P7_TA(2012)0237

Schutz kritischer Informationsinfrastrukturen: der Weg zur globalen Netzsicherheit

Entschließung des Europäischen Parlaments vom 12. Juni 2012 zu dem Schutz kritischer Informationsinfrastrukturen – Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit (2011/2284(INI))

Das Europäische Parlament,

– unter Hinweis auf seine Entschließung vom 5. Mai 2010 mit dem Titel „Eine neue Digitale Agenda für Europa: 2015.eu“[1],

– unter Hinweis auf seine Entschließung vom 15. Juni 2010 mit dem Titel „Internet-Governance: die nächsten Schritte“[2],

– unter Hinweis auf seine Entschließung vom 6. Juli 2011 mit dem Titel „Europäische Breitbandnetze: Investition in ein internetgestütztes Wachstum“[3],

– gestützt auf Artikel 48 seiner Geschäftsordnung,

– in Kenntnis des Berichts des Ausschusses für Industrie, Forschung und Energie und der Stellungnahme des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (A7-0167/2012),

A. in der Erwägung, dass die Informations- und Kommunikationstechnologien (IKT) ihre volle Kapazität zur Förderung von Wirtschaft und Gesellschaft nur dann entfalten können, wenn ihre Anwender Vertrauen in deren Sicherheit und Robustheit haben und die bestehende Gesetzgebung zu Angelegenheiten wie Datenschutz und Rechten des geistigen Eigentums im Umfeld des Internets wirksam durchgesetzt wird;

B. in der Erwägung, dass sich das Internet und die IKT immer stärker auf verschiedene Aspekte im Leben der Bürger auswirken, und in der Erwägung, dass sie wesentliche Antriebsfaktoren für soziale Interaktion, kulturelle Bereicherung und wirtschaftliches Wachstum sind;

C. in der Erwägung, dass IKT und Internetsicherheit ein umfassendes Konzept mit globalen Auswirkungen auf wirtschaftliche, soziale, technische und militärische Aspekte sind und eine klare Definition und Differenzierung der Verantwortlichkeit sowie einen robusten internationalen Kooperationsmechanismus erfordern;

D. in der Erwägung, dass die Leitinitiative „Digitale Agenda der EU“ darauf abzielt, die Wettbewerbsfähigkeit Europas auf Grundlage der Stärkung der IKT zu erhöhen und Bedingungen für ein hohes und stabiles Wachstum und technologiebasierte Arbeitsplätze zu schaffen;

---

1 ABl. C 81E vom 15.3.2011, S. 45.
2 ABl. C 236E vom 12.8.2011, S. 33
3 Angenommene Texte, P7_TA(2011)0322.

E. in der Erwägung, dass der private Sektor der erste Investor, Eigentümer und Manager bei Produkten der Informationssicherheit, Dienstleistungen, Anwendungen und Infrastruktur bleibt, wobei in den letzten zehn Jahren Milliarden von Euro investiert wurden; in der Erwägung, dass diese Beteiligung durch angemessene politische Strategien gestärkt werden soll, um die Zuverlässigkeit der Infrastrukturen in öffentlichem, privatem oder öffentlich-privatem Besitz oder Betrieb zu fördern;

F. in der Erwägung, dass die Entwicklung eines hohen Sicherheitsniveaus und die Zuverlässigkeit der Netze, Dienstleistungen und Technologien im Bereich IKT die Wettbewerbsfähigkeit der EU-Wirtschaft vermutlich stärken wird, sowohl durch die Verbesserung der Einschätzung und Bewertung von Cyberrisiken als auch durch eine Versorgung der EU-Wirtschaft insgesamt mit robusteren Informationsinfrastrukturen zur Unterstützung von Innovation und Wachstum, und dadurch neue Möglichkeiten für Unternehmen schafft, um produktiver arbeiten zu können;

G. in der Erwägung, dass verfügbare Daten bei der Verfolgung von Cyberkriminalität (die sich mit Cyber-Angriffen aber auch anderen Arten von Internet-Kriminalität beschäftigen) auf einen bedeutenden Anstieg in verschiedenen europäischen Ländern schließen lassen; in der Erwägung, dass jedoch statistisch repräsentative Daten zu Cyberangriffen von Strafverfolgung und der CERT-Gemeinschaft (Computer Emergency Response Team) die Ausnahme bleiben und künftig besser zusammengeführt werden müssen, damit Strafverfolger und besser informierte Gesetzgeber europaweit gezielter auf die sich immer weiter entwickelnden Cyberbedrohungen reagieren können;

H. in der Erwägung, dass der richtige Grad an Informationssicherheit für ein robustes Wachstum der internetbasierten Dienste wesentlich ist;

I. in der Erwägung, dass jüngste Vorfälle und Störungen im Cyberspace und daraus hervorgehende Angriffe auf EU-Institutionen und die Informationsinfrastrukturen von Mitgliedstaaten den Bedarf zur Einrichtung eines robusten, innovativen und wirksamen Systems zum Schutz kritischer Informationsstrukturen (CIIP) auf der Grundlage voller internationaler Kooperation und minimaler Zuverlässigkeitsstandards unter den Mitgliedstaaten aufzeigen;

J. in der Erwägung, dass die schnelle Entwicklung neuer Wege von IKT wie Cloud-Computing, einen starken Fokus auf Sicherheit erfordern, damit es möglich ist, den Nutzen der technischen Errungenschaften zu erschließen;

K. in der Erwägung, dass es wiederholt auf hohen Standards für Datenschutz, Netzneutralität und den Schutz des geistigen Eigentums bestanden hat;

Maßnahmen zur Stärkung von CIIP auf nationaler und Unionsebene

1. begrüßt die Durchführung des Europäischen Programms zu CIIP durch die Mitgliedstaaten einschließlich der Einrichtung des Warn- und Informationsnetzes für kritische Infrastrukturen (WINKI);

2. vertritt die Auffassung, dass die CIIP-Bemühungen nicht nur die allgemeine Sicherheit der Bürgerinnen und Bürger erhöhen werden, sondern auch deren Sicherheitsempfinden und ihr Vertrauen in die von der Regierung zu ihrem Schutz ergriffenen Maßnahmen verbessern werden;

3. nimmt zur Kenntnis, dass die Kommission eine Überarbeitung der Richtlinie 2008/114/EG[1] des Rates in Betracht zieht, und fordert Beweise für die Effizienz und die Auswirkungen der Richtlinie, bevor weitere Schritte unternommen werden; fordert dazu auf, eine Erweiterung ihres Anwendungsbereichs in Betracht zu ziehen, insbesondere durch die Einbeziehung des IKT-Sektors und der Finanzdienstleistungen; fordert weiterhin dazu auf, in diesem Zusammenhang Bereichen wie Gesundheit, Ernährung und Wasserversorgung, Kernforschung und Atomindustrie (sofern diese nicht durch spezifische Bestimmungen abgedeckt sind) Beachtung zu schenken; ist der Ansicht, dass diese Sektoren ebenfalls von einem durch WINKI eingesetzten sektorübergreifenden Konzept (bestehend aus Kooperation, einem Warnsystem und dem Austausch optimaler Verfahren) profitieren sollten;

4. betont, wie wichtig es ist, eine dauerhafte Einbindung der europäischen Forschung zu erreichen, um die führende Stellung Europas im CIIP-Bereich zu behalten und auszubauen;

5. fordert angesichts der ineinander verflochtenen und stark voneinander abhängigen, sensiblen, strategischen und verletzlichen Natur der nationalen und europäischen kritischen Informationsstrukturen die regelmäßige Aktualisierung von Mindestnormen zur Zuverlässigkeit, um bei Störungen, Vorfällen, Zerstörungsversuchen oder Angriffen, wie zum Beispiel solchen, die aus unzureichend robuster Infrastruktur oder ungenügend gesicherten Endgeräten resultieren, vorbereitet zu sein und reagieren zu können;

6. unterstreicht die Wichtigkeit der Cyber-Sicherheitsstandards und -protokolle und begrüßt den CEN-, CENELEC- und ETSI-Auftrag von 2011 über die Festlegung von Sicherheitsstandards;

7. erwartet, dass Besitzer und Betreiber von kritischen Informationsstrukturen Anwender in die Lage versetzen und gegebenenfalls dabei unterstützen, die entsprechenden Maßnahmen zu nutzen, um sich vor bösartigen Angriffen und/oder Störungen zu schützen, sowohl mithilfe menschlicher als auch automatisierter Überwachungssysteme, sofern nötig;

8. unterstützt die Zusammenarbeit zwischen öffentlichen und privaten Interessenträgern auf Unionsebene und ermutigt deren Anstrengungen, Standards für Sicherheit und Zuverlässigkeit für zivile (öffentliche, private oder öffentlich/private) nationale und europäische kritische Informationsstrukturen zu entwickeln und umzusetzen;

9. unterstreicht die Bedeutung von europaweiten Übungen als Vorbereitung für den Fall von Netzsicherheitsverletzungen großen Ausmaßes sowie der Festlegung gemeinsamer Standards für die Einschätzung von Bedrohungen;

10. fordert die Kommission auf, in Zusammenarbeit mit den Mitgliedstaaten die Einführung des CIIP-Aktionsplans zu bewerten; fordert die Mitgliedstaaten nachdrücklich dazu auf, gut funktionierende nationale bzw. staatliche CERT einzuführen, nationale Cyber-Sicherheitsstrategien zu entwickeln, regelmäßige nationale und europaweite Übungen für den Fall von Netzstörungen zu organisieren, nationale Notfallpläne für Netzstörungen zu entwickeln und zur Entwicklung eines europäischen Notfallplans für Netzstörungen bis Ende 2012 beizutragen;

11. empfiehlt, dass Operator-Security-Pläne aufgestellt oder gleichwertige Maßnahmen für alle

---

[1] ABl. L 345 vom 23.12.2008, S. 75.

europäischen kritischen Informationsstrukturen ergriffen werden und dass Sicherheitsbeauftragte ernannt werden;

12. begrüßt die aktuelle Überprüfung des Rahmenbeschlusses 2005/222/JI[1] des Rates über Angriffe auf Informationssysteme; weist auf die Notwendigkeit der Koordination der EU-Bemühungen bei der Bekämpfung von Cyberangriffen in großem Maßstab durch Einschluss von ENISA, Mitgliedstaaten-CERT und der künftigen europäischen CERT-Kompetenzen hin;

13. vertritt die Auffassung, dass die ENISA im Hinblick auf den Schutz kritischer Informationsinfrastrukturen eine Schlüsselrolle auf europäischer Ebene spielen kann, indem sie den Mitgliedstaaten und den Organen und Einrichtungen der Europäischen Union Fachwissen zur Verfügung stellt sowie Berichte und Analysen über die Sicherheit der Informationssysteme auf europäischer und globaler Ebene erstellt;

Weitere EU-Aktivitäten für eine robuste Internetsicherheit

14. hält ENISA dazu an, jährliche Internet-Security-Awareness-Monate der EU zu koordinieren und umzusetzen, sodass Angelegenheiten im Zusammenhang mit Cybersicherheit zu einem besonderen Schwerpunkt für die Mitgliedstaaten und EU-Bürger werden;

15. unterstützt ENISA in Übereinstimmung mit den Zielen der Digitalen Agenda bei der Ausübung der Verpflichtungen hinsichtlich Netzinformationssicherheit, insbesondere über Anleitung und Beratung der Mitgliedstaaten, wie diese die Grundanforderungen für ihre CERT erfüllen können, sowie die Unterstützung des Austauschs optimaler Verfahren durch die Entwicklung einer vertrauensvollen Umgebung; fordert die Agentur auf, zur Festlegung ähnlicher Cyber-Sicherheitsmaßnahmen für private Netz- und Infrastrukturbesitzer/-betreiber die betroffenen Interessenträger zu konsultieren sowie die Kommission und die Mitgliedstaaten durch die Entwicklung und Übernahme von Informationssicherheitsplänen, Verhaltensregeln und Kooperationspraktiken bei nationalen und europäischen CERT sowie Infrastrukturbesitzer und -betreiber bei Bedarf durch die Festlegung technologieneutraler gemeinsamer Mindestanforderungen zu unterstützen;

16. begrüßt den aktuellen Vorschlag zur Überprüfung des ENISA-Mandats, vor allem dessen Verlängerung sowie die Erweiterung der Aufgaben der Agentur; ist der Ansicht, dass ENISA neben ihrer Unterstützung für Mitgliedstaaten mit Fachwissen und Analyse dazu berechtigt sein sollte, hinsichtlich Vorbeugen und Erkennen von Störungen der Netz- und Informationssicherheit sowie der Verbesserung der Kooperation unter den Mitgliedstaaten eine Reihe exekutiver Aufgaben auf EU-Ebene und in Kooperation mit den entsprechenden US-Partnern auszuführen; weist darauf hin, dass der Agentur im Rahmen der ENISA-Verordnung auch zusätzliche Aufgaben bezüglich der Reaktionen auf Internetangriffe übertragen werden könnten, sofern dies einen klaren Mehrwert für den bestehenden nationalen Reaktionsmechanismus bringt;

17. begrüßt die Ergebnisse der europaweiten Übungen zu Cybersicherheit 2010 und 2011, die unionsübergreifend durchgeführt und von ENISA überwacht wurden und deren Ziel die Unterstützung der Mitgliedstaaten bei Entwurf, Pflege und Testen eines europaweiten Notfallplans war; ruft ENISA auf, solche Übungen weiterhin zu planen und ggf. zunehmend relevante private Betreiber zu beteiligen, um die Internetsicherheit Europas insgesamt zu

---

[1] ABl. L 69 vom 16.3.2005, S. 67.

steigern, und begrüßt eine weitere internationale Erweiterung mit gleichgesinnten Partnern;

18. fordert die Mitgliedstaaten dazu auf, nationale Notfallpläne für Störungen auszuarbeiten und die Schlüsselelemente wie zum Beispiel einschlägige Anlaufstellen, Bestimmungen zu Hilfestellung, Eindämmung und Reparatur im Fall von Cyber-Störungen oder Angriffen mit grenzüberschreitender Relevanz einzubeziehen; merkt an, dass die Mitgliedstaaten darüber hinaus angemessene Koordinierungsmechanismen und -strukturen auf nationaler Ebene einrichten sollten, die dabei helfen würden, eine bessere Koordinierung der zuständigen nationalen Behörden sicherzustellen und ihre Handlungen kohärenter zu gestalten;

19. empfiehlt, dass die Kommission über den Notfallplan der EU für Cyber-Störungen bindende Maßnahmen zur besseren Koordination der technischen und steuernden Funktionen auf EU-Ebene unter den nationalen oder staatlichen CERT vorschlägt;

20. fordert die Kommission und die Mitgliedstaaten auf, die notwendigen Maßnahmen zu ergreifen, um kritische Infrastrukturen vor Cyber-Angriffen zu schützen, und Mittel dafür bereitzustellen, den Zugriff auf kritische Informationsinfrastrukturen gänzlich zu unterbinden, falls ein direkter Cyber-Angriff deren ordnungsgemäßes Funktionieren stark bedroht;

21. begrüßt die vollständige Umsetzung von CERT-EU, einem Schlüsselfaktor, was Prävention, Erkennung, Reaktion und Wiederherstellung im Zusammenhang mit absichtlichen und bösartigen Cyber-Angriffen auf EU-Institutionen angeht;

22. empfiehlt, dass die Kommission verbindliche Maßnahmen vorschlägt, um den nationalen CERT Mindestnormen bei Sicherheit und Zuverlässigkeit auferlegen und die Koordinierung unter ihnen verbessern zu können;

23. ruft die Mitgliedstaaten und die EU-Institutionen auf, das Vorhandensein von gut funktionierenden CERT sicherzustellen, die basierend auf den vereinbarten optimalen Verfahren für ein Minimum an Sicherheit und Zuverlässigkeit sorgen; weist darauf hin, dass nationale CERT Teil eines effizienten Netzwerks sein sollten, in dem relevante Informationen in Übereinstimmung mit den nötigen Standards für Vertraulichkeit ausgetauscht werden; fordert die Einrichtung eines durchgehenden CIIP-Dienstes für jeden Mitgliedstaat sowie eines gemeinsamen europäischen Notfallprotokolls, das zwischen den nationalen Anlaufstellen eingesetzt wird;

24. betont, dass Aufbau von Vertrauen und Förderung der Kooperation zwischen Mitgliedstaaten für den Schutz von Daten sowie nationalen Netzen und Infrastrukturen wesentlich sind; ruft die Kommission auf, ein gemeinsames Verfahren zur Ermittlung und Ausweisung eines gemeinsamen Ansatzes zu grenzübergreifenden IKT-Bedrohungen vorzuschlagen, in der Erwartung, dass die Mitgliedstaaten der Kommission allgemeine Informationen hinsichtlich Risiken, Bedrohungen und Verletzungen ihrer kritischen Informationsinfrastrukturen bereitstellen;

25. begrüßt die Initiative der Kommission zur Entwicklung eines European Information Sharing and Alert System bis 2013;

26. begrüßt die verschiedenen durch die Kommission veranlassten Anhörungen der Interessenträger zu Internet-Sicherheit und CIIP wie die European Public-Private Partnership for Resilience; nimmt die bereits einschlägige Beteiligung und

Einsatzbereitschaft der IKT-Dienstleister in diesen Bereichen zur Kenntnis; ermutigt die Kommission zu weiteren Bemühungen, die akademischen Verbände und die Vereinigungen von IKT-Anwendern zu unterstützen, eine aktivere Rolle zu spielen und einen konstruktiven Dialog mehrerer Interessenträger zu Angelegenheiten rund um die Cybersicherheit zu fördern;

27. begrüßt die bisher durch das Europäische Forum der Mitgliedstaaten geleistete Arbeit im Hinblick darauf, sektorspezifische Kriterien zur Identifizierung kritischer europäischer Infrastrukturen mit einem Schwerpunkt auf Festnetz- und mobiler Kommunikation festzulegen sowie Grundsätze und Richtlinien der EU für die Zuverlässigkeit und Stabilität des Internets zu diskutieren; erwartet die weitere Konsensbildung unter den Mitgliedstaaten und empfiehlt in diesem Zusammenhang dem Forum, den aktuellen Ansatz mit Fokus auf Sachanlagen zu ergänzen, in dem Bemühen, auch logische Infrastrukturanlagen zu erfassen, die im Zuge der weiteren Entwicklung von Virtualisierung und Cloud-Technologien zunehmend relevant für die Effizienz von CIIP sein werden;

28. schlägt vor, dass die Kommission eine europaweite öffentliche Bildungsinitiative startet, die darauf abzielt, private und geschäftliche Endanwender für potenzielle Bedrohungen im Internet und bei festen und mobilen IKT-Geräten auf jeder Ebene der Nutzungskette zu unterrichten und das Bewusstsein dafür zu wecken sowie sicheres individuelles Online-Verhalten zu fördern; erinnert in diesem Zusammenhang an die Risiken, die mit veralteter IT-Hardware und Software einhergehen;

29. fordert die Mitgliedstaaten auf, mit Unterstützung der Kommission Schulungen und Ausbildungsprogramme zur Informationssicherheit zu stärken, die auf nationale Strafverfolgungs- und Justizbehörden und die einschlägigen Agenturen der EU abzielen;

30. unterstützt die Erstellung eines EU-Lehrplans für akademische Experten im Bereich der Informationssicherheit, da dies einen positiven Einfluss auf die Fachkenntnisse und die Vorsorge der EU hinsichtlich des sich konstant entwickelnden Cyberspace und seiner Bedrohungen hat;

31. ist der Auffassung, dass die Unterweisung im Bereich Netzsicherheit (z. B. durch Praktika für Promovierende, Universitätslehrgänge, Workshops oder Schulungen für Studierende) sowie spezialisierte Schulungsübungen im CIIP-Bereich gefördert werden sollten;

32. fordert die Kommission auf, bis Ende 2012 auf der Grundlage einer eindeutigen Terminologie eine umfassende Internetsicherheitsstrategie für die Union vorzulegen; ist der Ansicht, dass die Internetsicherheitsstrategie zum Ziel haben sollte, einen durch eine sichere und zuverlässige Infrastruktur und offene Standards gestützten Cyberspace zu schaffen, der für die Innovation und den Wohlstand durch den freiem Informationsfluss förderlich ist, während für die Privatsphäre sowie andere Bürgerrechte ein robuster Schutz gewährleistet sein muss; besteht darauf, dass die Strategie die (sowohl internen als auch externen) Grundsätze, Ziele, Methoden, Instrumente und Richtlinien angeben sollte, die erforderlich sind, um die nationalen und EU-weiten Bemühungen sowie minimale Zuverlässigkeitsstandards unter den Mitgliedstaaten zur Sicherstellung eines sicheren, dauerhaften, robusten und zuverlässigen Dienstes, ob in Verbindung mit kritischer Infrastruktur oder allgemeiner Internetnutzung, zu vereinheitlichen;

33. betont, dass die anstehende „Internet-Sicherheitsstrategie“ der Kommission die Arbeit am Schutz kritischer Informationsinfrastrukturen als zentralen Bezugspunkt aufnehmen und

einen ganzheitlichen und systematischen Ansatz hin zur Netzsicherheit anstreben sollte, indem sowohl proaktive Maßnahmen, wie beispielsweise die Einführung von Mindeststandards für Sicherheitsmaßnahmen oder die Unterweisung von einzelnen Anwendern, Unternehmen und öffentlichen Einrichtungen, als auch reaktive Maßnahmen, wie z. B. strafrechtliche, zivilrechtliche und administrative Sanktionen, einbezogen werden;

34. fordert die Kommission auf, einen robusten Mechanismus vorzuschlagen, mit dem die Implementierung und die regelmäßige Aktualisierung der Internetsicherheitsstrategie koordiniert werden sollen; ist der Ansicht, dass dieser Mechanismus von ausreichend Verwaltungs-, Fach- und Finanzressourcen getragen werden sollte und es zu ihren Aufgaben zählen sollte, die Ausarbeitung der EU-Positionen in Bezug auf Themen zur Internetsicherheit im Verhältnis zu internen und internationalen Beteiligten zu ermöglichen;

35. fordert die Kommission dazu auf, einen EU-Rahmen für die Meldung von Sicherheitsverletzungen in kritischen Sektoren, beispielsweise dem Energie-, Verkehrs- und Wassersektor und der Nahrungsmittelversorgung, aber auch im IKT-Sektor und bei Finanzdienstleistungen, aufzustellen, um zu gewährleisten, dass betroffene Behörden und Anwender der Mitgliedstaaten über Vorfälle, Angriffe und Störungen im bzw. aus dem Cyberspace informiert werden;

36. fordert die Kommission auf, die Verfügbarkeit statistisch repräsentativer Daten zu verbessern, die die Kosten von Cyber-Angriffen in der EU, den Mitgliedstaaten und der Industrie (vor allem in den Sektoren Finanzdienstleistungen und IKT) betreffen, indem sie die Datenerhebungsmöglichkeiten des geplanten European Cybercrime Centre, dessen Einrichtung für 2013 geplant ist, der CERT und von anderen Initiativen der Kommission wie des European Information Sharing and Alert System verbessert, um die systematische Berichterstattung und die Weitergabe von Daten in Bezug auf Cyber-Angriffe und andere Formen der Cyber-Kriminalität, die die europäische Industrie und Mitgliedstaaten betreffen, sicherzustellen und um damit die Strafverfolgung zu stärken;

37. vertritt die Ansicht, dass eine enge Abstimmung und Interaktion zwischen den Privatsektoren in den einzelnen Mitgliedstaaten und der ENISA stattfinden sollte, um die nationalen bzw. staatlichen CERT mit der Entwicklung des Europäischen Informations- und Warnsystems (EISAS) zu verbinden;

38. weist darauf hin, dass die IKT-Branche die treibende Kraft hinter der Entwicklung und Anwendung von Technologien zur Erhöhung der Internetsicherheit ist; erinnert daran, dass die EU-Politik die europäische Internetwirtschaft nicht hemmen darf und die erforderlichen Anreize berücksichtigen muss, damit das Potenzial geschäftlicher und öffentlich/privater Partnerschaften voll ausgeschöpft werden kann; empfiehlt die Untersuchung weiterer Anreize für die Industrie, damit diese robustere Betreibersicherheitspläne gemäß 2008/114/EG entwickelt;

39. fordert die Kommission auf, einen legislativen Vorschlag vorzulegen, um Cyber-Angriffe weiterzuverfolgen (d. h. Spear-Phishing, Internet-Betrug usw.);

Internationale Zusammenarbeit

40. erinnert daran, dass internationale Zusammenarbeit das Kerninstrument für die Einleitung wirksamer Maßnahmen zur Cybersicherheit ist; stellt fest, dass die EU zum gegenwärtigen Zeitpunkt nicht aktiv und kontinuierlich an internationalen Kooperationsprozessen und

Dialogen hinsichtlich Cybersicherheit beteiligt ist; fordert die Kommission und den Europäischen Auswärtigen Dienst (EAD) dazu auf, mit allen gleichgesinnten Ländern mit Blick auf die Entwicklung einer gemeinsamen Auslegung und einer gemeinsamen Politik mit dem Ziel der Erhöhung der Zuverlässigkeit des Internets und der kritischen Infrastruktur einen konstruktiven Dialog zu beginnen; besteht darauf, dass die EU Angelegenheiten zur Internetsicherheit gleichzeitig dauerhaft in den Wirkungsbereich ihrer Außenbeziehungen einbindet, unter anderem bei der Ausarbeitung verschiedener Finanzierungsinstrumente oder bei der Verpflichtung zu internationalen Vereinbarungen, die den Austausch und die Speicherung von sensiblen Daten betreffen;

41. nimmt die positiven Errungenschaften der Budapester Konvention 2001 des Europarats zur Cyberkriminalität zur Kenntnis; weist jedoch darauf hin, dass der EAD, während er dazu aufruft, dass mehr Länder die Konvention unterzeichnen und ratifizieren, auch bilaterale und multilaterale Abkommen über Internetsicherheit und -zuverlässigkeit mit gleichgesinnten internationalen Partnern aufbauen sollte;

42. betont, dass die große Anzahl laufender Aktivitäten, die von verschiedenen internationalen Institutionen, den Organen, Einrichtungen und sonstigen Stellen der EU sowie von den Mitgliedstaaten durchgeführt werden, koordiniert werden müssen, um Doppelarbeit zu vermeiden; ist der Ansicht, dass zu diesem Zweck erwogen werden sollte, einen offiziellen Verantwortlichen für die Koordination einzusetzen, gegebenenfalls durch die Ernennung eines EU-Koordinators für Netzsicherheit;

43. betont, dass ein strukturierter Dialog zwischen den wichtigsten CIIP-Akteuren und den Gesetzgebern in der EU und den Vereinigten Staaten für den Aufbau einer gemeinsamen Verständigung über einen Rechts- und Regulierungsrahmen sowie für gemeinsame Auslegungen und Standpunkte bezüglich dieses Rahmens ist;

44. begrüßt die Einrichtung der Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität anlässlich des EU/USA-Gipfels im November 2010 und unterstützt deren Bemühungen zur Aufnahme von Internetsicherheitsfragen in den transatlantischen Politikdialog; begrüßt, dass die Kommission und die US-Regierung unter dem Dach der Arbeitsgruppe EU/USA zusammen ein gemeinsames Programm und einen Fahrplan für eine gemeinsame bzw. synchronisierte transkontinentale Cyber-Übung 2012-2013 ausgearbeitet haben;

45. schlägt vor, einen strukturierten Dialog zwischen US- und EU-Gesetzgebern zu begründen, um Angelegenheiten zum Thema Internet als Bestandteil einer Suche nach Verständigung, Interpretation und Positionen zu diskutieren;

46. fordert den EAD und die Kommission auf der Grundlage der durch das Europäische Forum der Mitgliedstaaten durchgeführten Arbeit dazu auf, eine aktive Position innerhalb der einschlägigen internationalen Foren zu sichern, unter anderem durch die Koordinierung der Positionen der Mitgliedstaaten mit Blick auf die Förderung der grundlegenden Werte, Ziele und Grundsätze der EU im Bereich Sicherheit und Zuverlässigkeit des Internets; bemerkt, dass zu diesen Foren die Nato, die UN (insbesondere durch die Internationale Fernmeldeunion und das Internet-Verwaltungs-Forum), die Internet Corporation for Assigned Names and Numbers, die Internet Assigned Numbers Authority, die OSZE, die OECD und die Weltbank gehören;

47. empfiehlt der Kommission und Enisa, an den Dialogen der Hauptinteressenträger teilzunehmen, um auf internationaler Ebene technische und rechtliche Normen im Cyberspace festzulegen;

o

o o

48. beauftragt seinen Präsidenten, diese Entschließung dem Rat und der Kommission zu übermitteln.