EUROPEISKA KOMMISSIONEN

Bryssel den 30.9.2010
KOM(2010) 517 slutlig

2010/0273 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om angrepp mot informationssystem och om upphävande av rådet rambeslut 2005/222/RIF

{SEK(2010) 1122 final}
{SEK(2010) 1123 final}

MOTIVERING

1. MOTIV OCH SYFTE

Syftet med detta förslag är att ersätta rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem[1]. Som framgår av skälen antogs rambeslutet för att svara upp till målsättningen att förbättra samarbetet mellan rättsliga och andra behöriga myndigheter, inklusive polis och andra specialiserade brottsbekämpande myndigheter i medlemsstaterna, genom att tillnärma medlemsstaternas straffrättsliga bestämmelser om angrepp mot informationssystem. Genom rambeslutet infördes EU-bestämmelser för att hantera lagöverträdelser såsom intrång i informationssystem, olaglig systemstörning och olaglig datastörning, samt särskilda bestämmelser om juridiska personers ansvar, om behörighet och om informationsutbyte. Medlemsstaterna ålades att senast den 16 mars 2007 vidta de åtgärder som är nödvändiga för att följa bestämmelserna i rambeslutet.

Den 14 juli 2008 offentliggjorde kommissionen en rapport om genomförandet av rambeslutet[2]. I rapportens slutsatser konstaterades att betydande framsteg hade gjorts i de flesta medlemsstater och att genomförandenivån var relativt hög, men att genomförandet i vissa medlemsstater ännu inte var fullbordat. Längre fram i rapporten sades att ”[s]edan rambeslutet antogs har angrepp på informationssystem i Europa på senare tid satt fokus på flera nya hot, särskilt massiva samtidiga angrepp mot informationssystem och ökad olaglig användning av så kallade botnät (botnets)”. Denna typ av angrepp stod inte i fokus när rambeslutet antogs. Som svar på denna utveckling kommer kommissionen att överväga åtgärder för att utforma lösningar som är bättre lämpade att möta detta hot (se nästa avsnitt för en förklaring av begreppet botnät).

Vikten av att vidta ytterligare åtgärder för att intensifiera kampen mot it-brottslighet betonades i 2004 års Haagprogram för ett stärkt område med frihet, säkerhet och rättvisa och i 2009 års Stockholmsprogram med tillhörande handlingsplan[3]. Den nyligen framlagda digitala agendan för Europa[4], som är det första riktigt betydande initiativet inom ramen för Europa 2020-strategin, bekräftade behovet av att möta nya former av brottslighet, särskilt it-brott, på EU-nivå. Inom det insatsområde som är inriktat på förtroende och säkerhet har kommissionen åtagit sig att vidta åtgärder för att bekämpa it-angrepp mot informationssystem.

Internationellt anses Europarådets konvention om it-relaterad brottlighet, som undertecknades den 23 november 2001, vara den mest fullständiga internationella standarden hittills, eftersom den ger en övergripande och sammanhängande ram som omfattar de olika aspekterna av it-brottslighet[5]. Konventionen har undertecknats av alla 27 medlemsstater, men hittills har endast 15 medlemsstater ratificerat den[6]. Konventionen trädde i kraft den 1 juli 2004. EU hör inte till signatärerna. Med hänsyn till denna rättsakts betydelse uppmanar kommissionen aktivt de återstående EU-medlemsstaterna att ratificera konventionen så snart som möjligt.

---

1 EUT L 69, 16.3.2005, s. 68.

2 Rapport från kommissionen till rådet på grundval av artikel 12 i rådets rambeslut av den 24 februari 2005 om angrepp mot informationssystem, KOM(2008) 0488 slutlig.

3 EUT C 198, 12.8.2005, EUT C 115, 4.5.2010, KOM(2010) 171, 20.4.2010.

4 Meddelande från kommissionen KOM(2010) 245, 19.5.2010.

5 Europarådets konvention om it-relaterad brottslighet, Budapest den 23 november 2001, CETS nr 185.

6 För en översikt över ratificeringarna av konventionen (CETS nr 185), se: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=&DF=&CL=ENG.

- **Allmän bakgrund**

It-brottsligheten främjas av brister som kan härledas till en rad faktorer. Tillkortakommanden i brottsbekämpningsmekanismerna bidrar till att fenomenet breder ut sig, och problemen förvärras av att vissa former av it-brott överskrider de nationella gränserna. Det räcker ofta inte att anmäla denna typ av brottslighet, dels eftersom vissa brott aldrig upptäcks och dels för att offren (ekonomiska aktörer och företag) ibland avstår från att anmäla av rädsla för att deras rykte ska lida skada och att deras framtida affärsprojekt ska påverkas negativt när eventuella svagheter exponeras offentligt.

Vidare kan skillnader i den nationella straff- och straffprocesslagstiftningen leda till att förfarandena för utredning och åtal sköts på olika sätt, med följden att hanteringen av dessa brott skiljer sig åt mellan medlemsstaterna. Informationsteknikens utveckling har förvärrat dessa problem genom att det blivit lättare att producera och sprida verktyg (sabotageprogram och botnät) samtidigt som gärningsmännen kunnat förbli anonyma och ansvaret spridits över jurisdiktionsgränserna. Eftersom organiserad brottslighet är svår att lagföra kan gärningsmännen göra betydande vinster utan att ta några större risker.

Detta förslag tar hänsyn till de nya metoderna för att begå it-brott, särskilt användningen av så kallade botnät. Med termen botnät avses ett nätverk av datorer som har infekterats av sabotageprogram (datorvirus). Ett sådant nät av infekterade datorer (*zombier*) kan aktiveras för att utföra särskilda uppgifter, till exempel angripa informationssystem (it-angrepp). Dessa zombier kan styras via en annan dator, ofta utan att de som använder de infekterade datorerna är medvetna om det. Den ”styrande” datorn kallas även kommando- och styrcentral (*command-and-control centre*). De personer som kontrollerar denna ”central” är också gärningsmän, eftersom de använder infekterade datorer för att angripa informationssystem. Att spåra förövarna är mycket svårt, eftersom de datorer som bildar botnätet och utför attackerna kan finnas på en annan plats än gärningsmannen själv.

Angrepp via botnät är ofta storskaliga. Storskaliga angrepp är angrepp som kan utföras antingen med hjälp av verktyg som påverkar ett betydande antal informationssystem (datorer), eller angrepp som orsakar betydande skada, exempelvis i form av störda systemtjänster, ekonomiska kostnader, förlust av personuppgifter m.m. Den skada som vållas vid storskaliga angrepp har betydande inverkan på funktionen hos föremålet för angreppet och/eller påverkar dess arbetsmiljö. I detta sammanhang ska ”stort botnät” förstås som ett botnät med kapacitet att orsaka allvarlig skada. Det är svårt att definiera botnät i storlekstermer, men de största botnät som har iakttagits har uppskattats ha mellan 40 000 och 100 000 anslutningar (det vill säga infekterade datorer) per 24-timmarsperiod[7].

[7] Antal anslutningar per 24 timmar är den mätenhet som vanligtvis används för att beräkna storleken på botnät.

- **Gällande bestämmelser**

Genom rambeslutet infördes en EU-miniminivå för tillnärmningen av den lagstiftning som medlemsstaterna inför i syfte att straffbelägga ett antal it-brott, inklusive olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning samt anstiftan av och medhjälp till sådana brott.

Även om bestämmelserna i rambeslutet generellt sett har genomförts av medlemsstaterna har det visat sig att det i flera avseenden inte längre räcker till, vilket hänger samma med brottens (it-angreppens) allt större omfattning och antal. Rambeslutet syftar endast till att tillnärma lagstiftningen om ett begränsat antal brott, och tar inte upp det potentiella samhällshot som storskaliga angrepp innebär. Inte heller tar det tillräcklig hänsyn till brottens svårhetsgrad och påföljdsfrågan.

Även andra befintliga eller planerade EU-initiativ och EU-program tar upp problem med anknytning till it-angrepp eller it-frågor, såsom nätsäkerhet och skydd för Internetanvändare. De inbegriper insatser inom ramen för programmet ”Förebyggande och bekämpande av brott”[8], programmet ”Straffrätt”[9], programmet ”Ett säkrare Internet”[10] och initiativet rörande kritisk IT-infrastruktur[11]. Ett annan relevant rättsakt som trätt i kraft är rambeslut 2004/68/RIF om bekämpande av sexuellt utnyttjande av barn och barnpornografi.

På administrativ nivå är handlingar som syftar till att infektera datorer och därigenom skapa botnät redan förbjudna enligt EU:s lagstiftning om skydd av privatliv och personuppgifter[12]. Nationella administrativa myndigheter samarbetar redan inom ramen för det europeiska kontaktnätet för myndigheter som arbetar med att motverka elektronisk skräppost. Enligt dessa bestämmelser är medlemsstaterna skyldiga att förbjuda sådan avlyssning av kommunikation i offentliga kommunikationsnät och offentligt tillgängliga elektroniska kommunikationstjänster som äger rum utan de berörda användarnas medgivande eller utan lagligt tillstånd.

Detta förslag är förenligt med de bestämmelserna. Medlemsstaterna bör sträva efter att förbättra samarbetet mellan administrativa och rättsliga myndigheter i sådana fall där både administrativa sanktioner och straffrättsliga påföljder är tillämpliga.

- **Förenlighet med Europeiska unionens politik och mål på andra områden**

Målen är förenliga med EU:s politik för att bekämpa organiserad brottslighet, öka datornätverkens motståndskraft, skydda kritisk informationsinfrastruktur och skydda personuppgifter. Dessa mål överensstämmer också med det program som upprättades för att främja en säkrare användning av Internet och ny online-teknik samt bekämpa olagligt innehåll.

Detta förslag har granskats ingående för att se till att bestämmelserna i förslaget överensstämmer helt med de grundläggande rättigheterna och, i synnerhet, med skyddet av

---

8 Se vidare: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm
9 Se vidare: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm
10 Se vidare: http://ec.europa.eu/information_society/activities/sip/index_en.htm
11 Se vidare: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm
12 Direktiv om integritet och elektronisk kommunikation, EUT L 201, 31.7.2002, i dess ändrade lydelse enligt direktiv 2009/136/EU, EUT L 337, 18.12.2009.

personuppgifter, yttrande- och meddelandefriheten, rätten till en rättvis rättegång, oskuldspresumtionen och rätten till ett försvar, samt med legalitetsprincipen och principen om proportionalitet mellan brott och påföljd.

2. SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSANALYS

- **Samråd med berörda parter**

En rad olika experter på området har konsulterats vid ett antal möten om olika aspekter av kampen mot it-brottslighet, inklusive den rättsliga uppföljningen (åtal) av dessa brott. Det rörde sig i synnerhet om företrädare för medlemsstaternas regeringar och den privata sektorn, domare och åklagare med specialkompetens på området, internationella organisationer, EU-byråer och branschorgan. Flera experter och organisationer har därefter kommit med synpunkter och lämnat information.

De viktigaste slutsatserna av samrådet är att det finns ett behov av att

– EU vidtar åtgärder på området,

– straffbelägga brottsformer som inte omfattas av det nuvarande rambeslutet, i synnerhet nya former av it-angrepp (botnät),

– undanröja hindren mot utredning och lagföring i gränsöverskridande fall.

De uppgifter som mottogs under samrådet har beaktats i konsekvensanalysen.

Extern experthjälp

Extern sakkunskap har inhämtats under olika möten med berörda aktörer.

Konsekvensanalys

Flera politiska alternativ har granskats i syfte att uppnå målet.

- Alternativ 1: Status Quo/inga nya EU-åtgärder

Detta alternativ innebär att EU inte vidtar några ytterligare åtgärder för att bekämpa denna särskilda form av it-brott, det vill säga angrepp mot informationssystem. Pågående åtgärder ska fortsätta, särskilt programmen för att stärka skyddet av kritisk it-infrastruktur och förbättra samarbetet mellan den offentliga och den privata sektorn i kampen mot it-brott.

- Alternativ 2: Utveckling av ett program som syftar till att i ökad utsträckning bekämpa angrepp mot informationssystem genom andra åtgärder än lagstiftning

Dessa åtgärder skulle, med undantag för programmet för skydd av kritisk it-infrastruktur, vara inriktade på gränsöverskridande brottsbekämpning och samarbete mellan den offentliga och den privata sektorn. Dessa icke-bindande instrument (*soft-law*) skulle ha till syfte att främja ytterligare samordnade insatser på EU-nivå, inklusive att stärka det befintliga nätverket av ständigt tillgängliga kontaktpunkter för brottsbekämpande myndigheter, inrätta ett EU-nätverk av offentlig-privata kontaktpunkter för it-brottsexperter och brottsbekämpande myndigheter, utarbeta en tjänsteavtalsmodell för de brottsbekämpande myndigheternas samarbete med

aktörer inom den privata sektorn och stödja organiseringen av fortbildningsprogram för brottsbekämpande myndigheter på temat utredning av it-brottslighet.

- Alternativ 3: En målinriktad uppdatering av bestämmelserna i rambeslutet (i form av ett nytt direktiv som ersätter det nuvarande rambeslutet) för att möta hotet från storskaliga angrepp mot informationssystem (botnät) och – när dessa begås genom att gärningsmannens verkliga identitet döljs, till skada för den som identiteten faktiskt tillhör – vidta åtgärder för att öka effektiviteten hos medlemsstaternas kontaktpunkter för brottsbekämpande myndigheter och avhjälpa bristen på statistisk information om it-angrepp.

Detta alternativ innebär att man inför särskild och riktad (d.v.s. begränsad) lagstiftning för att förhindra storskaliga angrepp mot informationssystem. En sådan förstärkt lagstiftning skulle åtföljas av andra åtgärder än lagstiftning för att stärka det operativa gränsöverskridande samarbetet mot sådana angrepp, vilket skulle underlätta genomförandet av lagstiftningsåtgärderna. Syftet med dessa åtgärder skulle vara att förbättra beredskapen, säkerheten och motståndskraften hos kritisk it-infrastruktur och utbyta bästa praxis.

- Alternativ 4: Införande av övergripande EU-lagstiftning för att bekämpa it-brott

Detta alternativ innebär att man inför ny, övergripande EU-lagstiftning. Utöver införandet av andra åtgärder än lagstiftningsåtgärder enligt alternativ 2 och uppdatering enligt alternativ 3 skulle det här alternativet även tackla andra rättsliga problem med anknytning till Internetanvändning. Dessa åtgärder skulle inte endast omfatta angrepp mot informationssystem, utan även sådana frågor som it-relaterad finansiell brottslighet, olagligt Internetinnehåll, insamling/lagring/överföring av elektronisk bevisning samt mer detaljerade behörighetsbestämmelser. Lagstiftningen skulle fungera parallellt med Europarådets konvention om it-brottslighet och kompletteras av sådana icke-lagstiftningsåtgärder som nämns ovan.

- Alternativ 5: Uppdatering av Europarådets konvention om it-relaterad brottslighet

Detta alternativ skulle kräva en betydande omförhandling av den nuvarande konventionen. Det skulle bli en långdragen process som inte kan passas in i den tidsram för insatser som föreslås i konsekvensanalysen. Det tycks inte heller finnas någon vilja från internationellt håll att omförhandla konventionen. En uppdatering av konventionen kan därför inte betraktas som en möjligt alternativ, då en sådan åtgärd inte kan genomföras inom den fastställda tidsramen.

Förespråkat alternativ: En kombination av å ena sidan andra åtgärder än lagstiftning (alternativ 2), å andra sidan en riktad uppdatering av rambeslutet (alternativ 3)

Att döma av den analys som har gjorts av de ekonomiska konsekvenserna, de sociala verkningarna och verkningarna för de grundläggande rättigheterna synes alternativen 2 och 3 vara bäst ägnade att lösa problemen och uppnå målen med förslaget.

För att få underlag till förslaget genomförde kommissionen en konsekvensanalys.

3. RÄTTSLIGA ASPEKTER

- **Sammanfattning av den föreslagna åtgärden**

Även om direktivet innebär att rambeslut 2005/222/RIF upphävs, kommer det att överta rambeslutets bestämmelser samtidigt som följande nya delar läggs till:

– När det gäller materiell straffrätt i allmänhet innebär direktivet följande:

A. Enligt direktivet blir det straffbart att tillverka, sälja, anskaffa i syfte att använda och att importera, distribuera eller på annat sätt tillgängliggöra utrustning/verktyg som kan användas för att begå brotten i fråga.

B. Direktivet kommer att omfatta bestämmelser om försvårande omständigheter:

- Storskaligheten i angreppet – botnät och liknande verktyg beaktas genom att man inför en ny försvårande omständighet; installationen av ett botnät eller liknande instrument skulle således anses som en försvårande omständighet vid begåendet av brott som förtecknas i det befintliga rambeslutet.

- Det skulle också anses som försvårande när angrepp mot informationssystem begås genom att gärningsmannens verkliga identitet döljs, till skada för den som identiteten faktiskt tillhör. Varje sådan bestämmelse skulle omfattas av krav på överensstämmelse med legalitetsprincipen och principen om proportionalitet mellan brottet och påföljden samt krav på förenlighet med befintlig lagstiftning om skydd av personuppgifter[13].

C. Genom direktivet införs ”olaglig avlyssning” som en ny brottsrubricering.

D. Genom direktivet införs åtgärder för att förbättra det straffrättsliga samarbetet i EU genom att stärka den befintliga strukturen med ständigt tillgängliga kontaktpunkter[14]:

- En skyldighet att hörsamma en begäran om bistånd från de operativa kontaktpunkterna (artikel 14 i direktivet) inom en viss tidsfrist föreslås. Konventionen om it-relaterad brottslighet innehåller ingen bindande bestämmelse av detta slag. Syftet med denna åtgärd är att säkerställa att kontaktpunkterna inom en viss tid anger om de har möjlighet att hörsamma en begäran om bistånd, och i så fall när den anmodande kontaktpunkten kan förvänta sig att detta sker. Det specificeras inte vad biståndet ska bestå i.

E. Direktivet tar hänsyn till behovet av tillgänglig statistik om it-brott genom att ålägga medlemsstaterna att se till att det finns ett adekvat system för registrering, framtagande och förmedling av statistiska uppgifter om de brott som tas upp i det befintliga rambeslutet samt det nytillkomna ”olaglig avlyssning”.

---

13 Till exempel Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, s. 37 (för närvarande under revidering), men även det allmänna dataskyddsdirektivet 95/46/EG.

14 Kontaktpunkterna infördes genom konventionen och rambeslut 2005/222/RIF om angrepp mot informationssystem.

Direktivet innehåller i definitionerna av brott i artiklarna 3–5 (olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning) en bestämmelse som gör det möjligt att endast straffbelägga ”fall som inte är ringa” i samband med direktivets införlivande i nationell rätt. Detta inslag av valfrihet har införts för att medlemsstaterna ska kunna avstå från att straffbelägga gärningar som i princip omfattas av den grundläggande definitionen, men som inte anses skada det skyddade rättsliga intresset. Det kan till exempel vara fråga om handlingar av unga personer som försöker bevisa sina kunskaper inom informationsteknik. Denna möjlighet att begränsa kriminaliseringens omfattning bör emellertid inte leda till att det införs ytterligare brottsrekvisit utöver de som redan anges i direktivet, eftersom det skulle leda till en situation där endast brott som begås under försvårande omständigheter omfattas. Under införlivandet bör medlemsstaterna särskilt avstå från att lägga ytterligare rekvisit till den grundläggande brottsdefinitionen, till exempel att det ska finnas ett särskilt uppsåt att skaffa sig olaglig vinning av brottet eller att brottet ska ha vissa verkningar, till exempel orsaka avsevärd skada.

- **Rättslig grund**

Artikel 83.1 i fördraget om Europeiska unionens funktionssätt[15].

- **Subsidiaritetsprincipen**

Subsidiaritetsprincipen är tillämplig på Europeiska unionens åtgärder. Medlemsstaterna kan av följande skäl inte i tillräcklig utsträckning själva uppnå målen med förslaget:

It-brottslighet och, mer specifikt, angrepp mot informationssystem har en betydande gränsöverskridande dimension, som framgår tydligast när det gäller storskaliga angrepp, eftersom de olika element som tillsammans bildar ett angrepp ofta finns på olika platser och i olika länder. Detta kräver åtgärder på EU-nivå, särskilt för att hålla jämna steg med utvecklingen mot allt mer storskaliga angrepp i Europa och i världen som helhet. Insatser på EU-nivå och en uppdatering av rambeslut 2005/222/RIF efterlystes också i rådets slutsatser från november 2008[16], eftersom målet att på ett effektivt sätt skydda människor från it-brott inte i tillräcklig utsträckning kan uppnås av medlemsstaterna på egen hand.

Genom att Europeiska unionen vidtar åtgärder kommer det att bli lättare att uppnå målen, främst av följande skäl:

Förslaget innebär att medlemsstaternas materiella straffrätt och regler om straffrättsliga förfaranden tillnärmas ytterligare, vilket får positiva verkningar för kampen mot denna typ av brottslighet. För det första är det ett sätt att förhindra att gärningsmän flyttar till medlemsstater där lagstiftningen mot it-angrepp är mindre sträng. För det andra innebär gemensamma definitioner att det blir möjligt att utbyta information och jämföra relevanta data. För det tredje kan de förebyggande åtgärderna i EU göras mer effektiva och det internationella samarbetet förbättras.

Förslaget är sålunda förenligt med subsidiaritetsprincipen.

---

15 EUT C 83, 30.3.2010, s. 49.

16 En samordnad arbetsstrategi och konkreta åtgärder mot it-brottslighet, 2987:e mötet i rådet (rättsliga och inrikes frågor), Bryssel, 27–28 november 2008.

- **Proportionalitetsprincipen**

Förslaget är förenligt med proportionalitetsprincipen av följande skäl:

Direktivet begränsas till det minimum som krävs för att uppnå målen på europeisk nivå och går inte utöver vad som är nödvändigt för att uppnå detta syfte med beaktande av den straffrättsliga lagstiftningens krav på exakthet.

- **Val av regleringsform**

Föreslagen regleringsform: Direktiv.

Övriga regleringsformer skulle vara olämpliga av följande skäl:

Den rättsliga grunden kräver ett direktiv.

Åtgärder som inte är av lagstiftningskaraktär och självreglering skulle förbättra situationen på vissa områden, där ett genomförande är av avgörande betydelse. På andra områden där ny lagstiftning är nödvändig skulle fördelarna emellertid bli obetydliga.

4. BUDGETKONSEKVENSER

Förslaget har liten inverkan på unionens budget. Mer än 90 % av den beräknade kostnaden på 5 913 000 euro skulle bäras av medlemsstaterna och det finns möjlighet att ansöka om EU-finansiering för att minska bördan.

5. ÖVRIGA UPPLYSNINGAR

- **Upphävande av gällande lagstiftning**

Om förslaget antas kommer nuvarande lagstiftning att upphöra att gälla.

- **Territoriell tillämpning**

Detta direktiv riktar sig till medlemsstaterna i enlighet med fördragen.

2010/0273 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om angrepp mot informationssystem och om upphävande av rambeslut 2005/222/RIF

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt

artikel 83.1,

med beaktande av Europeiska kommissionens förslag[17],

efter översändande av utkastet till lagstiftningsakt till medlemsstaternas parlament,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande,

med beaktande av Regionkommitténs yttrande,

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Syftet med detta direktiv är att tillnärma medlemsstaternas strafflagstiftning på området för angrepp mot informationssystem och att förbättra samarbetet mellan rättsliga och andra behöriga myndigheter, inbegripet polismyndigheter och andra specialiserade brottsbekämpande organ i medlemsstaterna.

(2) Angrepp mot informationssystem är ett växande problem, särskilt till följd av hotet från den organiserade brottsligheten, och det finns en stigande oro för terroristattacker eller politiskt motiverade angrepp mot de informationssystem som ingår i medlemsstaternas och unionens kritiska infrastruktur. Detta hot mot arbetet för att skapa ett säkrare informationssamhälle och ett område med frihet, säkerhet och rättvisa kräver motåtgärder på EU-nivå.

(3) Det finns tydliga bevis för en utveckling mot allt farligare och mer återkommande storskaliga angrepp mot informationssystem som är av vital betydelse för stater eller särskilda funktioner i den offentliga eller privata sektorn. Till denna tendens kommer alltmer sofistikerade verktyg som brottslingar kan använda sig av för att genomföra it-angrepp av olika slag.

---

[17] EUT C […], […], s. […].

(4) Gemensamma definitioner på detta område, särskilt av informationssystem och datorbehandlingsbara uppgifter, betyder mycket för att säkra att detta direktiv tillämpas enhetligt i medlemsstaterna.

(5) Det finns ett behov av att fastställa en gemensam inställning i fråga om brottsrekvisit, genom att gemensamt kriminalisera olagligt intrång i informationssystem, olaglig systemstörning, olaglig datastörning och olaglig avlyssning.

(6) Medlemsstaterna bör fastställa påföljder för angrepp mot informationssystem. De påföljder som fastställs bör vara effektiva, proportionella och avskräckande.

(7) Det är lämpligt att föreskriva strängare påföljder när ett angrepp mot ett informationssystem sker inom ramen för en sådan kriminell organisation som avses i rambeslut 2008/841/RIF av den 24 oktober 2008 om kampen mot organiserad brottslighet[18], när det är fråga om ett storskaligt angrepp eller när angreppet görs genom att gärningsmannens verkliga identitet döljs, och detta är till skada för den som identiteten faktiskt tillhör. Det är också lämpligt att föreskriva strängare påföljder när ett sådant angrepp har orsakat allvarliga skador eller har påverkat väsentliga intressen.

(8) Enligt rådets slutsatser av den 27–28 november bör det utarbetas en ny strategi i samarbete med kommissionen och medlemsstaterna, med hänsyn till 2001 års Europarådskonvention om it-relaterad brottslighet. Konventionen är den viktigaste rättsliga referensramen när det gäller att bekämpa it-brottslighet, inklusive angrepp mot informationssystem. Det här direktivet bygger på den konventionen.

(9) Med hänsyn till de olika metoder som kan användas för att angripa informationssystem och till den snabba utvecklingen av hård- och programvara bör detta direktiv hänvisa till verktyg som kan användas för att begå brott som förtecknas i det här direktivet. Verktyg i denna mening är exempelvis sabotageprogram, inklusive botnät, som används för angrepp mot informationssystem.

(10) Detta direktiv syftar inte till att ålägga straffrättsligt ansvar för gärningar som begås utan brottsligt uppsåt, till exempel i syfte att genomföra tester eller vidta åtgärder för att skydd informationssystem.

(11) Genom detta direktiv stärks betydelsen av nätverk, såsom G8 eller Europarådets nätverk av kontaktpunkter som är tillgängliga 24 timmar om dygnet veckans alla dagar för att kunna ge omedelbart bistånd i utredningar eller rättegångar rörande brott med anknytning till informationssystem och data, eller för att samla in bevis rörande ett brott i elektronisk form. Med hänsyn till hur snabbt storskaliga angrepp kan utföras bör medlemsstaterna ha kapacitet att snabbt besvara brådskande förfrågningar från detta nät av kontaktpunkter. Ett sådant bistånd bör inbegripa insatser för att underlätta eller direkt utföra vissa arbetsuppgifter, som att tillhandahålla teknisk rådgivning, lagra uppgifter, samla in bevis, tillhandahålla rättslig information och lokalisera misstänkta.

(12) Det finns ett behov av att samla in uppgifter om sådana brott som tas upp i detta direktiv, för att skaffa en mer heltäckande bild av problemet på unionsnivå och därigenom medverka till utformningen av mer effektiva motåtgärder. Dessa uppgifter

[18] EUT L 300, 11.11.2008, s. 42.

kommer att göra det möjligt för specialiserade byråer, såsom Europol och Europeiska byrån för nät- och informationssäkerhet, att bättre bedöma it-brottslighetens omfattning och läget när det gäller nät- och informationssäkerhet i EU.

(13) Stora klyftor och skillnader i medlemsstaternas lagstiftning på detta område kan försvåra kampen mot organiserad brottslighet och terrorism och komplicera ett effektivt polisiärt och rättsligt samarbete när det gäller angrepp mot informationssystem. De moderna informationssystemens nationsöverskridande och gränslösa natur innebär att angrepp mot sådana system ofta har en gränsöverskridande dimension, vilket understryker det trängande behovet av ytterligare insatser för att tillnärma strafflagstiftningen på detta område. För övrigt torde antagandet av rådets rambeslut 2009/948/RIF om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden göra det lättare att samordna lagföringen av angrepp mot informationssystem.

(14) Eftersom målen för detta direktiv, nämligen att se till att angrepp mot informationssystem i medlemsstaterna blir föremål för effektiva, proportionella och avskräckande straffrättsliga påföljder och att förbättra och uppmuntra rättsligt samarbete genom att undanröja eventuella komplikationer, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, då bestämmelserna måste vara gemensamma och förenliga med varandra, och de därför bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. Detta direktiv går inte utöver vad som är nödvändigt för att uppnå detta mål.

(15) Personuppgifter som behandlas i samband med genomförandet av detta direktiv bör skyddas i enlighet med rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete[19], när det gäller behandling som faller inom dess tillämpningsområde, samt Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter[20].

(16) Detta direktiv står i överensstämmelse med de grundläggande rättigheter och principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna, inklusive skyddet av personuppgifter, yttrande- och meddelandefrihet, rätten till en rättvis rättegång, oskuldspresumtionen och rätten till ett försvar, samt med legalitets- och proportionalitetsprinciperna. Detta direktiv syftar särskilt till att sörja för att dessa rättigheter och principer respekteras fullt ut och måste genomföras i enlighet med detta.

(17) [I enlighet med artiklarna 1, 2, 3 och 4 i protokollet om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska unionens funktionssätt, har Förenade kungariket och Irland meddelat att de önskar delta i antagandet och tillämpningen av detta direktiv] ELLER [Utan att det påverkar tillämpningen av artikel 4 i protokollet om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och

---

19 EUT L 350, 30.12.2008, s. 60.
20 EGT L 8, 12.1.2001, s. 1.

rättvisa kommer Förenade kungariket och Irland inte att delta i antagandet av detta direktiv och är därför inte bundna av det och omfattas inte av dess tillämpning].

(18) I enlighet med artiklarna 1 och 2 i protokollet om Danmarks ställning, fogat till fördraget om Europeiska unionens funktionssätt, deltar Danmark inte i antagandet av detta direktiv och är därför inte bundet av det och omfattas inte av dess tillämpning.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1
Syfte

Detta direktiv syftar till att fastställa vilka gärningar som ska definieras som brott när det gäller angrepp mot informationssystem och till att införa miniminormer med avseende på påföljder för sådana brott. Det syftar också till att införa gemensamma bestämmelser för att förebygga sådana angrepp och förbättra det straffrättsliga samarbetet i EU inom detta område.

Artikel 2
Definitioner

I detta direktiv avses med

a) *informationssystem*: en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de ska kunna drivas, användas, skyddas och underhållas.

b) *datorbehandlingsbara uppgifter*: framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.

c) *juridisk person*: enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer.

d) *orättmätigt*: intrång eller störning som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta eller som inte medges i den nationella lagstiftningen.

Artikel 3
Olagligt intrång i informationssystem

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att straffbelägga uppsåtligt orättmätigt intrång i ett informationssystem som helhet eller en del av ett sådant system, åtminstone i fall som inte är ringa.

Artikel 4

Olaglig systemstörning

Medlemsstaterna ska vidta nödvändiga åtgärder för att se till att det är straffbart att uppsåtligen allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Artikel 5

Olaglig datastörning

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det är straffbart att uppsåtligen radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Artikel 6

Olaglig avlyssning

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att straffbelägga uppsåtlig avlyssning med tekniska hjälpmedel av icke-offentliga överföringar av datorbehandlingsbara uppgifter till, från eller inom ett informationssystem, inklusive elektromagnetisk strålning från informationssystem som innehåller sådana uppgifter, när gärningen utförs orättmätigt.

Artikel 7

Verktyg som används för att begå brott

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det är straffbart att tillverka, sälja, anskaffa i syfte att använda, importera, inneha, distribuera eller på annat sätt tillgängliggöra följande, om gärningen är uppsåtlig och utförs orättmätigt i syfte att begå något av de brott som anges i artiklarna 3–6:

   a) En anordning, inklusive datorprogram, som utformats eller anpassats i första hand för att begå något av de brott som fastställs i artiklarna 3–6.

   b) Ett lösenord, en åtkomstkod eller liknande uppgifter som gör det möjligt att få tillgång till ett informationssystem eller delar av ett sådant system.

Artikel 8

Anstiftan, medhjälp och försök

1. Medlemsstaterna ska straffbelägga anstiftan av och medhjälp till brott som avses i artiklarna 3–7.

2. Medlemsstaterna ska straffbelägga försök till de brott som avses i artiklarna 3–6.

Artikel 9

Påföljder

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–8 är belagda med effektiva, proportionerliga och avskräckande straffrättsliga påföljder.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–6 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst två års fängelse.

Artikel 10

Försvårande omständigheter

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–7 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst fem års fängelse, när de begås inom ramen för en sådan kriminell organisation som avses i rambeslut 2008/841/RIF.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–6 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst fem års fängelse, när de begås med hjälp av ett verktyg som är avsett antingen att skada ett betydande antal informationssystem eller att orsaka avsevärd skada, till exempel i form av störda systemtjänster, ekonomiska kostnader eller förlust av personuppgifter.

3. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–6 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst fem års fängelse, när de begås genom att gärningsmannens verkliga identitet döljs, och detta är till skada för den som den använda identiteten faktiskt tillhör.

Artikel 11

Juridiska personers ansvar

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar för de brott som avses i artiklarna 3–8 och som begås till deras förmån av en person som agerar antingen enskilt eller som en del av den juridiska personens organisation och har en ledande ställning inom den juridiska personen, grundad på någon av följande befogenheter:

   a) Befogenhet att företräda den juridiska personen.

   b) Befogenhet att fatta beslut på den juridiska personens vägnar.

   c) Befogenhet att utöva kontroll inom den juridiska personen.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar när brister i övervakning eller kontroll som ska utföras av en sådan person som avses i punkt 1 har gjort det möjligt för en person som är

underställd den juridiska personen att till förmån för denna juridiska person begå de brott som avses i artiklarna 3–8.

3. Juridiska personers ansvar enligt punkterna 1 och 2 ska inte utesluta lagföring av fysiska personer som begår eller medverkar till något av de brott som avses i artiklarna 3–8.

Artikel 12
Påföljder för juridiska personer

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 11.1 kan bli föremål för effektiva, proportionella och avskräckande påföljder, som ska innefatta bötesstraff eller administrativa avgifter och som får innefatta andra sanktioner, som

   a) fråntagande av rätt till offentliga förmåner eller stöd,

   b) tillfälligt eller permanent näringsförbud,

   c) rättslig övervakning,

   d) rättsligt beslut om upplösning av verksamheten,

   e) tillfällig eller permanent stängning av inrättningar som har använts för att begå brottet.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 11.2 kan bli föremål för effektiva, proportionella och avskräckande påföljder eller åtgärder.

Artikel 13
Behörighet

1. Medlemsstaterna ska fastställa sin behörighet beträffande de brott som avses i artiklarna 3–8, när brottet har begåtts

   a) helt eller delvis på medlemsstatens territorium, eller

   b) av en medborgare i medlemsstaten eller av en person som har hemvist på dess territorium, eller

   c) till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium.

2. Medlemsstaterna ska vid fastställandet av sin behörighet enligt punkt 1 a se till att behörigheten innefattar fall där

   a) gärningsmannen är fysiskt närvarande på den berörda medlemsstatens territorium när brottet begås, oavsett om brottet riktar sig mot ett informationssystem på medlemsstatens territorium eller inte, eller

b) brottet riktar sig mot ett informationssystem på den berörda medlemsstatens territorium, oavsett om gärningsmannen är fysiskt närvarande på medlemsstatens territorium när brottet begås eller inte.

Artikel 14
Utbyte av information

1. För utbyte av uppgifter om de brott som avses i artiklarna 3–8 ska medlemsstaterna, med iakttagande av bestämmelser om dataskydd, använda det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan. Medlemsstaterna ska också se till att ha förfaranden som gör att de kan svara på brådskande framställningar inom högst åtta timmar. Av dessa svar ska det åtminstone framgå huruvida framställan om bistånd kommer att beviljas och, om så är fallet, hur och när detta kommer att ske.

2. Medlemsstaterna ska underrätta kommissionen om sin utsedda kontaktpunkt för utbyte av uppgifter om de brott som anges i artiklarna 3–8. Kommissionen ska vidarebefordra denna information till de andra medlemsstaterna.

Artikel 15
Övervakning och statistik

1. Medlemsstaterna ska se till att det finns ett system för registrering, insamling och tillhandahållande av statistiska uppgifter om de brott som anges i artiklarna 3–8.

2. Den statistik som avses i punkt 1 ska åtminstone omfatta antalet sådana brott som avses i artiklarna 3–8 som rapporterats till medlemsstaterna och uppföljningen av dessa rapporter samt på årsbasis ange antalet fall som undersökts, antalet personer som åtalats och antalet personer som dömts för sådana brott som anges i artiklarna 3–8.

3. Medlemsstaterna ska översända de uppgifter som samlas in enligt denna artikel till kommissionen. De ska också se till att en samlad översikt över dessa statistiska rapporter offentliggörs.

Artikel 16
Upphävande av rambeslut 2005/222/RIF

Rambeslut 2005/222/RIF ska upphöra att gälla, dock utan att det påverkar medlemsstaternas skyldigheter när det gäller tidsfristen för införlivande med nationell lagstiftning.

Hänvisningar till det upphävda rambeslutet ska anses som hänvisningar till det här direktivet.

Artikel 17
Införlivande

1. Medlemsstaterna ska senast [två år från antagandet] sätta i kraft de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska till kommissionen genast överlämna texten till dessa bestämmelser tillsammans med en jämförelsetabell

över dessa bestämmelser och detta direktiv. När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i nationell lagstiftning som de antar inom det område som omfattas av detta direktiv.

Artikel 18
Rapportering

1. Senast [FYRA ÅR EFTER ANTAGANDET] och därefter vart tredje år ska kommissionen överlämna en rapport om medlemsstaternas tillämpning av detta direktiv till Europaparlamentet och rådet, med eventuella nödvändiga förslag.

2. Medlemsstaterna ska till kommissionen översända all information som behövs för att utarbeta den rapport som avses i punkt 1. Denna information ska omfatta en ingående beskrivning av lagstiftningsåtgärder och andra åtgärder som antas för att genomföra detta direktiv.

Artikel 19
Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 20
Adressater

Detta direktiv riktar sig till medlemsstaterna i enlighet med fördragen.

Utfärdat i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*