EUROPÄISCHES PARLAMENT 2009 – 2014

Plenarsitzungsdokument

A7-0335/2012

17.10.2012

BERICHT

über Cyber-Sicherheit und -Verteidigung
(2012/2096(INI))

Ausschuss für auswärtige Angelegenheiten

Berichterstatter: Tunne Kelam

INHALT

Seite

ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS

zu Cyber-Sicherheit und -Verteidigung
(2012/2096(INI))

Das Europäische Parlament,

– in Kenntnis des am 11. und 12. Dezember 2008 vom Europäischen Rat gebilligten Berichts über die Umsetzung der Europäischen Sicherheitsstrategie,

– in Kenntnis des Übereinkommens des Europarates über Computerkriminalität vom 23. November 2004 (Budapest),

– in Kenntnis der Schlussfolgerungen des Rates zum Schutz kritischer Informationsinfrastrukturen vom 27. Mai 2011 sowie der früheren Schlussfolgerungen des Rates zur Cyber-Sicherheit,

– in Kenntnis der Mitteilung der Kommission „Eine Digitale Agenda für Europa“ vom 19. Mai 2010 (COM(2010)0245),

– in Kenntnis der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern[1],

– in Kenntnis der vor kurzem vorgelegten Mitteilung der Kommission zur Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität als vorrangiges Ziel der Strategie der inneren Sicherheit (COM(2012)0140),

– unter Hinweis auf seine Entschließung vom 10. März 2010 zur Umsetzung der Europäischen Sicherheitsstrategie und der Gemeinsamen Sicherheits- und Verteidigungspolitik[2],

– unter Hinweis auf seine Entschließung vom 11. Mai 2011 zur Entwicklung der Gemeinsamen Sicherheits- und Verteidigungspolitik nach Inkrafttreten des Vertrags von Lissabon[3],

– unter Hinweis auf seine Entschließung vom 22. Mai 2012 zur Strategie der Europäischen Union zur inneren Sicherheit[4],

– unter Hinweis auf seine Entschließung vom 27. September 2011 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 1334/2000 über eine Gemeinschaftsregelung für die Kontrolle der

[1] ABl. L 345 vom 23.12.2008, S. 75.
[2] Angenommene Texte, P7_TA(2010)0061.
[3] Angenommene Texte, P7_TA(2011)0228.
[4] Angenommene Texte, P7_TA(2011)0207.

Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck[1],

– unter Hinweis seine Entschließung vom 12. Juni 2012 über den Schutz kritischer Informationsinfrastrukturen – Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit[2],

– in Kenntnis der Resolution des Menschenrechtsrats der Vereinten Nationen vom 5. Juli 2012 „Die Förderung, der Schutz und der Genuss der Menschenrechte im Internet“[3], in der die Bedeutung des Schutzes der Menschenrechte und des freien Informationsflusses im Internet anerkannt wird,

– in Kenntnis der Schlussfolgerungen des Gipfels in Chicago vom 20. Mai 2012,

– gestützt auf Titel V des EU-Vertrags,

– gestützt auf Artikel 48 seiner Geschäftsordnung,

– in Kenntnis des Berichts des Ausschusses für auswärtige Angelegenheiten (A7-0335/2012),

A. in der Erwägung, dass ein sicherer virtueller Raum, die sichere Nutzung von Informationen und digitalen Technologien sowie belastbare und zuverlässige Informationsdienste und die dazugehörigen Infrastrukturen für die EU und ihre Mitgliedstaaten in der heutigen globalisierten Welt von zentraler Bedeutung sind;

B. in der Erwägung, dass die Informations- und Kommunikationstechnologien auch als Unterdrückungsinstrumente angewendet werden; in der Erwägung, dass der Zusammenhang, in dem diese Technologien genutzt werden, in hohem Maße entscheidend dafür ist, ob mit ihrer Hilfe positive Entwicklungen herbeigeführt werden oder ob sie der Unterdrückung dienen;

C. in der Erwägung, dass Herausforderungen und Bedrohungen für die Cyber-Sicherheit in dramatischem Tempo zunehmen und eine vorrangige Bedrohung der Sicherheit, Verteidigung, Stabilität und Wettbewerbsfähigkeit der Nationalstaaten wie auch des privaten Sektors darstellen; in der Erwägung, dass derartige Bedrohungen daher nicht als für die Zukunft relevante Fragen betrachtet werden sollten; in der Erwägung, dass gegenwärtig die Mehrheit der besonders auffälligen und zerstörerischen Beeinträchtigungen der Cyber-Sicherheit politisch motiviert ist; in der Erwägung, dass eine deutliche Mehrheit der Beeinträchtigungen der Cyber-Sicherheit zwar nicht über ein primitives Niveau hinausgeht, die Bedrohungen der kritischen Infrastrukturen jedoch zunehmend ausgeklügelter werden und gründlichere Schutzmaßnahmen rechtfertigen;

D. in der Erwägung, dass der virtuelle Raum mit seinen an die 2 Milliarden weltweit miteinander vernetzten Nutzern eines der einflussreichsten und wirksamsten Werkzeuge ist, um demokratische Ideen voranzubringen und Menschen zu organisieren, die versuchen, ihr Streben nach Freiheit und der Bekämpfung von Diktaturen zu

[1] Angenommene Texte, P7_TA(2012)0406.
[2] Angenommene Texte, P7_TA(2012)0237.
[3] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

verwirklichen; in der Erwägung, dass die Nutzung des virtuellen Raums durch undemokratische und autoritäre Regime eine zunehmende Bedrohung der Rechte des Einzelnen auf Meinungs- und Versammlungsfreiheit darstellt; in der Erwägung, dass es deshalb von zentraler Bedeutung ist, dafür zu sorgen, dass der virtuelle Raum weiterhin für den ungehinderten Fluss von Ideen, Informationen und Meinungen offen ist;

E. in der Erwägung, dass der Entwicklung eines umfassenden und einheitlichen Ansatzes für die Cyber-Verteidigung und -Sicherheit in der EU und ihren Mitgliedstaaten zahlreiche Hindernisse politischer, legislativer und organisatorischer Art entgegenstehen; in der Erwägung, dass es in dem sensiblen und anfälligen Bereich der Cyber-Sicherheit an einer gemeinsamen Definition, gemeinsamen Standards und gemeinsamen Maßnahmen fehlt;

F. in der Erwägung, dass der Austausch und die Koordinierung innerhalb der Organe der EU, mit und zwischen den Mitgliedstaaten und auch mit externen Partnern nach wie vor unzureichend sind;

G. in der Erwägung, dass es auf EU-Ebene und auf internationaler Ebene keine klaren, harmonisierten Definitionen von „Cyber-Sicherheit“ und „Cyber-Verteidigung“ gibt; in der Erwägung, dass es zwischen den Ländern beträchtliche Unterschiede in Bezug darauf gibt, was unter Cyber-Sicherheit und anderen zentralen Termini verstanden wird;

H. in der Erwägung, dass die EU noch keine kohärenten eigenen Strategien für den Schutz kritischer Informationsinfrastrukturen erarbeitet hat, was einen multidisziplinären Ansatz erforderlich macht und so bei Einhaltung der Grundrechte eine Verbesserung der Sicherheit bewirkt;

I. in der Erwägung, dass die EU zwar verschiedene Initiativen zur Bekämpfung von Cyber-Kriminalität im zivilen Bereich vorgeschlagen hat, darunter auch die Einrichtung eines neuen europäischen Zentrums zur Bekämpfung der Cyber-Kriminalität, konkrete Pläne für den Sicherheits- und Verteidigungsbereich jedoch fehlen;

J. in der Erwägung, dass es bei der Bekämpfung der Cyber-Kriminalität von größter Wichtigkeit ist, Vertrauen zwischen dem privaten Sektor, den Strafverfolgungsbehörden, den Verteidigungsorganen und anderen zuständigen Einrichtungen aufzubauen;

K. in der Erwägung, dass bei den Beziehungen zwischen staatlichen und nichtstaatlichen Akteuren gegenseitiges Vertrauen eine Voraussetzung für verlässliche Cyber-Sicherheit ist;

L. in der Erwägung, dass aufgrund der Sensibilität der Informationen und des möglichen Schadens für das Image der beteiligten Unternehmen die meisten Beeinträchtigungen der Cyber-Sicherheit im privaten und im öffentlichen Sektor nicht gemeldet werden;

M. in der Erwägung, dass die Ursache zahlreicher Beeinträchtigungen der Cyber-Sicherheit die mangelnde Widerstandsfähigkeit und Robustheit der privaten und öffentlichen Netzinfrastruktur, der mangelhafte Schutz und die unzureichende Sicherung von Datenbanken und andere Mängel der kritischen Informationsinfrastruktur sind; in der

Erwägung, dass nur wenige Mitgliedstaaten den Schutz ihrer Netze und Informationssysteme und der damit in Zusammenhang stehenden Daten als Teil ihrer Sorgfaltspflicht betrachten, was den Mangel an Investitionen in moderne Sicherheitstechnologie, in die Ausbildung und in die Entwicklung geeigneter Leitlinien erklärt, und in der Erwägung, dass eine große Zahl von Mitgliedstaaten von Sicherheitstechnologie aus Drittstaaten abhängig ist und dass die Bemühungen dieser Mitgliedstaaten, diese Abhängigkeit zu verringern, verstärkt werden sollten;

N. in der Erwägung, dass die Mehrzahl der Täter, die Cyber-Angriffe auf hohem Niveau verüben, durch die die nationale oder internationale Sicherheit und die Verteidigung gefährdet werden, nie identifiziert und verfolgt wird; in der Erwägung, dass es keine international vereinbarte Reaktion auf einen von einem Staat ausgehenden Cyber-Angriff auf einen anderen Staat gibt und keine Einigung darüber besteht, ob dies als Casus Belli betrachtet werden könnte;

O. in der Erwägung, dass die Europäische Agentur für Netz- und Informationssicherheit (ENISA) als Vermittler für die Mitgliedstaaten herangezogen wird, um durch Empfehlungen dazu, wie eine Strategie für Internet-Sicherheit entwickelt, durchgeführt und aufrechterhalten werden kann, den Austausch bewährter Verfahren im Bereich der Internet-Sicherheit zu fördern, und dass sie bei nationalen Strategien für Internet-Sicherheit, bei nationalen Notfallplänen, bei der Organisation paneuropäischer und internationaler Übungen zum Schutz kritischer Informationsinfrastrukturen sowie bei der Ausarbeitung von Szenarien für nationale Übungen eine unterstützende Rolle spielt;

P. in der Erwägung, dass mit Stand vom Juni 2012 nur 10 EU-Mitgliedstaaten offiziell eine nationale Strategie für Internet-Sicherheit verabschiedet haben;

Q. in der Erwägung, dass die Cyber-Verteidigung eine der wichtigsten Prioritäten der EDA ist, die im Rahmen des Plans für den Ausbau der Fähigkeiten ein Projektteam zur Internet-Sicherheit eingerichtet hat, in dessen Rahmen die meisten Mitgliedstaaten daran arbeiten, Erfahrungen zu sammeln und Empfehlungen vorzuschlagen;

R. in der Erwägung, dass Investitionen in Forschung und Entwicklung zu Cyber-Sicherheit und -Verteidigung von zentraler Bedeutung für die Erreichung und Beibehaltung eines hohen Niveaus an Cyber-Sicherheit und -Verteidigung sind; in der Erwägung, dass die Verteidigungsausgaben für Forschung und Entwicklung zurückgegangen sind, anstatt die vereinbarten 2 % der gesamten Verteidigungsausgaben zu erreichen;

S. in der Erwägung, dass die Sensibilisierung und Schulung der Bürger in Fragen der Cyber-Sicherheit die Grundlage jeder umfassenden Strategie für Cyber-Sicherheit bilden sollte;

T. in der Erwägung, dass zwischen Sicherheitsmaßnahmen und den Rechten der Bürger gemäß dem Vertrag über die Arbeitsweise der Europäischen Union, wie zum Beispiel dem Recht auf Schutz der Privatsphäre, dem Recht auf Datenschutz und dem Recht auf freie Meinungsäußerung, ein eindeutiges Gleichgewicht hergestellt werden muss, wobei die einen nicht im Namen der anderen geopfert werden dürfen;

U. in der Erwägung, dass die Notwendigkeit wächst, die Rechte des Einzelnen auf Wahrung der Privatsphäre gemäß der EU-Charta und Artikel 16 AEUV konsequenter einzuhalten

und besser zu schützen; in der Erwägung, dass die Notwendigkeit, den virtuellen Raum für Institutionen und Stellen im Bereich der Verteidigung auf nationaler Ebene zu sichern und zu verteidigen, zwar wichtig ist, jedoch nie zur Rechtfertigung einer wie auch immer gearteten Einschränkung von Rechten und Freiheiten im virtuellen Raum und in der Informationssphäre benutzt werden sollte;

V. in der Erwägung, dass der weltumspannende und grenzenlose Charakter des Internets neue Formen der internationalen Zusammenarbeit und der Regierungsführung mit verschiedenen Akteuren erforderlich macht;

W. in der Erwägung, dass sich die Regierungen im Hinblick auf die Sicherheit ihrer kritischen Infrastruktur in zunehmendem Maße auf private Akteure verlassen;

X. in der Erwägung, dass der Europäische Auswärtige Dienst (EAD) noch nicht die Initiative ergriffen hat, in seine Beziehungen zu Drittstaaten einen Aspekt der Internet-Sicherheit aufzunehmen;

Y. in der Erwägung, dass das Stabilitätsinstrument bisher das einzige Programm der EU ist, das darauf ausgerichtet ist, auf Krisen, die umgehende Maßnahmen erfordern, oder auf weltweite bzw. transregionale Sicherheitsprobleme, einschließlich Bedrohungen der Cyber-Sicherheit, zu reagieren;

Z. in der Erwägung, dass eine gemeinsame Reaktion – über die Arbeitsgruppe der EU und der USA für Cyber-Sicherheit und Cyber-Kriminalität – auf Gefährdungen der Cyber-Sicherheit eines der prioritären Themen in den Beziehungen zwischen der EU und den USA ist;

Maßnahmen und Koordinierung innerhalb der EU

1. weist darauf hin, dass Cyber-Bedrohungen und Angriffe auf Stellen der Regierung, der Verwaltung und des Militärs und auf internationale Stellen sowohl in der EU als auch weltweit eine rasch wachsende Gefahr und rasch häufiger werdende Vorkommnisse sind und dass es erheblichen Anlass zu der Sorge gibt, dass staatliche und nichtstaatliche Akteure, insbesondere terroristische und kriminelle Organisationen, in der Lage sind, kritische Informationssysteme, Kommunikationsstrukturen und Infrastrukturen von EU-Organen und Mitgliedstaaten anzugreifen, wodurch erheblicher Schaden, einschließlich kinetischer Auswirkungen, verursacht werden kann;

2. hebt deshalb hervor, dass für die Abwehr dieser Gefahren ein umfassender und koordinierter Ansatz auf EU-Ebene geschaffen werden muss, indem eine umfassende EU-Strategie für die Internet-Sicherheit entwickelt wird, die eine gemeinsame Definition der Begriffe „Cyber-Sicherheit“, „Cyber-Verteidigung“ und „Cyber-Angriff auf die Verteidigung“ sowie gemeinsame Operationsziele enthalten und den Mehrwert der bestehenden Agenturen und Stellen und bewährte Verfahren aus den Mitgliedstaaten, die bereits über nationale Strategien für die Cyber-Sicherheit verfügen, berücksichtigen sollte; hebt die wesentliche Bedeutung der Koordinierung und der Schaffung von Synergien auf Unionsebene hervor, um dazu beizutragen, verschiedene militärische und zivile Initiativen, Programme und Aktivitäten zu kombinieren; betont, dass eine solche Strategie für Flexibilität sorgen und dass sie regelmäßig aktualisiert werden sollte, damit sie stets an

die rasch wechselnden Gegebenheiten im virtuellen Raum angepasst ist;

3. fordert die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik auf, in ihrem anstehenden Vorschlag für die Modalitäten der Anwendung der Solidaritätsklausel (Artikel 222 AEUV) die Möglichkeit eines schweren Cyber-Angriffs auf einen Mitgliedstaat zu berücksichtigen; ist darüber hinaus der Ansicht, dass Cyber-Angriffe, durch die die nationale Sicherheit gefährdet wird, zwar noch ihrer gemeinsam festgelegten Definition harren, jedoch, unbeschadet des Grundsatzes der Verhältnismäßigkeit, in den Anwendungsbereich der Klausel über gegenseitige Verteidigung (Artikel 42 Absatz 7 EUV) fallen könnten;

4. hebt hervor, dass die GSVP sicherstellen muss, dass Streitkräfte, die bei militärischen Operationen und zivilen Missionen der EU eingesetzt werden, gegen Cyber-Angriffe geschützt sind; betont, dass die GSVP zur aktiven Durchführung der Cyber-Verteidigung befähigt werden sollte;

5. betont, dass der maximale Schutz und die Bewahrung der digitalen Freiheiten und die Einhaltung der Menschenrechte im Online-Bereich Grundgedanke aller Strategien der EU im Bereich der Cyber-Sicherheit sein und sich in ihrer Gestaltung widerspiegeln sollten; ist der Ansicht, dass zur Förderung der entsprechenden Bemühungen das Internet und die Informations- und Kommunikationstechnologien in die außen- und sicherheitspolitischen Strategien der EU integriert werden sollten;

6. fordert die Kommission und den Rat auf, die digitalen Freiheiten unmissverständlich als Grundrechte und als unverzichtbare Voraussetzungen für den Genuss der universellen Menschenrechte anzuerkennen; betont, das die Mitgliedstaaten bei der Entwicklung ihrer Reaktionen auf Cyber-Bedrohungen und -angriffe danach streben sollten, niemals die Rechte und Freiheiten ihrer Bürger zu gefährden, und dass sie für angemessene Unterschiede in den Rechtsvorschriften zu Cyber-Störfällen im zivilen und militärischen Bereich Sorge tragen sollten; fordert, dass die Möglichkeiten der Bürger, Instrumente im Bereich der Informations- und Kommunikationstechnologien zu nutzen, nur mit ausgesprochener Vorsicht eingeschränkt werden dürfen;

7. fordert den Rat und die Kommission auf, gemeinsam mit den Mitgliedstaaten ein Weißbuch zur Cyber-Verteidigung zu erarbeiten, in dem klare Definitionen und Kriterien festgelegt werden, um anhand der zu Grunde liegenden Motive und Auswirkungen zwischen verschiedenen Ebenen von Cyber-Angriffen im zivilen und militärischen Bereich sowie zwischen Reaktionsebenen, einschließlich der Ermittlung, Aufspürung und Bestrafung der Täter, zu unterscheiden;

8. ist der Ansicht, dass es unbedingt notwendig ist, die Europäische Sicherheitsstrategie zu aktualisieren, damit Wege zur Aufspürung und Verfolgung einzelner, netzbezogener und staatlich unterstützter Cyber-Angreifer gefunden werden;

EU-Ebene

9. betont, dass die horizontale Zusammenarbeit und Koordinierung in Bezug auf die Cyber-Sicherheit innerhalb der EU-Organe und -agenturen sowie zwischen ihnen von großer Bedeutung ist;

10. betont, dass neue Technologien die Art und Weise infrage stellen, in der die Regierungen ihre traditionellen Kernaufgaben wahrnehmen; bekräftigt, dass die Verteidigungs- und Sicherheitspolitik letztenendes in der Hand der Regierungen liegt, einschließlich angemessener demokratischer Kontrolle; weist auf die wachsende Bedeutung von privaten Akteuren bei der Wahrnehmung von Aufgaben in den Bereichen Sicherheit und Verteidigung hin, die häufig ohne Transparenz, Rechenschaftspflicht oder demokratische Kontrollmechanismen erfolgt;

11. betont, dass sich die Regierungen bei der Anwendung neuer Technologien im Bereich der Sicherheits- und Verteidigungspolitik an grundlegende Prinzipien des internationalen öffentlichen und humanitären Rechts halten müssen, darunter die Einhaltung der Souveränität der Staaten und der Menschenrechte; weist auf die wertvollen Erfahrungen von EU-Mitgliedstaaten, wie zum Beispiel Estland, bei der Festlegung und Ausgestaltung von Strategien im Bereich der Cyber-Sicherheit und -verteidigung hin;

12. hält es für notwendig, das Gesamtausmaß der Cyber-Angriffe gegen EU-Informationssysteme und -infrastruktur zu bewerten; betont in diesem Zusammenhang, dass der Grad der Vorbereitung der EU-Organe auf die Abwehr möglicher Cyber-Angriffe kontinuierlich bewertet werden muss; hebt insbesondere die Notwendigkeit hervor, die kritischen Informationsinfrastrukturen zu verstärken;

13. hebt ferner die Notwendigkeit hervor, Informationen über Gefährdungen, Alarmmeldungen und Warnungen vor neuen Bedrohungen der IT-Systeme bereitzustellen;

14. weist darauf hin, dass die jüngsten Internet-Angriffe gegen europäische Informationsnetze und Informationssysteme der Regierungen erhebliche Schäden in der Wirtschaft und im Sicherheitsbereich verursacht haben, deren Ausmaß nicht hinreichend bewertet worden ist;

15. fordert sämtliche EU-Organe auf, ihre Strategien für die Internetsicherheit und die Notfallpläne für ihre eigenen Systeme so rasch wie möglich zu entwickeln;

16. fordert sämtliche EU-Organe auf, die Bewältigung von Cyber-Krisen in ihre Risikoanalysen und Krisenbewältigungspläne aufzunehmen; fordert darüber hinaus sämtliche EU-Organe auf, für ihr gesamtes Personal Fortbildungsmaßnahmen zur Sensibilisierung für die Cyber-Sicherheit durchzuführen; schlägt vor, ähnlich der generellen Praxis in Bezug auf Notfallübungen einmal jährlich Cyber-Notfallübungen durchzuführen;

17. betont, dass es wichtig ist, das Computer-Notfallteam (Computer Emergency Response Team) der EU (EU-CERT) und die nationalen Computer-Notfallteams zügig zu entwickeln und für den Maßnahmenfall nationale Notfallpläne zu arbeiten; begrüßt, dass sämtliche EU-Mitgliedstaaten bis Mai 2012 nationale Computer-Notfallteams eingerichtet haben; fordert, die nationalen Computer-Notfallteams und ein Computer-Notfallteam der EU so weiterzuentwickeln, dass sie in der Lage sind, im Bedarfsfall innerhalb von 24 Stunden zu handeln; hebt hervor, dass die Möglichkeit öffentlich-privater Partnerschaften in diesem Bereich ausgelotet werden muss;

18. weist darauf hin, dass sich „Cyber Europe 2010“, die erste gesamteuropäische Übung zum Schutz kritischer Informationsinfrastruktur, die unter Einbeziehung mehrerer Mitgliedstaaten und unter Leitung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) durchgeführt wurde, als nützliche Maßnahme und als ein Beispiel für die Anwendung bewährter Verfahren erwiesen hat; unterstreicht weiterhin die Notwendigkeit, das Warn- und Informationsnetz für kritische Infrastrukturen auf europäischer Ebene schnellstmöglich einzurichten;

19. 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;

20. fordert die Kommission auf, die Notwendigkeit und Machbarkeit einer Internet-Koordinierungsfunktion für die EU zu untersuchen;

21. ist der Ansicht, dass die Kommission, der Rat und die Mitgliedstaaten angesichts des hohen Kenntnisstandes, der sowohl für die adäquate Verteidigung von Cyber-Systemen und -infrastrukturen als auch für Angriffe auf sie notwendig ist, die Möglichkeit erwägen sollten, eine Strategie des „ethischen Hacking“ zu entwickeln; weist darauf hin, dass diese Fälle ein hohes Potenzial für einen „Intelligenztransfer“ aufweisen und dass insbesondere bei Minderjährigen, die wegen solcher Angriffe verurteilt wurden, gute Chancen sowohl für eine Rehabilitation als auch für eine Integration in Verteidigungsagenturen und -organen bestehen;

Europäische Verteidigungsagentur (EDA)

22. begrüßt die jüngsten Initiativen und Projekte im Bereich der Cyber-Verteidigung, insbesondere zur Sammlung und Darstellung wichtiger Daten für die Cyber-Sicherheit und -verteidigung sowie von Aufgaben und Notwendigkeiten, und fordert die Mitgliedstaaten auf, im Hinblick auf die Cyber-Verteidigung stärker mit der EVA zusammenzuarbeiten, auch auf militärischer Ebene;

23. hebt hervor, dass die enge Zusammenarbeit der Mitgliedstaaten mit der Europäischen Verteidigungsagentur bei der Entwicklung ihrer nationalen Verteidigungsressourcen gegen Cyber-Angriffe von großer Bedeutung ist; ist der Ansicht, dass die Schaffung von Synergien und die Zusammenlegung und gemeinsame Nutzung von Ressourcen auf EU-Ebene von grundlegender Bedeutung für eine wirksame Verteidigung gegen Internet-Angriffe auf der Ebene der EU und auf nationaler Ebene sind;

24. fordert die Europäische Verteidigungsagentur auf, ihre Zusammenarbeit mit der NATO, mit den nationalen und internationalen Spitzenforschungszentren und dem Europäischen Zentrum zur Bekämpfung der Cyber-Kriminalität im Rahmen von Europol, um zu schnelleren Reaktionen im Falle von Cyber-Angriffen beizutragen, und insbesondere mit dem Cooperative Cyber Defence Centre of Excellence (CCDCOE) zu vertiefen und sich auf den Aufbau von Kapazitäten, die Ausbildung und den Austausch von Informationen und Verfahren zu konzentrieren;

25. nimmt besorgt zur Kenntnis, dass lediglich ein Mitgliedstaat bis 2010 die Ausgabenhöhe von 2 % für Forschung und Entwicklung im Verteidigungsbereich erreicht hat und dass

fünf Mitgliedstaaten im Jahre 2010 keine Ausgaben für Forschung und Entwicklung getätigt haben; fordert die EVA und die Mitgliedstaaten auf, ihre Ressourcen zusammenzulegen und wirksam in gemeinschaftliche Forschung und Entwicklung zu investieren, insbesondere im Hinblick auf die Cyber-Sicherheit und -Verteidigung;

Mitgliedstaaten

26. fordert die Mitgliedstaaten auf, ihre jeweiligen nationalen Strategien für die Cyber-Sicherheit und -verteidigung ohne weitere Verzögerung zu entwickeln und zu vollenden und für eine solide Politikgestaltung, ein solides ordnungspolitisches Umfeld, umfassende Risikomanagementverfahren sowie angemessene Vorbereitungsmaßnahmen und -mechanismen Sorge zu tragen; fordert die ENISA auf, die Mitgliedstaaten dabei zu unterstützen; macht deutlich, dass es die ENISA bei der Entwicklung eines Leitfadens für bewährte Verfahren und Empfehlungen für die Entwicklung, Umsetzung und Einhaltung einer Strategie für die Cyber-Sicherheit unterstützt;

27. fordert alle Mitgliedstaaten auf, innerhalb ihrer militärischen Strukturen ausgewiesene Einheiten für die Cyber-Sicherheit und -verteidigung aufzustellen, um mit ähnlichen Stellen in anderen EU-Mitgliedstaaten zusammenzuarbeiten;

28. legt den Mitgliedstaaten nahe, spezielle gerichtliche Stellen auf regionaler Ebene einzurichten, die eine wirksamere Ahndung von Angriffen auf Informationssysteme gewährleisten sollen; hebt die Notwendigkeit hervor, eine Änderung der nationalen Rechtsvorschriften zu fördern, durch die eine Anpassung dieser Vorschriften an die Entwicklungen bei den Techniken und Praktiken ermöglicht wird;

29. fordert die Kommission auf, weiter an einem kohärenten und effizienten europäischen Ansatz zur Vermeidung redundanter Initiativen zu arbeiten und die Bemühungen der Mitgliedstaaten, Kooperationsmechanismen zu entwickeln und den Austausch von Informationen zu intensivieren, zu fördern und zu unterstützen; ist der Ansicht, dass ein verbindliches Mindestniveau der Zusammenarbeit und des Austauschs zwischen den Mitgliedstaaten festgelegt werden sollte;

30. fordert die Mitgliedstaaten auf, nationale Notfallpläne zu erarbeiten und die Bewältigung von Cyber-Krisen in ihre Krisenbewältigungspläne und Risikoanalysen einzubeziehen; unterstreicht außerdem, dass es wichtig ist, dass das gesamte Personal öffentlicher Einrichtungen in Bezug auf die wesentlichen Aspekte der Cyber-Sicherheit angemessen geschult wird und dass insbesondere den Mitgliedern der Justiz- und der Sicherheitsorgane eine angemessene Schulung in den Ausbildungseinrichtungen angeboten wird; fordert die ENISA und andere einschlägige Stellen auf, die Mitgliedstaaten bei der Zusammenlegung und gemeinsamen Nutzung ihrer Ressourcen und bei der Vermeidung von Doppelungen zu unterstützen;

31. fordert die Mitgliedstaaten auf, Forschung und Entwicklung zu einer der Grundsäulen der Cyber-Sicherheit und der Verteidigung gegen Cyber-Angriffe zu machen und die Ausbildung von Ingenieuren zu fördern, die auf den Schutz von Informationssystemen spezialisiert sind; fordert die Mitgliedstaaten auf, ihrer Verpflichtung zur Erhöhung der Verteidigungsausgaben im Bereich Forschung und Entwicklung auf mindestens 2 % unter besonderer Berücksichtigung der Cyber-Sicherheit und -Verteidigung nachzukommen;

32. fordert die Kommission und die Mitgliedstaaten auf, Programme vorzulegen, um Nutzer im privaten und im geschäftlichen Bereich für die umfassende sichere Nutzung des Internets, der Informationssysteme und der Informations- und Kommunikationstechnologien zu sensibilisieren bzw. diese Sensibilisierung zu fördern; regt an, dass die Kommission eine diesbezügliche EU-weite öffentliche Bildungsinitiative startet, und fordert die Mitgliedstaaten auf, die Bildung im Bereich der Cyber-Sicherheit vom frühestmöglichen Alter der Schüler an in die Lehrpläne der Schulen aufzunehmen;

Zusammenarbeit zwischen öffentlichen und privaten Stellen

33. betont die entscheidende Rolle einer sinnvollen Zusammenarbeit auf dem Gebiet der Internet-Sicherheit mit gegenseitiger Ergänzung zwischen Behörden und privaten Stellen auf EU-Ebene und auf nationaler Ebene zu dem Zweck, auf beiden Seiten Vertrauen zu schaffen; stellt fest, dass die weitere Verbesserung der Zuverlässigkeit und Effizienz der zuständigen Behörden zur Schaffung von Vertrauen und zur gemeinsamen Nutzung kritischer Informationen beitragen wird;

34. fordert die Partner im Privatsektor auf, bei der Gestaltung neuer Erzeugnisse, Geräte, Dienstleistungen und Anwendungen konzeptionsintegrierte Sicherheitslösungen in Erwägung zu ziehen und Anreize für diejenigen zu erwägen, die neue Erzeugnisse, Geräte, Dienstleistungen und Anwendungen gestalten, die wesentlich durch konzeptionsintegrierte Sicherheitslösungen gekennzeichnet sind; fordert, dass bei der Zusammenarbeit mit der Privatwirtschaft zur Verhinderung und zur Ahndung von Cyber-Angriffen Mindestnormen für Transparenz und Mechanismen für die Rechenschaftspflicht geschaffen werden;

35. hebt hervor, dass sich die EU-Strategie der inneren Sicherheit im Rahmen des Ziels eines besseren Schutzes der Bürger und Unternehmen im virtuellen Raum auch auf den Schutz kritischer Informationsinfrastrukturen erstreckt;

36. fordert, mit diesen Partnern einen ständigen Dialog über die optimale Nutzung und die Widerstandsfähigkeit von Informationssystemen sowie die gemeinsame Übernahme der Verantwortung für die zuverlässige und ordnungsgemäße Funktion dieser Systeme einzurichten;

37. vertritt die Auffassung, dass die Mitgliedstaaten, die EU-Organe und der private Sektor in Zusammenarbeit mit der ENISA Maßnahmen zur Verbesserung der Sicherheit und Integrität von Informationssystemen, zur Vorbeugung gegen Angriffe und zur Minimierung von deren Auswirkungen treffen sollten; unterstützt die Kommission bei ihren Bemühungen um die Konzipierung von Cyber-Mindestsicherheitsnormen und Zertifizierungssystemen für Unternehmen und bei der Schaffung der geeigneten Anreize für die Förderung von Bemühungen im Privatsektor, die auf die Verbesserung der Sicherheit abzielen;

38. fordert die Kommission und die Regierungen der Mitgliedstaaten auf, den Akteuren im Privatsektor und in der Zivilgesellschaft die Einbeziehung der Bewältigung von Cyber-Krisen in ihre Krisenbewältigungspläne und Risikoanalysen nahezulegen; fordert darüber hinaus die Einführung von Fortbildungen zur Sensibilisierung für elementare Cyber-Sicherheit und -Hygiene für sämtliche Mitarbeiter dieser Akteure;

39. fordert die Kommission auf, in Zusammenarbeit mit den Mitgliedstaaten und den zuständigen Einrichtungen und Gremien Rechtsrahmen und Instrumente für ein System des schnellen Informationsaustauschs zu schaffen, das für Anonymität bei der Meldung von Internet-Störfällen durch die Privatwirtschaft sorgt und den Akteuren des öffentlichen Sektors die Möglichkeit bietet, ständig aktuell unterrichtet zu sein und nötigenfalls Hilfe zu leisten;

40. betont, dass die EU die Entstehung eines wettbewerbsbestimmten und innovativen Markts für Cyber-Sicherheit in der EU begünstigen muss, damit KMU besser in der Lage sind, sich auf diesem Gebiet zu betätigen, was zur Ankurbelung des Wirtschaftswachstums und zur Schaffung neuer Arbeitsplätze beitragen wird;

Internationale Zusammenarbeit

41. fordert den EAD auf, in Eigeninitiative an das Thema Cyber-Sicherheit heranzugehen und den Aspekt der Cyber-Sicherheit in alle seine Maßnahmen, besonders die auf Drittstaaten bezogenen, zu integrieren; verlangt die Beschleunigung von Zusammenarbeit und Informationsaustausch bezüglich der Bewältigung von Internet-Sicherheitsproblemen in den Beziehungen mit Drittstaaten;

42. betont, dass die Ausarbeitung einer umfassenden EU-Strategie für Cyber-Sicherheit Voraussetzung für den Aufbau einer solchen effizienten internationalen Zusammenarbeit in Bezug auf die Cyber-Sicherheit ist, wie sie aufgrund des länderübergreifenden Charakters der Cyber-Bedrohungen gefordert ist;

43. fordert die Mitgliedstaaten, die das Übereinkommen des Europarats über Computer-Kriminalität (Budapester Übereinkommen) noch nicht unterzeichnet oder ratifiziert haben, auf, dies unverzüglich zu tun; unterstützt die Kommission und den EAD dabei, sich gegenüber Drittstaaten für das Übereinkommen und seine Werte einzusetzen;

44. ist sich der Notwendigkeit einer international vereinbarten, koordinierten Reaktion auf Cyber-Bedrohungen bewusst; fordert deshalb die Kommission, den EAD und die Mitgliedstaaten auf, bei den Bemühungen um eine umfassendere internationale Zusammenarbeit im Bereich der Cyber-Verhaltensnormen und um eine abschließende Übereinkunft zur Festlegung einer einheitlichen Auslegung dieser Normen in allen Foren und insbesondere bei den Vereinten Nationen eine Führungsrolle zu übernehmen und auch die Zusammenarbeit im Hinblick auf den Abschluss von Übereinkünften über die Kontrolle von Cyber-Waffen voranzutreiben;

45. fordert dazu auf, Wissenstransfers mit den BRICS-Staaten und mit anderen Schwellenländern im Bereich der Cyber-Sicherheit einzurichten, um auf ziviler und militärischer Ebene Möglichkeiten für gemeinsame Reaktionen auf zunehmende Cyber-Kriminalität, Cyber-Bedrohungen und Cyber-Angriffe zu sondieren;

46. fordert den EAD und die Kommission auf, sich in den einschlägigen internationalen Foren und Organisationen, insbesondere VN, OSZE, OECD und Weltbank, zukunftorientiert zu verhalten mit dem Ziel, das geltende internationale Recht zur Anwendung zu bringen und Konsens über Normen für ein verantwortungsvolles Verhalten von Staaten auf dem Gebiet der Internet-Sicherheit und der Internet-Verteidigung zu erreichen, und zwar indem sie die

Standpunkte der Mitgliedstaaten zur Förderung der elementaren Werte und Strategien der EU auf dem Gebiet Cyber-Sicherheit und -Verteidigung koordinieren;

47. fordert den Rat und die Kommission auf, im Rahmen ihrer Dialoge, Beziehungen und Kooperationsabkommen mit Drittstaaten, insbesondere solcher, die eine Zusammenarbeit oder einen Austausch im technologischen Bereich vorsehen, Mindestanforderungen für die Verhütung und Bekämpfung von Cyber-Kriminalität und Cyber-Angriffen sowie Mindestnormen für die Sicherheit von Informationssystemen zu verlangen;

48. fordert die Kommission auf, nötigenfalls Drittstaaten bei deren Bemühungen um den Aufbau von Fähigkeiten im Bereich der Cyber-Sicherheit und -Verteidigung Hilfe zu leisten;

Zusammenarbeit mit der NATO

49. weist erneut darauf hin, dass die EU und die NATO aufgrund ihrer gemeinsamen Werte und gemeinsamen strategischen Interessen besondere Verantwortung und besondere Fähigkeiten dafür haben, den wachsenden Herausforderungen an die Cyber-Sicherheit mit mehr Effizienz und in enger Zusammenarbeit zu begegnen, und zwar durch Ermittlung möglicher Komplementaritäten ohne Doppelarbeit und unter Achtung der Aufgaben der jeweils anderen Seite;

50. betont die Notwendigkeit, in Anbetracht der Komplementarität der Ansätze von EU und NATO zur Cyber-Sicherheit und -Verteidigung die Instrumente auf der konkreten Ebene zu bündeln und gemeinsam zu nutzen; hebt eine engere Zusammenarbeit als notwendig hervor, besonders in Bezug auf Planung, Technologie, Fortbildung und Ausstattung auf den Gebieten Cyber-Sicherheit und -Verteidigung;

51. fordert, ausgehend von den bisherigen sich ergänzenden Tätigkeiten beim Aufbau von Verteidigungsfähigkeiten, alle zuständigen Stellen in der EU, die mit Cyber-Sicherheit und -Verteidigung befasst sind, auf, ihre konkrete Zusammenarbeit mit der NATO zu vertiefen, um Erfahrungen auszutauschen und Kenntnisse über die Schaffung von Widerstandsfähigkeit bei den EU-Systemen zu erwerben;

Zusammenarbeit mit den Vereinigten Staaten

52. ist der Überzeugung, dass die EU und die USA ihre Zusammenarbeit bei der Bekämpfung von Cyber-Angriffen und Cyber-Kriminalität vertiefen sollten, weil dies im Anschluss an das Gipfeltreffen EU/USA in Lissabon von 2010 zu einer Priorität der transatlantischen Beziehungen erklärt wurde;

53. begrüßt, dass auf dem Gipfeltreffen EU/USA vom November 2010 die Arbeitsgruppe beider Seiten für Cyber-Sicherheit und Cyber-Kriminalität geschaffen wurde, und unterstützt deren Bemühungen um die Einbeziehung von Themen der Cyber-Sicherheit in den transatlantischen politischen Dialog;

54. begrüßt, dass die Kommission und die Regierung der USA unter dem Dach der Arbeitsgruppe EU/USA ein gemeinsames Programm und einen Fahrplan für eine gemeinsame bzw. synchronisierte transkontinentale Cyber-Übung 2012–2013

ausgearbeitet haben; verweist auf die erste transkontinentale Cyber-Übung im Jahre 2011;

55. hebt hervor, dass es sowohl für die Vereinigten Staaten als auch für die EU, die die größten Reservoirs in Bezug auf den virtuellen Raum und auf seine Nutzer darstellen, notwendig ist, zum Schutz der Rechte und Freiheiten ihrer Bürger bei der Nutzung dieses Raums zusammenzuarbeiten; betont, dass die nationale Sicherheit zwar ein überragendes Ziel verkörpert, jedoch auch der virtuelle Raum nicht nur gesichert, sondern auch geschützt werden sollte;

56. beauftragt seinen Präsidenten, diese Entschließung dem Rat und der Kommission, der Vizepräsidentin und Hohen Vertreterin, der EDA, der ENISA und der NATO zu übermitteln.

ERGEBNIS DER SCHLUSSABSTIMMUNG IM AUSSCHUSS

Datum der Annahme	10.10.2012
Ergebnis der Schlussabstimmung	+: 47 –: 3 0: 6
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	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
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter(innen)	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
Zum Zeitpunkt der Schlussabstimmung anwesende Stellv. (Art. 187 Abs. 2)	Joseph Cuschieri