhandel.

* * *

Jag har nu ägnat en stor del att tala om hoten och vad vi gör för att komma åt dem. Cyberbrott är verkligen gränsöverskridande, och det är viktigt att vi jobbar gemensamt inom EU för att möta dem. Det är sådan organiserad och allvarlig brottslighet vi måste samla våra insatser för att bekämpa.

Men att arbeta mot den organiserade brottsligheten innebär också svåra avvägningar. Polis och åklagares arbete mot kriminella nätverk handlar till stor del om tillgång till information. När jag träffar polismyndigheter runt om i Europa är de till exempel tydliga med att datalagringsdirektivet, som reglerar rättsbekämpande myndigheters tillgång till trafikuppgifter, är ett mycket användbart verktyg. Europaparlamentet tycker att direktivet är så användbart att vi borde se till att det också omfattar sökmotorer på Internet.

Jag tror absolut att polisen skulle ha nytta av att få tillgång till Google-sökningar, som Europaparlamentet vill. Men vi måste också fråga oss vad som är rimligt och proportionerligt. Och vi måste vara ödmjuka

för att vi kanske inte rakt av kan överföra mer traditionella verktyg för att bekämpa brott till den digitala verkligheten.

Jag hör ofta människor säga att "den som har rent mjöl i påsen har inget att dölja". Den som inte är brottsling behöver inte oroa sig. Men det är inte så enkelt. All information som kan brukas kan också missbrukas, och att ge polis tillgång till människors sökningar på Google på detta sätt är inte proportionerligt.

Jag har sedan tidigare varit riktat kritik mot datalagringsdirektivet och mot bland annat hur länge denna data kan lagras. Men jag är också väl medveten om att det rätt utformat är ett användbart och efterfrågat verktyg i arbetet mot den organiserade brottsligheten. Jag genomför därför just nu en bredare översyn av direktivet för att försöka hitta fram till en rimlig och proportionerlig avvägning.

En annan fråga där en del kritiserat mig för att jag gått för långt i kampen mot brottsligheten är mitt förslag för att stärka EU:s arbete mot sexuellt utnyttjande av barn. Det är ett brett förslag där jag bland

annat vill kriminalisera grooming, komma åt barnsexturism och ge de barn som utnyttjats tillgång till advokat utan kostnad.

Men mest uppmärksammat blev att jag ville att hela EU skulle göra som Sverige och ett antal andra länder och blockera tillgång till Internetsidor med barnpornografiskt innehåll. Jag har fått kritik för att detta är censur.

Att blockera sidor med barnporr är ingen mirakelkur. Det bästa är om vi kan ta bort dem helt från Internet. Men i de fall detta inte är möjligt är det just när det kommer till barnporr en befogad åtgärd att blockera dessa sidor.

Att utnyttja barn handlar inte om yttrandefrihet. Jag har ägnat en stor del av mitt politiska liv åt att kämpa för yttrandefrihet på Kuba. Jag har personliga vänner som fängslats för att de uttryckt en åsikt. Att tala om censur för att man stoppar människor från att titta på barnporr är att ta ifrån ordet dess rätta och viktiga betydelse.

* * *

Efter denna något dystra beskrivning över cyberhotet vill jag avsluta i en mer positiv anda. Skälet till min övertygelse om att vi måste jobba mer med cyberhotet är just för att kunna utveckla det digitala samhället.

Vi vill att EU ska ta sig upp ur den pågående ekonomiska krisen och bli världsledande i hur den nya tekniken kan användas för tillväxt och välstånd. Det är en målsättning som förpliktigar.

EU-kommissionen antog tidigare i våras en digital agenda, som ska ange riktningen för det här arbetet. Grundpelare är att skapa en digital inre marknad, främja bredbandsinvesteringar och, som vi redan pratat om, ett säkrare Internet. Detta gör vi för att dra nytta av Internets fulla potential.

Låt mig sluta där jag började. Jag citerade Erik Schmidt, som menar att Internet är den första sak 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 frihetsprojekt.

Men även frihet förutsätter vissa regler. En liberal grundprincip är att den enas frihet slutar där nästas börjar. Eller i enklare ordalag: du får gärna göra vad du vill så länge det inte skadar någon annan.

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 få fritt spelrum.

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

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

Och bara om vi är trygga med att våra barn inte kommer i kontakt med pedofiler på Internetforum kan vi släppa dem fria med egen dator och webbkamera.

Detta vill jag arbeta för. Men vi måste jobba tillsammans och i dialog för detta. Endast så kan vi få ett säkert Internet.

Tack.