65. zwraca uwagę na potrzebę promowania działalności wolontariackiej, szczególnie w trakcie Europejskiego Roku Obywateli w 2013 r.; wzywa Komisję do uwzględnienia wsparcia wolontariackiego w międzynarodowych strategiach na rzecz rozwoju, zwłaszcza w celu realizacji wszystkich zamierzeń określonych z Milenijnych Celach Rozwoju;

66. popiera formalne rozpatrzenie projektu „Solidarité" dotyczącego międzyinstytucjonalnego programu na rzecz zasobów kadrowych w instytucjach UE, aby ułatwić zaangażowanie się personelu i stażystów instytucji w wolontariat, działalność humanitarną i społeczną, zarówno w ramach szkoleń dla personelu, jak i dobrowolnych akcji podejmowanych we własnym zakresie;

67. podkreśla, że proponowany program przewiduje oszczędne gospodarowanie i dużą wartość dodaną oraz przyczyniłby się do realizacji strategii i programów UE;

68. zaleca Komisji utrzymanie użytecznych kontaktów nawiązanych zarówno z grupą „EYV 2011 Alliance", i jej następczynią, Platformą Wolontariatu, która obejmuje wiele organizacji wolontariackich i sieci społeczeństwa obywatelskiego, jak i z krajowymi organami koordynacyjnymi, będącymi strategicznymi partnerami oraz rzecznikami rządów krajowych w tym sektorze, mając na uwadze niezwykłą różnorodność podmiotów odpowiedzialnych za organizację wolontariatu w UE i zachęca, aby te punkty kontaktowe włączyły się w tworzenie proponowanego scentralizowanego portalu UE, mającego charakter ogólnoeuropejskiej platformy, tak aby ułatwiać dalszą koordynację i intensyfikować działalność transgraniczną;

69. podkreśla znaczenie sieci kontaktów i wymiany dobrych praktyk w rozpowszechnianiu informacji dotyczących obowiązujących procedur unijnych, co może pomóc i stymulować rozwój wolontariatu transgranicznego;

70. zwraca się do Komisji Europejskiej, by, o ile uzna to za właściwe, podjęła działania w związku z Agendą Działań na rzecz Wolontariatu w Europie (PAVE), która została opracowana przez organizacje wolontariackie skupione w grupie „EYV 2011 Alliance";

71. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie i Komisji, a także rządom i parlamentom państw członkowskich.

Ochrona krytycznej infrastruktury teleinformatycznej: działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni

P7_TA(2012)0237

Rezolucja Parlamentu Europejskiego z dnia 12 czerwca 2012 r. w sprawie ochrony krytycznej infrastruktury teleinformatycznej – „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni" (2011/2284(INI))

(2013/C 332 E/03)

Parlament Europejski,

— uwzględniając swoją rezolucję z dnia 5 maja 2010 r. zatytułowaną „Nowa agenda cyfrowa dla Europy: 2015.eu" ([1]),

— uwzględniając swoją rezolucję z dnia 15 czerwca 2010 r. zatytułowaną „Zarządzanie internetem: kolejne działania" ([2]),

— uwzględniając swoją rezolucję z dnia 6 lipca 2011 r. zatytułowaną „Internet szerokopasmowy w Europie: inwestycje na rzecz rozwoju opartego na technologiach szerokopasmowych" ([3]),

— uwzględniając art. 48 Regulaminu,

— uwzględniając sprawozdanie Komisji Przemysłu, Badań Naukowych i Energii oraz opinię Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (A7-0167/2012),

([1]) Dz.U. C 81E z 15.3.2011, s. 45.
([2]) Dz.U. C 236E z 12.8.2011, s. 33.
([3]) Teksty przyjęte, P7_TA(2011)0322.

A. mając na uwadze, że technologie informacyjno-komunikacyjne (TIK) są w stanie wykorzystać swój pełny potencjał w zakresie sprzyjania postępom gospodarki i społeczeństwa jedynie pod warunkiem, że użytkownicy mają pewność i zaufanie do ich bezpieczeństwa i odporności, oraz pod warunkiem, że przepisy dotyczące kwestii takich jak poufność danych czy prawo własności intelektualnej są w środowisku internetowym skutecznie egzekwowane;

B. mając na uwadze szybki wzrost wpływu internetu oraz TIK na różne aspekty życia obywateli oraz fakt, że pełnią one funkcję bodźca zachęcającego do interakcji społecznych, wzbogacenia kultury i wzrostu gospodarczego;

C. mając na uwadze, że TIK i bezpieczeństwo internetu stanowią całościową koncepcję o globalnym zasięgu ekonomicznym, społecznym, technologicznym i wojskowym, wymagającą precyzyjnej definicji i wyraźnego podziału obowiązków oraz sprawnego międzynarodowego mechanizmu współpracy;

D. mając na uwadze, że inicjatywa przewodnia dotycząca agendy cyfrowej UE ma na celu zwiększenie konkurencyjności Europy w oparciu o wzmocnienie TIK i stworzenie warunków dla wysokiego i silnego wzrostu oraz miejsc pracy związanych z technologią;

E. mając na uwadze, że sektor prywatny jest w dalszym ciągu głównym inwestorem, właścicielem i zarządcą produktów, usług, aplikacji i infrastruktury w dziedzinie bezpieczeństwa informacji, w które inwestował miliardy euro w ciągu ostatniej dekady; mając na uwadze, że zaangażowanie to powinno być wzmocnione właściwymi strategiami politycznymi na rzecz promowania odporności infrastruktury, której operatorami lub właścicielami są podmioty publiczne, prywatne lub publiczno-prywatne;

F. mając na uwadze, że rozwijanie wysokiego stopnia bezpieczeństwa i odporności sieci, usług i technologii TIK powinno zwiększyć konkurencyjność gospodarki UE zarówno poprzez usprawnienie oceny ryzyka w sieci i zarządzanie nim, jak i wyposażenie całej gospodarki UE w sprawniejszą infrastrukturę teleinformatyczną w celu wspierania innowacji i wzrostu, stwarzając firmom nowe możliwości zwiększenia wydajności;

G. mając na uwadze, że dostępne dane organów ścigania dotyczące cyberprzestępczości – obejmujące ataki w cyberprzestrzeni oraz inne typy przestępstw internetowych – wskazują na jej znaczny wzrost w wielu krajach europejskich; mając na uwadze, że statystycznie reprezentatywne dane dotyczące ataków cybernetycznych pochodzące od organów ścigania i społeczności CERT (zespołów reagowania na incydenty komputerowe) są jednak w dalszym ciągu niekompletne i w przyszłości należałoby usprawnić ich gromadzenie, dzięki czemu w całej UE reakcje organów ścigania na stale rosnące zagrożenia w sieci będą bardziej zdecydowane, a reakcje ustawodawców – bardziej świadome;

H. mając na uwadze, że odpowiedni poziom bezpieczeństwa informacji jest kluczowy dla silnej ekspansji usług internetowych;

I. mając na uwadze, że niedawne incydenty w cyberprzestrzeni, zakłócenia i ataki wymierzone w infrastrukturę teleinformatyczną instytucji UE, przemysłu oraz państw członkowskich uwidaczniają potrzebę utworzenia niezawodnego, innowacyjnego i efektywnego systemu ochrony krytycznej infrastruktury teleinformatycznej (CIIP) opartego na ścisłej współpracy międzynarodowej oraz minimalnych standardach w zakresie odporności obowiązujących państwa członkowskie;

J. mając na uwadze, że szybka ewolucja nowych dróg rozwoju TIK, np. przetwarzania danych w chmurze obliczeniowej, wymaga zdecydowanego ukierunkowania na bezpieczeństwo, aby umożliwić czerpanie pełnych korzyści z osiągnięć technologicznych;

K. mając na uwadze, że Parlament Europejski wielokrotnie domagał się zastosowania wysokich standardów prywatności i ochrony danych, ochrony neutralności sieci i praw własności intelektualnej;

Środki na rzecz usprawnienia ochrony krytycznej infrastruktury teleinformatycznej (CIIP) na szczeblu krajowym i unijnym

1. z zadowoleniem przyjmuje wdrożenie przez państwa członkowskie europejskiego programu na rzecz ochrony krytycznej infrastruktury teleinformatycznej (CIIP), w tym utworzenia sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (CIWIN);

2. jest zdania, że wysiłki podejmowane na rzecz ochrony krytycznej infrastruktury teleinformatycznej nie tylko zwiększą ogólne bezpieczeństwo obywateli, lecz również poprawią sposób postrzegania bezpieczeństwa przez obywateli i zwiększą ich zaufanie do środków przedsiębranych przez rząd w celu ochrony obywateli;

3. zwraca uwagę, że Komisja rozważa zmianę dyrektywy Rady 2008/114/WE ([1]), oraz apeluje o dostarczenie dowodów efektywności oraz skutków wdrożenia dyrektywy przed poczynieniem dalszych kroków; wzywa do rozważenia rozszerzenia zakresu jej stosowania, zwłaszcza poprzez uwzględnienie sektora TIK oraz usług finansowych; wzywa ponadto do wzięcia pod uwagę obszarów takich jak służba zdrowia, systemy dostaw żywności i wody, badania i przemysł atomowy (w odniesieniu do tych elementów, które nie są objęte odrębnymi przepisami szczegółowymi); stoi na stanowisku, że sektory te powinny także korzystać z przekrojowego podejścia międzysektorowego przyjętego przez CIWIN (obejmującego współpracę, system ostrzegawczy oraz wymianę najlepszych praktyk);

4. podkreśla znaczenie stworzenia i zapewnienia głębokiej integracji europejskiej infrastruktury badawczej dla utrzymania i wzmocnienia stopnia europejskiej sprawności w dziedzinie ochrony krytycznej infrastruktury teleinformatycznej;

5. wzywa, w związku ze wzajemnymi powiązaniami oraz wysokim stopniem współzależności, a także wrażliwym, strategicznym i podatnym na zagrożenia charakterem krajowych i unijnych krytycznych infrastruktur teleinformatycznych, do regularnego aktualizowania minimalnych standardów w zakresie odporności w celu zapewnienia gotowości i reagowania na wszelkie zakłócenia, incydenty, próby zniszczenia lub ataki, takie jak te, których przyczynami są niedostatecznie sprawna infrastruktura lub niewystarczająco zabezpieczone terminale końcowe;

6. podkreśla znaczenie norm i protokołów bezpieczeństwa informacji i z zadowoleniem przyjmuje mandat Europejskiego Komitetu Normalizacyjnego (CEN), Europejskiego Komitetu Normalizacyjnego Elektrotechniki (Celenec) i Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI) z 2011 r. w sprawie ustanowienia norm bezpieczeństwa;

7. oczekuje, że właściciele i operatorzy krytycznej infrastruktury teleinformatycznej umożliwią użytkownikom skorzystanie ze stosownych środków ochrony przed złośliwymi atakami lub zakłóceniami, a w razie konieczności udzielą użytkownikom pomocy w tym zakresie zarówno poprzez nadzór automatyczny, jak i sterowany przez człowieka;

8. wspiera współpracę na szczeblu unijnym pomiędzy publicznymi i prywatnymi zainteresowanymi podmiotami i zachęca je do podjęcia starań na rzecz opracowania i wprowadzenia norm dotyczących bezpieczeństwa i odporności cywilnej (publicznej, prywatnej lub publiczno-prywatnej) krajowej i europejskiej krytycznej infrastruktury teleinformatycznej;

9. 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;

10. wzywa Komisję do przeanalizowania we współpracy z państwami członkowskimi wdrożenia planu działania na rzecz ochrony krytycznej infrastruktury teleinformatycznej; wzywa państwa członkowskie do utworzenia sprawnie funkcjonujących krajowych/rządowych zespołów reagowania na incydenty komputerowe, do opracowania krajowych strategii na rzecz bezpieczeństwa cybernetycznego, do organizowania regularnych krajowych i ogólnoeuropejskich ćwiczeń w dziedzinie incydentów w cyberprzestrzeni, do opracowania krajowych planów awaryjnych na wypadek incydentów w cyberprzestrzeni oraz podjęcia działań na rzecz opracowania do końca 2012 r. europejskiego planu awaryjnego na wypadek incydentów w cyberprzestrzeni;

11. zaleca, aby wdrożyć plany zabezpieczeń operatorów lub inne środki równoważne w odniesieniu do całej europejskiej krytycznej infrastruktury teleinformatycznej, oraz aby wyznaczyć urzędników łącznikowych ds. ochrony;

12. z zadowoleniem przyjmuje obecną zmianę decyzji ramowej Rady 2005/222/WSiSW ([2]) w sprawie ataków na systemy informatyczne; zauważa potrzebę koordynacji starań UE w zakresie przeciwstawiania się atakom cybernetycznym na dużą skalę poprzez uwzględnienie kompetencji Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), zespołów reagowania na incydenty komputerowe państw członkowskich i przyszłego europejskiego zespołu reagowania na incydenty komputerowe;

13. uważa, że Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji może odgrywać kluczową rolę na szczeblu europejskim w zakresie ochrony krytycznej infrastruktury teleinformatycznej poprzez przekazywanie państwom członkowskim oraz instytucjom i organom Unii Europejskiej wiedzy technicznej oraz sporządzanie sprawozdań i analiz na temat sytuacji związanej z bezpieczeństwem systemów informatycznych w Europie i na świecie;

Dalsze działania UE na rzecz wysokiego poziomu bezpieczeństwa internetu

14. wzywa Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji do koordynowania i wdrażania corocznego unijnego miesiąca świadomości na temat bezpieczeństwa w internecie, aby zagadnienia dotyczące bezpieczeństwa cybernetycznego stały się szczególnym punktem zainteresowania państw członkowskich i obywateli UE;

([1]) Dz.U. L 345 z 23.12.2008, s. 75.
([2]) Dz.U. L 69 z 16.03.05, s. 67.

15. zgodnie z celami agendy cyfrowej wspiera Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w wykonywaniu jej zadań związanych z bezpieczeństwem informacji w sieci, polegających zwłaszcza na udzielaniu państwom członkowskim wskazówek i porad dotyczących wykorzystania podstawowych możliwości krajowych zespołów reagowania na incydenty komputerowe oraz wspierania wymiany najlepszych praktyk poprzez budowanie atmosfery zaufania; wzywa Agencję do przeprowadzenia konsultacji z właściwymi zainteresowanymi stronami w celu określenia podobnych środków bezpieczeństwa cybernetycznego dla prywatnych właścicieli i operatorów sieci oraz infrastruktury i do wspierania Komisji i państw członkowskich w ich działaniach na rzecz rozwoju i wdrożenia systemów certyfikacji w zakresie bezpieczeństwa informacji, norm postępowania i praktyk w zakresie współpracy dotyczących krajowych i europejskich zespołów reagowania na incydenty komputerowe oraz właścicieli i operatorów infrastruktury, a w uzasadnionych przypadkach – do wspierania ich poprzez określenie neutralnych technologicznie wymogów minimalnych;

16. z zadowoleniem przyjmuje wniosek dotyczący przeglądu mandatu Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, a zwłaszcza jego rozszerzenia oraz zwiększenia zakresu zadań Agencji; jest przekonany, że oprócz wspierania państw członkowskich poprzez dostarczanie wiedzy fachowej i analiz Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji powinna być uprawniona do wykonywania we współpracy z odpowiednikami z USA szeregu zadań wykonawczych na szczeblu UE dotyczących zapobiegania incydentom związanym z bezpieczeństwem sieci i informacji oraz wykrywania tych incydentów, a także zwiększeniem współpracy pomiędzy państwami członkowskimi; podkreśla, że na mocy rozporządzenia w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, można również przydzielić Agencji dodatkowe obowiązki dotyczące reagowania na ataki w internecie w takim zakresie, który w wyraźny sposób nadaje wartość dodaną istniejącym krajowym mechanizmom reagowania;

17. z zadowoleniem przyjmuje wyniki ogólnoeuropejskich ćwiczeń w dziedzinie bezpieczeństwa cybernetycznego z 2010 i 2011 r. przeprowadzonych w całej Unii i nadzorowanych przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, których celem było wspieranie państw członkowskich w opracowywaniu, utrzymywaniu i testowaniu ogólnoeuropejskiego planu awaryjnego; wzywa Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji do zachowania tego typu ćwiczeń w jej planie działania i stopniowego angażowania w uzasadnionych przypadkach odpowiednich operatorów prywatnych w celu zwiększenia ogólnego europejskiego potencjału w zakresie bezpieczeństwa internetu; oczekuje dalszego rozszerzenia działalności międzynarodowej wspólnie z partnerami o podobnych poglądach;

18. apeluje do państw członkowskich o opracowanie krajowych planów awaryjnych w zakresie bezpieczeństwa cybernetycznego i o uwzględnienie kluczowych elementów, takich jak odpowiednie punkty kontaktowe oraz przepisy dotyczące udzielania pomocy, hermetyzacja i usuwanie usterek w przypadku zakłóceń lub ataków w cyberprzestrzeni o zasięgu regionalnym, krajowym lub transgranicznym; zauważa, że państwa członkowskie powinny także uruchomić odpowiednie mechanizmy i struktury koordynacyjne na szczeblu krajowym, które pomogłyby w zapewnieniu lepszej koordynacji i większej spójności działań właściwych organów krajowych;

19. zaleca, aby za pośrednictwem unijnego planu awaryjnego na wypadek incydentów w cyberprzestrzeni Komisja zaproponowała wiążące środki na rzecz lepszej koordynacji na szczeblu UE technicznych i koordynacyjnych funkcji krajowych i rządowych zespołów reagowania na incydenty komputerowe;

20. wzywa Komisję i państwa członkowskie do podjęcia niezbędnych działań w celu ochrony krytycznej infrastruktury przed cyberatakami i zapewnienia sposobów na hermetyczne odcięcie dostępu do krytycznej infrastruktury w przypadku, gdy bezpośredni cyberatak poważnie zagraża jej właściwemu funkcjonowaniu;

21. oczekuje na powołanie unijnego zespołu reagowania na incydenty komputerowe, którego działalność będzie kluczowym czynnikiem w zapobieganiu celowym i złośliwym atakom cybernetycznym oraz atakom skierowanym przeciwko instytucjom UE i wykrywaniu tych ataków, reagowaniu na nie oraz usuwaniu ich skutków;

22. zaleca, aby Komisja zaproponowała wiążące środki mające na celu wdrożenie minimalnych standardów dotyczących bezpieczeństwa i odporności oraz poprawę koordynacji działań krajowych zespołów reagowania na incydenty komputerowe;

23. wzywa państwa członkowskie i instytucje UE do dopilnowania tego, by powołano sprawnie funkcjonujące zespoły reagowania na incydenty komputerowe, dysponujące minimalnymi zdolnościami w zakresie bezpieczeństwa i odporności opartymi na uzgodnionych sprawdzonych rozwiązaniach; podkreśla, że krajowe zespoły reagowania na incydenty komputerowe powinny być częścią efektywnej sieci, w której stosowne informacje są wymieniane zgodnie z niezbędnymi standardami poufności; wzywa do ustanowienia 24-godzinnej aktywności przez siedem dni w tygodniu usług ochrony krytycznej infrastruktury teleinformatycznej w każdym państwie członkowskim oraz utworzenia wspólnego europejskiego protokołu stosowanego w krajowych punktach kontaktowych na wypadek awarii;

24. podkreśla, że budowanie zaufania i promowanie współpracy pomiędzy państwami członkowskimi jest kluczowe dla ochrony danych oraz krajowych sieci i infrastruktur; wzywa Komisję do zaproponowania wspólnej procedury identyfikacji i ustalenia wspólnego podejścia do przeciwdziałania transgranicznym zagrożeniom dotyczącym TIK i oczekuje, że państwa członkowskie dostarczą Komisji stosowne informacje na temat ryzyka, zagrożeń oraz słabości ich krytycznej infrastruktury teleinformatycznej;

25. z zadowoleniem przyjmuje inicjatywę Komisji w zakresie opracowania do 2013 r. europejskiego systemu wymiany informacji i wczesnego ostrzegania;

26. z zadowoleniem przyjmuje zainicjowane przez Komisję konsultacje z poszczególnymi zainteresowanymi stronami w sprawie bezpieczeństwa internetu oraz ochrony krytycznej infrastruktury teleinformatycznej, np. europejskie partnerstwo publiczno-prywatne na rzecz odporności; przyznaje, że dostawcy TIK są już silnie zaangażowani w tego typu działania i podjęli zobowiązania w tym zakresie; zachęca Komisję do podejmowania dalszych wysiłków na rzecz zachęcania środowiska akademickiego oraz stowarzyszeń użytkowników TIK do odgrywania bardziej aktywnej roli i do sprzyjania konstruktywnemu dialogowi z udziałem wielu zainteresowanych stron na temat kwestii dotyczących bezpieczeństwa cybernetycznego; popiera dalszy rozwój zgromadzenia cyfrowego jako ram zarządzania ochroną krytycznej infrastruktury teleinformatycznej;

27. z zadowoleniem przyjmuje pracę dotychczas wykonaną przez europejskie forum państw członkowskich w zakresie ustanowienia dla poszczególnych sektorów kryteriów dotyczących rozpoznawania europejskiej krytycznej infrastruktury ze szczególnym uwzględnieniem łączności stacjonarnej i ruchomej, a także w zakresie prowadzenia dyskusji na temat unijnych zasad i wytycznych dotyczących odporności i stabilności w internecie; oczekuje na dalsze budowanie konsensusu w tym względzie wśród państw członkowskich i w tym kontekście zachęca forum do uzupełnienia obecnego podejścia ukierunkowanego na fizyczne zasoby infrastruktury o starania obejmujące również logiczne zasoby infrastruktury, których znaczenie dla skuteczności ochrony krytycznej infrastruktury teleinformatycznej będzie ciągle wzrastać z uwagi na rozwój wirtualizacji i technologii chmury;

28. proponuje, aby Komisja zapoczątkowała publiczną ogólnoeuropejską inicjatywę edukacyjną ukierunkowaną na kształcenie i podnoszenie świadomości prywatnych i korporacyjnych użytkowników końcowych w zakresie potencjalnych zagrożeń dotyczących internetu oraz stacjonarnych i przenośnych urządzeń TIK na każdym etapie łańcucha użytkowania, a także na promowanie bezpieczniejszych zachowań w sieci; przypomina w związku w tym o ryzyku związanym z używaniem przestarzałego sprzętu i oprogramowania komputerowego;

29. wzywa państwa członkowskie do wzmocnienia przy pomocy Komisji programów szkoleniowych i edukacyjnych z zakresu bezpieczeństwa informacji skierowanych do krajowych organów ścigania i organów sądowych oraz właściwych agencji UE;

30. popiera utworzenie unijnego programu kształcenia dla ekspertów akademickich w dziedzinie bezpieczeństwa informacji, ponieważ będzie on miał pozytywny wpływ na wiedzę fachową i gotowość UE w zakresie ciągle rozwijającej się cyberprzestrzeni i związanych z nią zagrożeń;

31. opowiada się za wspieraniem edukacji w obszarze bezpieczeństwa cyberprzestrzeni (staże dla doktorantów, uniwersyteckie programy nauczania, warsztaty, szkolenia dla studentów itp.) oraz specjalistyczne ćwiczenia w zakresie ochrony krytycznej infrastruktury teleinformatycznej;

32. wzywa Komisję do przedłożenia do końca 2012 r. wniosku w sprawie kompleksowej strategii na rzecz bezpieczeństwa internetu w Unii w oparciu o jasno sformułowaną terminologię; jest zdania, że celem strategii na rzecz bezpieczeństwa internetu powinno być utworzenie cyberprzestrzeni – wspieranej zabezpieczoną i odporną infrastrukturą oraz otwartymi standardami – sprzyjającej innowacyjności i dobrobytowi poprzez swobodny przepływ informacji oraz zapewnienie skutecznej ochrony prywatności i innych wolności obywatelskich; uważa, że w tej strategii należy szczegółowo określić zasady, cele, metody, instrumenty i rozwiązania polityczne (zarówno wewnętrzne jak i zewnętrzne) niezbędne dla ukierunkowania krajowych i unijnych wysiłków oraz ustanowienia minimalnych standardów odporności wśród państw członkowskich w celu zapewnienia bezpiecznych, ciągłych, niezawodnych i odpornych usług powiązanych zarówno z krytyczną infrastrukturą, jak i ogólnym korzystaniem z internetu;

33. podkreśla, że w kolejnej strategii Komisji na rzecz bezpieczeństwa internetowego za główny punkt odniesienia należy przyjąć prace dotyczące ochrony krytycznej infrastruktury teleinformatycznej i dążyć do określenia kompleksowego i systematycznego podejścia do bezpieczeństwa cyberprzestrzeni zarówno poprzez podejmowanie działań aktywnych, takich jak wprowadzenie minimalnych norm dla środków bezpieczeństwa lub szkolenie poszczególnych użytkowników, przedsiębiorstw i instytucji publicznych, jak i poprzez podejmowanie działań reaktywnych, takich jak nakładanie sankcji karnych, cywilnych i administracyjnych;

34. pilnie wzywa Komisję do zaproponowania sprawnego mechanizmu mającego na celu koordynację wdrażania i regularnego aktualizowania strategii na rzecz bezpieczeństwa internetu; uważa, że mechanizm ten powinien być wsparty wystarczającymi zasobami administracyjnymi, eksperckimi i finansowymi oraz ułatwiać opracowanie stanowiska UE dotyczącego spraw związanych z bezpieczeństwem internetu wspólnie z wewnętrznymi i międzynarodowymi zainteresowanymi podmiotami;

35. wzywa Komisję do zaproponowania unijnych ram powiadamiania o naruszeniach bezpieczeństwa w sektorach o największym znaczeniu, takich jak energia, transport, dostawy żywności i wody, a także w sektorze TIK i usług finansowych, w celu zapewnienia, że właściwe organy państw członkowskich i użytkownicy będą powiadamiani o incydentach, atakach lub zakłóceniach w cyberprzestrzeni;

36. pilnie wzywa Komisję do zwiększenia dostępności statystycznie reprezentatywnych danych dotyczących kosztów ataków cybernetycznych w UE, państwach członkowskich i przemyśle (zwłaszcza w sektorze usług finansowych i TIK) poprzez zwiększenie zdolności gromadzenia danych planowanego europejskiego centrum ds. walki z cyberprzestępczością, które ma zostać utworzone do 2013 r., zespołów reagowania na incydenty komputerowe oraz innych inicjatyw Komisji, takich jak europejski system wymiany informacji i wczesnego ostrzegania, aby zapewnić systematyczne składanie sprawozdań i współdzielenie danych dotyczących ataków cybernetycznych oraz innych form cyberprzestępczości szkodzących europejskiemu przemysłowi i państwom członkowskim oraz wesprzeć egzekwowanie prawa;

37. opowiada się za zacieśnieniem stosunków i interakcji między krajowym sektorem prywatnym i Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji, by stworzyć wspólną platformę dla krajowych/rządowych zespołów reagowania na incydenty komputerowe i rozwoju europejskiego systemu wymiany informacji i wczesnego ostrzegania (EISAS);

38. podkreśla, że główną siłą napędową rozwoju i wykorzystania technologii mających zwiększać bezpieczeństwo internetu jest przemysł TIK; przypomina, że w politykach UE należy unikać zakłócania rozwoju europejskiej gospodarki internetowej oraz uwzględnić konieczne bodźce w celu pełnego wykorzystania potencjału sektora przedsiębiorczości i partnerstw publiczno-prywatnych; proponuje rozważyć dodatkowe zachęty dla przemysłu w celu opracowania sprawniejszych planów ochrony infrastruktury zgodnie z dyrektywą 2008/114/WE;

39. wzywa Komisję do przedłożenia wniosku ustawodawczego w sprawie objęcia ataków cybernetycznych ((tj. phishingu profilowanego, oszustw internetowych itp.) surowszymi sankcjami karnymi;

Współpraca międzynarodowa

40. przypomina, że współpraca międzynarodowa stanowi zasadniczy instrument w zakresie wdrażania skutecznych środków bezpieczeństwa cybernetycznego; uznaje, że obecnie UE nie jest czynnie zaangażowana w sposób trwały w procesy współpracy międzynarodowej i dialogi dotyczące bezpieczeństwa cybernetycznego; wzywa Komisję i Europejską Służbę Działań Zewnętrznych (ESDZ) do rozpoczęcia konstruktywnego dialogu ze wszystkimi państwami mającymi podobne podejście do sprawy w celu wypracowania wspólnego zrozumienia i polityk zmierzających do podniesienia poziomu odporności internetu i krytycznej infrastruktury; uważa, że UE powinna jednocześnie w sposób stały uwzględniać kwestie bezpieczeństwa internetu w zakresie swoich stosunków zewnętrznych, między innymi podczas opracowywania różnych instrumentów finansowania lub przystępowania do międzynarodowych umów obejmujących wymianę i przechowywanie wrażliwych danych;

41. zauważa pozytywne skutki Konwencji Rady Europy o cyberprzestępczości, podpisanej w 2001 r. w Budapeszcie; podkreśla jednak, że oprócz zachęcania kolejnych krajów do podpisania i ratyfikowania przedmiotowej konwencji ESDZ powinna również zawrzeć dwustronne i wielostronne porozumienia w sprawie bezpieczeństwa internetu i odporności z międzynarodowymi partnerami o podobnych poglądach;

42. wskazuje, że duża liczba działań prowadzonych aktualnie przez różne międzynarodowe i unijne instytucje, organy i agencje, jak również przez państwa członkowskie wymaga koordynacji, tak aby unikać powielania, a w tym celu warto rozważyć mianowanie urzędnika odpowiedzialnego za koordynację, ewentualnie poprzez wyznaczenie unijnego koordynatora ds. bezpieczeństwa cyberprzestrzeni;

43. podkreśla, że ustrukturyzowany dialog między głównymi podmiotami i ustawodawcami w UE i USA zajmującymi się ochroną krytycznej infrastruktury teleinformatycznej ma szczególne znaczenie dla stworzenia wspólnego zrozumienia, interpretacji i stanowisk w odniesieniu do ram prawnych i zarządczych;

44. 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 internetu w dialogu w sprawie polityki transatlantyckiej; 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.;

45. sugeruje zainicjowanie zorganizowanego dialogu pomiędzy UE a amerykańskimi ustawodawcami w celu przedyskutowania kwestii dotyczących internetu w ramach poszukiwania wspólnego zrozumienia, interpretacji i stanowiska;

46. wzywa ESDZ i Komisję, na podstawie pracy wykonanej przez europejskie forum państw członkowskich, do zajęcia aktywnego stanowiska w ramach odnośnych forów międzynarodowych, między innymi poprzez koordynowanie stanowisk państw członkowskich w celu upowszechniania głównych unijnych wartości, celów i polityk w dziedzinie bezpieczeństwa i odporności internetu; zauważa, że do takich forów należą NATO, ONZ (zwłaszcza Międzynarodowy Związek Telekomunikacyjny i Forum Zarządzania Internetem), Internetowa Korporacja ds. Nadawania Nazw i Numerów, internetowy organ rejestracyjny IANA, OBWE, OECD oraz Bank Światowy;

47. zachęca Komisję i Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji do uczestnictwa w dialogach z najważniejszymi zainteresowanymi podmiotami w celu opracowania prawnych i technicznych norm dotyczących cyberprzestrzeni na szczeblu międzynarodowym;

*

* *

48. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie i Komisji.

Współpraca w zakresie polityki energetycznej z partnerami spoza UE

P7_TA(2012)0238

Rezolucja Parlamentu Europejskiego z dnia 12 czerwca 2012 r. w sprawie nawiązania współpracy w zakresie polityki energetycznej z partnerami spoza UE: podejście strategiczne do bezpiecznych, zrównoważonych i konkurencyjnych dostaw energii (2012/2029(INI))

(2013/C 332 E/04)

Parlament Europejski,

— uwzględniając komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie bezpieczeństwa dostaw energii i międzynarodowej współpracy energetycznej zatytułowany: „Polityka energetyczna UE: stosunki z partnerami spoza UE" COM(2011)0539),

— uwzględniając wniosek Komisji dotyczący decyzji Parlamentu Europejskiego i Rady ustanawiającej mechanizm wymiany informacji w odniesieniu do umów międzyrządowych w dziedzinie energii między państwami członkowskimi a państwami trzecimi (COM(2011)0540),

— uwzględniając konkluzje Rady z dnia 24 listopada 2011 r. w sprawie bezpieczeństwa dostaw energii i międzynarodowej współpracy energetycznej pt. „Polityka energetyczna UE: stosunki z partnerami spoza UE",

— uwzględniając własną rezolucję z dnia 25 listopada 2010 r. zatytułowaną „W kierunku nowej strategii energetycznej dla Europy na lata 2011-2020" ([1]),

— uwzględniając art. 48 Regulaminu,

— uwzględniając sprawozdanie Komisji Przemysłu, Badań Naukowych i Energii oraz opinie Komisji Spraw Zagranicznych, Komisji Rozwoju i Komisji Handlu Międzynarodowego (A7-0168/2012),

([1]) Dz.U. C 99 E, z 3.4.2012, s. 64.