EUROPAPARLAMENTET 2009 - 2014

Plenarhandling

A7-0335/2012

17.10.2012

BETÄNKANDE

om it-säkerhet och it-försvar
(2012/2096(INI))

Utskottet för utrikesfrågor

Föredragande: Tunne Kelam

PR_INI

INNEHÅLL

Sida

FÖRSLAG TILL EUROPAPARLAMENTETS RESOLUTION

om it-säkerhet och it-försvar

(2012/2096(INI))

Europaparlamentet utfärdar denna resolution

– med beaktande av betänkandet om genomförandet av den europeiska säkerhetsstrategin, som Europeiska rådet uttryckte sitt stöd för den 11 och 12 december 2008,

– med beaktande av Europarådets konvention om it-relaterad brottslighet, vilken ingicks i Budapest den 23 november 2004,

– med beaktande av rådets slutsatser om skydd av kritisk infrastruktur av den 27 maj 2011 samt rådets tidigare slutsatser om it-säkerhet,

– med beaktande av kommissionens meddelande ”En digital agenda för Europa” av den 19 maj 2010 (COM(2010)0245),

– 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[1],

– med beaktande av kommissionens nyliga meddelande om att skapa ett europeiskt centrum för frågor mot it-brottslighet (COM(2012)0140),

– med beaktande av sin resolution av den 10 mars 2010 om genomförandet av den europeiska säkerhetsstrategin och den gemensamma säkerhets- och försvarspolitiken[2],

– med beaktande av sin resolution av den 11 maj 2011 om utvecklingen av den gemensamma säkerhets- och försvarspolitiken efter Lissabonfördragets ikraftträdande[3],

– med beaktande av sin resolution av den 22 maj 2012 om Europeiska unionens strategi för inre säkerhet[4],

– med beaktande av sin resolution av den 27 september 2011 om förslaget till Europaparlamentets och rådets förordning om ändring av förordning (EG) nr 1334/2000 om upprättande av en gemenskapsordning för kontroll av export av produkter och teknik med dubbla användningsområden[5],

[1] EUT L 345, 23.12.2008, s. 75.
[2] Antagna texter, P7_TA(2010)0061.
[3] Antagna texter, P7_TA(2011)0228.
[4] Antagna texter, P7_TA(2012)0207.
[5] Antagna texter, P7_TA(2012)0406.

– med beaktande av sin resolution av den 12 juni 2012 om skydd av kritisk infrastruktur – resultat och kommande åtgärder: vägen mot global it-säkerhet”[1],

– med beaktande av den resolution som FN:s råd för mänskliga rättigheter antog den 5 juli 2012 om främjande, skydd och åtnjutande av mänskliga rättigheter på internet[2], där betydelsen av att skydda de mänskliga rättigheterna och ett fritt informationsflöde på nätet betonas,

– med beaktande av slutsatserna från toppmötet i Chicago av den 20 maj 2012,

– med beaktande av avdelning V i EU-fördraget,

– med beaktande av artikel 48 i arbetsordningen,

– med beaktande av betänkandet från utskottet för utrikesfrågor (A7-0335/2012), och av följande skäl:

A. I dagens globaliserade värld har EU och dess medlemsstater i hög grad blivit beroende av it-säkerhet samt av att informationstekniken och den digitala tekniken används på ett betryggande sätt. Dessutom är man beroende av motståndskraftiga och tillförlitliga informationstjänster och infrastrukturer med anknytning till dem.

B. Informations- och kommunikationsteknik används också som medel att utöva förtryck. Sammanhanget där sådan teknik används är i hög grad avgörande för om denna teknik kommer att användas som drivkraft för positiv utveckling eller som förtrycksredskap.

C. It-utmaningar, it-hot och it-angrepp växer i en dramatisk takt och utgör ett stort hot mot nationalstaternas och den privata sektorns säkerhet, försvar, stabilitet och konkurrenskraft. Sådana hot bör därför inte betraktas som framtidsfrågor. Merparten av de starkt framträdande och störande it-incidenterna är numera politiskt motiverade. Den stora merparten av alla it-incidenter fortfarande är primitiva, men likafullt blir hoten mot viktiga tillgångar alltmer utstuderade och kräver ett genomgripande skydd.

D. Med nästan två miljarder globalt sammanlänkade användare har internet blivit ett av de mest kraftfulla och effektiva sätten att främja demokratiska idéer och organisera människor i deras strävan att förverkliga sin strävan efter frihet och bekämpa diktaturer. Odemokratiska och auktoritära regimers utnyttjande av internet utgör ett växande hot mot individens rätt till yttrandefrihet och föreningsfrihet. Det är därför viktigt att se till att internet fortsätter att vara öppet för ett fritt flöde av idéer, information och uttryck.

E. Det finns många hinder av politiskt, rättsligt och organiserat slag inom EU och dess medlemsstater mot att det utvecklas en heltäckande och enhetlig syn på it-försvar och itsäkerhet. Det saknas en gemensam definition, gemensamma standarder och gemensamma åtgärder på det känsliga och utsatta området it-säkerhet.

F. Samarbetet och samordningen inom EU-institutionerna liksom med och mellan medlemsstaterna och med partner utanför EU är fortfarande inte tillfyllest.

---

[1] Antagna texter, P7_TA(2012)0237.
[2] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx

G. Tydliga och harmoniserade definitioner av ”it-säkerhet” och ”it-försvar” saknas både på EU-nivå och internationellt. Förståelsen av it-säkerhet och andra viktiga begrepp varierar avsevärt mellan olika länder.

H. EU har ännu inte utvecklat en egen enhetlig politik när det gäller skydd av kritisk informationsinfrastruktur, vilket förutsätter ett tvärvetenskapligt grepp, så att säkerheten förstärks samtidigt som de grundläggande rättigheterna respekteras.

I. EU har föreslagit olika initiativ för att komma till rätta med den civila it-brottsligheten, bland annat genom inrättandet av ett nytt europeiskt centrum mot it-brottslighet, men har fortfarande ingen konkret plan på säkerhets- och försvarsnivå.

J. Att skapa förtroende och tillit mellan den privata sektorn och de brottsbekämpande myndigheterna, totalförsvaret och andra behöriga institutioner är av yttersta vikt i kampen mot it-brottslighet.

K. Tillit och ömsesidigt förtroende i relationerna mellan statliga och icke-statliga aktörer är en förutsättning för tillförlitlig it-säkerhet.

L. Flertalet it-incidenter inom både de offentliga och privata sektorerna blir inte rapporterade på grund av den känsliga typen av information och risken att skada de berörda företagens image.

M. Ett stort antal it-incidenter inträffar till följd av att den privata och offentliga nätinfrastrukturen inte är tillräckligt motståndskraftig och tålig samt till följd av att databaserna är dåligt skyddade eller säkrade och på grund av andra brister i den kritiska informationsinfrastrukturen. Endast ett fåtal medlemsstater anser det ingå i deras respektive aktsamhetsplikt att skydda sina nät och informationssystem och uppgifterna i dem, vilket förklarar bristen på investeringar i toppmodern säkerhetsteknik samt i utbildning och framtagning av lämpliga riktlinjer. Många medlemsstater är beroende av säkerhetsteknik från tredjeländer och bör göra mer för att minska detta beroende.

N. Flertalet förövare av it-angrepp på hög nivå som hotar säkerhet och försvar på nationell eller internationell nivå blir aldrig igenkända och lagförda. Det finns ingen internationellt överenskommen form av svar på vad som bör göras om en stat stöder ett it-angrepp mot en annan stat och inte heller är man ense om huruvida detta kan anses som orsak till krig.

O. Europeiska byrån för nät- och informationssäkerhet (Enisa) arbetar för att göra det enklare för medlemsstaterna att stödja utbytet av god praxis på området it-säkerhet genom att rekommendera hur man kan utveckla, genomföra och upprätthålla en it-säkerhetsstrategi och har en stödjande roll för nationella it-säkerhetsstrategier och nationella beredskapsplaner och i arbetet med att anordna EU-omfattande och internationella övningar kring skydd av kritisk informationsinfrastruktur och utvecklingen av scenarier för nationella övningar.

P. I juni 2012 hade endast tio EU-medlemsstater officiellt antagit en nationell it-säkerhetsstrategi.

Q. It-försvar är en av de högst prioriterade frågorna för Europeiska försvarsbyrån, som inom ramen för kapacitetsutvecklingsplanen har inrättat en projektgrupp kring it-säkerhet tillsammans med en majoritet av medlemsstaterna, som arbetar med att samla erfarenheter och lägga fram rekommendationer.

R. Investeringar i forskning och utveckling om it-säkerhet och it-försvar är avgörande för att främja och upprätthålla en hög nivå av it-säkerhet och it-försvar. Försvarsutgifterna för forskning och utveckling har minskat i stället för att nå överenskomna 2 % av de totala försvarsutgifterna.

S. Att öka medvetenheten och utbilda medborgarna om it-säkerhet bör utgöra grunden för alla övergripande it-säkerhetsstrategier.

T. En tydlig balans måste upprättas mellan säkerhetsåtgärder och medborgerliga rättigheter i enlighet med EUF-fördraget, såsom rätten till integritet, uppgiftsskydd och yttrandefrihet. Ingen rättighet får offras till förmån för en annan.

U. Det finns ett växande behov av att bättre respektera och skydda individers rätt till integritet, som fastställs i EU:s stadga om de grundläggande rättigheterna och artikel 16 i EUF-fördraget. Visserligen är det viktigt att olika institutioner och försvarsorgan får säkerhet och skydd för internet på nationell nivå, men detta bör aldrig tas som förevändning för några som helst begränsningar av rättigheter och friheter på internet och i informationsrymden.

V. Internet är globalt och gränslöst, vilket kräver nya former av internationellt samarbete och internationell styrning under medverkan från olika intressenter.

W. Statsmakterna anlitar i allt högre grad privata aktörer i frågor som gäller säkerheten hos deras kritiska infrastruktur.

X. Europeiska utrikestjänsten har ännu inte aktivt inbegripit en it-säkerhetsaspekt i sina förbindelser med tredjeländer.

Y. Stabilitetsinstrumentet är det hittills enda EU-program som är utformat för att åtgärda akuta kriser eller globala/regionöverskridande säkerhetsutmaningar, däribland it-säkerhetshot.

Z. En av huvudfrågorna inom de transatlantiska förbindelserna mellan EU och Förenta staterna är gemensamma åtgärder mot it-säkerhetshot – genom EU:s och Förenta staternas gemensamma arbetsgrupp för it-säkerhet och it-brottslighet.

Åtgärder och samordning inom EU

1. Europaparlamentet noterar att it-hot och it-angrepp mot statsmakterna, förvaltningens och försvarets organ, samt mot internationella organ, är ett snabbt växande hot och blir allt vanligare, både inom EU och internationellt. Det finns betydande skäl till oro för att statliga och icke-statliga aktörer, framför allt terrororganisationer och brottsliga organisationer, kan gå till angrepp mot kritiska informations- och

kommunikationsstrukturer och infrastrukturer vid EU:s institutioner och i medlemsstaterna och vålla allvarliga skador, bland annat i form av kinetiska effekter.

2. Europaparlamentet understryker därför behovet av en övergripande och samordnad strategi för dessa utmaningar på EU-nivå genom utveckling av en övergripande säkerhetsstrategi för internet i EU som bör fastställa en gemensam definition av it-säkerhet och it-försvar, och av vad som ska anses vara ett försvarsrelaterat it-angrepp, samt en gemensam syn på hur it-säkerhet fungerar. Hänsyn bör tas till befintliga byråers och organs mervärde och till god praxis från de medlemsstater som redan har nationella it-säkerhetsstrategier. Parlamentet betonar den avgörande betydelsen av samordning och skapande av synergieffekter på unionsnivå för att hjälpa till att kombinera olika militära och civila initiativ, program och verksamheter. Parlamentet betonar att en sådan strategi bör säkerställa flexibilitet och uppdateras regelbundet för att anpassa sig till det snabbt föränderliga internet.

3. Europaparlamentet uppmanar enträget kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik att i sitt kommande förslag om arrangemangen för genomförandet av solidaritetsklausulen (artikel 222 i EUF-fördraget) överväga möjligheten att ett allvarligt it-angrepp kan riktas mot en medlemsstat. Även om it-angrepp som hotar den nationella säkerheten fortfarande måste definieras med hjälp av en gemensam terminologi skulle de kunna omfattas av klausulen om ömsesidigt försvar (artikel 42.7 i EU-fördraget) utan att detta påverkar proportionalitetsprincipen.

4. Europaparlamentet betonar att den gemensamma säkerhets- och försvarspolitiken måste garantera att styrkor som deltar i EU:s militära operationer och civila uppdrag skyddas mot it-angrepp. Parlamentet understryker att den gemensamma säkerhets- och försvarspolitiken aktivt måste kunna utföra it-försvar.

5. Europaparlamentet betonar att EU:s hela politik för it-säkerhet bör bygga på och vara utformad för att säkerställa att de digitala friheterna och respekten för mänskliga rättigheterna på internet skyddas och bevaras i så hög grad som det bara är möjligt. Parlamentet anser att internet och IKT bör integreras i EU:s utrikes- och säkerhetspolitik för att stärka dessa ansträngningar.

6. Europaparlamentet uppmanar kommissionen och rådet att klart och entydigt erkänna att de digitala friheterna är grundläggande rättigheter och ofrånkomliga förutsättningar för åtnjutandet av universella mänskliga rättigheter. Parlamentet betonar att medlemsstaterna, när de utvecklar sina sätt att bemöta it-hot och it-angrepp, bör sträva efter att aldrig ställa sina medborgares fri- och rättigheter på spel, samt att de i sin lagstiftning bör göra en tillräcklig åtskillnad mellan it-incidenter på civil respektive militär nivå. Parlamentet vill att man ska vara ytterst försiktig med att begränsa medborgarnas möjligheter att använda verktyg för kommunikations- och informationsteknik.

7. Europaparlamentet uppmanar rådet och kommissionen att tillsammans med medlemsstaterna sammanställa en vitbok om it-försvar där det fastställs klara definitioner och tydliga kriterier för olika nivåer av civila och militära it-angrepp i förhållande till de bakomliggande motiven och effekterna av dessa liksom också nivåerna för bemötande, bland annat när det gäller undersökning, uppspårning och lagföring av gärningsmän.

8. Europaparlamentet upplever ett tydligt behov av att uppdatera den europeiska säkerhetsstrategin så att man kan identifiera och finna fram till hur personer som gör sig skyldiga till it-angrepp kan uppspåras och lagföras, antingen de är enskilda individer, kopplade till nätverk eller arbetar med stöd av någon stat.

EU-nivå

9. Europaparlamentet betonar vikten av övergripande samarbete och samordning när det gäller it-säkerhet inom och mellan EU-institutionerna och EU-byråerna.

10. Europaparlamentet betonar att den nya tekniken innebär en utmaning för hur statsmakterna utför sina av hävd viktigaste uppgifter och bekräftar än en gång att försvars- och säkerhetspolitiken i sista hand ligger i statsmakternas händer, något som också innefattar en adekvat demokratisk tillsyn. Parlamentet konstaterar att privata aktörer blir allt viktigare för utförandet av uppgifter på säkerhets- och försvarsområdet och att det då ofta saknas både insyn och redovisningsskyldighet och likaså mekanismer för demokratisk tillsyn.

11. Europaparlamentet betonar att statsmakterna måste hålla sig till de grundläggande internationella principerna för offentlig rätt och humanitär rätt, såsom respekten för staternas suveränitet och de mänskliga rättigheterna, när de använder ny teknik inom säkerhets- och försvarspolitiken. Parlamentet påpekar de värdefulla erfarenheter som sådana EU-medlemsstater som Estland gjort med att fastställa och utforma it-säkerhetspolitik och it-försvar.

12. Europaparlamentet erkänner behovet av en övergripande bedömning av it-angrepp mot EU:s informationssystem och infrastruktur. Parlamentet betonar i detta sammanhang behovet av en kontinuerlig bedömning av beredskapsnivån för EU:s institutioner när det gäller att hantera potentiella it-angrepp. Parlamentet vidhåller framför allt att den kritiska informationsinfrastrukturen måste stärkas.

13. Europaparlamentet betonar också att det behövs information om sårbarheter och om varningar för nya hot mot informationssystemen.

14. Europaparlamentet noterar att den senaste tidens it-angrepp mot europeiska informationsnätverk och statliga informationssystem har orsakat betydande ekonomiska skador och säkerhetsskador, vars omfattning inte har utvärderats tillräckligt.

15. Europaparlamentet uppmanar samtliga EU-institutioner att utveckla sina it-säkerhetsstrategier och beredskapsplaner med avseende på sina egna system så fort som möjligt.

16. Europaparlamentet uppmanar samtliga EU-institutioner att låta frågan om it-relaterad krishantering ingå i riskanalyser och krishanteringsplaner. Parlamentet uppmanar dessutom samtliga EU-institutioner att tillhandahålla utbildningar för ökad medvetenhet om it-säkerhet för all sin personal. Parlamentet föreslår att it-övningar ska genomföras en gång om året på samma sätt som krisövningar.

17. Europaparlamentet understryker vikten av att EU:s incidenthanteringsorganisation (EU-Cert) och nationella incidenthanteringsorganisationer utvecklas på ett effektivt sätt samt att nationella beredskapsplaner utvecklas om åtgärder behöver vidtas. Parlamentet välkomnar det faktum att samtliga EU-medlemsstater i maj 2012 har inrättat nationella incidenthanteringsorganisationer. Parlamentet uppmanar enträget till en fortsatt utveckling av nationella incidenthanteringsorganisationer och en EU-incidenthanteringsorganisation som vid behov kan sättas in inom 24 timmar. Parlamentet betonar att möjligheten till offentlig-privata partnerskap inom detta område måste undersökas.

18. Europaparlamentet erkänner att ”Cyber Europe 2010”, den första EU-omfattade övningen kring skydd av kritisk informationsinfrastruktur, som genomfördes med medverkan av olika medlemsstater och under ledning av Enisa, visade sig vara en användbar åtgärd och ett exempel på god praxis. Parlamentet betonar också att nätverket för varningar om hot mot kritisk infrastruktur på EU-nivå måste inrättas så fort som möjligt.

19. Europaparlamentet understryker att det behövs EU-omfattande övningar för storskaliga säkerhetsincidenter i nätverk, liksom att det måste fastställas en enda uppsättning standarder för hotbildsbedömning.

20. Europaparlamentet uppmanar kommissionen att undersöka behovet och möjligheten av en it-samordningstjänst i EU.

21. Med tanke på den stora kunskapsmängd som krävs, både för att adekvat försvara it-system och it-infrastrukturer och angripa dem, anser Europaparlamentet att kommissionen, rådet och medlemsstaterna bör överväga att utveckla en strategi för att värva unionsmedborgare som dömts för it-angrepp. Parlamentet konstaterar att potentialen för kunskapsflykt i dessa fall är stor och att framför allt underåriga som dömts för sådana angrepp har goda utsikter till både återanpassning och arbete vid försvarets byråer och organ.

Europeiska försvarsbyrån

22. Europaparlamentet välkomnar de senaste initiativen och projekten som rör it-försvar, i synnerhet insamling och kartläggning av relevanta uppgifter, utmaningar och behov beträffande it-säkerhet och it-försvar. Parlamentet uppmanar enträget medlemsstaterna till ökat samarbete, också på militär nivå, med Europeiska försvarsbyrån om it-försvar.

23. Europaparlamentet understryker vikten av medlemsstaternas nära samarbete med Europeiska försvarsbyrån för att utveckla deras nationella it-försvarskapacitet. Parlamentet anser att skapandet av synergieffekter, sammanslagningar och utbyte på EU-nivå är avgörande för ett effektivt försvar på både europeisk och nationell nivå.

24. Europaparlamentet uppmanar Europeiska försvarsbyrån att fördjupa sitt samarbete med Nato, nationella och internationella centrum för spetskompetens, Europeiska it-brottscentrumet vid Europol som bidrar till snabbare reaktioner i händelse av it-angrepp, och i synnerhet med forskningscentrumet för samordnat försvar (CCDCOE), samt att inrikta sig på kapacitetsuppbyggnad, utbildning och utbyte av information och erfarenheter.

25. Europaparlamentet konstaterar med oro att endast en medlemsstat hade uppnått utgiftsnivån 2 % till forskning och utveckling om försvar under 2010, och att fem medlemsstater inte satsade någonting på FoU under 2010. Parlamentet uppmanar enträget Europeiska försvarsbyrån att tillsammans med medlemsstaterna slå samman resurser och effektivt investera i samarbeten kring forskning och utveckling, med särskild hänsyn till it-säkerhet och it-försvar.

Medlemsstaterna

26. Europaparlamentet uppmanar samtliga medlemsstater att omedelbart utveckla och slutföra sina respektive nationella it-säkerhets- och försvarsstrategier och skapa stabila förutsättningar för både politiskt beslutsfattande och för lagstiftning, tillsammans med heltäckande riskhanteringsförfaranden och lämpliga förberedande åtgärder och mekanismer. Parlamentet uppmanar Enisa att bistå medlemsstaterna. Parlamentet uttrycker sitt stöd för Enisa när det gäller att utveckla riktlinjer för god praxis och rekommendationer om hur man utvecklar, genomför och upprätthåller en it-säkerhetsstrategi.

27. Europaparlamentet uppmuntrar alla medlemsstater att inrätta utsedda enheter för it-säkerhet och it-försvar inom landets militära strukturer, för att samarbeta med liknande organ i andra EU-medlemsstater.

28. Europaparlamentet uppmuntrar medlemsstaterna att på regional nivå inrätta specialiserade domstolar med syfte att på ett bättre sätt förhindra angrepp på informationssystemen. Parlamentet vidhåller att man måste uppmuntra en anpassning av den nationella lagstiftningen, så att den kan anpassas till den tekniska utvecklingen och utvecklingen av praxis.

29. Europaparlamentet uppmanar enträget kommissionen att fortsätta arbetet med en konsekvent och effektiv europeisk strategi för att undvika onödiga insatser, uppmuntra och stödja medlemsstaterna i deras ansträngningar att utveckla samarbetsmekanismer och öka utbytet av information. Parlamentet anser att en miniminivå för obligatoriskt samarbete och utbyte bör upprättas mellan medlemsstaterna.

30. Europaparlamentet uppmanar enträget medlemsstaterna att utarbeta nationella beredskapsplaner och låta it-krishantering ingå i krishanteringsplaner och riskanalyser. Parlamentet betonar även vikten av adekvat utbildning om viktig it-säkerhet för all personal inom offentliga organ och framhåller i synnerhet vikten av adekvat utbildning vid läroanstalter för de rättsliga institutionernas och säkerhetsinstitutionernas ledamöter. Parlamentet uppmanar Enisa och andra berörda organ att hjälpa medlemsstaterna att säkerställa sammanslagning och utbyte av resurser samt att undvika dubbelarbete.

31. Europaparlamentet uppmanar enträget medlemsstaterna att göra forskning och utveckling till en grundpelare för it-säkerhet och it-försvar och att uppmuntra utbildning av ingenjörer som är specialiserade på skydd av informationssystem. Parlamentet uppmanar medlemsstaterna att uppfylla sina åtaganden att öka försvarsutgifterna för forskning och utveckling till minst 2 %, särskilt beträffande it-säkerhet och it-försvar.

32. Europaparlamentet uppmanar kommissionen och medlemsstaterna att lägga fram program för att främja och öka både privata och företagsbaserade användares kunskaper om en allmän säker användning av internet, informationssystem och kommunikationsteknik. Parlamentet föreslår att kommissionen lanserar ett offentligt EU-omfattande utbildningsinitiativ i denna fråga. Medlemsstaterna uppmanas att inkludera utbildning om it-säkerhet i skolornas läroplaner från så tidig ålder som möjligt.

Offentlig-privat samarbete

33. Europaparlamentet framhåller den avgörande roll som meningsfullt och kompletterande it-säkerhetssamarbete mellan offentliga myndigheter och privat sektor spelar, både på EU-nivå och nationell nivå, i syfte att generera ömsesidigt förtroende. Parlamentet är medvetet om att ytterligare förbättringar av tillförlitligheten och effektiviteten inom berörda offentliga institutioner kommer att bidra till att skapa förtroende och leda till utbyte av viktig information.

34. Europaparlamentet uppmanar partnerna inom den privata sektorn att överväga att bygga in säkerhetslösningarna redan i själva konstruktionen, när nya produkter, apparater, tjänster och tillämpningar tas fram. Dessutom bör de som tar fram sådana nya produkter, apparater, tjänster och tillämpningar, där säkerheten bildar ett centralt inslag redan i själva konstruktionen, ges incitament för sin verksamhet. Parlamentet begär att det, inom samarbetet med den privata sektorn för att förhindra och beivra it-angrepp, ska finnas minimistandarder för insyn och mekanismer för ansvarsutkrävande.

35. Europaparlamentet påminner om att skyddet av kritisk informationsinfrastruktur omfattas av EU:s strategi för den inre säkerheten, i samband med arbetet för att förbättra säkerheten för medborgare och företag på internet.

36. Europaparlamentet efterlyser en ständig dialog med dessa parter om hur informationssystem bäst bör utnyttjas och göras motståndskraftiga och om den ansvarsfördelning som krävs för att dessa system ska vara säkra och fungera korrekt.

37. Europaparlamentet anser att medlemsstaterna, EU-institutionerna och den privata sektorn bör, i samarbete med Enisa, vidta åtgärder för att öka informationssystemens säkerhet och integritet, i syfte att förebygga angrepp och minimera deras konsekvenser. Parlamentet stöder kommissionen i dess arbete med att lägga fram miniminormer och certifieringssystem för it-säkerhet för företag samt ge rätt incitament till den privata sektorns säkerhetsförbättrande strävanden.

38. Europaparlamentet uppmanar kommissionen och medlemsstaternas regeringar att uppmuntra den privata sektorn och det civila samhällets aktörer att låta it-krishantering ingå i krishanteringsplaner och riskanalyser. Parlamentet pekar vidare på behovet av att införa utbildning för ökad medvetenhet om grundläggande it-säkerhet och it-hygien för samtlig personal.

39. Europaparlamentet uppmanar kommissionen att i samarbete med medlemsstaterna och berörda byråer och organ utveckla ramar och instrument för ett snabbt system för informationsutbyte som kan garantera anonymitet vid rapportering av it-incidenter för den

privata sektorn samt göra det möjligt för offentliga aktörer att ständigt hålla sig uppdaterade och vid behov tillhandahålla stöd.

40. Europaparlamentet betonar att EU måste främja utvecklingen av en konkurrenskraftig och innovativ marknad för it-säkerhet inom EU i syfte att göra det lättare för små och medelstora företag att verka inom detta område, vilket bidrar till att öka den ekonomiska tillväxten och skapa nya arbetstillfällen.

Internationellt samarbete

41. Europaparlamentet uppmanar Europeiska utrikestjänsten att inta en föregripande hållning i fråga om it-säkerhet och integrera aspekten it-säkerhet i alla sina åtgärder, i synnerhet i förhållande till tredjeländer. Parlamentet kräver att samarbetet och utbytet av information påskyndas när det gäller att komma till rätta med it-säkerhetsproblem med tredjeländer.

42. Europaparlamentet betonar att genomförandet av en övergripande it-säkerhetsstrategi inom EU är en förutsättning för att man ska kunna fastställa vilken typ av effektivt internationellt samarbete kring it-säkerhet som krävs för att bekämpa gränsöverskridande it-hot.

43. Europaparlamentet uppmanar de medlemsstater som ännu inte har undertecknat eller ratificerat Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen) att göra det utan ytterligare dröjsmål. Parlamentet stöder kommissionen och Europeiska utrikestjänsten i deras ansträngningar att främja konventionen och dess värden bland tredjeländer.

44. Europaparlamentet är medvetet om behovet av internationellt överenskomna och samordnade åtgärder mot it-hot. Parlamentet uppmanar därför kommissionen, Europeiska utrikestjänsten och medlemsstaterna att i alla forum men framför allt FN ta ledningen i arbetet för ett bredare internationellt samarbete och en slutlig överenskommelse om hur man ska fastställa en samsyn på uppförandenormer på internet och att även främja samarbetet för att ta fram avtal om kontroll av it-vapen.

45. Europaparlamentet uppmuntrar kunskapsutbyten om it-säkerhet med Briks-länderna och andra länder med framväxande ekonomier, för att undersöka möjligheterna till gemensamma reaktioner mot växande it-brottslighet, it-hot och it-angrepp på både civil och militär nivå.

46. Europaparlamentet uppmanar enträget Europeiska utrikestjänsten och kommissionen att inta en föregripande hållning inom relevanta internationella forum och organisationer, särskilt FN, OSSE, OECD och Världsbanken, i syfte att tillämpa befintlig internationell rätt och uppnå konsensus om normer för ansvarsfullt statligt agerande om it-säkerhet och it-försvar, och genom att samordna medlemsstaternas ståndpunkter i syfte att främja EU:s grundläggande värden och politik inom it-säkerhet och it-försvar.

47. Europaparlamentet uppmanar rådet och kommissionen att inom ramen för sina dialoger, förbindelser och samarbetsavtal med tredjeländer, särskilt i de fall då tekniskt samarbete eller utbyte tas upp, insistera på minimikrav för att förebygga och bekämpa it-brottslighet och it-angrepp samt miniminormer för it-säkerhet.

48. Europaparlamentet uppmanar kommissionen att underlätta och bistå tredjeländer, vid behov, i deras arbete med att bygga upp sin kapacitet för it-säkerhet och it-försvar.

Samarbete med Nato

49. Europaparlamentet upprepar att EU och Nato, med utgångspunkt i deras gemensamma värderingar och strategiska intressen, har ett särskilt ansvar och kapacitet att ta itu med de växande utmaningarna inom it-säkerhet på ett mer effektivt sätt och i nära samarbete genom att söka möjliga sätt att komplettera varandra, utan dubbelarbete och med respekt för deras respektive ansvarsområden.

50. Europaparlamentet betonar behovet av sammanslagning och utbyte på ett praktiskt plan, med hänsyn till EU:s och Natos kompletterande strategi för it-säkerhet och it-försvar. Parlamentet poängterar behovet av närmare samarbete, särskilt när det gäller planering, teknik, utbildning och utrustning med hänsyn till it-säkerhet och it-försvar.

51. Med utgångspunkt i befintlig kompletterande verksamhet inom utvecklingen av försvarskapacitet uppmanar Europaparlamentet enträget alla relevanta organ i EU som arbetar med it-säkerhet och it-försvar att fördjupa sitt praktiska samarbete med Nato i syfte att utbyta erfarenheter och lära sig hur man bygger motståndskraft åt EU:s system.

Samarbete med Förenta staterna

52. Europaparlamentet anser att EU och Förenta staterna bör fördjupa sitt ömsesidiga samarbete för att motverka it-angrepp och it-brottslighet, eftersom detta blev de transatlantiska förbindelsernas huvudfråga efter toppmötet mellan EU och Förenta staterna i Lissabon 2010.

53. Europaparlamentet välkomnar inrättandet av EU:s och Förenta staternas gemensamma arbetsgrupp för it-säkerhet och it-brottslighet under toppmötet mellan EU och Förenta staterna i november 2010. Parlamentet stöder gruppens strävan att inbegripa frågor om it-säkerhet i den translantiska politiska dialogen.

54. Europaparlamentet välkomnar att kommissionen och den amerikanska regeringen, genom EU:s och Förenta staternas gemensamma arbetsgrupp, tillsammans utarbetar ett gemensamt program och en färdplan mot gemensamma/synkroniserade transkontinentala it-övningar under 2012–2013. Parlamentet noterar att den första it-övningen mellan EU och Förenta staterna gjordes 2011.

55. Europaparlamentet understryker att både internet och dess användare till största delen finns inom Förenta staterna och EU och att dessa bägge därför måste arbeta tillsammans för att skydda sina medborgares rättigheter och friheter att använda internet. Parlamentet understryker att nationell säkerhet visserligen är ett högprioriterat mål, men att internet också behöver inte bara säkerhet utan också skydd.

56. Europaparlamentet uppdrar åt talmannen att översända denna resolution till rådet, kommissionen, vice ordföranden/den höga representanten, Europeiska försvarsbyrån, Enisa och Nato.

RESULTAT AV SLUTOMRÖSTNINGEN I UTSKOTTET

Antagande	10.10.2012
Slutomröstning: resultat	+: 47 –: 3 0: 6
Slutomröstning: närvarande ledamöter	Bastiaan Belder, Franziska Katharina Brantner, Elmar Brok, Jerzy Buzek, Tarja Cronberg, Arnaud Danjean, Mário David, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Liisa Jaakonsaari, Anneli Jäätteenmäki, Jelko Kacin, Ioannis Kasoulides, Tunne Kelam, Nicole Kiil-Nielsen, Evgeni Kirilov, Maria Eleni Koppa, Wolfgang Kreissl-Dörfler, Eduard Kukan, Vytautas Landsbergis, Krzysztof Lisek, Sabine Lösing, Mario Mauro, Francisco José Millán Mon, Alexander Mirsky, María Muñiz De Urquiza, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Justas Vincas Paleckis, Bernd Posselt, Cristian Dan Preda, Fiorello Provera, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Sophocles Sophocleous, Laurence J.A.J. Stassen, Kristian Vigenin, Sir Graham Watson, Karim Zéribi
Slutomröstning: närvarande suppleanter	Charalampos Angourakis, Elena Băsescu, Jean-Jacob Bicep, Véronique De Keyser, Diogo Feio, Elisabeth Jeggle, Indrek Tarand, Sampo Terho, László Tőkés, Traian Ungureanu, Luis Yáñez-Barnuevo García
Slutomröstning: närvarande suppleanter (art. 187.2)	Joseph Cuschieri