EUROPEISKA UNIONENS RÅD

Bryssel den 22 juli 2013
(OR. en)

12109/13

POLGEN 138
JAI 612
TELECOM 194
PROCIV 88
CSC 69
CIS 14
RELEX 633
JAIEX 55
RECH 338
COMPET 554
IND 204
COTER 85
ENFOPOL 232
DROIPEN 87
CYBER 15
COPS 276
POLMIL 39
COSI 93
DATAPROTECT 94

LÄGESRAPPORT

från:	Rådets generalsekretariat
till:	Delegationerna
Föreg. dok. nr:	11357/13
Ärende:	Rådets slutsatser om det gemensamma meddelandet *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd* från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik

För delegationerna bifogas rådets slutsatser om det gemensamma meddelandet *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd* från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik som rådet (allmänna frågor) enades om den 25 juni 2013.

BILAGA

Rådets slutsatser om det gemensamma meddelandet *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd*
från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik

Europeiska unionens råd,

1. SOM INSER att cyberrymden, som är transnationell till sin karaktär, består av inbördes beroende nät- och informationsinfrastrukturer som bland annat omfattar internet och telekomnät, utgör en av de viktigaste nuvarande och framtida kanalerna för tillgodoseende av EU-medborgarnas och medlemsstaternas behov, intressen och rättigheter och är en oundgänglig tillgång för ekonomisk tillväxt i EU,

2. SOM UNDERSTRYKER de roller och rättigheter som de enskilda medborgarna, privata sektorn och civilsamhället har i cyberfrågor och EU:s viktiga roll för att stödja och bibehålla en öppen, säker och motståndskraftig cyberrymd grundad på EU:s centrala värden som demokrati, mänskliga rättigheter och rättsstatlighet för våra ekonomier och förvaltningar och vårt samhälle samt för en väl fungerande inre marknad,

3. SOM INSER behovet av att förbättra konfidentialiteten, tillgängligheten och integriteten i näten och infrastrukturen och när det gäller informationen i dessa,

4. 4. SOM INSER att skyddsåtgärder och andra åtgärder måste vidtas för att förebygga hot som har anknytning till eller är skadliga för de inbördes beroende nät- och informationsinfrastrukturerna och för att både inom det civila och det militära området skydda cyberrymden,

5. SOM BEKRÄFTAR EU:s ståndpunkt att samma normer, principer och värden som EU hävdar offline, framför allt i EU:s stadga om de grundläggande rättigheterna, bör gälla även i cyberrymden,

6. SOM INSER att den internationella rätten, bland annat internationella konventioner som konventionen om it-brottslighet (Budapestkonventionen) och relevanta konventioner om internationell humanitär rätt och mänskliga rättigheter, till exempel den internationella konventionen om medborgerliga och politiska rättigheter och den internationella konventionen om ekonomiska, sociala och kulturella rättigheter anger en rättslig ram som är tillämplig på cyberrymden; därför bör insatser göras för att se till att dessa instrument hävdas i cyberrymden; EU kräver därför inte att nya internationella rättsliga instrument skapas för cyberfrågor,

7. SOM BEKRÄFTAR att frågan om cybersäkerhet måste tas upp på ett integrerat, tvärvetenskapligt och horisontellt sätt och att åtgärderna bör omfatta en rad olika frågor som påverkar cyberrymden,

8. SOM ERINRAR om de många EU-initiativen och internationella initiativen på området för cybersäkerhet, bland annat de som anges i bilagan till detta dokument,

9. SOM ERINRAR om bestämmelserna i artikel 222 i fördraget om Europeiska unionens funktionssätt och beaktar de pågående diskussionerna om deras tillämpning,

10. SOM ÄR MEDVETET om att arbetet med att höja cybersäkerheten och förbättra bekämpningen av it-brottslighet måste bedrivas inte bara i Europeiska unionen utan även i tredjeländer, bland annat i de länder varifrån it-brottsorganisationer är verksamma,

11. VÄLKOMNAR det gemensamma meddelandet från kommissionen och EU:s höga representant om en EU-strategi för cybersäkerhet,

12. ANSER det är viktigt och hög tid att vidareutveckla och genomföra en heltäckande strategi för EU:s politik för cyberrymden som

    - skyddar och främjar utövandet av mänskliga rättigheter och grundas på EU:s grundläggande värderingar demokrati, mänskliga rättigheter och rättsstatlighet,

    - främjar europeiskt välstånd och de sociala och ekonomiska fördelarna med cyberrymden, även internet,

- främjar effektiv och förbättrad cybersäkerhet i och utanför EU,

- främjar insatserna för att överbrygga den globala it-klyftan och främjar internationellt samarbete på området för cybersäkerhet,

- återspeglar de roller och rättigheter som de enskilda medborgarna, privata sektorn och civilsamhället har i cyberfrågor, inbegripet stärkt offentlig–privat samarbete och informationsutbyte,

OCH

13. UPPMANAR medlemsstaterna, kommissionen och den höga representanten att samarbeta och då respektera varandras behörighetsområden och subsidiaritetsprincipen som svar på de strategiska mål som anges i dessa slutsatser,

Värden

14. UNDERSTRYKER att individers mänskliga rättigheter, inbegripet yttrandefrihet och rätten till privatliv, alltid måste respekteras när politik och praxis utformas i frågor som rör cybersäkerhet, samt i lagstiftningen, och noterar de pågående förhandlingarna om en rättslig EU-ram för skydd av personuppgifter som kan fungera effektivt i cyberrymden,

15. INSER att de värden och intressen som främjas och skyddas i unionen också bör främjas i dess yttre politik när det gäller cyberfrågor,

16. UPPMANAR EU och dess medlemsstater att

- försvara sin sammanhållna och bestämda ståndpunkt i fråga om den universella tillämpligheten av mänskliga rättigheter och grundläggande friheter, inbegripet åsikts-, yttrande-, informations-, mötes- och föreningsfrihet i cyberrymden,

- klarlägga hur gällande skyldigheter kan tillämpas i cyberrymden,

17. UPPMANAR EU och dess medlemsstater att främja digital kompetens och hjälpa användarna att bli mer medvetna om sitt eget ansvar för personuppgifter som de lämnar på internet,

18. UNDERSTRYKER EU:s viktiga roll när det gäller att bibehålla en flerpartsmodell för förvaltningen av internet,

19. UPPMANAR medlemsstaterna att vidta alla rimliga åtgärder för att se till att alla EU-medborgare kan få tillgång till och dra nytta av fördelarna med internet,

Välstånd

20. UPPMANAR kommissionen att göra särskilda insatser för att främja den inre e-marknaden och driva närliggande frågor i EU och internationella forum, t.ex. i Världshandelsorganisationen (WTO) och vid förhandlingarna om avtalet om handel med informationsteknikprodukter, samt att säkerställa marknadstillträde inom dessa sektorer när den förhandlar om avtal om frihandelsområden med tredjeländer,

21. UNDERSTRYKER vikten av att lagstiftningen inom denna sektor är teknikneutral och i största möjliga mån främjar nätneutralitet för att inte hindra konkurrensen genom diskriminering av gränsöverskridande näthandel och nya företagsmodeller,

22. VÄLKOMNAR att det erkänns att det behövs investeringar i forskning och utveckling om cyberrymden som ett viktigt område som kan ge arbetstillfällen av god kvalitet och ekonomisk tillväxt,

23. BETONAR att

- det är av kritisk betydelse att det finns en livaktig sektor för informations- och kommunikationsteknik (IKT) och IKT-säkerhet i EU när det gäller att höja cybersäkerheten och UPPMANAR medlemsstaterna och kommissionen att undersöka och rapportera om möjliga åtgärder för att stödja dess utveckling,

- den lagstiftning som ska stödja cybersäkerhet bör främja innovation och tillväxt och vara inriktad på skydd av infrastruktur och viktiga funktioner som medlemsstaterna bedömer ha kritisk betydelse,

- den digitala ekonomin är en viktig drivkraft för tillväxt, innovation och sysselsättning och att cybersäkerheten är avgörande för skyddet av den digitala ekonomin,

- skyddet av kritisk informationsinfrastruktur är viktigt på nationell nivå,

Att uppnå cyberberedskap

24. VÄLKOMNAR målen för kommissionens förslag till direktiv om åtgärder för att förstärka

    - nät- och informationssäkerheten i hela EU,

    - beredskapen och kapaciteten för cybersäkerhet på nationell nivå,

    - samarbetet mellan medlemsstaterna och i hela EU samt för att stimulera en kultur av riskhantering i den offentliga och den privata sektorn,

25. UPPMANAR alla EU:s institutioner, organ och byråer att i samarbete med medlemsstaterna vidta nödvändiga åtgärder för att säkerställa sin egen cybersäkerhet genom att öka sin säkerhet i enlighet med tillämpliga säkerhetsstandarder, i samarbete med Enisa för att uppnå bästa praxis i enlighet med förordning (EU) nr 526/2013[1],

26. ERINRAR om att en organisation för incidenthantering för EU:s institutioner, organ och byråer har inrättats efter en pilotfas på ett år och sedan en positiv bedömning gjorts av dess roll och effektivitet,

27. UNDERSTRYKER den yttersta vikten av att Enisa stöder medlemsstaternas och unionens ansträngningar för att nå en hög nivå av nät- och informationssäkerhet, i synnerhet genom att stödja medlemsstaternas kapacitetsuppbyggnad, och utarbeta stark nationell kapacitet för cyberberedskap, europeiska cyberövningar samt unionens FoU- och standardiseringsverksamhet och UPPMANAR Enisa att samarbeta med unionens övriga institutioner, organ och byråer när det gäller frågor som rör nät- och informationssäkerhet, i enlighet med förordning (EU) nr 526/2013,

[1] EUT L 165, 18.6.2013.

28. FRAMHÅLLER behovet av att höja beredskapen för kritisk infrastruktur i hela EU och förstärka ett nära samarbete och en nära samordning mellan relevanta aktörer, också mellan civila och militära EU-aktörer, inbegripet mellan den offentliga och den privata sektorn, för att hantera incidenter och utmaningar i fråga om cybersäkerhet, genom initiativ såsom utarbetande av gemensamma standarder, ökad medvetenhet, utbildning och fortlöpande översyn och testning (eller utarbetande) av mekanismer för tidig varning och för motåtgärder; att förstärka ett nära samarbete och en nära samordning avseende de åtgärder mot cyberincidenter som vidtas av aktörer inom försvaret, brottsbekämpning, den privata sektorn och cybersäkerhetsmyndigheter är också nödvändigt för att ta itu med cyberutmaningar, inklusive hantering av incidenter,

29. UPPMANAR medlemsstaterna

- att vidta åtgärder för att se till att de når en effektiv nationell nivå av cybersäkerhet genom att utveckla och tillämpa lämplig politik samt organisatorisk och operativ kapacitet för att skydda informationssystem i cyberrymden, i synnerhet dem som anses kritiska,

- att upprätta kontakter med industrin och den akademiska världen för att bygga upp förtroende som en central del av den nationella cybersäkerheten exempelvis genom att upprätta offentlig-privata partnerskap,

- att stödja en ökad medvetenhet om arten av hotet och grunderna för goda digitala rutiner på alla nivåer,

- att ge IKT-systemens ägare och leverantörer stöd för skyddet av deras egna system och de viktiga tjänster de tillhandahåller,

- att främja ett paneuropeiskt cybersäkerhetssamarbete, i synnerhet genom att utveckla paneuropeiska cybersäkerhetsövningar,

- att säkerställa ett effektivt samarbete och en effektiv samordning mellan medlemsstaterna på EU-nivå för att nå en gemensam hotbedömning,

- att stärka och utvidga samarbetet mellan medlemsstaterna och användarna inom EU, på grundval av befintliga strukturer,

- att beakta frågorna om cybersäkerhet mot bakgrund av det pågående arbetet med solidaritetsklausulen,

<u>It-brottslighet</u>

30. NOTERAR rådets slutsatser antagna av RIF-rådet den 6–7 juni 2013 om EU:s prioriteringar i kampen mot grov och organiserad brottslighet 2014–2017 där kampen mot it-brottslighet fastställs som en prioritering,

31. UNDERSTRYKER att enligt Europols hotbildsbedömning avseende den grova och organiserade brottsligheten (Socta) för 2013 anses it-brottslighet vara ett brottsområde som utgör ett allt större hot mot EU i form av storskaliga personuppgiftsbrott, it-bedrägeri och sexuellt utnyttjande av barn, samtidigt som vinstdrivande it-brottslighet blir ett redskap för annan brottslig verksamhet,

32. UTTRYCKER SIN UPPSKATTNING för inrättandet av Europeiska it-brottscentrumet vid Europol och UPPMANAR medlemsstaterna att använda centrumet som ett medel för att stärka samarbetet mellan nationella myndigheter inom dess mandat,

33. UPPMANAR Europol och Eurojust att fortsätta att stärka sitt samarbete med alla relevanta aktörer, inklusive EU-organ, Interpol, organisationen för incidenthantering och den privata sektorn i kampen mot it-brottslighet, inklusive genom att framhäva synergieffekter och komplementaritet i enlighet med sina respektive mandat och befogenheter,

34. RÄKNAR MED att Budapestkonventionen om it-brottslighet snabbt ratificeras av alla medlemsstater,

35. UPPMANAR kommissionen, Europol, Europeiska polisakademin och Enisa att stödja utbildning och kompetenshöjning i medlemsstater vars regeringar och brottsbekämpande myndigheter behöver bygga upp cyberkapacitet för att bekämpa it-brottslighet,

36. UPPMANAR kommissionen att

- hjälpa medlemsstater, som begär det, att upptäcka brister och stärka deras kapacitet för att undersöka och bekämpa it-brottslighet,

- använda fonden för inre säkerhet, inom dess budgetgräns (med beaktande av dess övriga prioriteringar) för att stödja relevanta myndigheter i kampen mot it-brottslighet,

- använda stabilitetsinstrumentet för att utveckla kampen mot it-brottslighet samt för initiativ för kapacitetsuppbyggnad inklusive polissamarbete och rättsligt samarbete i tredjeländer varifrån it-brottsorganisationer är verksamma,

- underlätta samordningen av program för kapacitetsuppbyggnad för att undvika dubbelarbete och skapa synergieffekter,

- tillhandahålla information om de framsteg som görs av den globala alliansen mot sexuell exploatering av barn på internet,

- fortsätta att underlätta övervakningen av det politiska klimatet i EU när det gäller kampen mot it-brottslighet, i synnerhet mot bakgrund av de resultat och den strategiska information som ges av Europol (Europeiska centrumet mot it-brottslighet),

- fortsätta att underlätta samarbetet inom gemenskapen, i synnerhet genom att stödja Europol (Europeiska centrumet mot it-brottslighet),

Gemensam säkerhets- och försvarspolitik (GSFP)

37. FRAMHÅLLER, inom ramen för GSFP,

- det brådskande behovet av att tillämpa och vidareutveckla de cyberförsvarsaspekter inom strategin som rör GSFP i syfte att utveckla en ram för cyberförsvaret, när så är lämpligt, och fastställa konkreta åtgärder i det avseendet, även inför den diskussion i Europeiska rådet om säkerhet och försvar som planeras i december 2013. En enda kontaktpunkt bör utses inom utrikestjänsten för att styra dessa insatser,

- behovet av att öka medlemsstaternas cyberförsvarskapacitet, inbegripet genom utarbetande av gemensamma standarder, och ökad medvetenhet genom utbildning i cybersäkerhet, med användning av Europeiska säkerhets- och försvarsakademin och ytterligare förbättra utbildnings- och övningsmöjligheterna för medlemsstaterna,

- användande av de befintliga mekanismerna för sammanslagning och gemensamt utnyttjande samt av synergieffekter med den bredare EU-politiken för att bygga upp nödvändig cyberförsvarskapacitet i medlemsstaterna på det mest effektiva sättet,

- behovet av forskning och utveckling. I första hand kommer medlemsstaterna att uppmanas att utveckla säker och motståndskraftig teknik för cyberförsvar med ett aktivt deltagande av den privata sektorn och den akademiska världen och att stärka cybersäkerhetsaspekter i Europeiska försvarsbyråns forskningsprojekt på grundval av en samarbetsinriktad strategi och som ett gott exempel på en dubbelanvändningskapacitet som ska samordnas mellan Europeiska försvarsbyrån och kommissionen inom europeiska samarbetsramen,

- att mekanismer för tidig varning och för motåtgärder bör ses över och testas mot bakgrund av nya cyberhot, genom dialog med utrikestjänsten, Enisa, Europeiska centrumet mot it-brottslighet, Europeiska försvarsbyrån, kommissionen och medlemsstaterna, i syfte att söka synergieffekter och förbindelser med försvarsgemenskapen,

- behovet av att fullfölja och stärka samarbetet mellan EU och Nato avseende cyberförsvar och fastställa prioriteringar för det fortsatta cyberförsvarssamarbetet mellan EU och Nato inom den befintliga ramen, inklusive ömsesidigt deltagande i cyberförsvarsövningar och utbildning,

- att cyberförsvarsaspekterna innesluts i den bredare politiken för cyberrymden,

Industri/teknik

38. INSER nödvändigheten för Europa att ytterligare utveckla sina industriresurser och teknologiska resurser för cybersäkerhet för att uppnå en lämplig nivå av mångfald och förtroende inom dess nät- och IKT-system, och VÄLKOMNAR varmt den uppmaning som finns i EU:s strategi för cybersäkerhet för Europa om att stödja en kraftfull industripolitik i syfte att främja tillförlitliga europeiska IKT- och cybersäkerhetsbranscher och stimulera den inre marknaden genom forskning och utveckling,

39. UPPMANAR medlemsstaterna, kommissionen och Enisa att stärka insatserna för forskning och utveckling på IKT- och cybersäkerhetsområdet samt tillgängligheten av branschfolk med god beredskap avseende cybersäkerhet, vilket är avgörande för att stimulera konkurrenskraften för den europeiska informations- och kommunikationstekniken (IKT), tjänste- och säkerhetsbranscherna och dessas förmåga att utveckla tillförlitliga och säkra lösningar, och UPPMANAR därför kommissionen att utnyttja Horisont 2020–ramprogrammet för forskning och innovation,

40. BETONAR att utvecklingen av offentlig-privata partnerskap kommer att utgöra ett relevant instrument för att förstärka cybersäkerhetskapaciteten, och UPPMANAR därför kommissionen att främja synergieffekter inom Horisont 2020 mellan operatörer av kritisk infrastruktur, IKT och säkerhetsforskning för frågor som rör cybersäkerhet och it-brottslighet och med unionens politik för inre och yttre säkerhet,

41. UPPMANAR medlemsstaterna och kommissionen att vidta särskilda åtgärder för att stödja cybersäkerheten i små och medelstora företag som är särskilt utsatta för it-attacker och uppmuntrar medlemsstaterna att utveckla en säker och motståndskraftig teknik för cybersäkerhet med ett samarbetsinriktat deltagande av den privata sektorn och den akademiska världen,

42. UPPMANAR kommissionen att beakta de standarder som finns på området för cybersäkerhet och UNDERSTRYKER att samarbete och informationsutbyte avseende standarder – t.ex. för riskhantering – bör utvecklas ytterligare, i samarbete med medlemsstaterna och branschen samt andra relevanta aktörer,

Internationellt cyberrymdssamarbete

43. UPPREPAR EU:s åtagande att stödja utvecklingen av förtroendeskapande åtgärder inom cybersäkerheten för att öka insynen och minska risken för missförstånd när det gäller länders agerande, genom att verka för att internationella standarder fastställs på detta område,

44. UPPMANAR kommissionen och den höga representanten att i enlighet med relevanta förfaranden i fördragen

- a) främja Budapestkonventionen som en modell för utformningen av nationell lagstiftning om it-brottslighet och som underlag för internationellt samarbete på detta område och b) främja respekten för grundläggande rättigheter i cyberrymden och c) till fullo utnyttja alla tillgängliga internationella samarbetsverktyg för att utveckla kampen mot it-brottslighet samt därtill hörande polissamarbete och rättsligt samarbete i tredjeländer varifrån it-brottsorganisationer är verksamma,

- inhämta medlemsstaternas cyberpolitiska expertis samt deras erfarenhet av bilaterala åtaganden/bilateralt samarbete för att utveckla gemensamma budskap från EU om frågor som rör cyberrymden och arbeta nära medlemsstaterna med de operativa aspekterna,

- i samarbete med medlemsstaterna och relevanta privata organisationer samt det civila samhället till fullo utnyttja EU:s relevanta stödinstrument för kapacitetsuppbyggnad avseende IKT, inklusive cybersäkerhet,

45. UPPMANAR medlemsstaterna, kommissionen och den höga representanten att arbeta med sikte på en enhetlig internationell politik för cybersäkerhet för EU, i enlighet med relevanta förfaranden i fördragen, genom att

- öka engagemanget med viktiga internationella partner och organisationer på ett sätt som garanterar att alla medlemsstater kan dra full nytta av ett sådant samarbete,

- införliva cyberfrågor i Gusp,

- förbättra samordningen av globala cyberfrågor och integrera cybersäkerhet inklusive förtroendeskapande åtgärder och åtgärder för insyn i den övergripande ramen för att sköta förbindelserna med tredjeländer och internationella organisationer, inklusive genom ökad samordning mellan medlemsstaterna, kommissionen och utrikestjänsten avseende genomförandet av dialoger och annan verksamhet för cybersäkerhet,

- förbättra samordningen genom rådets relevanta förberedande organ (inklusive Ordförandeskapets vänner (cyberfrågor)),

- stödja kapacitetsuppbyggnad i tredjeländer, genom utbildning och bistånd för upprättande av relevant nationell politik, strategier och institutioner i syfte att frigöra den fulla ekonomiska och sociala potential som finns inom IKT, stödja utvecklingen av motståndskraftiga system i de länderna och minska cyberriskerna för EU:s institutioner och medlemsstater, med fullt utnyttjande av befintliga nät och forum för politisk samordning och informationsutbyte,

Roller och ansvarsfördelning

46. UPPMANAR de övriga intressenterna – den privata sektorn, tekniska och akademiska samfund, det civila samhället, och enskilda medborgare att åta sig sina respektive roller och sitt ansvar för att skapa en öppen, fri och säker cyberrymd,

47. UPPMANAR kommissionen och den höga representanten att se till att de europeiska åtgärderna utformas så att de är förenliga med nationella strukturer, statsrätten och initiativ som rör cybersäkerhet, i syfte att garantera ett integrerat tillvägagångssätt och undvika överlappning,

OCH

48. UPPMANAR kommissionen och den höga representanten att utarbeta en lägesrapport om strategin för cybersäkerhet som ska läggas fram vid högnivåkonferensen i februari2014; och FÖRESLÅR att rådets behöriga förberedande organ håller regelbundna möten, (särskilt gruppen Ordförandeskapets vänner (cyberfrågor)) för att bidra till att fastställa EU:s prioriteringar i cyberfrågor och strategiska mål som en del av en övergripande politisk ram och se över och stödja det pågående genomförandet av strategin,

49. vid genomförandet av dessa slutsatser från rådet kommer endast befintliga fonder och finansieringsprogram att användas, utan att det påverkar förhandlingarna om den framtida budgetramen och därför UPPMANAR rådet kommissionen att lägga fram ett förslag till finansiering av strategin, med hänsyn tagen till de kommande förhandlingarna med Europaparlamentet.

Hänvisningar

1. Europaparlamentet, rådet och kommissionen

   – Europeiska unionens stadga om de grundläggande rättigheterna[2].

2. Europaparlamentet och rådet

   – Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet[3].

   – Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv), ändrat genom direktiv 2009/140/EG[4].

3. Europaparlamentet

   – Europaparlamentets resolution av den 11 december 2012 om en strategi för digital frihet i EU:s utrikespolitik.

   – Europaparlamentets betänkande från 2012 om it-säkerhet och it-försvar.

4. Rådet

   – Stockholmsprogrammet – Ett öppet och säkert Europa i medborgarnas tjänst och för deras skydd[5].

   – Ett säkert Europa i en bättre värld – En europeisk säkerhetsstrategi, av den 12 december 2003[6].

---

2 EUT C 364, 18.12.2010, s. 1.
3 EUT L 077, 13.3.2004.
4 EGT L 108, 24.4.2002 och EUT L 337, 18.12.2009, s. 37.
5 Dok. 17024/09 CO EUR PREP 3 JAI 896 POLGEN 229.
6 Dok. 15849/03 PESC 783.

– Strategi för inre säkerhet i Europeiska unionen: *Mot en europeisk säkerhetsmodell*[7].

– Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna[8].

– Rådets slutsatser om kommissionens meddelande om EU:s strategi för den inre säkerheten i praktiken[9].

– Rådets slutsatser om kommissionens meddelande om skydd av kritisk informationsinfrastruktur (*Resultat och kommande åtgärder: vägen mot global it-säkerhet*)[10].

– Rådets slutsatser om fastställande av EU:s prioriteringar i kampen mot grov och organiserad brottslighet 2014–2017[11].

– Rådets slutsatser om inrättandet av ett europeiskt centrum mot it-brottslighet[12].

---

7 Dok. 5842/2/10 JAI 90.

8 EUT L 345, 23.12.2008.

9 Dok. 6699/11 JAI 124.

10 Dok. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66. Detta meddelande är en uppföljning av kommissionens meddelande om skydd av kritisk informationsinfrastruktur – *Skydd mot storskaliga it-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa* (dok. 8375/09).

11 Dok. 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434.

12 Dok. 10603/12 ENFOPOL 154 TELECOM 116.

– Förslag till Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF 89. Godkännande av den slutliga kompromisstexten i syfte att nå en överenskommelse med Europaparlamentet vid första behandlingen[13].

– Rådets slutsatser om den europeiska strategin för ett bättre internet för barn[14].

– Rådets slutsatser om bekämpande av sexuellt utnyttjande av barn och barnpornografi på internet – effektivisering av polisens verksamhet i medlemsstaterna och tredjeländer[15].

– Rådets slutsatser om en global allians mot sexuell exploatering av barn på internet[16].

– Rådets slutsatser om en samordnad arbetsstrategi och konkreta åtgärder mot it-brottslighet[17] och rådets slutsatser om en handlingsplan för att genomföra den samordnade strategin för att bekämpa it-brottslighet[18].

– Rådets partiella allmänna riktlinje om kommissionens förslag till förordning om inrättande av Horisont 2020 – ramprogrammet för forskning och innovation (2014–2020)[19].

– Rådets gemensamma åtgärd om inrättande av en europeisk försvarsbyrå[20].

---

13 Dok. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673.
14 Dok. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81.
15 Dok. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53.
16 Dok. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46.
17 Dok. 15569/08 ENFOPOL 224 CRIMORG 190.
18 Dok. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32.
19 Dok. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511.
20 Dok. 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121.

– Gemensamt förslag till rådets beslut om närmare bestämmelser för hur unionen ska genomföra solidaritetsklausulen[21].

– Rådets slutsatser om mediekompetens i den digitala miljön[22].

– Mänskliga rättigheter och demokrati: EU:s strategiska ram och EU:s handlingsplan[23].

– Rapport om genomförandet av EU:s säkerhetsstrategi[24].

5. Kommissionen

– Den digitala agendan för Europa[25], som är ett av de sju flaggskeppsinitiativen i Europa 2020-strategin för smart och hållbar tillväxt för alla[26], och *Den digitala agendan för Europa – Drivkraft för den europeiska digitala tillväxten*[27], som ger den digitala agendan en ny inriktning.

– Meddelandet *Skydd av den personliga integriteten i en uppkopplad värld. En europeisk ram för personuppgiftsskydd för tjugohundratalet*[28].

– Meddelandet *Brottsbekämpning i vår digitala tidsålder: inrättande av ett Europeiskt centrum mot it-brottslighet*[29].

---

21 Dok. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165.

22 Dok. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380.

23 Dok. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603.

24 Dok. 17104/08 CAB 66 PESC 1687 POLGEN 139.

25 Dok. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.

26 Dok. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74.

27 Dok. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216.

28 Dok. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6.

29 Dok. 8543/12 ENFOPOL 94 TELECOM 72.

– Kommissionens meddelande *Att frigöra de molnbaserade datortjänsternas potential i Europa*[30].

– Kommissionens meddelande om skydd av kritisk infrastruktur *Resultat och kommande åtgärder: vägen mot global it-säkerhet*, [31].

– Kommissionens meddelande om skydd av kritisk informationsinfrastruktur – *Skydd mot storskaliga it-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa*[32].

6. FN

– FN:s generalförsamlings resolution A/RES 57/239 om inrättandet av en global kultur för it-säkerhet.

– Resolution A/HRC/20/L.13 av den 29 juni 2012 från FN:s råd för mänskliga rättigheter om främjande, skydd och åtnjutande av mänskliga rättigheter på internet.

– FN:s generalförsamlings resolution A/RES 67/27 om utvecklingen inom området för information och telekommunikation i fråga om internationell säkerhet.

– Inrättande av en öppen mellanstatlig expertgrupp om it-brottslighet vid FN:s drog- och brottsbekämpningsbyrå i enlighet med FN:s generalförsamlings resolution 65/230.

7. Europarådet

– Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter.

– Europarådets konvention av den 23 november 2001 om it-brottslighet.

---

30 Dok. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585.
31 Dok. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38.
32 Dok. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46.

8. Organisationen för säkerhet och samarbete i Europa (OSSE)

– Ständiga rådets beslut nr 1039 av den 26 april 2012: Utveckling av förtroendeskapande åtgärder för att minska riskerna för konflikter som härrör från användningen av informations- och kommunikationsteknik.

– Ministerbeslut nr 4/12 av den 7 december 2012: OSSE:s insatser för att hantera transnationella hot.

– OSSE:s öppna, informella arbetsgrupp för utarbetande av ett utkast till förtroendeskapande åtgärder för att öka det mellanstatliga samarbetet, öppenheten, förutsebarheten och stabiliteten, och för att minska riskerna för missförstånd, upptrappning och konflikter som kan härröra från användningen av informations- och kommunikationsteknik (OSSE:s ständiga råds beslut nr 1039 av den 26 april 2012).

9. Konferenser, initiativ och evenemang

– Den internationella konferensen om cyberrymden, som ägde rum i London den 1–2 november 2011 och följdes upp den 4–5 oktober 2012 genom en internationell konferens om cyberrymden i Budapest.

– Den gemensamma skrivbordsövningen mellan EU och USA om cyberincidenter, Cyber Atlantic 2011, och paneuropeiska övningar om cyberincidenter där alla medlemsstater deltog (Cyber Europe 2010 och Cyber Europe 2012).

– Ad hoc-gruppen för kärnsäkerhet, som i sin slutrapport diskuterade och vidareutvecklade frågan om datasäkerhet/cybersäkerhet[33].

[33] Dok. 10616/12 AHGS 20 ATO 84.

10. Övrigt

– Europols hotbildsbedömning avseende den grova organiserade brottsligheten (Socta) för 2013[34].

– Säkerhetsstrategin för informationssäkring[35] och riktlinjerna[36] för nätverksförsvar.

---

[34] Dok. 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211.

[35] Dok. 8408/12 CSCI 11 CSC 20.

[36] Dok. 10578/12 CSCI 20 CSC 34.