4. Europaparlamentet begär att kommissionen stöder medlemsstaternas insatser för att minska löneklyftan mellan könen med minst 5 procentenheter per år, med målet att avskaffa denna löneklyfta till 2020.

5. Europaparlamentet medger att ett mångfasetterat tillvägagångssätt på flera nivåer kräver att kommissionen stödjer medlemsstaterna då de främjar bra metoder och driver en politik för att motverka löneskillnaderna mellan kvinnor och män.

6. Europaparlamentet uppmanar kommissionen att utan dröjsmål se över direktiv 2006/54/EG och föreslå ändringar av det i enlighet med artikel 32 i det direktivet och på grundval av artikel 157 i FEUF, i överensstämmelse med de ingående rekommendationer som ges i bilagan till parlamentets resolution av den 24 maj 2012.

7. Europaparlamentet uppdrar åt talmannen att översända denna resolution till rådet, kommissionen och medlemsstaternas regeringar.

P7_TA(2013)0376

Strategi för cybersäkerhet i EU: En öppen, säker och skyddad cyberrymd

Europaparlamentets resolution av den 12 september 2013 om EU:s strategi för it-säkerhet: en öppen, säker och trygg cyberrymd (2013/2606(RSP))

(2016/C 093/16)

Europaparlamentet utfärdar denna resolution

— med beaktande av det gemensamma meddelandet av den 7 februari 2013 från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd* (JOIN (2013)0001),

— med beaktande av kommissionens förslag till direktiv av den 7 februari 2013 om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, (COM(2013)0048),

— med beaktande av kommissionens meddelanden av den 19 maj 2010 *En digital agenda för Europa* (COM(2010)0245) och av den 18 december 2012 *Den digitala agendan för Europa – Drivkraft för den europeiska digitala tillväxten* (COM(2012) 0784),

— med beaktande av kommissionens meddelande av den 27 september 2012 *Att frigöra de molnbaserade datortjänsternas potential i Europa* (COM(2012)0529),

— med beaktande av kommissionens meddelande av den 28 mars 2012 *Brottsbekämpning i vår digitala tidsålder: inrättande av ett Europeiskt centrum mot it-brottslighet* (COM(2012)0140) och av rådets slutsatser av den 7 juni 2012 om detta,

— med beaktande av Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om upphävande av rådets rambeslut 2005/222/RIF ([1]),

— med beaktande av 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 ([2]),

---

([1]) EUT L 218, 14.8.2013, s. 8.
([2]) EUT L 345, 23.12.2008, s. 75.

— med beaktande av Europaparlamentets och rådets direktiv 2011/92/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF ([1]),

— med beaktande av Stockholmsprogrammet ([2]) på området med frihet, säkerhet och rättvisa, kommissionens meddelanden *Att förverkliga ett område med frihet, säkerhet och rättvisa för EU-medborgarna – Handlingsplan för att genomföra Stockholmsprogrammet* (COM(2010)0171) och *EU:s strategi för den inre säkerheten i praktiken: Fem steg mot ett säkrare Europa* (COM(2010)0673) samt sin resolution av den 22 maj 2012 om Europeiska unionens strategi för inre säkerhet ([3]),

— med beaktande av kommissionens och den höga representantens gemensamma förslag till rådets beslut om närmare bestämmelser för hur unionen ska genomföra solidaritetsklausulen (JOIN(2012)0039),

— med beaktande av rådets rambeslut 2001/413/RIF av den 28 maj 2001 om bekämpning av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter ([4]),

— med beaktande av sin resolution av den 12 juni 2012 om skydd av kritisk infrastruktur ”Resultat och kommande åtgärder: vägen mot global it-säkerhet” ([5]) och av rådets slutsatser av den 27 maj 2011 om kommissionens meddelande om skydd av kritisk infrastruktur ”Resultat och kommande åtgärder: vägen mot global it-säkerhet” (COM(2011)0163),

— med beaktande av sin resolution av den 11 december 2012 om att fullborda en inre e-marknad ([6]),

— med beaktande av sin resolution av den 22 november 2012 om rättvis handel och utveckling ([7]),

— med beaktande av sin ståndpunkt av den 16 april 2013 vid första behandlingen om förslaget till Europaparlamentets och rådets förordning om Europeiska byrån för nät- och informationssäkerhet (Enisa) (COM(2010)0521) ([8]),

— med beaktande av sin resolution av den 11 december 2012 om en strategi för digital frihet i EU:s utrikespolitik ([9]),

— med beaktande av Europarådets konvention om it-relaterad brottslighet av den 23 november 2001,

— med beaktande av unionens internationella skyldigheter, särskilt enligt det allmänna tjänstehandelsavtalet (Gats),

— med beaktande av artikel 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 6, 8 och 11,

— med beaktande av de pågående förhandlingarna om det transatlantiska partnerskapet för handel och investeringar mellan Europeiska unionen och Amerikas förenta stater,

— med beaktande av artikel 110.2 i arbetsordningen, och av följande skäl:

A. De växande it-utmaningarna, i form av alltmer sofistikerade hot och angrepp, utgör ett stort hot mot säkerhet, stabilitet och ekonomiskt välstånd i medlemsstaterna och för den privata sektorn och allmänheten. Skyddet av vårt samhälle och vår ekonomi kommer därför att bli en utmaning som ständigt utvecklas.

([1]) EUT L 335, 17.12.2011, s. 1.
([2]) EUT C 115, 4.5.2010, s. 1.
([3]) Antagna texter, P7_TA(2012)0207.
([4]) EGT L 149, 2.6.2001, s. 1.
([5]) Antagna texter, P7_TA(2012)0237.
([6]) Antagna texter, P7_TA(2012)0468.
([7]) Antagna texter, P7_TA(2012)0457.
([8]) Antagna texter, P7_TA(2013)0103.
([9]) Antagna texter, P7_TA(2012)0470.

Torsdagen den 12 september 2013

B. Cyberrymden och it-säkerhet bör vara en av de strategiska pelarna i EU:s och varje medlemsstats säkerhets- och försvarspolitik. Det är viktigt att se till att cyberrymden fortsätter att vara öppen för ett fritt flöde av tankar, information och fritt uttryck.

C. E-handel och onlinetjänster är en vital del av internet och av avgörande betydelse för målen med Europa 2020-strategin, till nytta för både allmänheten och den privata sektorn. Unionen måste fullt ut förverkliga den potential och de möjligheter som erbjuds av internet i vidareutvecklingen av den inre marknaden, inbegripet den digitala inre marknaden.

D. De strategiska prioriteringar som anges i det gemensamma meddelandet om en it-säkerhetsstrategi för EU omfattar it-motståndskraft, minskad it-brottslighet, utveckling av en politik för it-försvar och it-kapacitet i anslutning till den gemensamma säkerhets- och försvarspolitiken (GSFP) samt fastställande av en sammanhängande och internationell EU-politik för cyberrymden.

E. Nät- och informationssystemen i hela unionen är i hög grad sammanlänkade. På grund av internets globala natur överskrider många tillbud som rör nät- och informationssäkerhet de nationella gränserna, vilket kan komma att undergräva den inre marknadens funktion och minska konsumenternas förtroende för den digitala inre marknaden.

F. It-säkerheten i unionen är precis som i övriga världen inte starkare än sin svagaste länk, och störningar i en sektor eller medlemsstat som påverkar en annan sektor eller medlemsstat skapar spridningseffekter med konsekvenser för unionens ekonomi som helhet.

G. I april 2013 hade endast 13 medlemsstater officiellt antagit nationella strategier för it-säkerhet. Grundläggande skillnader kvarstår mellan medlemsstaterna i fråga om deras beredskap, säkerhet, strategiska kultur samt förmåga att ta fram och genomföra nationella strategier för it-säkerhet, och dessa skillnader bör analyseras.

H. Olika säkerhetskulturer och bristen på rättsliga ramar leder till fragmentering, vilket har stor betydelse för den digitala inre marknaden. Frånvaron av en harmoniserad strategi för it-säkerhet innebär allvarliga hot mot det ekonomiska välståndet och säkerheten för transaktioner, och det krävs därför samordnade insatser och ett närmare samarbete mellan regeringar, den privata sektorn samt brottsbekämpande organ och underrättelsetjänster.

I. It-brottslighet är ett allt dyrare internationellt problem, som för närvarande kostar – enligt FN:s drog- och brottsbekämpningsbyrå – den globala ekonomin nästan 295 miljarder euro varje år.

J. Den internationella organiserade brottsligheten utnyttjar de tekniska framstegen och håller på att överföra sitt verksamhetsområde till cyberrymden, där it-brottslighet håller på att radikalt förändra de traditionella strukturerna inom den organiserade brottsligheten. Detta har lett till att den organiserade brottsligheten inte är lika bunden till en plats och i högre grad utnyttjar territorialitet och skilda nationella jurisdiktioner på global nivå.

K. De behöriga myndigheternas utredning av it-brottslighet hämmas fortfarande av åtskilliga hinder, bland annat användningen av ”virtuella valutor” för transaktioner i cyberrymden vilka kan utnyttjas för penningtvätt, frågorna om territorialitet och gränserna för domstolarnas behörighet, otillräcklig kapacitet för underrättelseutbyte, brist på utbildad personal samt inkonsekvent samarbete med andra intressenter.

L. Tekniken är grunden för utveckling av cyberrymden, och en kontinuerlig anpassning till de tekniska förändringarna är avgörande om motståndskraften och säkerheten för cyberrymden i EU ska kunna förbättras. Åtgärder måste vidtas för att se till att lagstiftningen hålls uppdaterad med den nyaste tekniska utvecklingen, så att det blir möjligt att på ett ändamålsenligt sätt identifiera och åtala it-brottslingar och skydda offer för it-brottslighet. EU:s strategi för it-säkerhet

måste omfatta åtgärder som är inriktade på medvetenhet, utbildning, utveckling av organisationer för incidenthantering (Cert), utveckling av en inre marknad för produkter och tjänster för it-säkerhet samt främjande av investeringar i forskning, utveckling och innovation.

1. Europaparlamentet välkomnar det gemensamma meddelandet om en it-säkerhetsstrategi för EU och förslaget till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen.

2. Europaparlamentet framhåller den yttersta vikt och allt större betydelse som internet och cyberrymden har för politiska, ekonomiska och samhälleliga transaktioner, inte bara inom unionen utan också i förhållande till andra aktörer runt om i världen.

3. Europaparlamentet betonar att det är nödvändigt att utveckla en politik för strategisk kommunikation om EU:s it-säkerhet, it-krissituationer, strategiöversyner, offentlig-privat samarbete och varning samt rekommendationer till allmänheten.

4. Europaparlamentet påminner om att en hög nivå på nät- och informationssäkerheten behövs inte bara för att upprätthålla tjänster som är av avgörande betydelse för ett smidigt fungerande samhälle och för ekonomin, utan också för att skydda medborgarnas fysiska integritet genom ökad effektivitet och ändamålsenlighet och ett säkrare funktionssätt för kritisk infrastruktur. Nät- och informationssäkerheten måste tas upp, men förbättrad fysisk säkerhet är också en viktig fråga. Parlamentet betonar att infrastrukturen bör vara motståndskraftiga mot både avsiktliga och oavsiktliga störningar. I detta sammanhang bör it-säkerhetsstrategin vara mer inriktad på de vanliga orsakerna till oavsiktliga systemfel.

5. Europaparlamentet upprepar sin uppmaning till medlemsstaterna att anta nationella it-säkerhetsstrategier som omfattar aspekter rörande teknik, samordning, mänskliga resurser och fördelning av ekonomiska medel och som innehåller särskilda regler om vinsterna och ansvaret för den privata sektorn, i syfte att utan onödigt dröjsmål säkra den privata sektorns deltagande, samt att tillhandahålla övergripande riskhanteringsförfaranden och skydda regelverket.

6. Europaparlamentet konstaterar att endast ett kombinerat ledarskap och politiskt ansvarstagande av unionens institutioner och medlemsstaterna kommer att möjliggöra en hög nivå på nät- och informationssäkerheten i hela unionen, och därmed bidra till en säker och smidigt fungerande inre marknad.

7. Europaparlamentet betonar att unionens it-säkerhetspolitik bör erbjuda en säker och tillförlitlig digital miljö som bygger på, och är utformad för att garantera, skyddet för och bevarandet av friheterna och respekten för de grundläggande rättigheterna online, enligt vad som anges i EU-stadgan och i artikel 16 i EUF-fördraget, särskilt rätten till personlig integritet och uppgiftsskydd. Parlamentet anser att särskild uppmärksamhet bör ägnas åt skyddet av barn online.

8. Europaparlamentet uppmanar medlemsstaterna och kommissionen att vidta alla åtgärder som är nödvändiga för att lägga fram utbildningsprogram som syftar till att främja och förbättra medvetenheten, kompetensen och utbildningen bland medborgarna i EU, i synnerhet med avseende på personlig säkerhet, som en del av en läroplan med digital kompetens från tidig ålder. Parlamentet välkomnar initiativet att anordna en europeisk månad för it-säkerhet. med stöd av Enisa och i samarbete med offentliga myndigheter och den privata sektorn, i syfte att öka medvetenheten om de utmaningar som skyddet av nät- och informationssystem är förknippat med.

9. Europaparlamentet anser att utbildning om it-säkerhet ökar de europeiska samhällenas medvetenhet om it-hoten, vilket främjar en ansvarsfull användning av cyberrymden och bidrar till att öka tillgången på it-kompetens. Europol och det nya Europeiska it-brottscentrumet, liksom Enisa och Eurojust, spelar en nyckelroll genom att tillhandahålla utbildningsinsatser på EU-nivå om användning av verktygen inom det internationella rättsliga samarbetet och om brottsbekämpning som rör olika aspekter av it-brottslighet.

10. Europaparlamentet upprepar behovet att ge teknisk rådgivning och juridisk information samt att inrätta program för att förebygga och bekämpa it-brottslighet. Parlamentet uppmuntrar utbildning av it-tekniker som är specialiserade på att skydda kritisk infrastruktur och informationssystem samt operatörer av transportkontrollsystem och trafikledningscentraler. Parlamentet understryker det akuta behovet av regelbunden utbildning i it-säkerhet för personalen inom den offentliga sektorn på alla nivåer.

11. Europaparlamentet upprepar sin uppmaning till försiktighet i begränsningar av allmänhetens möjlighet att använda kommunikations- och it-verktyg, och betonar att medlemsstaterna bör sikta på att aldrig äventyra medborgarnas fri- och rättigheter vid utarbetandet av reaktioner på it-hot och it-angrepp. Medlemsstaterna bör också ha tillräckligt lagstiftningsutrymme för att kunna göra en åtskillnad mellan it-tillbud av civil respektive militär omfattning.

12. Europaparlamentet anser att regleringar på it-säkerhetsområdet bör vara riskorienterade, inriktade på kritisk infrastruktur – då det är ett viktigt allmänintresse att denna fungerar – och utgå från befintliga marknadsbaserade insatser i branschen för att säkerställa nätens motståndskraft. Parlamentet understryker den avgörande roll som samarbete på operativ nivå spelar för att främja ett effektivare utbyte av information om it-hot mellan offentliga myndigheter och den privata sektorn – både på unionsnivå och på nationell nivå, liksom med strategiska partner för unionen – med målet att garantera nät- och informationssäkerhet genom ökat ömsesidigt förtroende, värde och engagemang samt utbyte av sakkunskap. Parlamentet anser att offentlig-privata partnerskap bör bygga på nät- och teknikneutralitet och inriktas på insatser för att hantera problem med stora återverkningar för allmänheten. Parlamentet uppmanar kommissionen att uppmuntra alla inblandade marknadsaktörer att bli mer vaksamma och mer samarbetsinriktade, i syfte att skydda andra aktörer från skada på deras tjänster.

13. Upptäckt och rapportering av it-säkerhetstillbud är centralt för att främja it-motståndskraften i unionen. Europaparlamentet anser att proportionerliga och nödvändiga krav på att lämna ut upplysningar bör införas för att möjliggöra rapportering av tillbud som är förknippade med betydande säkerhetsöverträdelser till de behöriga nationella myndigheterna, och därmed möjliggöra en bättre övervakning av it-brottstillbud och underlätta insatser för att öka medvetenheten på alla nivåer.

14. Europaparlamentet uppmanar kommissionen och andra aktörer att införa en politik för it-säkerhet och it-motståndskraft som omfattar ekonomiska incitament som främjar en hög nivå på it-säkerhet och it-motståndskraft.

It-motståndskraft

15. Europaparlamentet konstaterar att olika sektorer och medlemsstater har olika nivåer på sin kapacitet och kompetens, och detta hindrar en utveckling av ett samarbete som präglas av tillit och undergräver den inre marknadens funktion.

16. Europaparlamentet anser att kraven på små och medelstora företag bör följa en proportionerlig och riskbaserad strategi.

17. Europaparlamentet insisterar på att it-motståndskraft måste utvecklas för kritisk infrastruktur, och påminner om att de kommande arrangemangen för att genomföra solidaritetsklausulen (artikel 222 i EUF-fördraget) bör beakta risken för it-angrepp mot en medlemsstat. Parlamentet uppmanar kommissionen och den höga representanten att ta hänsyn till denna risk i sina gemensamma integrerade hot- och riskutvärderingsrapporter som ska avges från och med 2015.

18. Europaparlamentet betonar att man för att garantera integritet, tillgänglighet och sekretess för i synnerhet kritiska tjänster måste ha en aktuell identifiering och klassificering av kritisk infrastruktur, och de nödvändiga minimisäkerhetskraven för nät och informationssystem måste vara fastställda.

19. Europaparlamentet framhåller att förslaget till direktiv om åtgärder för att garantera en hög gemensam nivå på nät- och informationssäkerheten i EU föreskriver sådana minimisäkerhetskrav för leverantörer av informationssamhällets tjänster och operatörer av kritisk infrastruktur.

20. Europaparlamentet uppmanar medlemsstaterna och unionen att fastställa lämpliga ramar för system för snabbt, ömsesidigt informationsutbyte som garanterar anonymitet för den privata sektorn och håller den offentliga sektorn konstant uppdaterad och, om så krävs, ge stöd till den privata sektorn.

21. Europaparlamentet välkomnar kommissionens tanke om att skapa en riskhanteringskultur för it-säkerhet och uppmanar medlemsstaterna och unionens institutioner att snarast inbegripa it-krishantering i sina krishanteringsplaner och riskanalyser. Parlamentet uppmanar vidare medlemsstaternas regeringar och kommissionen att uppmuntra privata aktörer att inbegripa it-krishantering i sina förvaltningsplaner och riskanalyser och att utbilda personalen i it-säkerhet.

22. Europaparlamentet uppmanar alla medlemsstater och unionens institutioner att inrätta ett nätverk med välfungerande organisationer för incidenthantering (Cert) som är operativa dygnet runt, sju dagar i veckan. Parlamentet påpekar att nationella incidenthanteringsorganisationer bör utgöra en del av ett ändamålsenligt nätverk i vilket den relevanta informationen utbyts under uppfyllande av erforderliga normer för förtroende och sekretess. Parlamentet konstaterar att övergripande initiativ som sammanför incidenthanteringsorganisationer och andra relevanta säkerhetsorgan kan fungera som värdefulla verktyg i skapandet av förtroende i ett gränsöverskridande och sektorsövergripande sammanhang. Parlamentet betonar vikten av ett effektivt och ändamålsenligt samarbete mellan incidenthanteringsorganisationer och brottsbekämpande myndigheter i kampen mot it-brottslighet.

23. Europaparlamentet stöder Enisa i utövandet av byråns arbetsuppgifter med avseende på nät- och informationssäkerhet, i synnerhet genom att tillhandahålla vägledning och ge råd åt medlemsstaterna samt genom att stödja utbyte av bästa praxis och skapandet av ett klimat av förtroende.

24. Europaparlamentet betonar att branschen behöver införa lämpliga prestandakrav på it-säkerhet längs hela värdekedjan för IKT-produkter som används i transportnät och informationssystem, utföra lämplig riskhantering, anta standarder och lösningar för säkerhet och utveckla bästa praxis och informationsutbyte i syfte att säkerställa it-säkra transportsystem.

Industri- och teknikresurser

25. Europaparlamentet anser att garantier för en hög nivå på nät- och informationssäkerheten spelar en central roll för att öka konkurrenskraften för både leverantörer och användare av säkerhetslösningar i unionen. It-säkerhetsbranschen i unionen har en betydande outnyttjad potential, men användare som är privata och offentliga aktörer och företag är ofta inte informerade om kostnader och fördelar med att investera i it-säkerhet, och därmed fortfarande sårbara för skadliga it-hot. Parlamentet betonar att införandet av incidenthanteringsorganisationer är en relevant faktor i detta avseende.

26. Europaparlamentet anser att ett starkt utbud av, och efterfrågan på, it-säkerhetslösningar kräver tillräckliga investeringar i akademiska resurser, forskning och utveckling (FoU) samt kunskaps- och kapacitetsuppbyggnad om den del av de nationella myndigheterna som sysslar med IKT-frågor, i syfte att främja innovationer och skapa tillräcklig medvetenhet om risker när det gäller nät- och informationssäkerhet, vilket leder till en samordnad säkerhetsbransch i Europa.

27. Europaparlamentet uppmanar EU-institutionerna och medlemsstaterna att vidta nödvändiga åtgärder för att inrätta en ”inre marknad för it-säkerhet” där användare och leverantörer på bästa sätt kan använda sig av de innovationer, synergier och kombinerade sakkunskaper som står till buds och som gör det möjligt för små och medelstora företag att ta sig in på marknaden.

28. Europaparlamentet uppmanar medlemsstaterna att överväga gemensamma investeringar i den europeiska it-säkerhetsbranschen, ungefär på samma sätt som har gjorts inom andra branscher, exempelvis luftfartssektorn.

It-brottslighet

29. Europaparlamentet anser att brottslig verksamhet i cyberrymden kan vara lika skadlig för samhällets välfärd som brott i den fysiska världen, och att dessa former av brottslighet ofta förstärker varandra, vilket kan observeras exempelvis när det gäller sexuellt utnyttjande av barn och organiserad brottslighet och penningtvätt.

30. Europaparlamentet konstaterar att det i vissa fall finns en koppling mellan laglig och olaglig näringsverksamhet. Parlamentet framhåller den koppling, som underlättas genom internet, som finns mellan finansiering av terrorism och grov organiserad brottslighet. Parlamentet betonar att allmänheten måste göras medveten om allvaret i att bli inblandad i it-brottslighet och om att det som vid första anblicken kan förefalla vara ett ”socialt acceptabelt” brott – såsom olaglig nedladdning av filmer – ofta genererar stora belopp för internationella brottssyndikat.

31. Europaparlamentet håller med kommissionen om att samma normer och principer som gäller offline också gäller online, och att kampen mot it-brottslighet därför behöver trappas upp med hjälp av aktuell lagstiftning och operativ kapacitet.

32. Europaparlamentet anser att gemensamma insatser som genomförs och sakkunskap som erbjuds på unionsnivå, ovanför nivån för de enskilda medlemsstaterna, med tanke på it-brottslighetens gränsöverskridande natur är särskilt viktiga, och att Eurojust, Europeiska it-brottscentrumet inom Europol, incidenthanteringsorganisationer samt universitet och forskningscentrum därför måste förses med tillräckliga resurser och kapaciteter för att kunna fungera som knutpunkter för sakkunskap, samarbete och informationsutbyte.

33. Europaparlamentet välkomnar varmt inrättandet av Europeiska it-brottscentrumet, och uppmuntrar denna byrås framtida utveckling, med dess centrala roll för att samordna ett snabbt och effektivt gränsöverskridande utbyte av information och sakkunskap till stöd för insatser för att förebygga, upptäcka och utreda it-brottslighet.

34. Europaparlamentet uppmanar medlemsstaterna att se till att medborgarna enkelt kan få tillgång till information om it-hot och hur man kan bekämpa dem. Parlamentet anser att sådan vägledning bör omfatta information om hur användarna kan skydda sin personliga integritet på internet, hur man upptäcker och anmäler fall av gromning, hur man installerar programvara och brandväggar, hur man hanterar lösenord samt hur man upptäcker nätfiske (phishing), falska webbplatser (pharming) och andra angrepp.

35. Europaparlamentet insisterar på att de medlemsstater som ännu inte har ratificerat Europarådets konvention om it-brottslighet gör detta utan onödigt dröjsmål. Parlamentet välkomnar Europarådets synpunkter angående behovet att uppdatera denna konvention i ljuset av den tekniska utvecklingen, för att säkerställa att den är fortsatt effektiv i kampen mot it-brottslighet, och uppmanar kommissionen och medlemsstaterna att delta i denna debatt. Parlamentet stöder de insatser som görs för att främja ratificeringen av konventionen bland andra länder, och uppmanar kommissionen att främja den på ett aktivt sätt utanför unionen.

It-försvar

36. Europaparlamentet betonar att it-utmaningar, it-hot och it-angrepp utsätter medlemsstaternas försvar och nationella säkerhetsintressen för risker, och att civila och militära strategier för att skydda kritisk infrastruktur bör maximera nyttan på båda områden genom ansträngningar för att uppnå synergieffekter.

37. Europaparlamentet uppmanar därför medlemsstaterna att intensifiera sitt samarbete med Europeiska försvarsbyrån i syfte att utveckla förslag och initiativ till it-försvarskapacitet och bygga vidare på den senaste tidens initiativ och projekt. Parlamentet understryker behovet att stärka FoU, bland annat genom sammanslagning och gemensamt utnyttjande av resurser.

38. Europaparlamentet upprepar att en övergripande europeisk it-säkerhetsstrategi bör beakta mervärdet med befintliga byråer och organ samt god praxis från de medlemsstater som redan har infört nationella it-säkerhetsstrategier på egen hand.

39. Europaparlamentet uppmanar vice ordföranden/den höga representanten att inbegripa it-krishantering i krishanteringsplaneringen, och betonar behovet att medlemsstaterna i samarbete med Europeiska försvarsbyrån utarbetar planer för att skydda GSFP-uppdrag och GSFP-insatser mot it-angrepp. Parlamentet uppmanar dem också att bilda en gemensam europeisk styrka för it-försvar.

40. Europaparlamentet framhåller det goda praktiska samarbetet med Nato på området it-säkerhet, och understryker behovet att intensifiera detta samarbete, särskilt genom närmare samordning i fråga om planering, teknik, utbildning och utrustning.

41. Parlamentet efterlyser insatser från unionens sida för att inleda utbyte med internationella partner, inbegripet Nato, identifiera samarbetsområden, undvika dubbelarbete och komplettera verksamhet, där så är möjligt.

Internationell politik

42. Europaparlamentet anser att internationellt samarbete och dialog spelar en väsentlig roll för att skapa förtroende och öppenhet och för att främja en hög nivå på nätverksbyggandet och informationsutbytet globalt sett. Parlamentet uppmanar därför kommissionen och Europeiska utrikestjänsten att inrätta en arbetsgrupp för it-diplomati vars ansvarsområden skulle omfatta främjande av dialog med likasinnade länder och organisationer. Parlamentet efterlyser ett mer aktivt deltagande från EU:s sida i de många olika internationella konferenser för it-säkerhet på hög nivå som unionen deltar i.

43. Europaparlamentet anser att man måste hitta en jämvikt mellan de konkurrerande målen gränsöverskridande uppgiftsöverföring, uppgiftsskydd och it-säkerhet, i linje med unionens internationella åtaganden, i synnerhet inom ramen för Gats.

44. Europaparlamentet uppmanar vice ordföranden/den höga representanten att integrera it-säkerhetsdimension i EU:s yttre åtgärder, särskilt i förhållande till tredjeländer, i syfte att intensifiera samarbetet och utbytet av erfarenheter och information om hur man hanterar it-säkerheten.

45. Europaparlamentet efterlyser insatser av unionen för att inleda ett utbyte med internationella partner i syfte att identifiera samarbetsområden, undvika dubbelarbete och komplettera verksamhet, där så är möjligt. Parlamentet uppmanar vice ordföranden/den höga representanten och kommissionen att agera med framförhållning i internationella organisationer och att samordna medlemsstaternas ståndpunkter om hur man ska främja lösningar och politik på it-området på ett bra sätt.

46. Europaparlamentet anser att insatser bör göras för att se till att befintliga internationella rättsliga instrument, särskilt Europarådets konvention om it-brottslighet, blir verklighet i cyberrymden. Parlamentet anser därför att det för närvarande inte finns något behov att skapa nya rättsliga instrument på internationell nivå. Parlamentet välkomnar dock internationellt samarbete för att ta fram normer för uppträdandet i cyberrymden, och stöder rättsstaten i cyberrymden. Parlamentet anser att en uppdatering av de befintliga rättsliga instrumenten vilken återspeglar teknikens framsteg bör övervägas. Parlamentet menar att frågor om domstolars behörighet kräver en djupgående diskussion om rättsligt samarbete och lagföring av gränsöverskridande brott.

47. Europaparlamentet anser att i synnerhet arbetsgruppen EU–USA för it-säkerhet och mot it-brottslighet bör tjäna som ett verktyg med vilket EU och USA i lämpliga fall kan utbyta bästa praxis inom it-säkerhetspolitik. Parlamentet noterar i detta sammanhang att områden med anknytning till it-säkerhet, såsom tjänster som är beroende av att nät- och informationssystem fungerar säkert, kommer att tas upp i de kommande förhandlingarna om det transatlantiska partnerskapet för handel och investeringar, vilket måste ingås på ett sätt som skyddar EU:s suveränitet och oberoendet för EU:s institutioner.

48. Europaparlamentet konstaterar att it-säkerhetskompetensen och kapaciteten att förebygga, upptäcka och effektivt motverka hot och angrepp inte är jämnt utvecklade runt om i världen. Parlamentet betonar att insatser för att öka it-motståndskraften och bekämpa it-hot inte får begränsas till likasinnade partner, utan också bör riktas mot regioner som ligger efter i utvecklingen av kapacitet, teknisk infrastruktur och rättsliga ramar. Parlamentet anser att samordningen av incidenthanteringsorganisationer är avgörande i denna fråga. Parlamentet uppmanar kommissionen att underlätta – och vid behov bistå – satsningar i tredjeländer för att bygga upp it-säkerhetskapacitet på egen hand, med hjälp av lämpliga medel.

Genomförande

49. Europaparlamentet efterlyser regelbundna utvärderingar av de nationella it-säkerhetsstrategiernas inverkan på högsta politiska nivå, i syfte att säkerställa en anpassning till nya globala hot och att garantera samma nivå på it-säkerheten i olika medlemsstater.

50. Europaparlamentet uppmanar kommissionen att utarbeta en tydlig färdplan med tidsramar för när målen ska vara uppnådda på unionsnivå enligt it-säkerhetsstrategin och för bedömning av detta. Parlamentet uppmanar medlemsstaterna att enas om en liknande leveransplan för nationell verksamhet inom ramen för denna strategi.

Torsdagen den 12 september 2013

51. Europaparlamentet efterlyser regelbundna rapporter – från kommissionen, medlemsstaterna, Europol och det nyinrättade Europeiska it-brottscentrumet, Eurojust samt Enisa – med bedömning av de framsteg som gjorts i förhållande till de mål som anges i it-säkerhetsstrategin, inklusive nyckelresultatindikatorer som mäter framstegen med genomförandet.

o

o o

52. Europaparlamentet uppdrar åt talmannen att översända denna resolution till rådet, kommissionen, medlemsstaternas regeringar och parlament, Europol, Eurojust och Europarådet.

P7_TA(2013)0377

Digital agenda för tillväxt, rörlighet och sysselsättning

Europaparlamentets resolution av den 12 september 2013 om den digitala agendan för tillväxt, rörlighet och sysselsättning: dags att lägga in en högre växel (2013/2593(RSP))

(2016/C 093/17)

Europaparlamentet utfärdar denna resolution

— med beaktande av kommissionens meddelande av den 18 december 2012 *Den digitala agendan för Europa – Drivkraft för den europeiska digitala tillväxten* (COM(2012)0784),

— med beaktande av frågorna till kommissionen och rådet om ”den digitala agendan för tillväxt, rörlighet och sysselsättning: dags att lägga in en högre växel” (O-000085 – B7-0219/2013 och O-000086 – B7-0220/2013),

— med beaktande av Europaparlamentets och rådets förordning (EU) nr 531/2012 av den 13 juni 2012 om roaming i allmänna mobilnät i unionen ([1]),

— med beaktande av Europaparlamentets och rådets beslut nr 243/2012/EU av 14 mars 2012 om att upprätta ett ramprogram för konkurrenskraft och innovation (2007–2013) ([2]),

— med beaktande av de pågående förhandlingarna om Fonden för ett sammanlänkat Europa och framför allt av det ändrade förslaget till Europaparlamentets och rådets förordning om riktlinjer för transeuropeiska telekommunikationsnät och upphävande av beslut nr 1336/97/EG (COM(2013)0329),

— med beaktande av sin resolution av den 5 maj 2010 om en digital agenda för Europa: 2015.eu ([3]),

— med beaktande av kommissionens meddelande av den 27 september 2012 *Handlingsplan för energieffektivitet: att förverkliga möjligheterna* (COM(2012)0529),

— med beaktande av förslaget av den 25 januari 2012 till Europaparlamentets och rådets förordning om skydd av enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning) (COM(2012)0011),

---

([1]) EUT L 172, 30.6.2012, s. 10.
([2]) EUT L 81, 21.3.2012, s. 7.
([3]) EUT C 81 E, 15.3.2011, s. 45.