EUROPEISKA KOMMISSIONEN

EUROPEISKA UNIONENS HÖGA REPRESENTANT FÖR UTRIKES FRÅGOR OCH SÄKERHETSPOLITIK

Bryssel den 7.2.2013
JOIN(2013) 1 final

GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

EU:s strategi för cybersäkerhet:

En öppen, säker och trygg cyberrymd

GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

EU:s strategi för cybersäkerhet:

En öppen, säker och trygg cyberrymd

1. INLEDNING

1.1. Bakgrund

Under de senaste två decennierna har internet och cyberrymden haft en mycket stor inverkan på alla delar av samhället. Vår vardag, våra grundläggande rättigheter, vår sociala samverkan och våra ekonomier är beroende av att informations- och kommunikationstekniken fungerar. En öppen och fri cyberrymd har gynnat den politiska och sociala integrationen över hela världen. Den har rivit murar mellan länder, samhällen och medborgare genom att göra det möjligt att interagera och dela information och tankar med andra över hela världen. Den har fungerat som ett forum för yttrandefrihet och utövandet av grundläggande rättigheter, och hjälpt människor i deras strävan efter demokratiska och mer rättvisa samhällen. Det mest talande exemplet är den arabiska våren.

För att cyberrymden även fortsättningsvis ska vara öppen och fri bör samma normer, principer och värden som EU värnar om utanför internet även gälla på internet. Grundläggande rättigheter, demokrati och rättsstatsprincipen måste skyddas i cyberrymden. Vår frihet och välfärd är i allt högre utsträckning beroende av ett starkt och innovativt internet som fortsätter att blomstra om den privata sektorn bidrar med innovation och det civila samhället främjar dess tillväxt. Det krävs emellertid även säkerhet och trygghet på internet. Cyberrymden måste skyddas från incidenter, skadliga aktiviteter och missbruk. Myndigheterna har en viktig roll när det gäller att garantera en fri och säker cyberrymd. Myndigheterna har flera uppgifter: Att värna om tillgängligheten och öppenheten, respektera och skydda de grundläggande rättigheterna och upprätthålla tillförlitlighet och interoperabilitet på internet. Eftersom den privata sektorn äger och använder sig av så stora delar av cyberrymden måste emellertid även dess ledande roll beaktas om detta ska lyckas.

Informations- och kommunikationstekniken har kommit att bli själva ryggraden för vår ekonomiska tillväxt och är en mycket viktig resurs som alla ekonomiska sektorer är beroende av. Den utgör grunden för de komplexa system som ser till att våra ekonomier är igång i viktiga sektorer såsom finans, hälsa, energi och transport. Många verksamhetsmodeller är beroende av oavbruten tillgänglighet på internet och av att informationssystemen fungerar friktionsfritt.

Genom att fullborda den digitala inre marknaden kan Europa öka sin BNP med nästan 500 miljarder euro om året[1], dvs. i genomsnitt 1 000 euro per person. För att ny teknik såsom e-betalningar, molnbaserade datortjänster och kommunikation från maskin till maskin ska kunna ta fart[2] måste medborgarna lita på den. Dessvärre visar en Eurobarometerundersökning

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] Exempelvis växter som är utrustade med sensorer för att kommunicera med sprinklersystemet och meddela när det är dags att bli vattnade.

från 2012[3] att nästan en tredjedel av européerna inte vågar använda internet för bankärenden eller köp. En överväldigande majoritet uppgav även att de undviker att uppge personuppgifter på internet eftersom de oroar sig för säkerheten. Inom EU har en av tio internetanvändare redan drabbats av internetbedrägeri.

Under de senaste åren har det blivit alltmer tydligt att samtidigt som den digitala världen innebär enorma fördelar så är den även sårbar. Såväl avsiktliga som oavsiktliga incidenter i fråga om cybersäkerhet[4] ökar i en oroväckande takt och kan störa tillhandahållandet av nödvändiga tjänster som vi tar för givet, exempelvis vatten, hälso- och sjukvård, elektricitet och mobila tjänster. Hot kan ha olika ursprung – de kan vara brottsliga eller politiskt motiverade angrepp eller angrepp som stöds av terrorister eller är statsunderstödda eller utgöras av naturkatastrofer och oavsiktliga misstag.

EU:s ekonomi har redan nu drabbats av aktiviteter kopplade till cyberbrottslighet[5] mot den privata sektorn och enskilda individer. Cyberbrottslingar använder sig av alltmer avancerade metoder för att ta sig in i informationssystem där de stjäl viktiga uppgifter eller bedriver utpressning mot företag. Ökningen av ekonomiskt spionage och statsunderstödda aktiviteter inom cyberrymden utgör en ny kategori av hot för myndigheter och företag inom EU.

I länder utanför EU kan myndigheterna även missbruka cyberrymden för att övervaka och kontrollera sina medborgare. EU kan hantera detta genom att främja friheten och garantera respekten av de grundläggande rättigheterna på internet.

Dessa faktorer förklarar varför regeringar världen över har börjat utveckla strategier för cybersäkerhet och betrakta cybersäkerhet som en allt viktigare internationell fråga. Nu är tiden inne för EU att öka sina insatser på detta område. I det förslag till en strategi för cybersäkerhet för EU som kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik har lagt fram beskrivs EU:s vision på detta område. Roller och ansvarsområden tydliggörs och nödvändiga åtgärder som baseras på ett starkt och effektivt skydd och främjande av medborgarnas rättigheter fastställs för att göra EU:s internetmiljö till den säkraste i världen.

1.2. Principer för cybersäkerhet

Ett mångsidigt internet utan gränser har blivit ett av de mest kraftfulla instrumenten för globala framsteg utan tillsyn eller regleringar. Den privata sektorn bör även fortsättningsvis ha en ledande roll när det gäller uppbyggnaden och den dagliga hanteringen av internet, men samtidigt har kraven på insyn, ansvarsskyldighet och säkerhet ökat och blivit alltmer tydliga. I den här strategin tydliggörs de principer som bör styra riktlinjerna för cybersäkerhet inom EU och internationellt.

---

3 2012 Särskild Eurobarometer 390 om cybersäkerhet.

4 Cybersäkerhet omfattar de skydd och åtgärder som kan användas för att skydda cyberrymden, både på det civila och militära området, från hot som är förknippade med eller som kan skada nät och informationsinfrastruktur. Målet med cybersäkerheten är att bevara tillgängligheten och integriteten i näten och infrastrukturen och konfidentialiteten när det gäller informationen i dessa. Begreppet cybersäkerhet omfattar även förebyggande åtgärder och åtgärder för att bekämpa cyberbrottslighet.

5 Cyberbrottslighet avser en mängd olika brottsliga aktiviteter där datorer och informationssystem används, antingen som verktyg eller mål. Cyberbrottslighet omfattar traditionella brott (t.ex. bedrägeri, förfalskning och identitetsstöld), innehållsrelaterade brott (t.ex. spridning av barnpornografi eller uppmuntran till rashat på internet) och brott som är unika för datorer och informationssystem (t.ex. angrepp mot informationssystem, överbelastningsattacker och skadlig programvara).

EU:s kärnvärden är lika viktiga i den digitala världen som i den fysiska världen

Samma lagar och normer som gäller på andra områden av våra dagliga liv gäller även i cyberrymden.

Att skydda grundläggande rättigheter, yttrandefrihet, personuppgifter och sekretess

Cybersäkerheten måste baseras på grundläggande rättigheter och friheter för att vara effektiv, i enlighet med Europeiska unionens stadga om de grundläggande rättigheterna och EU:s kärnvärden. På samma sätt kan inte enskilda individers rättigheter skyddas utan säkra nät och system. Informationsdelning som sker i syfte att skydda cybersäkerheten, när personuppgifter äventyras, måste ske i enlighet med EU:s dataskyddslagstiftning och individers rättigheter på detta område måste respekteras till fullo.

Tillgänglighet för alla

Begränsad tillgänglighet eller total avsaknad av tillgänglighet och digital analfabetism utgör stora nackdelar för medborgarna med tanke på hur mycket den digitala världen präglar vårt samhälle. Alla bör ha tillgång till internet och till ett obehindrat informationsflöde. Integriteten och säkerheten på internet måste garanteras för att säker tillgång för alla ska bli möjlig.

Demokratisk och effektiv styrning av flera intressenter

Den digitala världen styrs inte av en enda enhet. För närvarande finns det flera aktörer, varav många är kommersiella och icke-statliga enheter, som arbetar med den dagliga hanteringen av resurser, protokoll och standarder på internet och med den framtida utvecklingen av internet. EU bekräftar återigen hur viktiga alla aktörer är i den nuvarande modellen för styrning av internet och stöder strategin för styrning av flera intressenter[6].

Ett gemensamt ansvar för att garantera säkerheten

Det ökade beroendet av informations- och kommunikationsteknik på alla områden har lett till sårbarheter som måste identifieras för att därefter noggrant analyseras, åtgärdas eller minskas. Alla relevanta aktörer, oavsett om det rör sig om offentliga myndigheter, den privata sektorn eller enskilda medborgare, måste erkänna detta gemensamma ansvar, vidta åtgärder för att skydda sig själva och om nödvändigt genomföra en samordnad svarsinsats för att stärka cybersäkerheten.

2. STRATEGISKA PRIORITERINGAR OCH ÅTGÄRDER

EU måste värna om en internetmiljö som erbjuder största möjliga frihet och säkerhet för att gynna alla. Samtidigt som man i strategin erkänner att det främst är medlemsstaternas uppgift att ta itu med säkerhetsutmaningar i cyberrymden föreslås det även specifika åtgärder som kan förbättra EU:s resultat på området. Dessa åtgärder är både kort- och långsiktiga, de omfattar en rad politiska instrument[7] och olika typer av aktörer, oavsett om det handlar om EU-institutioner, medlemsstater eller branschen.

---

6 Se även KOM(2009) 277, Meddelande från kommissionen till Europaparlament och rådet *Förvaltning av Internet – framtida åtgärder*.

7 Åtgärder kopplade till informationsdelning som berör personuppgifter bör uppfylla EU:s dataskyddslagstiftning.

Den vision som presenteras i den här strategin består av fem strategiska prioriteringar för att anta utmaningarna ovan:

- Att uppnå cyberberedskap.
- Att drastiskt minska cyberbrottsligheten.
- Att utforma en policy för cyberförsvar och funktioner kopplade till den gemensamma säkerhets- och försvarspolitiken (GSFP).
- Att utveckla industriresurser och teknologiska resurser för cybersäkerhet.
- Att upprätta en sammanhängande internationell policy för cybersäkerhet för EU och främja EU:s kärnvärden.

2.1. Att uppnå cyberberedskap

För att främja cyberberedskap inom EU måste både offentliga myndigheter och den privata sektorn utveckla kapacitet och samarbeta effektivt. Genom att bygga vidare på de positiva resultat som uppnåtts hittills[8] kan ytterligare EU-åtgärder framför allt vara till hjälp när det gäller att bekämpa cyberrisker och hot som har en gränsöverskridande dimension, och bidra till en samordnad svarsåtgärd vid nödsituationer. Detta kommer på ett tydligt sätt att främja en välfungerande inre marknad och öka EU:s inre säkerhet.

Europa kommer att förbli sårbart om inte omfattande insatser genomförs för att öka den offentliga och privata kapaciteten och tillföra resurser och processer för att förebygga, upptäcka och hantera incidenter gällande cybersäkerhet. Därför har kommissionen utformat en politik för nät- och informationssäkerhet[9]. **Europeiska byrån för nät- och informationssäkerhet (Enisa)** upprättades 2004[10] och för närvarande är rådet och parlamentet i färd med att förhandla fram en ny förordning för att stärka Enisa och modernisera dess uppdrag[11]. Dessutom innebär ramdirektivet om elektronisk kommunikation[12] att leverantörer av elektronisk kommunikation måste hantera riskerna mot deras nät på ett lämpligt sätt och rapportera allvarliga brott mot säkerheten. EU:s dataskyddslagstiftning[13] innebär att de dataregisteransvariga måste garantera att dataskyddskrav efterlevs och säkerhetsåtgärder genomförs. När det gäller e-kommunikationstjänster som är tillgängliga för allmänheten måste de dataregisteransvariga rapportera personuppgiftsöverträdelser till de behöriga nationella myndigheterna.

Trots att framsteg har gjorts genom frivilliga åtaganden är skillnaderna inom EU fortfarande mycket stora, framför allt när det gäller nationell kapacitet, samordning vid gränsöverskridande incidenter och engagemang och beredskap inom den privata sektorn. Denna strategi åtföljs av ett förslag till **lagstiftning** om att i synnerhet göra följande:

---

8 Se hänvisningar i detta meddelande samt i kommissionens arbetsdokument om konsekvensanalys som åtföljer kommissionens förslag till direktiv om nät- och informationssäkerhet, framför allt avsnitten 4.1.4, 5.2, bilaga 2, bilaga 6 och bilaga 8.

9 År 2001 antog kommissionen meddelandet *Nät- och informationssäkerhet: Förslag till en europeisk strategi* (KOM(2001) 298). År 2006 antogs en strategi för ett säkert informationssamhälle (KOM(2006) 251). Sedan 2009 har kommissionen även antagit en handlingsplan och ett meddelande om skydd av kritisk infrastruktur (KOM(2009) 149) som fick stöd i rådets resolution 2009/C 321/01 och KOM(2011) 163 som fick stöd i rådets slutsatser 10299/11**).**

10 Förordning (EG) nr 460/2004.

11 KOM(2010) 521. De åtgärder som föreslås i den här strategin omfattar inte ändringar av det befintliga eller framtida Enisas mandat.

12 Artiklarna 13a och b i direktiv 2002/21/EG.

13 Artikel 17 i direktiv 95/46/EG, artikel 4 i direktiv 2002/58/EG.

- Upprätta gemensamma minimikrav för nät- och informationssäkerhet på nationell nivå som innebär att medlemsstaterna måste utse nationella behöriga myndigheter för nät- och informationssäkerhet, upprätta en välfungerande organisation för incidenthantering och anta en strategi för nät- och informationssäkerhet och en nationell samarbetsplan för nät- och informationssäkerhet. Kapacitetsskapande och samordning påverkar även EU-institutionerna. Under 2012 upprättades en permanent organisation för incidenthantering som ansvarar för säkerheten i it-systemen hos EU:s institutioner, byråer och organ (Cert-EU).
- Inrätta samordnade mekanismer för att förebygga, upptäcka, lindra och hantera hot, och på så sätt möjliggöra informationsdelning och ömsesidigt stöd mellan de behöriga myndigheter som ansvarar för nät- och informationssäkerhet. Nationella behöriga myndigheter som ansvarar för nät- och informationssäkerhet kommer att ombes garantera EU-omfattande samarbete, framför allt utifrån en samarbetsplan avseende nät- och informationssäkerhet för EU för att hantera cyberincidenter med gränsöverskridande dimension. Det här samarbetet kommer även att bygga på de framsteg som görs inom ramen för EU-forumet för medlemsstaterna (EFMS)[14], där man har genomfört produktiva diskussioner och samtal om offentlig politik för nät- och informationssäkerhet och kan införas i samarbetsmekanismen när en sådan har inrättats.
- Förbättra beredskap och engagemang inom den privata sektorn. Eftersom den stora majoriteten nät- och informationssystem ägs och drivs av privata aktörer måste engagemanget inom den privata sektorn när det gäller att främja cybersäkerhet förbättras. Den privata sektorn bör utveckla egen kapacitet för cyberberedskap på teknisk nivå och dela bästa praxis mellan sektorer. Den offentliga sektorn bör också få ta del av de redskap som utvecklas av branschen för att hantera incidenter, upptäcka orsaker och genomföra kriminaltekniska undersökningar.

Privata aktörer saknar emellertid fortfarande effektiva incitament när det gäller att tillhandahålla tillförlitliga uppgifter om förekomsten och effekterna av incidenter i fråga om nät- och informationssäkerhet, anamma en riskhanteringskultur eller investera i säkerhetslösningar. Syftet med den föreslagna lagstiftningen är därför att se till att aktörer på ett antal nyckelområden (närmare bestämt inom energi-, transport- och banknäringen, på börsen, hos leverantörerna av viktiga internettjänster samt de offentliga förvaltningarna) bedömer de risker i fråga om cybersäkerhet som de möter och ser till att nät- och informationssystem är tillförlitliga och motståndskraftiga genom lämplig riskhantering och delar sin information med de nationella behöriga myndigheter som ansvarar för nät- och informationssäkerheten. Anammandet av en kultur för cybersäkerhet skulle förbättra affärsmöjligheterna och konkurrenskraften inom den privata sektorn, vilket skulle göra cybersäkerheten till ett försäljningsargument.

Dessa enheter skulle vara tvungna att till de behöriga nationella myndigheter som ansvarar för nät- och informationssäkerhet rapportera incidenter med stora effekter på kontinuiteten i kärntjänster och tillhandahållandet av varor som är beroende av nät- och informationssystem.

Nationella behöriga myndigheter som ansvarar för nät- och informationssäkerhet bör samarbeta och utbyta information med andra regleringsorgan, och då framför allt myndigheter med ansvar för personuppgiftsskydd. Nationella behöriga myndigheter som ansvarar för nät- och informationssäkerhet bör även rapportera incidenter som misstänks vara av allvarlig

[14] EU-forumet för medlemsstaterna lanserades via KOM(2009) 149 som en plattform för att främja diskussioner mellan medlemsstaternas offentliga myndigheter om god praxis i fråga om säkerhet och beredskap för kritisk infrastruktur.

brottslig karaktär till brottsbekämpande myndigheter. De bör dessutom regelbundet offentliggöra icke sekretessbelagd information om pågående tidiga varningar för incidenter och risker och samordnade åtgärder på en särskild webbplats. De rättsliga skyldigheterna bör vare sig ersätta eller förebygga det informella och frivilliga samarbete, även mellan den offentliga och privata sektorn, som sker i syfte att förbättra säkerheten och utbyta information och bästa praxis. Framför allt är det offentligt-privata EU-partnerskapet för motståndskraft (EP3R[15]) en viktig plattform på EU-nivå som bör vidareutvecklas.

Fonden för ett sammanlänkat Europa[16] ska tillhandahålla ekonomiskt stöd för viktig infrastruktur och samordna medlemsstaternas kapacitet i fråga om nät- och informationssäkerhet och på så sätt göra det lättare att samarbeta inom EU.

Slutligen är övningar med cyberincidenter på EU-nivå nödvändiga för att simulera samarbete mellan medlemsstaterna och den privata sektorn. Den första övningen med medlemsstaterna genomfördes 2010 (Cyber Europe 2010) och en andra övning där även den privata sektorn deltog ägde rum i oktober 2012 (Cyber Europe 2012). En skrivbordsövning mellan EU och USA genomfördes i november 2011 (Cyber Atlantic 2011). Fler övningar är inplanerade för de kommande åren, bl.a. med internationella samarbetspartner.

Kommissionen kommer att göra följande:

- Fortsätta med den verksamhet som genomförs av det gemensamma forskningscentret i samarbete med medlemsstaternas myndigheter och viktiga ägare till och användare av infrastruktur för att identifiera sårbarheter i fråga om nät- och informationssäkerhet i kritisk infrastruktur inom EU och främja utvecklingen av motståndskraftiga system.
- Starta ett EU-finansierat pilotprojekt[17] i början av 2013 för att **bekämpa botnät och skadlig programvara,** erbjuda en ram för samordning och samarbete mellan EU:s medlemsstater och organisationer inom den privata sektorn, såsom internetleverantörer och internationella samarbetspartner.

Kommissionen uppmanar Enisa att göra följande:

- Hjälpa medlemsstaterna att utarbeta stark **nationell kapacitet för cyberberedskap**, framför allt genom att bygga upp sakkunskaper när det gäller säkerhet och beredskap inom industriella styrsystem, transport och energiinfrastruktur.
- Under 2013 undersöka genomförbarheten för CSIRT för industriella styrsystem (ICS-CSIRT) för EU.
- Fortsätta stödja medlemsstaterna och EU-institutionerna i genomförandet av regelbundna **övningar med it-incidenter på EU-nivå** som även ger praktiska

15 Det offentligt-privata EU-partnerskapet för motståndskraft lanserades genom KOM(2009) 149. Via denna plattform inleddes arbete samtidigt som samarbete främjades mellan den offentliga och privata sektorn för att fastställa viktiga tillgångar, resurser, funktioner, grundläggande krav för beredskap, samarbetsbehov och mekanismer för att hantera omfattande störningar som påverkar elektronisk kommunikation.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Budgetrubrik 09.03.02 för Fonden för ett sammanlänkat Europa – Telekommunikationsnät (för att främja samtrafik och interoperabilitet mellan medlemsstaternas nationella offentliga tjänster på nätet samt tillgång till sådana nät).

17 Ramprogrammet för konkurrenskraft och innovation – IKT-stödprogrammet – 2012-6, 325188 har en övergripande budget på 15 miljoner euro, varav EU-finansieringen uppgår till 7,7 miljoner euro.

förutsättningar för EU:s deltagande i internationella övningar med it-incidenter.

Kommissionen uppmanar Europaparlamentet och rådet att göra följande:

- Snabbt **anta** förslaget till direktiv om en **nät- och informationssäkerhet på hög nivå** inom unionen, hantera nationell kapacitet och beredskap, samarbete på EU-nivå, använda riskhanteringsrutiner och informationsdelning om nät- och informationssäkerhet.

Kommissionen uppmanar branschen att göra följande:

- Ta en ledande roll när det gäller att **investera** i en hög cybersäkerhet och utveckla bästa praxis och informationsdelning på sektorsnivå och med offentliga myndigheter i syfte att garantera ett starkt och effektivt skydd av tillgångar och individer, framför allt genom offentlig-privata partnerskap som EP3R och Trust in Digital Life (TDL)[18].

Öka medvetenheten

Att garantera cybersäkerheten är ett gemensamt ansvar. Slutanvändarna spelar en avgörande roll när det gäller säkerheten i nät- och informationssystem. De måste vara medvetna om de risker de ställs inför på internet och få möjlighet att vidta enkla åtgärder för att skydda sig.

Flera initiativ har utvecklats de senaste åren och dessa bör fortsätta. Framför allt Enisa har arbetat för att öka medvetenheten genom att offentliggöra rapporter, organisera expertseminarier och utveckla offentlig-privata partnerskap. Europol, Eurojust och nationella dataskyddsmyndigheter är också aktiva när det gäller att öka medvetenheten. I oktober 2012 genomförde Enisa tillsammans med några medlemsstater en europeisk månad för cybersäkerhet. Att öka medvetenheten är en av de frågor som EU:s och USA:s arbetsgrupp för cybersäkerhet och cyberbrottslighet[19] prioriterar. Frågan är även mycket viktig inom programmet för ett säkrare internet[20] (som är inriktat på säkerhet för barn på internet).

Kommissionen uppmanar Enisa att göra följande:

- Under 2013 föreslå att ett körkort för nät- och informationssäkerhet införs som ett frivilligt certifieringsprogram för att främja bättre kunskaper och kompetens hos datatekniker (t.ex. webbplatsadministratörer).

Kommissionen kommer att göra följande:

- Med hjälp av Enisa anordna ett **mästerskap** i cybersäkerhet under 2014, där universitetsstudenter tävlar mot varandra genom att föreslå lösningar inom nät-

---

18 http://www.trustindigitallife.eu/

19 Den här arbetsgruppen, som inrättades vid toppmötet mellan EU och USA i november 2010 (MEMO/10/597), har fått i uppdrag att utveckla samarbetsstrategier i en mängd frågor kopplade till cybersäkerhet och cyberbrottslighet.

20 Programmet för ett säkrare internet finansierar ett nätverk av icke-statliga organisationer som är aktiva på området barns välbefinnande på internet, ett nätverk av brottsbekämpande organ som utbyter information och bästa praxis kopplat till brottsligt utnyttjande av internet för att sprida material där sexuella övergrepp mot barn begås och ett nätverk av forskare som sammanställer information om användare, risker och konsekvenser av internetteknik för barns liv.

och informationssäkerhet.

Kommissionen uppmanar medlemsstaterna[21] att göra följande:

- Anordna en årlig **månad för cybersäkerhet** med hjälp av Enisa och den privata sektorn från 2013 och framåt. Målet ska vara att öka medvetenheten hos slutanvändare. En samordnad månad för cybersäkerhet för EU och USA kommer att anordnas med början år 2014.
- **Öka de nationella insatserna när det gäller utbildning inom nät- och informationssäkerhet** genom att införa följande: Utbildning om nät- och informationssäkerhet i skolor till år 2014, utbildning om nät- och informationssäkerhet och säker programvaruutveckling och personuppgiftsskydd för personer som studerar datavetenskap och systemvetenskap och grundläggande utbildning inom nät- och informationssäkerhet för personal som arbetar inom offentlig förvaltning.

Kommissionen uppmanar branschen att göra följande:

- Främja **medvetenheten på alla nivåer** när det gäller cybersäkerhet både inom affärsvärlden och i kontakten med kunderna. Framför allt bör branschen främja metoder för att göra verkställande direktörer och styrelser mer ansvariga för att garantera cybersäkerhet.

2.2. Drastiskt minska cyberbrottsligheten

Ju mer digital den värld vi lever i blir desto fler blir exploateringsmöjligheterna för cyberbrottslingarna. Cyberbrottsligheten är en av de snabbast växande brottsformerna och fler än en miljon människor världen över drabbas av den varje dag. Cyberbrottslingar och nätverk av cyberbrott blir allt mer avancerade och vi måste ha rätt operativa verktyg och kapacitet för att hantera dem. Cyberbrott är förknippade med hög vinst och låga risker, och brottslingar utnyttjar ofta anonymiteten på webbplatsdomäner. Cyberbrottsligheten känner inga gränser. Den globala räckvidden för internet innebär att brottsbekämpande myndigheter måste anta en samordnad och samarbetsinriktad gränsöverskridande strategi för att ta itu med det här växande hotet.

Stark och effektiv lagstiftning.

EU och medlemsstaterna behöver stark och effektiv lagstiftning för att ta itu med cyberbrottsligheten. Europarådets konvention om cyberbrottslighet, även kallad Budapestkonventionen, är en bindande internationell överenskommelse som utgör en effektiv ram för antagandet av nationell lagstiftning.

EU har redan antagit lagstiftning om cyberbrottslighet, däribland ett direktiv om bekämpande av sexuell exploatering av barn på internet och barnpornografi[22]. EU kommer även inom kort enas om ett direktiv om angrepp mot informationssystem, framför allt genom användning av botnät.

---

[21] Även med deltagande av relevanta nationella myndigheter, däribland behöriga myndigheter som ansvarar för nät- och informationssäkerhet och dataskyddsmyndigheter.

[22] Direktiv 2011/93/EU om ersättande av rådets rambeslut 2004/68/RIF.

Kommissionen kommer att göra följande:

- Se till att direktiven om cyberbrottslighet införlivas och genomförs snabbt.
- Uppmana de medlemsstater som ännu inte har ratificerat **Europarådets Budapestkonvention om cyberbrottslighet** att göra det och att så snart som möjligt genomföra dess bestämmelser.

Ökad operativ kapacitet för att bekämpa cyberbrottslighet

Utvecklingen av teknik inom cyberbrottslighet har ökat snabbt. De brottsbekämpande organen kan inte bekämpa cyberbrottslighet med omoderna operativa verktyg. För närvarande har inte alla EU-medlemsstater den operativa kapacitet de behöver för att effektivt kunna ta itu med cyberbrottsligheten. Alla medlemsstater behöver effektiva nationella enheter för cyberbrottslighet.

Kommissionen kommer att göra följande:

- Genom sina finansieringsprogram[23] hjälpa medlemsstaterna att **upptäcka brister och stärka sin kapacitet** för att undersöka och bekämpa cyberbrottslighet. Kommissionen kommer även stödja de organ som arbetar för att stärka kopplingen mellan forskningsvärlden/den akademiska världen, brottsbekämpande myndigheter och den privata sektorn så att deras samarbete i högre grad liknar det arbete som de kommissionsfinansierade kompetenscentrum för cyberbrottslighet som redan har inrättats i vissa medlemsstater bedriver.
- Tillsammans med medlemsstaterna samordna insatser för att fastställa bästa praxis och bästa tillgängliga teknik, bland annat med stöd av gemensamma forskningscenter för att bekämpa cyberbrottslighet (t.ex. när det gäller utveckling och användning av kriminaltekniska verktyg eller hotanalys).
- Inleda ett nära samarbete med **Europeiska centrumet mot it-brottslighet (EC3), inom Europol och med Eurojust** för att anpassa politiska strategier med bästa praxis på den operativa sidan.

Förbättrad samordning på EU-nivå

EU kan komplettera medlemsstaternas arbete genom att underlätta en samordnad och samarbetsinriktad strategi där brottsbekämpande myndigheter och rättsliga myndigheter förenas med offentliga och privata intressenter inom och utanför EU.

Kommissionen kommer att göra följande:

- Stödja det nystartade **Europeiska centrumet mot it-brottslighet** (EC3) som en central punkt i kampen mot it-brottslighet. EC3 bistår med analys och kunskap, stöder utredningar, tillhandahåller kriminalteknik på hög nivå, främjar samarbete, skapar kanaler för att dela information mellan medlemsstaternas behöriga

[23] För 2013, inom ramen för programmet Förebyggande och bekämpande av brott (Isec). Efter 2013 inom ramen för Fonden för inre säkerhet (ett nytt instrument som ingår i den fleråriga budgetramen).

myndigheter, den privata sektorn och andra intressenter och för de brottsbekämpande myndigheternas talan[24].

- Främja insatser för att öka ansvaret hos domänregistratorer och garantera att information om webbplatsägande är korrekt, framför allt utifrån rekommendationerna för brottsbekämpning för Internet Corporation for Assigned Names and Numbers (ICANN) i enlighet med EU:s lagstiftning, däribland reglerna om uppgiftsskydd.
- Bygga vidare på ny lagstiftning för att fortsätta stärka EU:s insatser när det gäller att ta itu med sexuella övergrepp mot barn på internet. Kommissionen har antagit en EU-strategi för ett bättre internet för barn[25] och har tillsammans med både EU-länder och icke-EU-länder startat en **global allians för att motverka sexuella övergrepp mot barn på internet**[26]. Alliansen är ett redskap för att genomföra ytterligare åtgärder från medlemsstaterna med stöd av kommissionen och EC3.

Kommissionen uppmanar Europol (EC3) att göra följande:

- Först koncentrera sitt analytiska och operativa stöd till medlemsstaternas utredningar av cyberbrottslighet, för att hjälpa till att komma tillrätta med nätverk för cyberbrottslighet, framför allt när det gäller sexuella övergrepp mot barn, betalningsbedrägerier, botnät och intrång.
- Regelbundet upprätta strategiska och operativa rapporter om kommande trender och hot för att fastställa prioriteringar och skräddarsy de insatser som särskilda team specialiserade på cyberbrottslighet genomför i medlemsstaterna.

Kommissionen uppmanar Europeiska polisbyrån (Cepol) att i samarbete med Europol göra följande:

- Samordna utformningen och planeringen av utbildning för att förse de brottsbekämpande myndigheterna med den kunskap och expertis som krävs för att effektivt ta itu med cyberbrottslighet.

Kommissionen uppmanar Eurojust att göra följande:

- Fastställa de huvudsakliga hindren mot rättsligt samarbete i utredningar av cyberbrottslighet och mot samordning mellan medlemsstaterna samt med tredjeländer och stödja utredning av och åtal mot cyberbrottslighet, på såväl operativ som strategisk nivå samt utbildning på området.

Kommissionen uppmanar Eurojust och Europol (EC3) att göra följande:

- Inleda ett nära samarbete, bl.a. genom informationsutbyte för att öka sin effektivitet när det gäller att bekämpa cyberbrottslighet, i enlighet med deras respektive mandat och behörighet.
-

[24] Den 28 mars 2012 antog Europeiska kommissionen meddelandet *Brottsbekämpning i vår digitala tidsålder: inrättande av ett Europeiskt centrum mot it-brottslighet.*

[25] COM(2012) 196 final.

[26] Rådets slutsatser om en global allians mot sexuella övergrepp mot barn på internet (gemensamt uttalande från EU och USA) av den 7 och 8 juni 2012 och förklaringen om lanseringen av den globala alliansen mot sexuella övergrepp mot barn på internet (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

2.3. Utforma en politik för cyberförsvar och funktioner kopplade till den gemensamma säkerhets- och försvarspolitiken (GSFP)

Insatser i fråga om cybersäkerhet inom EU omfattar även dimensionen för cyberförsvar. För att öka beredskapen i de kommunikations- och informationssystem som används för att stödja medlemsstaternas försvarsintressen och nationella säkerhetsintressen bör kapacitetsutvecklingen i fråga om cyberförsvar vara koncentrerad på att upptäcka, åtgärda och återhämta sig från avancerade cyberhot.

Med tanke på att hoten är mångfacetterade bör samverkan mellan civila och militära strategier när det gäller att skydda viktiga it-tillgångar förbättras. Dessa insatser bör stödjas av forskning och utveckling, och tätare samarbete mellan regeringar, den privata sektorn och den akademiska världen inom EU. För att undvika dubbelarbete kommer EU att utforska möjligheter för EU och Nato att samordna sina insatser när det gäller att höja beredskapen för kritisk infrastruktur i fråga om myndigheter, försvar och annan information som medlemmar av båda organisationerna är beroende av.

Den höga representanten kommer att fokusera på och uppmana medlemsstaterna och Europeiska försvarsbyrån att samarbeta när det gäller följande viktiga insatser:

- Bedöma de operativa kraven för EU:s cyberförsvar och främja utvecklingen av EU:s kapacitet när det gäller cyberförsvar och teknik för att ta itu med alla aspekter av kapacitetsutveckling – däribland undervisning, ledarskap, organisation, personal, utbildning, teknik, infrastruktur, logistik och interoperabilitet.

- Utveckla en ram för EU:s politik när det gäller cyberförsvar för att skydda nät vid uppdrag och verksamhet inom GSFP, däribland dynamisk riskhantering, förbättrad hotanalys och informationsdelning. Förbättra utbildning för cyberförsvar och övningsmöjligheter för militären inom EU och multinationellt, bl.a. genom att införa aspekter av cyberförsvar i befintliga kursplaner.

- Främja dialog och samordning mellan civila och militära aktörer inom EU – med särskild tonvikt på utbyte av god praxis, informationsutbyte och tidig varning, incidenthantering, riskbedömning, kunskapshöjande insatser och upprättande av cybersäkerhet som prioriteringar.

- Skapa en dialog med internationella samarbetspartner, däribland Nato, andra internationella organisationer och multinationella kompetenscentrum för att garantera ett effektivt försvar, fastställa samarbetsområden och undvika dubbelarbete.

2.4. Utveckla branschresurser och tekniska resurser för cybersäkerhet

Europa har fantastiska resurser när det gäller forskning och utveckling, men många av de globala ledare som tillhandahåller innovativa IKT-produkter och tjänster finns utanför EU. Det finns en risk för att Europa inte bara blir alltför beroende av IKT som produceras på annan plats, utan även av säkerhetslösningar som utvecklats utanför dess gränser. Det är avgörande att se till att maskinvaru- och programvarukomponenter som tillverkas inom EU och i tredjeländer som används i kritiska tjänster och infrastruktur, och allt mer i mobila enheter, är tillförlitliga, säkra och garanterar skydd av personuppgifter.

Främja en inre marknad för cybersäkerhetsprodukter

En hög nivå av säkerhet kan endast garanteras om alla aktörer i värdekedjan (t.ex. tillverkare av utrustning, programvaruutvecklare och leverantörer av tjänster till informationssamhället) gör säkerheten till en prioritering. Det förefaller[27] emellertid som om många aktörer fortfarande betraktar säkerhet som ytterligare en börda och efterfrågan på säkerhetslösningar är begränsad. Det krävs lämpliga krav när det gäller resultat inom cybersäkerhet inom hela värdekedjan för IKT-produkter som används i Europa. Den privata sektorn behöver incitament för att garantera en hög nivå av cybersäkerhet. Exempelvis kommer märkning som anger att cybersäkerheten är hög göra det möjligt för företag med goda resultat och meriter när det gäller cybersäkerhet att göra detta till ett försäljningsargument och få en konkurrensfördel. Dessutom skulle de skyldigheter som anges i förslaget till direktiv om nät- och informationssäkerhet påtagligt bidra till att öka verksamhetens konkurrenskraft i de sektorer som omfattas.

En efterfrågan på hela den europeiska marknaden av mycket säkra produkter bör också stimuleras. För det första är syftet med den här strategin att öka samarbetet och insynen i säkerhet när det gäller IKT-produkter. Den uppmanar till ett upprättande av en plattform där relevanta offentliga och privata intressenter i Europa sammanförs för att fastställa god praxis i fråga om cybersäkerhet inom hela värdekedjan och skapa gynnsamma marknadsvillkor för utveckling och antagande av säkra IKT-lösningar. En viktig prioritering bör vara att skapa incitament för att utföra lämplig riskhantering och anta säkerhetsstandarder och lösningar, samt eventuellt upprätta frivilliga certifieringssystem inom EU som bygger på befintliga system inom EU och internationellt. Kommissionen kommer att främja antagandet av sammanhängande strategier bland medlemsstaterna för att undvika att skillnader orsakar lokala nackdelar för företag.

För det andra kommer kommissionen stödja utvecklingen av säkerhetsstandarder och bistå med EU-omfattande frivilliga certifieringssystem när det gäller molnbaserade datortjänster samtidigt som man tar vederbörlig hänsyn till behovet av att garantera uppgiftsskydd. Arbetet kommer att vara inriktat på säkerheten i leveranskedjan, framför allt i viktiga ekonomiska sektorer (industriella styrsystem samt energi- och transportinfrastruktur) och bör bygga vidare på det pågående standardiseringsarbete som europeiska standardiseringsorganisationer (CEN, CENELEC och ETSI)[28] samt Cybersecurity Coordination Group (CSCG) utför samt på sakkunskaperna hos Enisa, kommissionen och andra relevanta aktörer.

Kommissionen kommer att göra följande:

- Under 2013 lansera en offentlig-privat **plattform för lösningar när det gäller nät- och informationssäkerhet** för att utveckla incitament för antagandet av säkra IKT-lösningar och användningen av goda resultat när det gäller cybersäkerhet för IKT-produkter som används i Europa.
- Under 2014 föreslå rekommendationer för att garantera cybersäkerhet inom hela IKT-värdekedjan som utgår från det arbete som utförs inom ramen för plattformen.
- Undersöka hur viktiga leverantörer av IKT-maskinvara och programvara kan informera nationella behöriga myndigheter om identifierade sårbarheter som kan

[27] Se kommissionens arbetsdokument om konsekvensanalys som åtföljer kommissionens förslag till direktiv om nät- och informationssäkerhet, avsnitt 4.1.5.2.

[28] I synnerhet inom ramen för standardiseringsmandatet M/490 för smarta nät och referensstrukturer.

ha påtagliga effekter på säkerheten.

Kommissionen uppmanar Enisa att göra följande:

- I samarbete med relevanta nationella behöriga myndigheter, relevanta intressenter, internationella och europeiska standardiseringsorgan och Europeiska kommissionens gemensamma forskningscenter utarbeta **tekniska riktlinjer och rekommendationer för antagandet av standarder och god praxis i fråga om nät- och informationssäkerhet** i den offentliga och privata sektorn.

Kommissionen uppmanar offentliga och privata intressenter att göra följande:

- Stimulera utvecklingen och antagandet av branschledda **säkerhetsstandarder**, tekniska normer och principer för security-by-design och privacy-by-design hos tillverkare av IKT-produkter och tjänsteleverantörer, däribland molnleverantörer. Ny programvara och maskinvara bör utrustas med **starkare inbyggda och användarvänliga säkerhetsfunktioner**.
- Utveckla branschledda standarder för företagens resultat när det gäller cybersäkerhet och förbättra den information som är tillgänglig för allmänheten genom att utveckla **säkerhetsmärkning** eller kvalitetsmärken som hjälper kunden att navigera på marknaden.

Främja investeringar i forskning och utveckling samt innovation

Forskning och utveckling kan gynna en stark branschpolitik, främja en tillförlitlig europeisk IKT-bransch, stimulera den inre marknaden och minska beroendet av utländsk teknik. Forskning och utveckling bör leda till att de brister som finns när det gäller IKT-säkerhet åtgärdas, förbereda systemen för kommande säkerhetsutmaningar, beakta de ständigt förändrade användarbehoven och utnyttja fördelarna med teknik med dubbla användningsområden. Man bör även fortsätta att stödja utvecklingen av kryptografi. Detta måste kompletteras av insatser för att omvandla resultaten av forskning och utveckling till kommersiella lösningar genom att tillhandahålla nödvändiga incitament och inrätta lämpliga politiska villkor.

EU bör göra så mycket som möjligt av Horisont 2020[29]–ramprogrammet för forskning och innovation som kommer att inledas 2014. Kommissionens förslag omfattar särskilda mål som gäller tillförlitlig IKT och bekämpande av cyberbrottslighet i linje med denna strategi. Horisont 2020 kommer att stödja säkerhetsforskning som är kopplad till IKT-teknik som är under utveckling, tillhandahålla lösningar för obrutna och säkra IKT-system, tjänster och applikationer, tillhandahålla incitament för genomförande och antagande av befintliga lösningar och hantera interoperabilitet inom nät- och informationssystem. Särskild uppmärksamhet kommer att ägnas åt att på EU-nivå optimera och på ett bättre sätt samordna olika finansieringsprogram (Horisont 2020, Fonden för inre säkerhet, forskning som bedrivs av Europeiska försvarsbyrån, däribland europeiskt ramsamarbete).

[29] Horisont 2020 är det finansieringsinstrument som används för att genomföra Innovationsunionen, ett flaggskeppsinitiativ som är en del av Europa 2020 och vars syfte är att stärka Europas globala konkurrenskraft. EU:s nya ramprogram för forskning och innovation, som kommer att pågå 2014–2020, kommer att vara en del av satsningen på att skapa ny tillväxt och nya arbetstillfällen i Europa.

Kommissionen kommer att göra följande:

- Använda Horisont 2020 för att ta itu med en rad frågor som rör IKT, sekretess och säkerhet, från forskning och utveckling till innovation och införande. Inom Horisont 2020 kommer dessutom verktyg och instrument för att bekämpa kriminell verksamhet och terrorism som riktas mot cybermiljön att främjas.
- Upprätta mekanismer för bättre samordning av EU-institutionernas och medlemsstaternas forskningsdagordningar och uppmuntra medlemsstaterna att investera mer i forskning och utveckling.

Kommissionen uppmanar medlemsstaterna att göra följande:

- Till slutet av 2013 utveckla god praxis för att utnyttja **offentliga förvaltningars köpkraft** (exempelvis via offentlig upphandling) för att stimulera utveckling och införande av säkerhetsfunktioner i IKT-relaterade produkter och tjänster.
- Främja tidigt engagemang från branschen och den akademiska världen i utvecklingen och samordningen av lösningar. Detta bör ske genom användning av Europas industriella bas och tekniska innovationer inom forskning och utveckling och samordning mellan civila och militära organisationers forskningsdagordningar.

Kommissionen uppmanar Europol och Enisa att göra följande:

- Fastställa trender och behov när det gäller mönster i fråga om cyberbrottslighet och cybersäkerhet för att utveckla lämpliga digitala kriminaltekniska verktyg och teknik.

Kommissionen uppmanar offentliga och privata intressenter att göra följande:

- Tillsammans med försäkringsbranschen ta fram **harmoniserade parametrar för att beräkna riskpremier** som gör det möjligt för företag som har investerat i säkerheten att gynnas av lägre riskpremier.

2.5. Upprätta en enhetlig internationell politik för cybersäkerhet för EU och främja EU:s kärnvärden

Att bevara en öppen, fri och säker cyberrymd är en global utmaning som EU bör anta tillsammans med berörda internationella partner och organisationer, den privata sektorn och det civila samhället.

I sin internationella politik för cyberrymden kommer EU att sträva efter att främja öppenheten och friheten på internet samt uppmuntra insatser för att utveckla beteendenormer och tillämpa befintliga internationella lagar i cyberrymden. EU kommer även att arbeta för att komma tillrätta med de digitala klyftorna och aktivt delta i internationella insatser för att bygga upp kapacitet när det gäller cybersäkerheten. EU:s internationella engagemang i cyberfrågor präglas av EU:s kärnvärden mänsklig värdighet, frihet, demokrati, jämlikhet, rättsstatsprincipen och respekten för de grundläggande rättigheterna.

Integrera frågor kopplade till cyberrymden i EU:s yttre förbindelser och den gemensamma utrikes- och säkerhetspolitiken

Kommissionen, den höga representanten och medlemsstaterna bör utforma en enhetlig internationell cyberpolitik för EU, där målet är ökat engagemang och starkare förbindelser

med viktiga internationella partner och organisationer samt med det civila samhället och den privata sektorn. EU:s samråd med internationella partner i cyberfrågor bör utformas, samordnas och genomföras för att tillföra mervärde till de befintliga bilaterala dialogerna mellan EU-medlemsstater och tredjeländer. EU kommer återigen att betona dialogen med tredjeländer och i synnerhet med likasinnade partner som delar EU:s värden. Man kommer att arbeta för att uppnå en hög nivå dataskydd, bland annat när det gäller överföring av personuppgifter till tredjeland. För att ta itu med globala utmaningar i cyberrymden kommer EU att sträva efter ett närmare samarbete med organisationer som är aktiva på det här området, såsom Europarådet, OECD, FN, OSSE, Nato, AU, Asean och OAS. På bilateral nivå är samarbetet med USA särskilt viktigt och kommer att vidareutvecklas, framför inom ramen för EU:s och USA:s arbetsgrupp för cybersäkerhet och cyberbrottslighet.

En av de viktigaste delarna av EU:s internationella cyberpolitik kommer att vara att främja cyberrymden som ett område för frihet och grundläggande rättigheter. Att öka tillgången till internet bör gynna demokratiska reformer världen över. Ökad global konnektivitet bör inte åtföljas av censur eller massövervakning. EU bör främja företagens sociala ansvar[30], och lansera internationella initiativ för att förbättra den globala samordningen på detta område.

Ansvaret för en säkrare cyberrymd vilar på alla aktörer i det globala informationssamhället, såväl medborgare som myndigheter. EU stöder insatserna för att definiera beteendenormer i cyberrymden som alla intressenter bör följa. På samma sätt som EU förväntar sig att medborgarna ska respektera medborgerliga skyldigheter, socialt ansvar och lagar på internet bör även länder följa normer och lagstiftning. När det gäller internationell säkerhet uppmanar EU utvecklingen av förtroendeskapande åtgärder inom cybersäkerhet för att öka insynen och minska risken för missförstånd när det gäller länders agerande.

EU anser inte att det krävs nya internationella rättsliga instrument för cyberfrågor.

De rättsliga skyldigheterna i Internationella konventionen om medborgerliga och politiska rättigheter, Europeiska konventionen om skydd för de mänskliga rättigheterna och EU:s stadga om de grundläggande rättigheterna bör också respekteras på internet. EU kommer att fokusera på hur dessa åtgärder även ska följas i cyberrymden.

När det gäller åtgärder mot cyberbrottslighet är Budapestkonventionen ett instrument som tredjeländer fritt kan ansluta sig till. Den står som modell för nationell lagstiftning om cyberbrottslighet och utgör underlag för internationellt samarbete på detta område.

Om väpnade konflikter sträcker sig ända ut i cyberrymden tillämpas internationell humanitär rätt och eventuellt människorättslagstiftning.

Att utveckla kapacitetsskapande i fråga om cybersäkerhet och motståndskraftig informationsinfrastruktur i tredjeländer

Välfungerande infrastruktur som tillhandahåller och underlättar kommunikationstjänster gynnas av ett ökat internationellt samarbete. Detta omfattar utbyte av bästa praxis, informationsdelning, gemensamma övningar för tidig varning och hantering av incidenter osv. EU kommer att sträva mot detta mål genom att intensifiera de pågående internationella ansträngningarna för att stärka samarbetet mellan myndigheter och den privata sektorn när det gäller skydd av kritisk infrastruktur.

[30] *En förnyad EU-strategi 2011–2014 för företagens sociala ansvar***,** KOM(2011) 681 slutlig.

Alla delar av världen har inte fått ta del av internets positiva effekter, på grund av att det saknas öppen, säker, driftskompatibel och tillförlitlig tillgång. Därför kommer EU fortsätta att stödja ländernas ansträngningar att utveckla tillgång och användning av internet för medborgarna, garantera dess integritet och säkerhet och effektivt bekämpa cyberbrottsligheten.

I samarbete med medlemsstaterna kommer kommissionen och den höga representanten att göra följande:

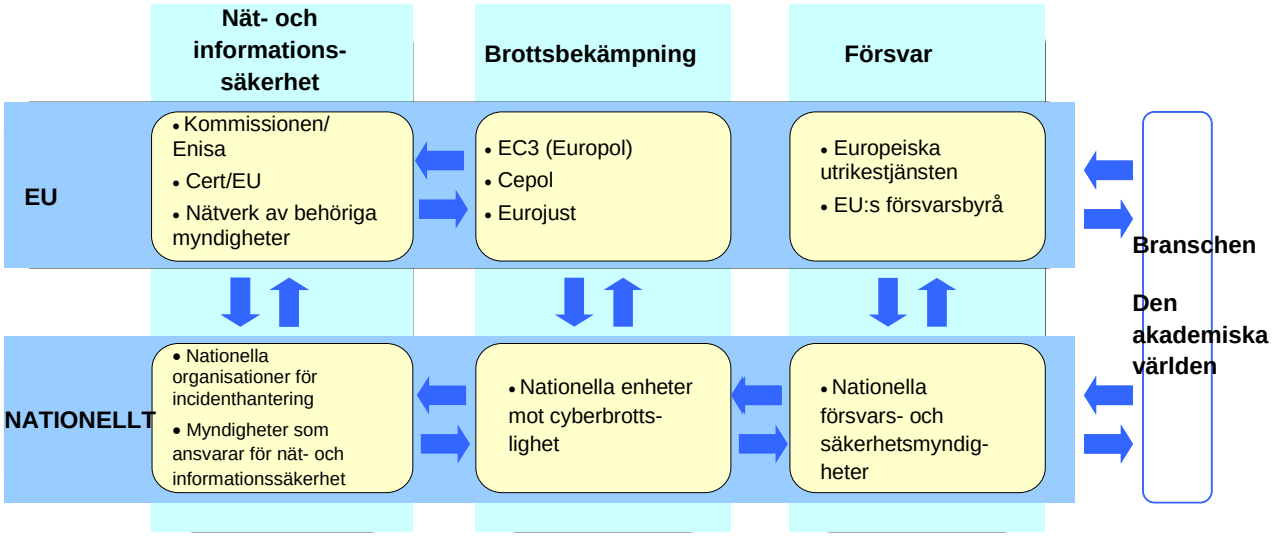
- Arbeta för en enhetlig internationell cyberpolitik för EU för att öka engagemanget hos viktiga internationella partner och organisationer, integrera frågor kopplade till cyberrymden i den gemensamma utrikes- och säkerhetspolitiken och förbättra samordningen av globala cyberfrågor.
- Stödja utvecklingen av beteendenormer och förtroendeskapande åtgärder inom cybersäkerhet. Främja en dialog om hur man tillämpar befintlig internationell lagstiftning i cyberrymden och främja Budapestkonventionen för att ta itu med cyberbrottslighet.
- Stödja främjandet och skyddet av grundläggande rättigheter, däribland tillgång till information och yttrandefrihet med fokus på följande: a) ta fram nya offentliga riktlinjer för yttrandefrihet på och utanför internet, b) övervaka exporten av produkter eller tjänster som kan användas för censur eller massövervakning på internet, c) utveckla åtgärder och redskap för att öka tillgången till internet, öppenheten och beredskapen när det gäller att ta itu med censur eller massövervakning genom kommunikationsteknik, d) ge intressenterna möjlighet att använda kommunikationsteknik för att främja grundläggande rättigheter.
- Samarbeta med internationella partner och organisationer, den privata sektorn och det civila samhället i syfte att stödja globalt kapacitetsskapande i tredjeländer för att förbättra tillgången till information och till ett öppet internet, förhindra och bekämpa cyberhot, däribland tillbud, cyberbrottslighet och cyberterrorism och utveckla givarsamordning för att styra kapacitetsskapande insatser.
- Utnyttja EU:s olika stödinstrument för kapacitetsskapande när det gäller cybersäkerhet, bl.a. bistå vid utbildning av brottsbekämpande myndigheter, rättslig och teknisk personal för att ta itu med cyberhot samt upprättandet av relevant nationell politik, strategier och institutioner i tredjeländer.
- Öka den politiska samordningen och informationsdelningen genom de internationella näten för skydd av kritisk infrastruktur såsom Meridian, samarbete mellan behöriga myndigheter som ansvarar för nät- och informationssäkerhet och andra.

3. ROLLER OCH ANSVARSOMRÅDEN

Cyberincidenter känner inga gränser i vår uppkopplade digitala ekonomi och vårt digitala samhälle. Alla aktörer, behöriga myndigheter som ansvarar för nät- och informationssäkerhet, organisationer för incidenthantering, brottsbekämpande myndigheter och branschen måste ta ansvar både nationellt och på EU-nivå och samarbeta för att stärka cybersäkerheten. Eftersom

olika rättsliga system och jurisdiktioner kan vara inblandade är en av de största utmaningarna för EU att tydliggöra roller och ansvarsområden för de många aktörer som berörs.

Med tanke på frågans komplexitet och de många inblandade aktörerna är centraliserad övervakning på EU-nivå inte någon lösning. Nationella myndigheter är de som är bäst lämpade att organisera förebyggande och hantering av cyberincidenter och angrepp och ett upprättande av kontakter och nätverk med den privata sektorn och allmänheten genom etablerade ramar. Med tanke på att riskerna kan vara eller faktiskt är gränslösa krävs det emellertid även engagemang på EU-nivå utöver en effektiv nationell hantering. För att hantera cybersäkerhet på ett heltäckande sätt bör verksamheten omfatta tre pelare – nät- och informationssäkerhet, brottsbekämpning och försvar – som även fungerar inom olika rättsliga system.



3.1. Samordning mellan behöriga myndigheter med ansvar för nät- och informationssäkerhet, organisationer för incidenthantering, brottsbekämpande myndigheter och försvar

Nationell nivå

Medlemsstaterna bör antingen redan nu ha eller genom den här strategin få strukturer för att ta itu med cyberberedskap, cyberbrottslighet och försvar och de bör ha den kapacitet som krävs för att ta itu med cyberincidenter. Med tanke på att flera enheter kan ha driftsansvar över olika dimensioner av cybersäkerhet, och med tanke på vikten av att engagera den privata sektorn bör samordningen mellan departement på nationell nivå optimeras. Medlemsstaterna bör i sina nationella strategier för cybersäkerhet fastställa roller och ansvarsområden för olika nationella enheter.

Informationsdelning mellan nationella enheter och med den privata sektorn bör uppmuntras för att göra det möjligt för medlemsstaterna och den privata sektorn att få en överblick över olika hot och bättre kunskaper om nya trender och tekniker som används både för att begå cyberangrepp och snabbare reagera på dem. Genom att upprätta nationella samarbetsplaner för nät- och informationssäkerhet som ska aktiveras vid cyberincidenter bör medlemstaterna tydligt kunna fördela roller och ansvarsområden och optimera svarsåtgärder.

EU-nivå

På såväl nationell nivå som EU-nivå finns det flera aktörer som hanterar cybersäkerhet. Framför allt Enisa, Europol/EC3 och Europeiska försvarsbyrån är aktiva när det gäller nät- och informationssäkerhet, brottsbekämpning och försvar. Dessa organ har styrelser där medlemsstaterna är representerade och erbjuder plattformar för samordning på EU-nivå.

Samordning och samarbete uppmuntras hos Enisa, Europol/EC3 och Europeiska försvarsbyrån på flera områden där de gemensamt är engagerade, framför allt när det gäller trendanalys, riskbedömning, utbildning och delande av bästa praxis. De bör samarbeta samtidigt som de var för sig fortsätter att arbeta med det de är specialiserade på. Tillsammans med Cert-EU, kommissionen och medlemsstaterna bör dessa myndigheter stödja utvecklingen av en grupp tekniska och politiska experter på detta område.

Informationskanaler för samordning och samarbete kommer att kompletteras av mer strukturella kopplingar. EU:s militära personal och Europeiska försvarsbyråns projektteam för cyberförsvar kan användas för samordning inom försvar. Europol/EC3:s programstyrelse kommer bland annat att samla Eurojust, Cepol, medlemsstaterna[31], Enisa och kommissionen och ge dem möjlighet att dela sina särskilda sakkunskaper och se till att EC3:s åtgärder utförs gemensamt, samt erkänna de expertkunskaper som alla intressenter kan bidra med och respektera deras mandat. Enisas nya mandat bör göra det möjligt att öka dess samarbete med Europol och stärka kopplingen till branschintressenter. Det viktigaste av allt är att kommissionens lagstiftningsförslag om nät- och informationssäkerhet skulle leda till upprättandet av en samarbetsram via ett nätverk av nationella behöriga myndigheter som ansvarar för nät- och informationssäkerhet och hanterar informationsdelning mellan myndigheter som arbetar med nät- och informationssäkerhet respektive brottsbekämpning.

Internationellt

Kommissionen och den höga representanten genomför tillsammans med medlemsstaterna samordnade internationella åtgärder på området cybersäkerhet. På så sätt upprätthåller de EU:s kärnvärden och främjar en fredlig och öppen användning av cyberteknik. Kommissionen, den höga representanten och medlemsstaterna engagerar sig i en politisk dialog med internationella partner och med internationella organisationer såsom Europarådet, OECD. OSSE, Nato och FN.

3.2. EU-stöd vid en större cyberincident eller ett angrepp

Större cyberincidenter eller angrepp påverkar EU:s myndigheter, företag och individer. Som ett resultat av den här strategin, och framför allt förslaget till direktiv om nät- och informationssäkerhet, bör förebyggande, upptäckt och hantering av cyberincidenter förbättras och medlemsstaterna och kommissionen bör hålla varandra informerade om större cyberincidenter eller angrepp. Svarsmekanismerna ser emellertid annorlunda ut beroende på incidentens karaktär, storlek och gränsöverskridande effekter.

Om incidenten har en allvarlig inverkan på affärsvärlden föreslås det i direktivet om nät- och informationssäkerhet att nationella samarbetsplaner och planer på EU-nivå för nät- och informationssäkerhet ska aktiveras, beroende på incidentens gränsöverskridande karaktär. Nätverket av behöriga myndigheter med ansvar för nät- och informationssäkerhet används i

[31] Via representationen inom EU:s arbetsgrupp om it-brottslighet som består av cheferna för EU:s cyberbrottslighetsenheter i medlemsstaterna.

detta sammanhang för att dela information och stöd. Detta skulle möjliggöra bevarande och/eller återställande av drabbade nät och tjänster.

Om incidenten förefaller vara kopplad till ett brott bör Europol/EC3 informeras så att de – tillsammans med de brottsbekämpande myndigheterna från de drabbade länderna – kan starta en utredning, spara bevisen, identifiera förövarna och se till att de åtalas.

Om incidenten förefaller vara relaterad till cyberspionage eller ett statsunderstött angrepp, eller har konsekvenser för den nationella säkerheten, ska nationella säkerhets- och försvarsmyndigheter varna sina motparter om att de är under attack så att de kan försvara sig. Mekanismer för tidig varning aktiveras sedan och om nödvändigt även krishantering eller andra förfaranden. En särskilt allvarlig cyberincident eller ett angrepp kan utgöra tillräckliga grunder för att en medlemsstat ska kunna åberopa EU:s solidaritetsklausul (artikel 222 i fördraget om Europeiska unionens funktionssätt).

Om incidenten tycks ha äventyrat personuppgifter bör de nationella dataskyddsmyndigheterna eller den nationella regleringsmyndigheten involveras i enlighet med direktiv 2002/58/EG.

Slutligen kommer hanteringen av cyberincidenter och angrepp gynnas av kontaktnät och stöd från internationella partner. Detta kan inbegripa teknisk begränsning, brottsutredningar eller aktivering av svarsmekanismer för krishantering.

4. SLUTSATSER OCH UPPFÖLJNING

I det här förslaget till strategi för cybersäkerhet för EU som kommissionen och den höga representanten för utrikes frågor och säkerhetspolitik har lagt fram, beskrivs EU:s vision och de åtgärder som krävs. Dessa baseras på ett starkt skydd och främjande av medborgarnas rättigheter för att göra EU:s internetmiljö till den säkraste i världen.[32]

Den här visionen kan endast förverkligas genom ett partnerskap mellan många aktörer som tar ansvar och antar de utmaningar som väntar.

Därför uppmanar kommissionen och den höga representanten rådet och Europaparlamentet att stödja strategin och hjälpa till att genomföra de åtgärder som beskrivs. Starkt stöd och engagemang krävs även från den privata sektorn och det civila samhället som är mycket viktiga för att förbättra vår säkerhetsnivå och skydda medborgarnas rättigheter.

Nu är tiden inne att agera. Kommissionen och den höga representanten är fast beslutna att samarbeta med alla aktörer för att uppnå den säkerhet som krävs i Europa. För att se till att strategin snabbt genomförs och utvärderas när det gäller möjlig utveckling kommer de att samla alla berörda parter till en högnivåkonferens och utvärdera framstegen inom ett år.

---

[32] Finansieringen av strategin kommer att ske med de planerade beloppen för varje relevant politikområde (Fonden för ett sammanlänkat Europa, Horisont 2020, Fonden för inre säkerhet, den gemensamma utrikes- och säkerhetspolitiken samt yttre samarbete, framför allt Stabilitetsinstrumentet) i enlighet med beskrivningen i kommissionens förslag till den fleråriga budgetramen för 2014–2020 (ska godkännas av budgetmyndigheten och slutbeloppen i den antagna fleråriga budgetramen för 2014–2020). När det gäller behovet av att garantera övergripande kompatibilitet med de poster som är tillgängliga för decentraliserade organ och taket för decentraliserade organ i varje utgiftsrubrik i nästa fleråriga budgetram kommer de organ (Cepol, Europeiska försvarsbyrån, Enisa, Eurojust och Europol/EC3) som genom detta meddelande ombes ta sig an nya uppgifter uppmanas att göra det i den mån organets faktiska kapacitet att ta upp växande resurser har fastställts och alla möjligheter till omfördelning har identifierats.