4. zwraca się do Komisji o wsparcie państw członkowskich z myślą o zmniejszaniu zróżnicowania wynagrodzenia ze względu na płeć o co najmniej pięć punktów procentowych rocznie i całkowitym jego wyeliminowaniu do roku 2020;

5. przyznaje, że wielopoziomowe i wieloaspektowe podejście wymaga od Komisji wspierania państw członkowskich w propagowaniu dobrych praktyk i we wdrażaniu strategii politycznych na rzecz eliminowania zróżnicowania wynagrodzenia ze względu na płeć;

6. wzywa Komisję do niezwłocznego dokonania przeglądu dyrektywy 2006/54/WE oraz do zaproponowania do niej zmian zgodnie z art. 32 tej dyrektywy i na podstawie art. 157 TFUE, przy uwzględnieniu szczegółowych zaleceń przedstawionych w załączniku do rezolucji Parlamentu z dnia 24 maja 2012 r.;

7. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji i rządom państw członkowskich.

P7_TA(2013)0376

Strategia bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń

Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP))

(2016/C 093/16)

Parlament Europejski,

— uwzględniając wspólny komunikat Komisji Europejskiej i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 7 lutego 2013 r. zatytułowany „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń” (JOIN(2013)0001),

— uwzględniając wniosek Komisji z dnia 7 lutego 2013 r. dotyczący dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (COM(2013)0048),

— uwzględniając komunikat Komisji z dnia 19 maja 2010 r. zatytułowany „Europejska agenda cyfrowa” (COM(2010) 0245) oraz komunikat Komisji z dnia 18 grudnia 2012 r. zatytułowany „Europejska agenda cyfrowa – cyfrowe pobudzenie wzrostu w Europie” (COM(2012)0784),

— uwzględniając komunikat Komisji z dnia 27 września 2012 r. zatytułowany „Wykorzystanie potencjału chmury obliczeniowej w Europie” (COM(2012)0529),

— uwzględniając komunikat Komisji z dnia 28 marca 2012 r. zatytułowany „Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością” (COM(2012)0140) oraz konkluzje Rady z dnia 7 czerwca 2012 r. w tej sprawie,

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW ([1]),

— 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 ([2]),

---

([1]) Dz.U. L 218 z 14.8.2013, s. 8.
([2]) Dz.U. L 345 z 23.12.2008, s. 75.

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującą decyzję ramową Rady 2004/68/WSiSW ([1]),

— uwzględniając program sztokholmski ([2]), komunikaty Komisji zatytułowane „Przestrzeń wolności, bezpieczeństwa i sprawiedliwości dla europejskich obywateli – plan działań służący realizacji programu sztokholmskiego" (COM(2010) 0171) oraz „Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy" (COM(2010)0673), a także swoją rezolucję z dnia 22 maja 2012 r. w sprawie strategii bezpieczeństwa wewnętrznego Unii Europejskiej ([3]),

— uwzględniając wspólny wniosek Komisji i Wysokiego Przedstawiciela dotyczący decyzji Rady w sprawie ustaleń dotyczących zastosowania przez Unię klauzuli solidarności (JOIN(2012)0039),

— uwzględniając decyzję ramową Rady 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi ([4]),

— uwzględniając swoją rezolucję z dnia 12 czerwca 2012 r. w sprawie ochrony krytycznej infrastruktury teleinformatycznej – „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni" ([5]) oraz konkluzje Rady z dnia 27 maja 2011 r. w sprawie komunikatu Komisji zatytułowanego „Ochrona krytycznej infrastruktury teleinformatycznej – osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni" (COM(2011)0163),

— uwzględniając swoją rezolucję z dnia 11 grudnia 2012 r. w sprawie stworzenia jednolitego rynku cyfrowego ([6]),

— uwzględniając swoją rezolucję z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony ([7]),

— uwzględniając swoje stanowisko w pierwszym czytaniu z dnia 16 kwietnia 2013 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) (COM(2010)0521) ([8]),

— uwzględniając swoją rezolucję z dnia 11 grudnia 2012 r. w sprawie strategii wolności cyfrowej w polityce zagranicznej UE ([9]),

— uwzględniając Konwencję Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.,

— uwzględniając międzynarodowe zobowiązania Unii, wynikające w szczególności z Układu ogólnego w sprawie handlu usługami (GATS),

— uwzględniając art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 6, 8 i 11,

— uwzględniając toczące się negocjacje w sprawie transatlantyckiego partnerstwa na rzecz handlu i inwestycji (TTIP) między Unią Europejską a Stanami Zjednoczonymi Ameryki,

— uwzględniając art. 110 ust. 2 Regulaminu,

A. mając na uwadze, że rosnące wyzwania cybernetyczne w postaci coraz bardziej wyrafinowanych zagrożeń i ataków stanowią poważne zagrożenie dla bezpieczeństwa, stabilności i dobrobytu gospodarczego państw członkowskich, jak również sektora prywatnego i szerszej społeczności; mając na uwadze, że w związku z tym ochrona naszego społeczeństwa i naszej gospodarki będzie wciąż zmieniającym się wyzwaniem;

([1]) Dz.U. L 335 z 17.12.2011, s. 1.
([2]) Dz.U. C 115 z 4.5.2010, s. 1.
([3]) Teksty przyjęte, P7_TA(2012)0207.
([4]) Dz.U. L 149 z 2.6.2001, s. 1.
([5]) Teksty przyjęte, P7_TA(2012)0237.
([6]) Teksty przyjęte, P7_TA(2012)0468.
([7]) Teksty przyjęte, P7_TA(2012)0457.
([8]) Teksty przyjęte, P7_TA(2013)0103.
([9]) Teksty przyjęte, P7_TA(2012)0470.

B. mając na uwadze, że cyberprzestrzeń i bezpieczeństwo cybernetyczne powinny być jednym ze strategicznych filarów polityki bezpieczeństwa i obrony UE oraz poszczególnych państw członkowskich; mając na uwadze, że podstawowe znaczenie ma dbanie o to, by cyberprzestrzeń pozostała otwarta na swobodny przepływ idei i informacji oraz na wolność wypowiedzi;

C. mając na uwadze, że handel elektroniczny i usługi online są główną siłą internetu i mają podstawowe znaczenie dla osiągnięcia celów strategii „Europa 2020", przynosząc korzyści zarówno obywatelom, jak i sektorowi prywatnemu; mając na uwadze, że Unia musi w pełni wykorzystać potencjał i możliwości, jakie oferuje internet, w dalszym rozwijaniu jednolitego rynku, w tym jednolitego rynku cyfrowego;

D. mając na uwadze, że strategiczne priorytety przedstawione we wspólnym komunikacie w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej obejmują osiągnięcie odporności na zagrożenia cybernetyczne, ograniczenie cyberprzestępczości, opracowanie polityki obronnej i rozbudowę zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO) oraz ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla UE;

E. mając na uwadze, że systemy sieciowe i informatyczne w całej Unii są ze sobą ściśle powiązane; mając na uwadze, że ze względu na globalny charakter internetu wiele incydentów zagrażających bezpieczeństwu sieci i informacji wykracza poza granice krajowe i może zakłócić funkcjonowanie rynku wewnętrznego oraz podważyć zaufanie konsumentów do jednolitego rynku cyfrowego;

F. mając na uwadze, że bezpieczeństwo cybernetyczne w całej Unii, podobnie jak na całym świecie, jest tak duże, jak duże jest bezpieczeństwo najsłabszego ogniwa, oraz że zakłócenia w jednym sektorze lub państwie członkowskim wywierają wpływ na inny sektor lub inne państwo członkowskie, powodując skutki uboczne dotykające całą gospodarkę Unii;

G. mając na uwadze, że do kwietnia 2013 r. zaledwie 13 państw członkowskich oficjalnie przyjęło krajowe strategie bezpieczeństwa cybernetycznego; mając na uwadze, że wśród państw członkowskich wciąż istnieją zasadnicze różnice pod względem przygotowania, bezpieczeństwa, kultury strategicznej i zdolności do wypracowania i wdrożenia strategii bezpieczeństwa cybernetycznego, a także mając na uwadze, że należy przeprowadzić ocenę tych różnic;

H. mając na uwadze, że odmienna kultura strategiczna i brak ram prawnych prowadzą do rozdrobnienia jednolitego rynku cyfrowego i są głównym przedmiotem obaw; mając na uwadze, że brak ujednoliconego podejścia do bezpieczeństwa cybernetycznego stwarza poważne zagrożenia dla dobrobytu gospodarczego oraz bezpieczeństwa transakcji, oraz mając w związku z tym na uwadze konieczność wspólnych starań i zacieśnionej współpracy rządów, sektora prywatnego, organów ścigania i agencji wywiadu;

I. mając na uwadze, że cyberprzestępczość jest problemem międzynarodowym wymagającym coraz większych nakładów finansowych, który – według Biura Narodów Zjednoczonych ds. Narkotyków i Przestępczości – kosztuje obecnie gospodarkę światową 295 mld EUR każdego roku;

J. mając na uwadze, że terenem działań międzynarodowej przestępczości zorganizowanej, wykorzystującej osiągnięcia postępu technologicznego, w coraz większym stopniu staje się cyberprzestrzeń, gdzie cyberprzestępczość radykalnie zmienia tradycyjną strukturę zorganizowanych grup przestępczych; mając na uwadze, że doprowadziło to do tego, iż działalność zorganizowanych grup przestępczych w mniejszym stopniu ogranicza się do jednego obszaru i że coraz częściej wykorzystują one zasadę terytorialności oraz różne jurysdykcje krajowe na poziomie globalnym;

K. mając na uwadze, że dochodzenia w sprawie cyberprzestępczości prowadzone przez właściwe organy są wciąż utrudnione ze względu na wiele przeszkód, które obejmują wykorzystywanie w transakcjach odbywających się w cyberprzestrzeni „walut wirtualnych", których można używać do prania pieniędzy, kwestie terytorialności i granic jurysdykcji, niewystarczające zdolności do dzielenia się informacjami wywiadowczymi, brak wyszkolonego personelu oraz niespójną współpracę z innymi zainteresowanymi stronami;

L. mając na uwadze, że technologia jest filarem rozwoju cyberprzestrzeni, a ciągłe podążanie za zmianami technologicznymi ma zasadnicze znaczenie dla poprawy odporności i bezpieczeństwa UE w cyberprzestrzeni; mając na uwadze, że konieczne jest podjęcie kroków w celu zapewnienia, że prawodawstwo nadąża za nowymi zmianami technologicznymi, umożliwiając skuteczną identyfikację i ściganie cyberprzestępców oraz ochronę ofiar cyberprzestępczości; mając na uwadze, że strategia bezpieczeństwa cybernetycznego UE musi obejmować środki ukierunkowane

na propagowanie wiedzy, edukację, rozwój zespołów reagowania na incydenty komputerowe (CERT), rozwój wewnętrznego rynku produktów i usług z zakresu bezpieczeństwa cybernetycznego, a także inwestycje w badania, rozwój i innowacje;

1. z zadowoleniem przyjmuje wspólny komunikat w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej oraz wniosek dotyczący dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii;

2. podkreśla rosnące żywotne znaczenie internetu i cyberprzestrzeni dla transakcji politycznych, gospodarczych i społecznych nie tylko na terytorium Unii, lecz również transakcji, w których uczestniczą inne podmioty na całym świecie;

3. podkreśla konieczność opracowania strategicznej polityki komunikacji dotyczącej bezpieczeństwa cybernetycznego UE, sytuacji związanych z kryzysem cybernetycznym, przeglądów strategicznych, współpracy publiczno-prywatnej oraz ostrzeżeń, a także zaleceń dla ogółu społeczeństwa;

4. przypomina, że wysoki poziom bezpieczeństwa sieci i informacji jest konieczny nie tylko do utrzymania usług o zasadniczym znaczeniu dla niezakłóconego funkcjonowania społeczeństwa i gospodarki, lecz również do ochrony integralności fizycznej obywateli dzięki większej skuteczności i wydajności oraz bardziej bezpiecznemu funkcjonowaniu krytycznej infrastruktury; podkreśla, że niezależnie od konieczności poprawy bezpieczeństwa sieci i informacji ważna jest poprawa bezpieczeństwa fizycznego; podkreśla, że infrastruktura powinna być odporna zarówno na zakłócenia zamierzone, jak niezamierzone; podkreśla, że w związku z tym w strategii bezpieczeństwa cybernetycznego należy położyć większy nacisk na częste przyczyny niezamierzonych awarii systemu;

5. ponawia apel do państw członkowskich o przyjęcie bez zbędnej zwłoki krajowych strategii bezpieczeństwa cybernetycznego obejmujących aspekty techniczne oraz zagadnienia związane z koordynacją, zasobami ludzkimi i przydziałem środków finansowych, w których to strategiach uwzględniono by odmienne zasady dotyczące korzyści i obowiązków sektora prywatnego, tak aby zagwarantować ich udział; apeluje również o określenie kompleksowych procedur zarządzania ryzykiem, a także o ochronę środowiska regulacyjnego;

6. zauważa, że jedynie przywództwo oraz odpowiedzialność polityczna ze strony instytucji unijnych oraz państw członkowskich pozwolą osiągnąć wysoki poziom bezpieczeństwa sieci i informacji w całej Unii, a tym samym przyczynią się do bezpiecznego i niezakłóconego funkcjonowania jednolitego rynku;

7. podkreśla, że polityka bezpieczeństwa cybernetycznego Unii powinna zapewnić bezpieczne i wiarygodne środowisko cyfrowe, u którego podstaw leżą ochrona i zachowanie swobód oraz poszanowanie podstawowych praw w internecie i które to środowisko zostało zaprojektowane w sposób to gwarantujący, zgodnie z kartą UE oraz art. 16 TFUE, w szczególności w odniesieniu do prawa do prywatności oraz prawa do ochrony danych osobowych; sądzi, że szczególną uwagę należy zwrócić na ochronę dzieci online;

8. wzywa państwa członkowskie i Komisję do podjęcia wszelkich działań koniecznych do opracowania programów szkoleń służących uświadamianiu, poprawie umiejętności i zwiększaniu wiedzy obywateli europejskich, w szczególności w zakresie bezpieczeństwa osobistego, jako elementu programu rozwijania umiejętności cyfrowych od najmłodszych lat; przychylnie odnosi się do inicjatywy dotyczącej zorganizowania europejskiego miesiąca bezpieczeństwa cybernetycznego przy wsparciu ENISA oraz we współpracy z organami publicznymi oraz sektorem prywatnym w celu zwiększenia świadomości na temat wyzwań związanych z ochroną systemów sieciowych i informatycznych;

9. jest zdania, że kształcenie w zakresie bezpieczeństwa cybernetycznego zwiększa świadomość społeczeństwa europejskiego dotyczącą zagrożeń cybernetycznych, zachęcając tym samym do odpowiedzialnego korzystania z cyberprzestrzeni, oraz przyczynia się do rozwijania bazy umiejętności cybernetycznych; podkreśla kluczową rolę, jaka odgrywają Europol i jego nowo utworzone Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), a także ENISA i Eurojust, w zapewnianiu działań szkoleniowych na poziomie UE dotyczących korzystania z narzędzi międzynarodowej współpracy sądowej oraz organów ścigania w odniesieniu do różnych aspektów cyberprzestępczości;

10. przypomina o potrzebie zapewnienia doradztwa technicznego i informacji prawnych, jak również ustanowienia programów dotyczących zapobiegania cyberprzestępczości i zwalczania jej; zachęca do kształcenia inżynierów cybernetycznych wyspecjalizowanych w ochronie krytycznej infrastruktury i systemów informatycznych, jak również operatorów systemów kontroli transportu oraz ośrodków zarządzania ruchem; podkreśla pilną potrzebę wprowadzenia regularnych programów szkoleń z zakresu bezpieczeństwa cybernetycznego przeznaczonych dla personelu sektora publicznego na wszystkich poziomach;

11. ponawia apel o zachowanie ostrożności w nakładaniu ograniczeń na możliwości stosowania przez obywateli narzędzi komunikacyjnych i informatycznych oraz podkreśla, że państwa członkowskie powinny dążyć do tego, by opracowywane przez nie reakcje na zagrożenia i ataki cybernetyczne nigdy nie zagrażały prawom i wolnościom obywateli, a także że państwa członkowskie powinny dysponować odpowiednimi środkami prawnymi pozwalającymi na rozróżnienie incydentów cybernetycznych na poziomie obywateli oraz na poziomie wojskowym;

12. jest zdania, że działalność regulacyjna w dziedzinie bezpieczeństwa cybernetycznego powinna być ukierunkowana na ryzyko, z naciskiem na infrastrukturę krytyczną, której prawidłowe funkcjonowanie leży w ogromnym stopniu w interesie publicznym, oraz że w działalności tej należy wykorzystać czynione już przez sektor przemysłu starania o charakterze rynkowym służące zapewnieniu odporności sieci; podkreśla doniosłą rolę współpracy na szczeblu operacyjnym we wspieraniu skuteczniejszej wymiany informacji dotyczących zagrożeń cybernetycznych między organami publicznymi a sektorem prywatnym – zarówno na poziomie Unii, jak i na poziomie krajowym, jak również ze strategicznymi partnerami Unii – w celu zapewnienia bezpieczeństwa sieci i informacji dzięki wypracowaniu wzajemnego zaufania, wartości i zaangażowania, a także dzięki wymianie wiedzy specjalistycznej; jest zdania, że partnerstwo publiczno-prywatne powinno opierać się ma neutralności sieciowej i technologicznej i że powinno koncentrować się na dążeniach do zaradzenia problemom o dużym wpływie na społeczeństwo; wzywa Komisję, aby zachęcała wszystkich uczestników rynku do większej czujności i woli współpracy w celu ochrony innych uczestników przed szkodami dotyczącymi świadczonych przez nich usług;

13. przyznaje, że wykrywanie incydentów związanych z bezpieczeństwem cybernetycznym oraz zgłaszanie takich incydentów ma kluczowe znaczenie dla promowania odporności na zagrożenia cybernetyczne w Unii; uważa, że należy określić proporcjonalne i konieczne wymogi dotyczące ujawniania informacji, aby umożliwić zgłaszanie właściwym władzom krajowym incydentów związanych z poważnym naruszeniem bezpieczeństwa i tym samym umożliwić lepsze monitorowanie cyberprzestępstw oraz wesprzeć starania na rzecz podnoszenia świadomości na wszystkich szczeblach;

14. zachęca Komisję i inne podmioty do wprowadzenia polityki bezpieczeństwa cybernetycznego i polityki w zakresie odporności na zagrożenia cybernetyczne uwzględniających zachęty ekonomiczne w celu promowania wysokiego stopnia bezpieczeństwa cybernetycznego i dużej odporności na zagrożenia cybernetyczne;

Odporność na zagrożenia cybernetyczne

15. zauważa, że różne sektory i państwa członkowskie mają różne poziomy zdolności i umiejętności oraz że przeszkadza to w rozwoju opartej na zaufaniu współpracy i zakłóca funkcjonowanie jednolitego rynku;

16. uważa, że wymogi w stosunku do małych i średnich przedsiębiorstw powinny bazować na proporcjonalnym i opartym na analizie ryzyka podejściu;

17. nalega na rozwój odporności infrastruktury krytycznej na zagrożenia cybernetyczne oraz przypomina, że w zbliżających się ustaleniach w sprawie wdrożenia klauzuli solidarności (art. 222 TFUE) należy wziąć pod uwagę ryzyko ataku cybernetycznego na państwo członkowskie; wzywa Komisję oraz Wysoką Przedstawiciel do wzięcia tego ryzyka pod uwagę we wspólnych sprawozdaniach ze zintegrowanej oceny zagrożenia i ryzyka, które będą sporządzane począwszy od roku 2015;

18. podkreśla, że aby zagwarantować integralność, dostępność i poufność zwłaszcza najważniejszych służb, identyfikacja i kategoryzacja infrastruktury krytycznej musi być uaktualniana; należy również nałożyć na sieć tych służb i ich systemy informacji minimalne wymogi bezpieczeństwa;

19. uznaje, że wniosek dotyczący dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii przewiduje takie minimalne wymogi bezpieczeństwa w odniesieniu do dostawców usług społeczeństwa informacyjnego i operatorów infrastruktury krytycznej;

20. wzywa państwa członkowskie i Unię do stworzenia odpowiednich ram dla szybkich, obustronnych systemów wymiany informacji, które zagwarantują sektorowi prywatnemu anonimowość, a jednocześnie będą na bieżąco dostarczały informacje sektorowi publicznemu, a w razie konieczności, będą stanowić wsparcie dla sektora prywatnego;

21. z zadowoleniem przyjmuje pomysł Komisji stworzenia kultury zarządzania ryzykiem w odniesieniu do bezpieczeństwa cybernetycznego i wzywa państwa członkowskie oraz instytucje Unii do bezzwłocznego uwzględnienia zarządzania kryzysem cybernetycznym w ich planach zarządzania ryzykiem i analizach ryzyka; ponadto wzywa rządy państw członkowskich i Komisję do mobilizowania podmiotów sektora prywatnego, by włączały zarządzanie kryzysem cybernetycznym do swoich planów zarządzania i analiz ryzyka oraz szkoliły swoich pracowników w dziedzinie bezpieczeństwa cybernetycznego;

22. wzywa wszystkie państwa członkowskie i instytucje Unii do stworzenia sprawnie funkcjonujących sieci zespołów reagowania na incydenty komputerowe (CERT), które działałyby siedem dni w tygodniu 24 godziny na dobę; zwraca uwagę, że krajowe zespoły reagowania na incydenty komputerowe powinny być częścią efektywnej sieci, w której stosowne informacje wymienia się zgodnie z niezbędnymi standardami poufności; zauważa, że projekty parasolowe zrzeszające CERT i inne odnośne organy bezpieczeństwa mogą być użytecznym narzędziem w procesie rozwoju zaufania w kontekście transgranicznym i międzysektorowym; uznaje znaczenie sprawnej i skutecznej współpracy między CERT a innymi organami ścigania w walce z cyberprzestępczością;

23. wspiera Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w prowadzeniu działalności związanej z bezpieczeństwem sieci i informacji, w szczególności udzielając wskazówek oraz doradzając państwom członkowskim oraz wspierając wymianę najlepszych praktyk i rozwój klimatu zaufania;

24. zwraca uwagę na potrzebę wdrożenia przez branżę stosownych wymogów dotyczących bezpieczeństwa cybernetycznego w całym łańcuchu wartości w odniesieniu do produktów ICT wykorzystywanych w sieciach transportowych i systemach informacyjnych, właściwego zarządzania ryzykiem, przyjmowania norm i rozwiązań w zakresie bezpieczeństwa oraz rozwoju najlepszych praktyk i wymiany informacji w celu zagwarantowania cybernetycznie bezpiecznych systemów transportowych;

Zasoby przemysłowe i technologiczne

25. uważa, że zagwarantowanie wysokiego poziomu bezpieczeństwa sieci i informacji odgrywa kluczową rolę w zwiększaniu konkurencyjności zarówno dostawców, jak i użytkowników rozwiązań w zakresie bezpieczeństwa w Unii; uważa, że chociaż branża bezpieczeństwa informatycznego w Unii ma istotny niewykorzystany potencjał, użytkownicy prywatni, publiczni i biznesowi często nie posiadają informacji na temat kosztów i korzyści inwestycji w bezpieczeństwo cybernetyczne, a zatem nadal są podatni na zagrożenia cybernetyczne; podkreśla, że powołanie CERT jest w tym względzie istotnym czynnikiem;

26. uważa, że dostarczanie dużej liczby rozwiązań dotyczących bezpieczeństwa cybernetycznego i popyt na nie wymaga odpowiednich inwestycji w zasoby akademickie, badania i rozwój oraz rozwój wiedzy i budowanie zdolności ze strony krajowych organów odpowiedzialnych za kwestie ICT, tak aby wspierać innowacje i dostatecznie rozpowszechnić wiedzę na temat zagrożeń dla bezpieczeństwa sieci i informacji, co ma doprowadzić do utworzenia wspólnej europejskiej branży bezpieczeństwa;

27. wzywa instytucje Unii i państwa członkowskie do przedsięwzięcia koniecznych środków w celu utworzenia „jednolitego rynku bezpieczeństwa cybernetycznego", na którym użytkownicy i dostawcy mogliby robić najlepszy użytek z dostępnych innowacji, synergii i połączonej ekspertyzy, i który dopuszczałby udział MŚP;

28. zachęca państwa członkowskie do rozważenia wspólnych inwestycji w europejską branżę bezpieczeństwa cybernetycznego, idąc za przykładem innych sektorów, takich jak sektor lotnictwa;

Cyberprzestepczość

29. uważa, że działalność przestępcza w cyberprzestrzeni może mieć tak samo szkodliwy wpływ na dobro społeczeństw jak przestępstwa w realnym świecie oraz że te formy przestępczości często się wzajemnie umacniają, czego przykładem może być seksualne wykorzystywanie dzieci czy przestępczość zorganizowana i pranie pieniędzy;

30. uważa, że w niektórych przypadkach istnieje połączenie między legalną a niedozwoloną działalnością gospodarczą; podkreśla znaczenie ułatwianego przez Internet połączenia między finansowaniem terroryzmu a poważną przestępczością zorganizowaną; podkreśla, że społeczeństwo musi być informowane o tym, jak poważny charakter ma udział w cyberprzestępczości oraz o tym, że chociaż to co na pierwszy rzut oka może się wydać przestępczością, na którą jest przyzwolenie społeczne – jak nielegalne pobieranie filmów – często generuje ogromne zyski dla międzynarodowych organizacji przestępczości zorganizowanej;

31. zgadza się z Komisją, że takie same normy i zasady, jakie obowiązują poza siecią, powinny obowiązywać również w niej, a zatem, że zwalczanie cyberprzestępczości należy usprawnić za sprawą aktualnych przepisów i potencjału operacyjnego;

32. uważa, że biorąc pod uwagę, iż cyberprzestępczość funkcjonuje ponad granicami, szczególne znaczenie mają wspólne wysiłki i ekspertyza na szczeblu Unii, na szczeblu wyższym niż szczebel poszczególnych państw członkowskich, a Eurojust, należące do Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością, CERT oraz uniwersytety i ośrodki badawcze muszą mieć odpowiednie zasoby i potencjał, by właściwie funkcjonować jako centralne ośrodki wiedzy specjalistycznej, współpracy i wymiany informacji;

33. z dużym zadowoleniem przyjmuje utworzenie Europejskiego Centrum ds. Walki z Cyberprzestępczością i zachęca do przyszłego rozwoju tej agencji oraz jej kluczowej roli w koordynowaniu terminowej i sprawnej transgranicznej wymiany informacji i wiedzy specjalistycznej wspierającej wysiłki na rzecz zapobiegania cyberprzestępczości, wykrywania jej i prowadzenia dochodzeń w sprawach z nią związanych;

34. wzywa państwa członkowskie do dopilnowania, by obywatele mieli łatwy dostęp do informacji o zagrożeniach cybernetycznych oraz o tym, jak z nimi walczyć; uważa, że takie wskazówki powinny zawierać informacje o tym, jak użytkownicy mogą chronić swoją prywatność w sieci, jak wykryć i zgłosić przypadki uwodzenia (grooming), jak zainstalować oprogramowanie i zapory sieciowe (firewalls), jak zarządzać hasłami i jak rozpoznać przypadki podszywania się pod kogoś (phishing), zwabiania (pharming) i inne zagrożenia;

35. nalega na to, by państwa członkowskie, które nie ratyfikowały jeszcze Konwencji Rady Europy o cyberprzestępczości, bezzwłocznie to uczyniły; z zadowoleniem przyjmuje uwagi Rady Europy na temat potrzeby uaktualnienia konwencji w świetle postępów technologicznych, tak by zagwarantować jej stałą skuteczność w zwalczaniu cyberprzestępczości oraz wzywa Komisję i państwa członkowskie do wzięcia udziału w tej debacie; popiera starania na rzecz promowania ratyfikowania konwencji przez inne kraje oraz wzywa Komisję do aktywnego jej promowania w krajach poza Unią;

Obrona cybernetyczna

36. podkreśla, że wyzwania, zagrożenia i ataki cybernetyczne zagrażają obronie państw członkowskich i interesom bezpieczeństwa narodowego, a cywilne i wojskowe strategie na rzecz ochrony infrastruktury krytycznej powinny maksymalizować wzajemne korzyści dzięki wysiłkom na rzecz osiągnięcia synergii;

37. wzywa zatem państwa członkowskie do nasilenia współpracy z Europejską Agencją Obrony w celu opracowania wniosków i inicjatyw dotyczących potencjału obrony cybernetycznej, bazując na ostatnich projektach i inicjatywach; podkreśla potrzebę zwiększenia środków na badania i rozwój, między innymi dzięki łączeniu i udostępnianiu zasobów;

38. powtarza, że wszechstronna strategia bezpieczeństwa cybernetycznego UE powinna uwzględniać wartość dodaną istniejących agencji i organów oraz dobre praktyki uzyskane od tych państw członkowskich, które wprowadziły już swoje własne krajowe strategie bezpieczeństwaa cybernetycznego;

39. wzywa Wiceprzewodniczącą/Wysoką Przedstawiciel do uwzględnienia zarządzania kryzysami cybernetycznymi w planowaniu zarządzania kryzysowego i zwraca uwagę na potrzebę opracowania przez państwa członkowskie we współpracy z Europejską Agencją Obrony planów ochrony misji i operacji prowadzonych w ramach WPBiO przed atakami cybernetycznymi; wzywa je do wspólnego zorganizowania europejskich sił obrony cybernetycznej;

40. podkreśla dobrą praktyczną współpracę z NATO w dziedzinie bezpieczeństwa cybernetycznego oraz potrzebę nasilenia tej współpracy, w szczególności dzięki lepszej koordynacji w obszarach planowania, technologii, szkoleń i sprzętu;

41. wzywa Unię do podjęcia starań na rzecz rozpoczęcia dialogu z międzynarodowymi partnerami, w tym NATO, w celu określenia obszarów współpracy, uniknięcia powielania się działań i ich uzupełniania, tam gdzie jest to możliwe;

Polityka międzynarodowa

42. uważa, że międzynarodowa współpraca i dialog odgrywają podstawową rolę w budowie zaufania i przejrzystości oraz w promowaniu intensywnego tworzenia sieci i intensywnej wymiany informacji na szczeblu światowym; wzywa zatem Komisję i Europejską Służbę Działań Zewnętrznych do utworzenia zespołu ds. dyplomacji cybernetycznej, którego zadania obejmowałyby promowanie dialogu z podobnie myślącymi krajami i organizacjami; wzywa do bardziej aktywnego udziału UE w często odbywających się międzynarodowych konferencjach wysokiego szczebla poświęconych bezpieczeństwu cybernetycznemu;

43. uważa, że należy zachować równowagę między sprzecznymi celami transgranicznego transferu danych, ochrony danych i bezpieczeństwa cybernetycznego zgodnie z międzynarodowymi zobowiązaniami Unii, w szczególności wynikającymi z Układu ogólnego w sprawie handlu usługami (GATS);

44. wzywa Wiceprzewodniczącego/Wysokiego Przedstawiciela do włączenia wymiaru bezpieczeństwa cybernetycznego w działania zewnętrzne UE, zwłaszcza w odniesieniu do krajów trzecich, w celu zacieśnienia współpracy oraz wymiany doświadczeń i informacji na temat sposobów zapewniania bezpieczeństwa cybernetycznego;

45. wzywa Unię do podjęcia starań na rzecz rozpoczęcia dialogu z międzynarodowymi partnerami w celu określenia obszarów współpracy, uniknięcia powielania się działań i ich uzupełniania, tam gdzie jest to możliwe; wzywa Wiceprzewodniczącą/Wysoką Przedstawiciel do aktywnego działania w międzynarodowych organizacjach oraz do koordynowania stanowisk państw członkowskich dotyczących tego, jak skutecznie promować rozwiązania i politykę w dziedzinie bezpieczeństwa cybernetycznego;

46. jest zdania, że należy podjąć starania, aby zagwarantować, że istniejące międzynarodowe instrumenty prawne, w szczególności Konwencja Rady Europy o cyberprzestępczości, obowiązują w odniesieniu do cyberprzestrzeni; uważa zatem, że nie ma obecnie potrzeby tworzenia nowych instrumentów prawnych na poziomie międzynarodowym; z zadowoleniem przyjmuje jednak międzynarodową współpracę na rzecz rozwoju norm zachowania w cyberprzestrzeni, wspierając przestrzeganie w niej prawa; uważa, że należy się zastanowić nad aktualizacją istniejących instrumentów prawnych, aby odzwierciedlić postępy technologiczne; uważa, że problemy dotyczące jurysdykcji wymagają wszechstronnej debaty na temat współpracy sądowniczej oraz postępowania karnego w przypadku przestępstw o charakterze ponadnarodowym;

47. uważa, że w szczególności grupa robocza UE-USA ds. bezpieczeństwa cybernetycznego i cyberprzestępczości powinna w stosownych przypadkach służyć za instrument wymiany najlepszych praktyk w zakresie polityki bezpieczeństwa cybernetycznego między UE a USA; zauważa w tym kontekście, że obszary związane z bezpieczeństwem cybernetycznym, takie jak usługi zależne od bezpiecznego funkcjonowania systemów sieciowych i informacyjnych, zostaną uwzględnione w zbliżających się negocjacjach transatlantyckiego partnerstwa na rzecz handlu i inwestycji (TTIP), które powinny zostać zakończone w sposób, który będzie chronić suwerenność UE i niezależność jej instytucji;

48. zauważa, że umiejętności w zakresie bezpieczeństwa cybernetycznego oraz zdolność zapobiegania zagrożeniom i celowym atakom, wykrywania i skutecznego zwalczania tych ataków, nie są równomiernie rozwinięte w skali światowej; podkreśla, że starania na rzecz zwiększenia odporności na zagrożenia cybernetyczne oraz walki z zagrożeniami cybernetycznymi nie mogą się ograniczać do współpracy z partnerami myślącymi podobnie, lecz muszą również objąć regiony, gdzie zdolności, infrastruktura techniczna i ramy prawne są mniej rozwinięte; uważa, że w tej kwestii kluczowe znaczenie ma koordynacja CERT; wzywa Komisję, by ułatwiła, a w stosownych przypadkach wsparła działania krajów trzecich w budowie ich własnego potencjału w zakresie bezpieczeństwa cybernetycznego, z wykorzystaniem odpowiednich środków;

Wdrażanie

49. wzywa do dokonywania regularnej oceny skuteczności krajowych strategii bezpieczeństwa cybernetycznego na najwyższym politycznym szczeblu w celu dostosowania się do nowych światowych zagrożeń oraz zagwarantowania takiego samego poziomu bezpieczeństwa cybernetycznego w różnych państwach członkowskich;

50. wzywa Komisję do opracowania jasnego planu działania określającego ramy czasowe na osiągnięcie celów na szczeblu unijnym w ramach strategii bezpieczeństwa cybernetycznego oraz na przeprowadzenie oceny tego planu; zwraca się do państw członkowskich o uzgodnienie podobnego planu dotyczącego działań krajowych w ramach powyższej strategii;

Czwartek, 12 września 2013 r.

51. wzywa Komisję, państwa członkowskie, Europol i nowo utworzone Europejskie Centrum ds. Walki z Cyberprzestępczością, Eurojust i Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji do regularnego sporządzania sprawozdań oceniających postępy, jeśli chodzi o cele określone w strategii bezpieczeństwa cybernetycznego, łącznie z kluczowymi wskaźnikami efektywności mierzącymi postępy we wdrażaniu;

o

o o

52. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, rządom i parlamentom państw członkowskich, Europolowi, Eurojustowi oraz Radzie Europy.

P7_TA(2013)0377

Agenda cyfrowa na rzecz wzrostu, mobilności i zatrudnienia

Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie agendy cyfrowej na rzecz wzrostu, mobilności i zatrudnienia: pora przyspieszyć (2013/2593(RSP))

(2016/C 093/17)

Parlament Europejski,

— uwzględniając komunikat Komisji z dnia 18 grudnia 2012 r. zatytułowany „Europejska agenda cyfrowa – cyfrowe pobudzenie wzrostu w Europie" (COM(2012)0784),

— uwzględniając pytania skierowane do Komisji i Rady w sprawie agendy cyfrowej na rzecz wzrostu, mobilności i zatrudnienia: pora przyspieszyć (O-000085 – B7-0219/2013 i O-000086 – B7-0220/2013),

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 531/2012 z dnia 13 czerwca 2012 r. w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii ([1]),

— uwzględniając decyzję Parlamentu Europejskiego i Rady nr 243/2012/UE z dnia 14 marca 2012 r. w sprawie ustanowienia wieloletniego programu dotyczącego polityki w zakresie widma radiowego ([2]),

— uwzględniając trwające negocjacje w sprawie instrumentu „Łącząc Europę", w szczególności zmieniony wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie wytycznych dla transeuropejskich sieci telekomunikacyjnych, uchylającego decyzję nr 1336/97/WE (COM(2013)0329),

— uwzględniając swoją rezolucję z dnia 5 maja 2010 r. w sprawie nowej agendy cyfrowej dla Europy: 2015.eu ([3]),

— uwzględniając komunikat Komisji z dnia 27 września 2012 r. zatytułowany „Wykorzystanie potencjału chmury obliczeniowej w Europie" (COM(2012)0529),

— uwzględniając wniosek z dnia 25 stycznia 2012 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011),

---

([1]) Dz.U. L 172 z 30.6.2012, s. 10.
([2]) Dz.U. L 81 z 21.3.2012, s. 7.
([3]) Dz.U. C 81 E z 15.3.2011, s. 45.