P7_TA(2012)0457

Cyberbezpieczeństwo i obrona

Rezolucja Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony (2012/2096(INI))

Parlament Europejski,

– uwzględniając sprawozdanie na temat wdrożenia europejskiej strategii bezpieczeństwa zatwierdzone przez Radę Europejską w dniach 11 i 12 grudnia 2008 r.,

– uwzględniając Konwencję Rady Europy o cyberprzestępczości przyjętą w Budapeszcie dnia 23 listopada 2001 r.,

– uwzględniając konkluzje Rady w sprawie ochrony krytycznej infrastruktury teleinformatycznej z dnia 27 maja 2011 r. oraz wcześniejsze konkluzje Rady dotyczące bezpieczeństwa cybernetycznego,

– uwzględniając komunikat Komisji z dnia 19 maja 2010 r. zatytułowany „Europejska agenda cyfrowa” (COM(2010)0245),

– uwzględniając dyrektywę Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[1],

– uwzględniając niedawny komunikat Komisji w sprawie ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością jako priorytetu strategii bezpieczeństwa wewnętrznego (COM(2012)0140),

– uwzględniając swoją rezolucję z dnia 10 marca 2010 r. w sprawie wdrażania europejskiej strategii bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony[2],

– uwzględniając swoją rezolucję z dnia 11 maja 2011 r. w sprawie rozwoju wspólnej polityki bezpieczeństwa i obrony po wejściu w życie Traktatu z Lizbony[3],

– uwzględniając swoją rezolucję z dnia 22 maja 2012 r. w sprawie strategii bezpieczeństwa wewnętrznego Unii Europejskiej[4],

– uwzględniając swoją rezolucję z dnia 27 września 2011 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1334/2000 ustanawiającego wspólnotowy system kontroli eksportu produktów i technologii podwójnego zastosowania[5],

– uwzględniając swoją rezolucję z dnia 12 czerwca 2012 r. w sprawie ochrony krytycznej

[1] Dz.U. L 345 z 23.12.2008, s. 75.
[2] Dz.U. C 349 E z 22.12.2010, s. 63.
[3] Teksty przyjęte, P7_TA(2011)0228.
[4] Teksty przyjęte, P7_TA(2012)0207.
[5] Teksty przyjęte, P7_TA(2011)0406.

infrastruktury teleinformatycznej „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni”[1],

– uwzględniając rezolucję Rady Praw Człowieka ONZ z dnia 5 lipca 2012 r. pt. „Promowanie, ochrona i korzystanie z praw człowieka w internecie”[2], w której podkreślono znaczenie ochrony praw człowieka i swobodny przepływ informacji w internecie,

– uwzględniając konkluzje przyjęte na szczycie w Chicago w dniu 20 maja 2012 r.,

– uwzględniając Tytuł V Traktatu UE,

– uwzględniając art. 48 Regulaminu,

– uwzględniając sprawozdanie Komisji Spraw Zagranicznych (A7-0335/2012),

A. mając na uwadze, że w dzisiejszym zglobalizowanym świecie UE i jej państwa członkowskie stały się w dużym stopniu uzależnione od bezpiecznej przestrzeni cybernetycznej, od bezpiecznego korzystania z technologii informacyjnej i cyfrowej oraz od odpornych i wiarygodnych usług informacyjnych i związanej z nimi infrastruktury;

B. mając na uwadze, że technologie informacyjne i komunikacyjne są także wykorzystywane jako narzędzia represji; mając na uwadze, że kontekst, w jakim wykorzystywane są technologie, w ogromnym stopniu determinuje wpływ, jaki mogą one wywierać jako siła napędowa zmian pozytywnych lub represji;

C. mając na uwadze, że cybernetyczne wyzwania, niebezpieczeństwa i ataki rosną w dramatycznym tempie i stanowią podstawowe zagrożenie dla bezpieczeństwa, obrony, stabilności i konkurencyjności państw, jak i sektora prywatnego; mając na uwadze, że w związku z tym nie należy traktować takich zagrożeń jako kwestii dotyczących przyszłości; mając na uwadze, że większość znacznie widocznych i zakłócających incydentów cybernetycznych jest coraz częściej umotywowana politycznie; mając na uwadze, że choć znaczna większość incydentów cybernetycznych okazuje się mieć podstawowy charakter, to zagrożenia dla kluczowych elementów infrastruktury stają się coraz bardziej wyrafinowane i uzasadniają potrzebę dogłębnej ochrony;

D. mając na uwadze, że cyberprzestrzeń, z blisko dwoma miliardami połączonych ze sobą użytkowników na świecie, stała się jednym z najsilniejszych i najskuteczniejszych sposobów przekazywania demokratycznych idei i organizowania ludzi, którzy starają się zrealizować swoje aspiracje dotyczące wolności i walczyć z dyktaturami; mając na uwadze, że wykorzystywanie cyberprzestrzeni przez niedemokratyczne i autorytarne rządy stanowi coraz większe zagrożenie dla indywidualnego prawa do wolności wypowiedzi i zrzeszania się; mając na uwadze, że podstawowe znaczenie ma w związku z tym dbanie o to, by cyberprzestrzeń pozostała otwarta na swobodny przepływ idei, informacji i wypowiedzi;

E. mając na uwadze, że w UE i jej państwach członkowskich istnieją liczne przeszkody natury politycznej, ustawodawczej i organizacyjnej dla rozwoju kompleksowego i jednolitego podejścia do cyberobrony i bezpieczeństwa cybernetycznego; mając na uwadze, że w sensytywnym i podatnym na zagrożenia obszarze bezpieczeństwa cybernetycznego brakuje

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

wspólnej definicji oraz wspólnych norm i środków;

F. mając na uwadze wciąż niewystarczający stopień dzielenia się informacjami i koordynacji w instytucjach UE, z państwami członkowskimi, a także z partnerami zewnętrznymi, oraz między nimi;

G. mając na uwadze, że brakuje jasnych i jednolitych definicji „bezpieczeństwa cybernetycznego" i „cyberobrony" na szczeblu unijnym i międzynarodowym; mając na uwadze, że w różnych krajach różnie pojmuje się bezpieczeństwo cybernetyczne i inne kluczowe terminy;

H. mając na uwadze, że UE nie opracowała jeszcze własnej spójnej polityki w zakresie ochrony krytycznej infrastruktury i informacji, która wymaga wielodyscyplinarnego podejścia, zwiększając tym samym bezpieczeństwo przy jednoczesnym poszanowaniu praw podstawowych;

I. mając na uwadze, że UE zaproponowała różne inicjatywy służące zwalczaniu cyberprzestępczości na poziomie cywilnym, w tym utworzenie nowego Europejskiego Centrum ds. Walki z Cyberprzestępczością, lecz brakuje jej konkretnego planu działania na poziomie bezpieczeństwa i obrony;

J. mając na uwadze, że budowanie zaufania między sektorem prywatnym a organami ścigania i obrony oraz innymi kompetentnymi instytucjami ma ogromne znaczenie w walce z cyberprzestępczością;

K. mając na uwadze, że wzajemne zaufanie w stosunkach między podmiotami państwowymi i niepaństwowymi jest warunkiem wstępnym solidnego bezpieczeństwa cybernetycznego;

L. mając na uwadze, że większość incydentów cybernetycznych w sektorze publicznym i prywatnym nie jest zgłaszana z uwagi na sensytywny charakter informacji i ewentualne szkody dla wizerunku odnośnych przedsiębiorstw;

M. mając na uwadze, że wiele incydentów cybernetycznych wynika z braku odporności i solidności publicznej i prywatnej infrastruktury sieciowej, słabo chronionych lub zabezpieczonych baz danych i innych wad krytycznej infrastruktury i informacji; mając na uwadze, że jedynie nieliczne państwa członkowskie uważają ochronę systemów informacyjnych i związanych z nimi danych za element spoczywającego na nich obowiązku należytej staranności, co tłumaczy brak inwestycji w nowoczesną technologię bezpieczeństwa, szkolenie i opracowanie odpowiednich wytycznych; mając na uwadze, że wiele państw członkowskich jest uzależnionych od technologii bezpieczeństwa z krajów trzecich i powinno nasilić starania na rzecz zmniejszenia tego uzależnienia;

N. mając na uwadze, że większość sprawców wysoko wyspecjalizowanych ataków zagrażających bezpieczeństwu krajowemu lub międzynarodowemu oraz obronie nigdy nie zostaje zidentyfikowana ani postawiona przed sądem; mając na uwadze, że brak jest uzgodnionej na poziomie międzynarodowym formy reakcji w przypadku wspieranego przez państwo ataku cybernetycznego na inne państwo, oraz brak jednoznacznej odpowiedzi, czy należy traktować taki atak jako casus belli;

O. mając na uwadze, że Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji angażuje się po stronie państw członkowskich, pomagając im w wymianie dobrych praktyk w

obszarze bezpieczeństwa cybernetycznego i zalecając, jak opracować, wdrożyć i utrzymać strategię bezpieczeństwa cybernetycznego; agencja ta odgrywa również rolę wspierającą w zakresie krajowych strategii bezpieczeństwa cybernetycznego, krajowych planów na wypadek zagrożenia, przy organizacji paneuropejskich i międzynarodowych ćwiczeń dotyczących ochrony krytycznej infrastruktury teleinformatycznej oraz przy opracowywaniu scenariuszy ćwiczeń krajowych;

P. mając na uwadze, że do czerwca 2012 r. tylko 10 państw członkowskich UE oficjalnie przyjęło krajową strategią bezpieczeństwa cybernetycznego;

Q. mając na uwadze, że cyberobrona jest jednym z priorytetów EAO, która utworzyła w ramach planu rozwoju zdolności zespół projektowy ds. bezpieczeństwa cybernetycznego, w obrębie którego większość państw członkowskich współpracuje przy gromadzeniu doświadczeń i formułowaniu zaleceń;

R. mając na uwadze, że inwestycje w działania badawczo-rozwojowe w zakresie bezpieczeństwa cybernetycznego i cyberobrony mają podstawowe znaczenie dla osiągania postępów i dla utrzymania wysokiego poziomu bezpieczeństwa cybernetycznego i cyberobrony; mając na uwadze, że wydatki z tytułu obrony na badania i rozwój zmniejszyły się zamiast osiągnąć poziom 2% całkowitych wydatków z zakresu obrony;

S. mając na uwadze, że uświadamianie i kształcenie obywateli w zakresie bezpieczeństwa cybernetycznego powinno stanowić podstawę każdej kompleksowej strategii bezpieczeństwa cybernetycznego;

T. mając na uwadze, że należy ustanowić wyraźną równowagę między środkami bezpieczeństwa a prawami obywateli wynikającymi z TFUE, jak prawo do prywatności, ochrona danych i wolność wypowiedzi, nie poświęcając jednego kosztem drugiego;

U. mając na uwadze rosnącą potrzebę lepszego szanowania i ochrony praw jednostki do prywatności zapisanych w Karcie praw podstawowych UE i w art. 16 TFUE; mając na uwadze, że konieczność zabezpieczenia i ochrony cyberprzestrzeni na szczeblu krajowym, w odniesieniu do instytucji i organów obrony – choć jest ważna – nie powinna usprawiedliwiać jakiegokolwiek ograniczania praw i swobód w przestrzeni cybernetycznej i informatycznej;

V. mając na uwadze, że globalny i nieograniczony charakter internetu wymaga nowych form współpracy międzynarodowej i zarządzania z udziałem wielu zainteresowanych stron;

W. mając na uwadze, że rządy coraz bardziej polegają na prywatnych podmiotach w celu zapewnienia bezpieczeństwa krytycznej infrastruktury;

X. mając na uwadze, że Europejska Służba Działań Zewnętrznych (ESDZ) nie włączyła jeszcze aktywnie aspektu bezpieczeństwa cybernetycznego do swoich relacji z krajami trzecimi;

Y. mając na uwadze, że Instrument na rzecz Stabilności jest jak na razie jedynym unijnym programem opracowanym w celu reagowania na nagłe kryzysy lub globalne/transregionalne wyzwania w zakresie bezpieczeństwa, w tym na zagrożenia cybernetyczne;

Z. mając na uwadze, że wspólna reakcja – za pośrednictwem grupy roboczej UE-USA ds.

bezpieczeństwa cybernetycznego i cyberprzestępczości – na zagrożenia cybernetyczne jest jednym z priorytetów w stosunkach UE-USA;

Działania i koordynacja w UE

1. odnotowuje, że zagrożenia cybernetyczne i ataki na rząd oraz organy administracyjne, wojskowe i międzynarodowe są coraz bardziej niebezpieczne dla UE, jak i całego świata, i zdarzają się coraz częściej, oraz że istnieją poważne powody do obawy, iż publiczne i niepubliczne podmioty, w szczególności organizacje terrorystyczne i przestępcze, mogą zaatakować krytyczne systemy i infrastruktury informacyjne i komunikacyjne instytucji i państw członkowskich UE i wyrządzić poważne szkody, w tym wywołać reakcję łańcuchową;

2. podkreśla zatem konieczność przyjęcia globalnego i skoordynowanego podejścia do tych wyzwań na szczeblu UE poprzez opracowanie kompleksowej unijnej strategii bezpieczeństwa cybernetycznego, która powinna zapewnić wspólną definicję bezpieczeństwa cybernetycznego i cyberobrony oraz cyberataku z nią związanego, wspólną wizję działań, a także uwzględnić wartość dodaną istniejących agencji i organów oraz dobre praktyki tych państw członkowskich, które posiadają już krajowe strategie bezpieczeństwa cybernetycznego; podkreśla kluczowe znaczenie koordynacji i utworzenia synergii na poziomie Unii, aby wspomóc łączenie różnych inicjatyw, programów i działań o charakterze zarówno wojskowym, jak i cywilnym; kładzie nacisk na fakt, że taka strategia powinna zapewniać elastyczność i być regularnie uaktualniana celem dostosowania jej do szybko zmieniającego się charakteru cyberprzestrzeni;

3. nalega, aby Komisja i wysoka przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa rozważyły w swojej przyszłej propozycji dotyczącej warunków stosowania klauzuli solidarności (artykuł 222 TFUE) możliwość poważnego ataku cybernetycznego przeciwko któremukolwiek państwu członkowskiemu; jest ponadto zdania, że choć ataki cybernetyczne zagrażające bezpieczeństwu narodowemu nadal należy definiować przy użyciu wspólnej terminologii, mogłyby zostać objęte klauzulą wzajemnej obrony (artykuł 42 ust. 7 Traktatu UE), bez uszczerbku dla zasady proporcjonalności;

4. podkreśla, że we WPBiO należy zagwarantować, że jednostki przeprowadzające unijne operacje wojskowe i misje cywilne będą chronione przed cyberatakami; podkreśla, że cyberobrona powinna stać się aktywną zdolnością WPBiO;

5. podkreśla, że wszystkie dziedziny unijnej polityki bezpieczeństwa cybernetycznego powinny zmierzać do zapewnienia maksymalnego poziomu ochrony i zachowania swobód cyfrowych oraz poszanowania praw człowieka w internecie, a także opierać się na tych zasadach; uważa, że polityka zagraniczna i bezpieczeństwa UE powinna obejmować internet i ICT, by pogłębić wysiłki w tym zakresie;

6. wzywa Komisję i Radę, by jednoznacznie uznały swobody cyfrowe za prawa podstawowe oraz za niezbędne warunki korzystania z powszechnych praw człowieka; podkreśla, że państwa członkowskie powinny zmierzać do sytuacji, w której nigdy nie zagrożą prawom i swobodom swoich obywateli przy opracowywaniu reakcji na zagrożenia i ataki cybernetyczne, a także że powinny dokonywać legislacyjnego rozróżnienia między cywilnym i wojskowym poziomem incydentów cybernetycznych; wzywa do rozważnego stosowania wszelkich ograniczeń dotyczących korzystania z narzędzi komunikacyjnych i informacyjnych przez obywateli;

7. wzywa Radę i Komisję oraz państwa członkowskie, by opracowały białą księgę w sprawie cyberobrony, w której ustanowią jasną definicję i kryteria dokonujące podziału poziomów cyberataków w dziedzinie cywilnej i wojskowej, zgodnie z ich założeniami i skutkami, a także poziomów reakcji, w tym śledztwa, wykrywania i ścigania sprawców;

8. odnotowuje wyraźną potrzebę zaktualizowania europejskiej strategii bezpieczeństwa w celu ustalenia i znalezienia sposobów wykrywania i ścigania indywidualnych, sieciowych bądź wspieranych przez państwo sprawców cyberataków;

Szczebel UE

9. podkreśla znaczenie horyzontalnej współpracy i koordynacji w zakresie bezpieczeństwa cybernetycznego w instytucjach i agencjach UE i między nimi;

10. podkreśla, że nowe technologie stanowią wyzwanie dla sposobu realizacji przez rządy ich podstawowych, tradycyjnych zadań; ponownie potwierdza, że polityka obrony i bezpieczeństwa ostatecznie jest w rękach rządu, przy należytej demokratycznej kontroli; zauważa coraz większą rolę podmiotów prywatnych w realizacji zadań z zakresu bezpieczeństwa i obrony, co odbywa się często w braku przejrzystości, odpowiedzialności lub mechanizmów demokratycznej kontroli;

11. podkreśla, że rządy powinny stosować się do podstawowych zasad wynikających z międzynarodowego prawa publicznego i humanitarnego, takich jak poszanowanie suwerenności państwowej i praw człowieka, przy stosowaniu nowych technologii w ramach polityki bezpieczeństwa i obrony; wskazuje na cenne doświadczenie państw członkowskich UE, takich jak Estonia, w definiowaniu i opracowywaniu polityki bezpieczeństwa cybernetycznego oraz cyberobrony;

12. uznaje konieczność dokonania oceny ogólnego poziomu ataków cybernetycznych przeciwko unijnym systemom i infrastrukturze informacji; podkreśla w tym kontekście konieczność ciągłej oceny stopnia gotowości instytucji UE do reagowania na potencjalne ataki cybernetyczne; podkreśla w szczególności konieczność wzmocnienia krytycznej infrastruktury informatycznej;

13. podkreśla też konieczność udostępniania w ramach systemów informatycznych informacji na temat słabych punktów, a także alarmów i ostrzeżeń dotyczących nowych zagrożeń;

14. odnotowuje, że niedawne ataki cybernetyczne przeciwko europejskim sieciom informacji i rządowym systemom informacji spowodowały znaczne szkody dla gospodarki i bezpieczeństwa, których zakres nie został odpowiednio oceniony;

15. wzywa wszystkie instytucje UE do jak najszybszego opracowania strategii bezpieczeństwa cybernetycznego i planów awaryjnych w odniesieniu do ich własnych systemów;

16. zwraca się do wszystkich instytucji UE o włączenie do ich analiz ryzyka i planów zarządzania kryzysowego kwestii zarządzania w sytuacji kryzysu cybernetycznego; ponadto apeluje do wszystkich instytucji UE o zapewnienie wszystkim swoim pracownikom szkoleń uświadamiających dotyczących bezpieczeństwa cybernetycznego; sugeruje przeprowadzanie raz w roku ćwiczeń cybernetycznych podobnych do ćwiczeń reagowania w nagłych wypadkach;

17. podkreśla znaczenie skutecznego rozwijania działalności unijnego zespołu reagowania na incydenty komputerowe (EU-CERT) i CERT krajowych, jak również znaczenie opracowywania krajowych planów awaryjnych na wypadek konieczności podjęcia działań; z zadowoleniem przyjmuje fakt, że do maja 2012 r. wszystkie państwa członkowskie UE powołały krajowe CERT; nalega na dalsze rozwijanie krajowych CERT i unijnego CERT, które będą w stanie w razie konieczności podjąć działania w przeciągu 24 godzin; podkreśla konieczność rozpatrzenia możliwości utworzenia partnerstw publiczno-prywatnych w tym obszarze;

18. uznaje, że „Cyber Europe 2010" – pierwsze europejskie ćwiczenie w zakresie ochrony krytycznej infrastruktury teleinformatycznej, które przeprowadzono z udziałem różnych państw członkowskich i pod przewodnictwem Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji – okazało się być przydatnym działaniem i przykładem dobrej praktyki; podkreśla także potrzebę jak najszybszego utworzenia sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej na szczeblu europejskim;

19. podkreśla znaczenie ogólnoeuropejskich ćwiczeń w procesie przygotowania do reagowania w przypadku zakrojonych na szeroką skalę ataków zagrażających bezpieczeństwu sieci, a także zdefiniowania jednolitego zestawu norm oceny zagrożeń;

20. zwraca się do Komisji o zbadanie konieczności i możliwości utworzenia stanowiska ds. unijnej koordynacji cybernetycznej;

21. uważa, że z uwagi na wysoki poziom umiejętności wymagany zarówno w odpowiedniej obronie cybernetycznych systemów i infrastruktury, jak i w ataku na nie, należy rozważyć możliwość opracowania strategii „białych kapeluszy" między Komisją, Radą i państwami członkowskimi; zauważa, że w takich przypadkach wysoki jest potencjał „drenażu mózgów" oraz że zwłaszcza niepełnoletni skazani za takie ataki mają duży potencjał do zrehabilitowania się i uzyskania zatrudnienia w agencjach i organach obrony;

Europejska Agencja Obrony (EAO)

22. z zadowoleniem przyjmuje ostatnie inicjatywy i projekty dotyczące cyberobrony, zwłaszcza w zakresie gromadzenia i klasyfikowania odnośnych danych dotyczących bezpieczeństwa cybernetycznego i cyberobrony oraz związanych z tym wyzwań i potrzeb, oraz wzywa państwa członkowskie do szerszej współpracy z EAO w dziedzinie cyberobrony, także na szczeblu wojskowym;

23. podkreśla znaczenie bliskiej współpracy państw członkowskich z EAO przy rozwijaniu krajowych zdolności cyberobrony; jest zdania, że tworzenie synergii, gromadzenie zasobów i dzielenie się nimi na szczeblu europejskim mają podstawowe znaczenie dla skutecznej cyberobrony na poziomie europejskim i krajowym;

24. zachęca EAO do zacieśnienia współpracy z NATO, krajowymi i międzynarodowymi centrami doskonałości, Europejskim Centrum ds. Walki z Cyberprzestępczością w ramach Europolu, przyczyniającym się do szybszych reakcji na cyberataki, a zwłaszcza z Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony, oraz do skoncentrowania się na budowaniu zdolności i szkoleniach, jak również na wymianie informacji i praktyk;

25. z niepokojem odnotowuje, że do 2010 r. tylko jednemu państwu członkowskiemu udało się przeznaczyć 2% wydatków na badania i rozwój z zakresu obrony i że pięć państw

członkowskich nie wydało w 2010 r. żadnych środków na badania i rozwój; nalega, aby EAO wraz z państwami członkowskimi zgromadziła zasoby i poczyniła skuteczne inwestycje we wspólne badania i rozwój, ze szczególnym uwzględnieniem bezpieczeństwa cybernetycznego i cyberobrony;

Państwa członkowskie

26. apeluje do wszystkich państw członkowskich o niezwłoczne opracowanie i uzupełnienie ich krajowych strategii bezpieczeństwa cybernetycznego i cyberobrony oraz o opracowywanie solidnej polityki i zapewnienie trwałego otoczenia regulacyjnego, kompleksowych procedur zarządzania ryzykiem i odpowiednich środków i mechanizmów przygotowawczych; wzywa Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji do wspierania państw członkowskich; wyraża swoje wsparcie dla Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji przy opracowywaniu przewodnika dobrych praktyk zawierającego dobre praktyki i zalecenia na temat tego, jak opracować, wdrożyć i utrzymać strategię bezpieczeństwa cybernetycznego;

27. zachęca wszystkie państwa członkowskie do utworzenia w swoich strukturach wojskowych specjalnych działów zajmujących się bezpieczeństwem cybernetycznym i cyberobroną w celu współpracy z podobnymi organami w innych państwach członkowskich UE;

28. zachęca państwa członkowskie do tworzenia na poziomie regionalnym wyspecjalizowanych sądów mających na celu skuteczniejsze karanie ataków na systemy informatyczne; podkreśla konieczność zachęcania do wprowadzenie zmian w przepisach krajowych, aby zapewnić ich dostosowanie do postępu technicznego i zastosowań;

29. zwraca się do Komisji, aby nadal pracowała nad spójnym i skutecznym europejskim podejściem pozwalającym uniknąć zbędnych inicjatyw, zachęcając i wspierając państwa członkowskie w ich staraniach na rzecz rozwijania mechanizmów współpracy i zintensyfikowania wymiany informacji; jest zdania, że należy ustalić minimalny poziom obowiązkowej współpracy i dzielenia się informacjami między państwami członkowskimi;

30. nalega, aby państwa członkowskie opracowały krajowe plany awaryjne i włączyły do planów zarządzania kryzysowego i analiz ryzyka zarządzanie w razie kryzysu cybernetycznego; podkreśla także znacznie odpowiedniego przeszkolenia wszystkich pracowników podmiotów publicznych w zakresie bezpieczeństwa cybernetycznego, a w szczególności zapewnienia członkom organów sądowych i organów bezpieczeństwa dostosowanych szkoleń w placówkach szkoleniowych; wzywa Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji i inne stosowne organy do wspierania państw członkowskich w zapewnianiu gromadzenia zasobów i dzielenia się nimi oraz w unikaniu powielania działań;

31. apeluje do państw członkowskich o uczynienie badań i rozwoju jednym z podstawowych filarów bezpieczeństwa cybernetycznego i cyberobrony oraz o wspieranie kształcenia inżynierów specjalizujących się w ochronie systemów informatycznych; zwraca się do państw członkowskich o wypełnienie zobowiązania do zwiększenia części wydatków na obronę przypadającej na badania i rozwój do co najmniej 2%, ze specjalnym uwzględnieniem bezpieczeństwa cybernetycznego i cyberobrony;

32. wzywa Komisję i państwa członkowskie do zaproponowania programów propagujących ogólnie bezpieczne korzystanie z internetu, systemów informacyjnych i technologii

komunikacyjnych oraz podnoszących świadomość na ten temat wśród użytkowników prywatnych i korporacyjnych; proponuje, aby Komisja zapoczątkowała publiczną ogólnoeuropejską inicjatywę edukacyjną na ten temat; zwraca się do państw członkowskich o włączenie do programów szkolnych w jak najmłodszych klasach kwestii bezpieczeństwa cybernetycznego;

Współpraca publiczno-prywatna

33. podkreśla podstawową rolę konstruktywnej i uzupełniającej współpracy w zakresie bezpieczeństwa cybernetycznego między władzami publicznymi a sektorem prywatnym, zarówno na szczeblu unijnym, jak i krajowym, z myślą o budowaniu wzajemnego zaufania; zdaje sobie sprawę z tego, że dalsze zwiększanie wiarygodności i skuteczności właściwych instytucji publicznych przyczyni się do budowania zaufania i wymiany krytycznych informacji;

34. wzywa partnerów z sektora prywatnego, by rozważyli zastosowanie rozwiązań w zakresie bezpieczeństwa już na etapie projektowania nowych produktów, sprzętu, usług i aplikacji, a także zachęty dla podmiotów projektujących nowe produkty, sprzęt, usługi i aplikacje, których zasadniczym elementem będzie bezpieczeństwo na etapie projektowania; domaga się, by w ramach współpracy z sektorem prywatnym w zakresie zapobiegania atakom cybernetycznym i ich zwalczania istniały minimalne standardy przejrzystości i mechanizmy sprawozdawczości;

35. podkreśla, że ochrona krytycznej infrastruktury teleinformatycznej uwzględniona jest w strategii bezpieczeństwa wewnętrznego UE w kontekście zwiększania poziomu bezpieczeństwa obywateli i przedsiębiorstw w cyberprzestrzeni;

36. apeluje o ustanowienie ciągłego dialogu z tymi partnerami na temat najlepszego wykorzystania systemów informacyjnych i ich odporności oraz na temat wspólnego ponoszenia odpowiedzialności, niezbędnego do bezpiecznego i właściwego funkcjonowania tych systemów;

37. jest zdania, że państwa członkowskie, instytucje UE i sektor prywatny powinni, we współpracy z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji, podjąć działania na rzecz zwiększenia bezpieczeństwa i integralności systemów informacyjnych, zapobiegania atakom i ograniczania ich skutków; wspiera Komisję w jej staraniach na rzecz opracowania minimalnych norm bezpieczeństwa cybernetycznego i systemów certyfikacji dla firm oraz w tworzeniu odpowiednich zachęt mających na celu pobudzanie wysiłków sektora prywatnego na rzecz poprawy bezpieczeństwa;

38. zwraca się do Komisji i rządów państw członkowskich o zachęcanie podmiotów sektora prywatnego i społeczeństwa obywatelskiego do włączania zarządzania w sytuacji kryzysu cybernetycznego do swoich planów zarządzania kryzysowego i analiz ryzyka; apeluje ponadto o wprowadzenie podnoszących świadomość szkoleń dla wszystkich ich pracowników z zakresu głównych aspektów bezpieczeństwa cybernetycznego i higieny cybernetycznej;

39. wzywa Komisję, aby we współpracy z państwami członkowskimi i odpowiednimi agencjami i organami opracowała ramy i instrumenty dla systemu szybkiej wymiany informacji, który zapewniałby anonimowość przy zgłaszaniu incydentów cybernetycznych w sektorze prywatnym, umożliwiałby podmiotom publicznym otrzymywanie bieżących

informacji i w razie potrzeby zapewniałby wsparcie;

40. podkreśla, że UE powinna ułatwić rozwój konkurencyjnego i innowacyjnego rynku bezpieczeństwa cybernetycznego w UE, aby umożliwić MŚP prowadzenie działalności w tym obszarze, co przyczyni się do intensywniejszego wzrostu i tworzenia miejsc pracy;

Współpraca międzynarodowa

41. zwraca się do ESDZ o przyjęcie aktywnego podejścia do bezpieczeństwa cybernetycznego oraz o włączenie aspektów bezpieczeństwa cybernetycznego do wszystkich swoich działań, zwłaszcza w odniesieniu do krajów trzecich; apeluje o zacieśnienie współpracy i zintensyfikowanie wymiany informacji na temat tego, jak radzić sobie z problemami bezpieczeństwa cybernetycznego z krajami trzecimi;

42. podkreśla, że ukończenie kompleksowej unijnej strategii bezpieczeństwa cybernetycznego jest warunkiem wstępnym ustanowienia skutecznej współpracy międzynarodowej w zakresie bezpieczeństwa cybernetycznego, której wymaga transgraniczny charakter zagrożeń cybernetycznych;

43. wzywa państwa członkowskie, które jeszcze nie podpisały lub ratyfikowały Konwencji Rady Europy o cyberprzestępczości (konwencja z Budapesztu), do niezwłocznego uczynienia tego; wspiera Komisję i ESDZ w ich staraniach na rzecz promowania konwencji i jej wartości wśród krajów trzecich;

44. jest świadomy konieczności uzgodnionej i koordynowanej na poziomie międzynarodowym reakcji na zagrożenia cybernetyczne; w związku z tym wzywa Komisję, ESDZ i państwa członkowskie do odgrywania przewodniej roli na wszystkich forach, zwłaszcza w ONZ, podejmując działania na rzecz osiągnięcia szerszej międzynarodowej współpracy i ostatecznego porozumienia dotyczącego ustalenia wspólnego rozumienia norm zachowania w cyberprzestrzeni, a także do wspierania współpracy w celu wypracowania umów dotyczących kontroli broni cybernetycznej;

45. zachęca do wymiany wiedzy w dziedzinie bezpieczeństwa cybernetycznego z krajami BRICS i innymi krajami o wschodzących gospodarkach w celu zbadania możliwości ewentualnych wspólnych reakcji na rosnącą cyberprzestępczość i coraz częstsze zagrożenia i ataki cybernetyczne, zarówno na szczeblu cywilnym, jak i wojskowym;

46. nalega, aby ESDZ i Komisja przyjęły aktywne stanowisko na odpowiednich międzynarodowych forach i w organizacjach międzynarodowych, zwłaszcza w ONZ, OBWE, OECD i Banku Światowym, aby zapewnić stosowanie istniejącego prawa międzynarodowego i osiągnąć konsensus w sprawie norm dotyczących odpowiedzialnego zachowania państwa względem bezpieczeństwa cybernetycznego i cyberobrony, oraz aby koordynowały stanowiska państw członkowskich z myślą o promowaniu podstawowych unijnych wartości i strategii w obszarze bezpieczeństwa cybernetycznego i cyberobrony;

47. wzywa Radę i Komisję, aby w ramach dialogu, kontaktów i umów o współpracy z krajami trzecimi, a w szczególności umów przewidujących współpracę i wymianę w dziedzinie technologii, kładły nacisk na minimalne wymogi dotyczące zapobiegania cyberprzestępczości i atakom cybernetycznym oraz zwalczania ich, a także na minimalne normy z zakresu bezpieczeństwa systemu informacji;

48. zwraca się do Komisji o wspieranie w razie potrzeby krajów trzecich w ich staraniach na rzecz budowania ich zdolności z zakresu bezpieczeństwa cybernetycznego i cyberobrony oraz o ułatwianie tych starań;

Współpraca z NATO

49. powtarza, że w oparciu o ich wspólne wartości i strategiczne interesy UE i NATO ponoszą szczególną odpowiedzialność i dysponują zdolnościami umożliwiającymi skuteczniejsze wspólne reagowanie na rosnące wyzwania dotyczące bezpieczeństwa cybernetycznego poprzez poszukiwanie możliwej komplementarności, bez powielania działań i z uwzględnieniem swoich obowiązków;

50. zważywszy na uzupełniający się charakter podejścia UE i NATO do bezpieczeństwa cybernetycznego i cyberobrony, podkreśla konieczność gromadzenia zasobów i dzielenia się nimi w praktycznym wymiarze; uwypukla konieczność zacieśnienia współpracy, zwłaszcza w zakresie planowania, technologii, szkoleń i wyposażenia w odniesieniu do bezpieczeństwa cybernetycznego i cyberobrony;

51. nalega, aby w oparciu o istniejącą komplementarność działań w zakresie rozwijania zdolności do obrony wszystkie właściwe unijne organy zajmujące się bezpieczeństwem cybernetycznym i cyberobroną pogłębiły praktyczną współpracę z NATO z myślą o wymianie doświadczenia i uczeniu się, jak zapewnić odporność systemów UE;

Współpraca ze Stanami Zjednoczonymi

52. jest zdania, że UE i USA powinny zacieśnić wzajemną współpracę, aby zaradzić atakom cybernetycznym i cyberprzestępczości, jako że stało się to priorytetem stosunków transatlantyckich po szczycie UE-USA w Lizbonie w 2010 r.;

53. z zadowoleniem przyjmuje utworzenie, na szczycie UE-USA w listopadzie 2010 r., grupy roboczej UE-USA ds. bezpieczeństwa cybernetycznego i cyberprzestępczości, oraz wspiera jej wysiłki na rzecz uwzględnienia kwestii dotyczących bezpieczeństwa cybernetycznego w transatlantyckim dialogu politycznym;

54. z zadowoleniem przyjmuje wspólne ustanowienie przez Komisję i rząd USA, pod patronatem grupy roboczej UE-USA, wspólnego programu i planu działania na rzecz wspólnych/zsynchronizowanych międzykontynentalnych ćwiczeń w dziedzinie bezpieczeństwa cybernetycznego w 2012/2013 r.; odnotowuje pierwsze ćwiczenie cyberatlantyckie z 2011 r.;

55. podkreśla, że zarówno UE, jak i USA – jako największe źródła cyberprzestrzeni i jej użytkowników – powinny współpracować nad ochroną praw i wolności swoich obywateli, dotyczących korzystania z tej przestrzeni; podkreśla, że skoro bezpieczeństwo narodowe jest kluczowym celem, cyberprzestrzeń należy zabezpieczyć, a także chronić;

o

o o

56. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, wysokiej przedstawiciel do spraw zagranicznych i polityki bezpieczeństwa/

wiceprzewodniczącej Komisji, EAO, Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji oraz NATO.