RAT DER EUROPÄISCHEN UNION

Brüssel, den 22. Juli 2013 (OR. en)

12109/13

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

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Nr. Vordok.:	11357/13
Betr.:	Schlussfolgerungen des Rates zur gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum"

Die Delegationen erhalten anbei die Schlussfolgerungen des Rates zur gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum" in der Fassung, über die der Rat (Allgemeine Angelegenheiten) am 25. Juni 2013 Einigung erzielt hat.

ANLAGE

Schlussfolgerungen des Rates zur gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum"

DER RAT DER EUROPÄISCHEN UNION –

1. IN ANBETRACHT dessen, dass der Cyberraum, der schon an sich grenzüberschreitend angelegt ist, aus miteinander verknüpften Netzen und Informationsinfrastrukturen besteht und unter anderem das Internet und die Telekommunikationsnetze umfasst, derzeit und auch künftig eines der wichtigsten Mittel zur Erfüllung der Bedürfnisse und Wahrnehmung der Interessen und der Rechte der EU-Bürger und der Mitgliedstaaten darstellt und einen unabdingbaren Vorteil für das Wirtschaftswachstum in der EU bietet;

2. UNTER BETONUNG der Rolle und der Rechte der einzelnen Bürger, der Privatwirtschaft und der Zivilgesellschaft in Fragen des Cyberraums und der wichtigen Rolle der EU bei der Förderung und Erhaltung eines offenen, sicheren und widerstandsfähigen Cyberraums, der sich auf die zentralen Werte der EU wie Demokratie, Menschenrechte und Rechtsstaatlichkeit stützt, zum Wohle unserer Volkswirtschaften, Verwaltungen und unserer Gesellschaft sowie zugunsten des reibungslosen Funktionierens des Binnenmarkts;

3. IN ANERKENNUNG dessen, dass die Vertraulichkeit, die Verfügbarkeit und die Integrität der Netze und Infrastrukturen und der darin enthaltenen Informationen verbessert werden müssen;

4. IN ANERKENNUNG dessen, dass Sicherheitsfunktionen eingeführt und Maßnahmen getroffen werden müssen, um Gefahren, die mit den miteinander verknüpften Netzen und Informationsinfrastrukturen zusammenhängen oder ihnen Schaden zufügen könnten, abzuwehren und den Cyberraum sowohl im zivilen als auch im militärischen Bereich zu schützen

5. UNTER BESTÄTIGUNG des Standpunkts der EU, dass dieselben Normen, Grundsätze und Werte, zu denen die Union sich außerhalb des Netzes bekennt, insbesondere die EU-Grundrechtecharta, auch im Cyberraum gelten sollten;

6. IN ANBETRACHT dessen, dass das Völkerrecht einschließlich der internationalen Übereinkünfte wie das Übereinkommen des Europarates über Computerkriminalität (Übereinkommen von Budapest) und der einschlägigen Übereinkünfte über das internationale humanitäre Völkerrecht und die Menschenrechte, des Internationalen Pakts über bürgerliche und politische Rechte und des Internationalen Pakts über wirtschaftliche, soziale und kulturelle Rechte einen für den Cyberraum geltenden Rechtsrahmen bereitstellt, weshalb darauf hingearbeitet werden sollte, diesen Instrumenten im Cyberraum Geltung zu verschaffen, und die EU keine neuen internationalen Rechtsinstrumente für Cyberangelegenheiten fordert;

7. UNTER ERNEUTEM HINWEIS darauf, dass die Cybersicherheit eines integrierten, bereichsübergreifenden und horizontalen Ansatzes bedarf und die Maßnahmen ein vielschichtiges Spektrum an den Cyberraum betreffenden Themen abdecken sollten;

8. UNTER HINWEIS auf die zahlreichen Initiativen der EU und internationalen Initiativen im Bereich der Cybersicherheit, einschließlich der in der Anlage genannten Initiativen;

9. UNTER HINWEIS auf Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union und unter Berücksichtigung der derzeitigen Beratungen über dessen Umsetzung;

10. IN DEM BEWUSSTSEIN, dass sowohl die Bemühungen um eine Erhöhung der Cybersicherheit als auch die Bekämpfung der Cyberkriminalität nicht nur in der Europäischen Union, sondern auch in Drittländern – auch in denjenigen, von den aus die Organisationen der Cyberkriminalität operieren – unternommen werden müssen –

11. BEGRÜSST die gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union über eine Cybersicherheitsstrategie der Europäischen Union;

12. ERACHTET es als wesentlich und dringlich, ein umfassendes Konzept für eine Cyberraumstrategie der EU weiterzuentwickeln und umzusetzen, das

- die Ausübung der Menschenrechte schützt und fördert und sich auf die von der EU vertretenen Grundwerte Demokratie, Menschenrechte und Rechtsstaatlichkeit stützt;

- den Wohlstand in Europa und den sozialen und wirtschaftlichen Nutzen des Cyberraums einschließlich des Internets erhöht;

- eine echte und höhere Cybersicherheit in der gesamten EU und über ihre Grenzen hinaus fördert;

- die Bemühungen zur Überbrückung der weltweiten digitalen Kluft vorantreibt und die internationale Zusammenarbeit bei der Cybersicherheit fördert;

- der Rolle und die Rechte der einzelnen Bürger, der Privatwirtschaft und der Zivilgesellschaft in Cyberfragen widerspiegelt, einschließlich einer Intensivierung der Zusammenarbeit und des Informationsaustauschs zwischen dem öffentlichen und dem privaten Sektor;

UND

13. ERSUCHT die Mitgliedstaaten, die Kommission und die Hohe Vertreterin, unter Wahrung der jeweiligen Zuständigkeitsbereiche und des Subsidiaritätsprinzips entsprechend den in diesen Schlussfolgerungen niedergelegten strategischen Zielen zusammenzuarbeiten;

Werte

14. HEBT HERVOR, dass die Menschenrechte des Einzelnen einschließlich der Meinungsfreiheit und der Schutz der Privatsphäre bei der Konzipierung von Maßnahmen und Vorgehensweisen betreffend Cyberfragen stets gewahrt werden müssen, und nimmt Kenntnis von den derzeitigen Verhandlungen über einen Rechtsrahmen der EU zum Schutz personenbezogener Daten, der im Cyberraum effektiv funktionieren kann;

15. ERKENNT AN, dass die in der Union geförderten und geschützten Werte und Interessen auch bei ihren außenpolitischen Maßnahmen in Bezug auf Cyberangelegenheiten gefördert werden sollten;

16. RUFT die EU und ihre Mitgliedstaaten auf,

- ihre einheitliche und feste Haltung zur universellen Geltung der Menschenrechte und Grundfreiheiten einschließlich der Meinungsfreiheit, der freien Meinungsäußerung sowie der Informations-, Versammlungs- und Vereinigungsfreiheit zu verteidigen;

- festzulegen, wie die bestehenden Verpflichtungen im Cyberraum durchgesetzt werden können;

17. ERSUCHT die EU und ihre Mitgliedstaaten, die digitale Kompetenz zu fördern und die Nutzer stärker für ihre individuelle Verantwortung bei der Einstellung personenbezogener Daten ins Internet zu sensibilisieren;

18. BETONT die wichtige Rolle der EU bei der Erhaltung des auf einer Vielzahl von Akteuren beruhenden Modells für die Verwaltung des Internets;

19. ERSUCHT die Mitgliedstaaten, alle sinnvollen Maßnahmen zu treffen, damit sichergestellt ist, dass alle EU-Bürger Zugang zum Internet und zu den mit ihm verbundenen Vorteilen haben;

Wohlstand

20. ERSUCHT die Kommission, sich speziell um die Förderung des digitalen Binnenmarkts zu bemühen und diesbezügliche Fragen in der Union und internationalen Gremien (z.B. der Welthandelsorganisation (WTO) und bei den Verhandlungen über das Übereinkommen über Informationstechnologie (ITA)) voranzubringen und bei der Aushandlung von Freihandelsabkommen mit Drittländern den Marktzugang in diesen Bereichen sicherzustellen;

21. BETONT, wie wichtig es ist, dass die Rechtsvorschriften für diesen Sektor technologieneutral sind und die Netzneutralität so weit wie möglich fördern, damit der Wettbewerb nicht durch die Diskriminierung des grenzüberschreitenden Online-Handels und neuer Geschäftsmodelle behindert wird;

22. BEGRÜSST, dass Investitionen in Forschung und Entwicklung im Cyberbereich als einem wichtigen Bereich, der für hochwertige Arbeitsplätze und Wirtschaftswachstum sorgen könnte, als notwendig anerkannt werden;

23. UNTERSTREICHT,

- welch kritische Bedeutung einem dynamischen Sektor der Informations- und Kommunikationstechnologie (IKT) und IKT-Sicherheitssektor in der EU im Hinblick auf die Erhöhung der Cybersicherheit zukommt, und FORDERT die Mitgliedstaaten und die Kommission AUF, zu sondieren, welche Schritte zur Förderung dieser Entwicklung unternommen werden könnten, und darüber Bericht zu erstatten;

- dass die Gesetzgebung zur Förderung der Cybersicherheit Innovation und Wachstum begünstigen und den Schutz der Infrastruktur und der vitalen Funktionen, die die Mitgliedstaaten als kritisch erachten, in den Mittelpunkt stellen sollte;

- dass die digitale Wirtschaft eine wichtige Triebkraft für Wachstum, Innovation und Beschäftigung darstellt und die Cybersicherheit für den Schutz der digitalen Wirtschaft von entscheidender Bedeutung ist;

- welche Bedeutung der Schutz kritischer Informationsinfrastrukturen auf nationaler Ebene hat;

Widerstandsfähigkeit gegenüber Cyberangriffen

24. BEGRÜSST die Ziele des Kommissionsvorschlags für eine Richtlinie mit Maßnahmen zur Verbesserung der

    - Netz- und Informationssicherheit in der gesamten EU,

    - Abwehrbereitschaft in Bezug auf Cybersicherheit und der diesbezüglichen Fähigkeiten auf nationaler Ebene,

    - Zusammenarbeit zwischen den Mitgliedstaaten und in der gesamten EU und zur Förderung einer Kultur des Risikomanagements im öffentlichen und privaten Sektor;

25. RUFT alle Organe, Stellen sowie Ämter und Agenturen der EU auf, in Zusammenarbeit mit den Mitgliedstaaten die erforderlichen Maßnahmen zu treffen, um durch die Verstärkung ihrer Sicherheit nach angemessenen Sicherheitsstandards – in Zusammenarbeit mit der ENISA im Hinblick auf die Etablierung bewährter Verfahren gemäß der Verordnung (EU) Nr. 526/2013[1] – ihre eigene Cybersicherheit zu gewährleisten;

26. WEIST darauf HIN, dass – im Anschluss an eine einjährige Pilotphase und die erfolgreiche Evaluierung von Funktion und Effektivität – ein CERT (Computer Emergency Response Team) für die Organe und Stellen sowie Ämter und Agenturen der EU geschaffen wurde;

27. BETONT die außerordentliche Bedeutung der ENISA bei der Unterstützung der Bemühungen der Mitgliedstaaten und der Union um ein hohes Maß an Netz- und Informationssicherheit, insbesondere durch die Unterstützung des Kapazitätsaufbaus in den Mitgliedstaaten, bei der Unterstützung der Entwicklung starker nationaler Fähigkeiten für die Widerstandsfähigkeit gegen Cyberangriffe, bei der Unterstützung europäischer Cyberübungen sowie bei der Unterstützung der Bemühungen der Union in den Bereichen Forschung und Entwicklung und Normung und ERSUCHT die ENISA, im Einklang mit der Verordnung (EU) Nr. 526/2013 mit anderen Organen und Stellen sowie Ämtern und Agenturen der EU in Netz- und Informationssicherheitsangelegenheiten (NIS) zusammenzuarbeiten;

---

[1] ABl. L 165 vom 18.6.2013.

28. BETONT, dass die Widerstandsfähigkeit kritischer Infrastrukturen unionsweit erhöht und die enge Zusammenarbeit und Koordinierung zwischen den einschlägigen Akteuren – auch zwischen zivilen und militärischen Akteuren der EU, einschließlich zwischen dem öffentlichen und dem privaten Sektor – bei der Reaktion auf Sicherheitszwischenfälle und -probleme im Cyberraum durch Initiativen wie Entwicklung gemeinsamer Normen, Sensibilisierung, Schulung und Ausbildung und laufende Überprüfungen und Tests (oder Entwicklung) von Frühwarn- und Reaktionsmechanismen verstärkt werden müssen. Für ein wirksames Vorgehen bei Cyberangriffen, einschließlich der Bewältigung von Zwischenfällen, müssen ferner die enge Zusammenarbeit und Koordinierung bei der Reaktion auf Cyberzwischenfälle durch die Akteure der Verteidigung, die Strafverfolgungsbehörden, den Privatsektor und die für die Cybersicherheit zuständigen Behörden noch verstärkt werden;

29. FORDERT die Mitgliedstaaten AUF,

- durch entsprechende Maßnahmen zu gewährleisten, dass sie ein effizientes nationales Cybersicherheitsniveau erreichen, indem die geeigneten Strategien, organisatorischen und operativen Fähigkeiten entwickelt und umgesetzt werden, um die Informationssysteme im Cyberraum – insbesondere die als kritisch geltenden – zu schützen;

- sich mit der Industrie und den Hochschulen ins Benehmen zu setzen, um das Vertrauen als Kernbestandteil der nationalen Cybersicherheit, beispielsweise durch die Verwirklichung öffentlich-privater Partnerschaften, zu fördern;

- die Sensibilisierung für die Art der Bedrohung und die Grundlagen bewährter digitaler Vorgehensweisen auf allen Ebenen zu unterstützen;

- die Eigentümer und Anbieter von IKT-Systemen beim Schutz ihrer eigenen Systeme und der vitalen Dienstleistungen, die sie erbringen, zu unterstützen;

- die gesamteuropäische Zusammenarbeit bei der Cybersicherheit insbesondere durch die Intensivierung von gesamteuropäischen Cybersicherheitsübungen zu fördern;

- eine effektive Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten auf EU-Ebene im Hinblick auf eine gemeinsame Analyse der Bedrohungslage zu gewährleisten;

- ausgehend von den bestehenden Strukturen die Zusammenarbeit zwischen den Nutzern in den Mitgliedstaaten und der EU zu intensivieren und auszuweiten;

- Fragen der Cybersicherheit im Lichte der laufenden Beratungen über die Solidaritätsklausel Rechnung zu tragen;

Cyberkriminalität

30. WÜRDIGT die vom JI-Rat am 6./7. Juni 2013 angenommenen Schlussfolgerungen des Rates über die Festlegung der EU-Prioritäten für die Bekämpfung der schweren und organisierten Kriminalität in den Jahren 2014-2017, in denen die Bekämpfung der Cyberkriminalität zur Priorität erhoben wurde;

31. BETONT, dass die Cyberkriminalität in der von Europol für 2013 vorgelegten Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA) als Kriminalitätsbereich betrachtet wird, der in Form von Datenschutzverletzungen in großem Maßstab, Online-Betrug und sexueller Ausbeutung von Kindern eine immer stärkere Bedrohung für die EU darstellt, während die profitorientierte Cyberkriminalität zusehends zum Wegbereiter für andere kriminelle Aktivitäten wird;

32. EMPFIEHLT die Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3) bei Europol und ERSUCHT die Mitgliedstaaten, dieses EC3 im Rahmen seines Aufgabenbereichs zur Intensivierung der Zusammenarbeit zwischen den nationalen Stellen zu nutzen;

33. FORDERT Europol und Eurojust AUF, ihre Zusammenarbeit mit allen einschlägigen Akteuren, einschließlich der EU-Agenturen, Interpols, der CERT-Gemeinschaft und des Privatsektors, bei der Bekämpfung der Cyberkriminalität auszubauen, indem unter anderem der Schwerpunkt auf Synergien und Komplementarität im Einklang mit den jeweiligen Aufgaben und Zuständigkeiten gelegt wird;

34. RECHNET DAMIT, dass alle Mitgliedstaaten das Übereinkommen von Budapest über Computerkriminalität in Kürze ratifizieren;

35. FORDERT die Kommission, Europol, CEPOL und die ENISA AUF, die Schulung und Weiterbildung in den Mitgliedstaaten zu unterstützen, deren Regierungen und Strafverfolgungsbehörden digitale Fähigkeiten zur Bekämpfung der Cyberkriminalität aufbauen müssen;

36. ERSUCHT die Kommission,

- die Mitgliedstaaten auf deren Ersuchen hin bei der Ermittlung von Lücken und bei der Stärkung ihrer Fähigkeit zu Ermittlungen bei Cyberstraftaten und zur Bekämpfung dieser Straftaten zu unterstützen;

- den Fonds für die innere Sicherheit im Rahmen seiner Haushaltsmittel (unter Berücksichtigung seiner übrigen Prioritäten) zur Unterstützung der einschlägigen Behörden heranzuziehen, die gegen die Cyberkriminalität vorgehen;

- das Stabilitätsinstrument zu nutzen, um die Bekämpfung der Cyberkriminalität sowie die Initiativen zum Kapazitätsaufbau einschließlich der polizeilichen und justiziellen Zusammenarbeit in Drittländern, aus denen die Organisationen der Cyberkriminalität operieren, voranzutreiben;

- die Koordinierung der Programme für den Kapazitätsaufbau zu erleichtern, um Doppelarbeit zu vermeiden und Synergien zu bewirken;

- Informationen über die Fortschritte beim Globalen Bündnis gegen sexuellen Missbrauch von Kindern im Internet vorzulegen;

- die Beobachtung des politischen Umfelds in der EU in Bezug auf die Bekämpfung der Cyberkriminalität weiterhin zu erleichtern, insbesondere unter Berücksichtigung der von Europol (EC3) bereitgestellten Ergebnisse und strategischen Informationen;

- die gemeinschaftsübergreifende Zusammenarbeit insbesondere durch die Unterstützung von Europol (EC3) weiterhin zu erleichtern;

Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP)

37. BETONT im Rahmen der GSVP

- die dringende Notwendigkeit, die die Cyberabwehr betreffenden und mit der GSVP zusammenhängenden Aspekte der Strategie umzusetzen und voranzubringen, um gegebenenfalls einen Rahmen für die Cyberabwehr zu entwickeln, und auch im Hinblick auf die für Dezember 2013 geplante Aussprache des Europäischen Rates über Sicherheit und Verteidigung konkrete diesbezügliche Schritte festzulegen. Zur Steuerung dieser Bemühungen sollte im EAD eine einzige Anlaufstelle benannt werden;

- die Notwendigkeit, die Cyberabwehrfähigkeiten der Mitgliedstaaten auch durch die Entwicklung gemeinsamer Normen und die Sensibilisierung durch Schulung und Ausbildung in Cybersicherheit zu erhöhen, wozu das Europäische Sicherheits- und Verteidigungskolleg und weitere Möglichkeiten zur Optimierung von Schulung und Übung für die Mitgliedstaaten nutzbar zu machen sind;

- den Rückgriff auf die bestehenden Mechanismen für Bündelung und gemeinsame Nutzung sowie die Nutzung von Synergien mit umfassenderen politischen Maßnahmen der EU, um die erforderlichen Cyberabwehrfähigkeiten in den Mitgliedstaaten auf möglichst effiziente Weise aufzubauen;

- die Notwendigkeit von Forschung und Entwicklung. In erster Linie müssen die Mitgliedstaaten dazu angehalten werden, unter enger Einbindung der Privatwirtschaft und der Hochschulen sichere und widerstandsfähige Technologien für die Cyberabwehr zu entwickeln und auf der Grundlage eines auf Kooperation beruhenden Konzepts und als Vorbild für eine Fähigkeit mit doppeltem Verwendungszweck, die zwischen der EDA und der Kommission im Rahmen der Europäischen Rahmenvereinbarung zu koordinieren ist, den Aspekten der Cybersicherheit in den Forschungsprojekten der EDA mehr Gewicht zu verleihen;

- dass die Frühwarn- und Reaktionsmechanismen in Anbetracht neuer Cyberbedrohungen mittels eines Dialogs zwischen dem EAD, der ENISA, EC3, der EDA, der Kommission und den Mitgliedstaaten im Hinblick auf Synergien und Verbindungen mit der Verteidigungsgemeinschaft überprüft und getestet werden müssen;

- die Notwendigkeit, die Zusammenarbeit zwischen der EU und der NATO bei der Cyberabwehr fortzusetzen und zu intensivieren, wobei Prioritäten für eine weitere Zusammenarbeit zwischen der EU und der NATO bei der Cyberabwehr innerhalb des bestehenden Rahmens einschließlich beiderseitiger Teilnahme an Cyberverteidigungsübungen und -schulungen bestimmt werden müssen;

- die Einbettung der Cyberabwehraspekte in die umfassende Cyberraum-Politik;

Industrie/Technologie

38. BEGRÜSST – IN ANERKENNUNG dessen, dass Europa seine industriellen und technologischen Ressourcen weiterentwickeln muss, um in seinen Netzen und IKT-Systemen ein angemessenes Maß an Vielfalt und Vertrauen zu erreichen – entschieden den Aufruf in der Cybersicherheitsstrategie für Europa, eine überzeugende Industriepolitik zu betreiben, um die Vertrauenswürdigkeit der europäischen IKT- und Cyberabwehrbranche zu stärken und den Binnenmarkt durch Impulse für Forschung und Entwicklung zu fördern;

39. ERSUCHT die Mitgliedstaaten, die Kommission und die ENISA, die Bemühungen um Forschung und Entwicklung in den Bereichen IKT und Cybersicherheit sowie die Verfügbarkeit gut vorbereiteter Fachleute für Cybersicherheit zu verstärken, die wesentlich ist für die Förderung der Wettbewerbsfähigkeit der europäischen Informations- und Kommunikationstechnologie (IKT), der Dienstleistungs- und Sicherheitsindustrien und ihrer Fähigkeit, vertrauenswürdige und sichere Lösungen zu entwickeln, und FORDERT daher die Kommission AUF, das Rahmenprogramm für Forschung und Innovation "Horizont 2020" wirksam einzusetzen;

40. BETONT, dass die Entwicklung öffentlich-privater Partnerschaften ein wichtiges Instrument zum Ausbau der Cybersicherheitsfähigkeiten darstellen wird, und RUFT daher die Kommission AUF, innerhalb von Horizont 2020 Synergien zwischen den Betreibern kritischer Infrastrukturen, IKT- und Sicherheitsforschung für Cybersicherheit und Fragen im Zusammenhang mit Cyberkriminalität sowie mit den politischen Maßnahmen der Union für die innere und äußere Sicherheit zu fördern;

41. FORDERT die Mitgliedstaaten und die Kommission AUF, spezielle Maßnahmen zur Förderung der Cybersicherheit in kleinen und mittleren Unternehmen zu treffen, die für Cyberangriffe besonders anfällig sind, und HÄLT die Mitgliedstaaten dazu AN, unter Beteiligung und Mitarbeit der Privatwirtschaft und der Hochschulen sichere und widerstandsfähige Technologien für Cybersicherheit zu entwickeln;

42. ERSUCHT die Kommission, die im Bereich der Cybersicherheit vorhandenen Normen zu berücksichtigen, und BETONT, dass die Zusammenarbeit und der Informationsaustausch über Normen – z.B. über Risikomanagement – in Zusammenarbeit mit den Mitgliedstaaten, der Industrie und anderen einschlägigen Akteuren weiter ausgebaut werden sollte;

Internationale Zusammenarbeit in Bezug auf den Cyberraum

43. BEKRÄFTIGT die Zusage der EU, die Entwicklung von vertrauensbildenden Maßnahmen im Bereich der Cybersicherheit zu unterstützen, um die Transparenz zu erhöhen und das Risiko einer falschen Einschätzung des staatlichen Vorgehens durch die Förderung der Schaffung internationaler Normen in diesem Bereich zu verringern;

44. FORDERT die Kommission und die Hohe Vertreterin AUF, gemäß den in den Verträgen niedergelegten einschlägigen Verfahren

- a) das Übereinkommen von Budapest als Vorbild für die Abfassung nationaler Rechtsvorschriften über Cyberkriminalität und als Grundlage für die internationale Zusammenarbeit in diesem Bereich zu fördern, b) die Wahrung der Grundrechte im Cyberraum voranzubringen und c) alle vorhandenen Mittel der internationalen Zusammenarbeit voll zu nutzen, um die Bekämpfung der Cyberkriminalität sowie die diesbezügliche polizeiliche und justizielle Zusammenarbeit in Drittländern, aus denen cyberkriminelle Organisationen operieren, voranzubringen;

- auf die Fachkenntnisse der Mitgliedstaaten im Bereich der Cyberpolitik und ihre Erfahrungen mit bilateralen Verpflichtungen und bilateraler Zusammenarbeit zurückzugreifen, um gemeinsame Botschaften der EU zu Fragen des Cyberraums auszuarbeiten und bei den operativen Aspekten eng mit den Mitgliedstaaten zusammenzuarbeiten;

- in Zusammenarbeit mit den Mitgliedstaaten und einschlägigen privaten Organisationen und der Zivilgesellschaft die relevanten Hilfsinstrumente der EU für den Kapazitätsaufbau im IKT-Bereich, einschließlich der Cybersicherheit, uneingeschränkt zu nutzen;

45. RUFT die Mitgliedstaaten, die Kommission und die Hohe Vertreterin auf, auf eine kohärente internationale Cyberraumpolitik der EU im Einklang mit den in den Verträgen niedergelegten einschlägigen Verfahren hinzuarbeiten, und zwar durch

- die Intensivierung des Dialogs mit den wichtigsten internationalen Partnern und Organisationen, so dass sichergestellt ist, dass diese Zusammenarbeit allen Mitgliedstaaten zugute kommen kann;

- die Einbeziehung von Cyberfragen in die GASP;

- die verbesserte Koordinierung globaler Cyberfragen und die durchgängige Berücksichtigung der Cybersicherheit, einschließlich vertrauensbildender und transparenzfördernder Maßnahmen, im Gesamtrahmen für die Beziehungen zu Drittländern und internationalen Organisationen, auch durch verbesserte Koordinierung zwischen den Mitgliedstaaten, der Kommission und dem EAD in Bezug auf die Führung von Dialogen und andere Tätigkeiten in Bezug auf Cybersicherheit,

- die Verbesserung der Koordinierung durch die einschlägigen Vorbereitungsgremien des Rates (einschließlich der Gruppe der Freunde des Vorsitzes für Fragen des Cyberraums),

- die Unterstützung des Kapazitätsaufbaus in Drittländern, Schulung und Unterstützung der Schaffung einschlägiger nationaler politischer Maßnahmen, Strategien und Institutionen, um das gesamte wirtschaftliche und soziale Potenzial der IKT zu mobilisieren, die Entwicklung widerstandsfähiger Systeme in diesen Ländern zu unterstützen und Cybergefahren für die EU-Organe und die Mitgliedstaaten zu verringern und zugleich die bestehenden Netze und Gremien für die Koordinierung der politischen Maßnahmen und den Informationsaustausch zu nutzen;

Jeweilige Aufgaben und Verantwortlichkeiten

46. FORDERT die übrigen Akteure – die Privatwirtschaft, Techniker und Hochschulen, die Zivilgesellschaft – und die Bürger auf, ihre jeweiligen Aufgaben und Verantwortlichkeiten im Hinblick auf einen offenen, sicheren und geschützten Cyberraum wahrzunehmen;

47. APPELLIERT an die Kommission und die Hohe Vertreterin, dass die Tätigkeiten der EU so konzipiert werden sollten, dass sie mit den nationalen Strukturen, den Verfassungsbestimmungen und den Initiativen betreffend Cybersicherheit vereinbar sind, damit ein integrierter Ansatz sichergestellt wird und Überschneidungen vermieden werden,

UND

48. FORDERT die Kommission und die Hohe Vertreterin AUF, einen Sachstandsbericht über die Cybersicherheitsstrategie zu erstellen, der auf der für Februar 2014 geplanten hochrangigen Konferenz vorgelegt werden soll, und SCHLÄGT VOR, dass die zuständigen Vorbereitungsgremien des Rates (insbesondere die Gruppe der Freunde des Vorsitzes für Fragen des Cyberraums) regelmäßige Sitzungen abhalten, um die Festlegung der Prioritäten und strategischen Ziele der EU für den Cyberraum als Teil eines umfassenden politischen Rahmens zu unterstützen und die laufende Umsetzung der Strategie zu überprüfen und zu fördern.

49. Unbeschadet der Verhandlungen über den künftigen Finanzrahmen werden bei der Umsetzung dieser Schlussfolgerungen des Rates nur die bestehenden Finanzmittel und Finanzierungsprogramme genutzt, und daher ERSUCHT der Rat die Kommission, unter Berücksichtigung der bevorstehenden Verhandlungen mit dem Europäischen Parlament die Finanzierung der Strategie zu erläutern.

ANHANG ZUR ANLAGE

Bezugsdokumente

1. Europäisches Parlament, Rat und Kommission

   – Charta der Grundrechte der Europäischen Union[2]

2. Europäisches Parlament und Rat

   – Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit[3]

   – Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), geändert durch die Richtlinie 2009/140/EG[4]

3. Europäisches Parlament

   – Entschließung des Europäischen Parlaments vom 11. Dezember 2012 zu einer digitalen Freiheitsstrategie in der Außenpolitik der EU

   – Bericht des Europäischen Parlaments von 2012 über Cybersicherheit und -verteidigung

4. Rat

   – Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger[5]

   – Ein sicheres Europa in einer besseren Welt – Europäische Sicherheitsstrategie, 12. Dezember 2003[6]

---

2 ABl. C 364 vom 18.12.2010, S. 1.
3 ABl. L 077 vom 13.3.2004.
4 ABl. L 108 vom 24.4.2002 und ABl. L 337 vom 18.12.2009, S. 37.
5 Dok. 17024/09 CO EUR-PREP 3 JAI 896 POLGEN 229.
6 Dok. 15849/03 PESC 783.

– Strategie der inneren Sicherheit der Europäischen Union: "Hin zu einem europäischen Sicherheitsmodell"[7]

– 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[8]

– Schlussfolgerungen des Rates zu der Mitteilung der Kommission zur EU-Strategie der inneren Sicherheit[9]

– Schlussfolgerungen des Rates zur Mitteilung der Kommission über den Schutz kritischer Informationsinfrastrukturen – "Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit"[10]

– Schlussfolgerungen des Rates über die Festlegung der EU-Prioritäten für die Bekämpfung der schweren und organisierten Kriminalität in den Jahren 2014-2017[11]

– Schlussfolgerungen des Rates zur Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität[12]

---

7 Dok. 5842/2/10 JAI 90.

8 ABl. L 345 vom 23.12.2008.

9 Dok. 6699/11 JAI 124.

10 Dok. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66. Diese Mitteilung schließt an an die Mitteilung der Kommission über den Schutz kritischer Informationsinfrastrukturen mit dem Titel "Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität" (Dok. 8375/09).

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

12 Dok. 10603/12 ENFOPOL 154 TELECOM 116.

– Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates. Billigung des endgültigen Kompromisstextes im Hinblick auf eine Einigung mit dem Europäischen Parlament in erster Lesung[13]

– Schlussfolgerungen des Rates zur Europäischen Strategie für ein besseres Internet für Kinder[14]

– Schlussfolgerungen des Rates zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie im Internet – Die Wirksamkeit der Polizeiarbeit in den Mitgliedstaaten und in Drittländern steigern[15]

– Schlussfolgerungen des Rates zu einem Globalen Bündnis gegen sexuellen Missbrauch von Kindern im Internet[16]

– Schlussfolgerungen des Rates über eine konzertierte Arbeitsstrategie und konkrete Maßnahmen zur Bekämpfung der Cyberkriminalität[17] und Schlussfolgerungen des Rates zu einem Aktionsplan für die Umsetzung der konzertierten Strategie zur Bekämpfung der Cyberkriminalität[18]

– Partielle allgemeine Ausrichtung des Rates zu dem Vorschlag der Kommission für eine Verordnung über das Rahmenprogramm für Forschung und Innovation "Horizont 2020" (2014-2020)[19]

– Gemeinsame Aktion des Rates über die Einrichtung der Europäischen Verteidigungsagentur[20]

---

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

– Gemeinsamer Vorschlag für einen Beschluss des Rates über die Vorkehrungen für die Anwendung der Solidaritätsklausel durch die Union[21]

– Schlussfolgerungen des Rates über die Medienkompetenz im digitalen Umfeld[22]

– Menschenrechte und Demokratie: Strategischer Rahmen und Aktionsplan der EU[23]

– Bericht über die Umsetzung der Europäischen Sicherheitsstrategie[24]

5. Kommission

– Die Digitale Agenda für Europa[25], eine der sieben Leitinitiativen der Strategie Europa 2020 für intelligentes, nachhaltiges und integratives Wachstum[26], und die Digitale Agenda für Europa – digitale Impulse für das Wachstum in Europa[27], mit der die Digitale Agenda neu ausgerichtet wird

– Mitteilung über den Schutz der Privatsphäre in einer vernetzten Welt: Ein europäischer Datenschutzrahmen für das 21. Jahrhundert[28]

– Mitteilung "Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität[29]

---

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

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

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

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

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

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

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

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

29 Dok. 8543/12 ENFOPOL 94 TELECOM 72.

– Mitteilung "Freisetzung des Cloud-Computing-Potenzials in Europa"[30]

– Mitteilung über den Schutz kritischer Informationsinfrastrukturen – "Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit"[31]

– Mitteilung über den "Schutz kritischer Informationsinfrastrukturen – Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität"[32]

6. VN

– Resolution der VN-Generalversammlung A/RES 57/239 "Schaffung einer globalen Kultur der Cyber-Sicherheit"

– Resolution des VN-Menschenrechtsrates A/HRC/20L.13 vom 29. Juni 2012 "Förderung, Schutz und Genuss der Menschenrechte im Internet"

– Resolution der VN-Generalversammlung A/RES 67/27 "Entwicklungen im Bereich Information und Telekommunikation im Kontext der internationalen Sicherheit"

– Einsetzung einer offenen zwischenstaatlichen Sachverständigengruppe für Computerkriminalität mit dem UNODC gemäß der Resolution 65/230 der VN-Generalversammlung

7. Europarat

– Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

– Übereinkommen des Europarates vom 23. November 2001 über Computerkriminalität

---

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

8. Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

   – Beschluss Nr. 1039 des Ständigen Rates vom 26. April 2012: Entwicklung vertrauensbildender Maßnahmen zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben

   – Ministerbeschluss Nr. 4/12 vom 7. Dezember 2012: Die Bemühungen der OSZE zur Bekämpfung transnationaler Bedrohungen

   – Offene informelle OSZE-Arbeitsgruppe zur Ausarbeitung eines Satzes von Entwürfen für vertrauensbildende Maßnahmen (VBM), die die zwischenstaatliche Zusammenarbeit, Transparenz, Berechenbarkeit und Stabilität stärken und das gegebenenfalls durch den ICT-Einsatz verursachte Risiko einer Fehleinschätzung, Eskalation oder eines Konflikts vermindern sollen (Beschluss Nr. 1039 des Ständigen Rates vom 26. April 2012)

9. Konferenzen, Initiativen und Veranstaltungen

   – Internationale Konferenz über den Cyberraum vom 1./2. November 2011 in London, gefolgt von der Internationalen Konferenz über den Cyberraum vom 4./5. Oktober 2012 in Budapest

   – Gemeinsame Planübung EU/USA zu Cybervorfällen "Cyber Atlantic 2011" und paneuropäische Übungen zu Cybervorfällen mit Beteiligung sämtlicher Mitgliedstaaten (Cyber Europe 2010 und Cyber Europe 2012)

   – Ad-hoc-Gruppe "Nukleare Sicherung", die die Frage der Computersicherheit/Cybersicherheit in ihrem Abschlussbericht erörtert und dargelegt hat[33]

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

10. Sonstige

– Europol: Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität 2013 (SOCTA)[34]

– Sicherheitskonzept[35] und Leitlinien[36] für die Netzwerkverteidigung im Rahmen der Informationssicherung.

_____

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

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

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