P8_TA(2017)0366

Zwalczanie cyberprzestępczości

Rezolucja Parlamentu Europejskiego z dnia 3 października 2017 r. w sprawie walki z cyberprzestępczością (2017/2068(INI))

(2018/C 346/04)

Parlament Europejski,

— uwzględniając art. 2, 3 i 6 Traktatu o Unii Europejskiej (TUE),

— uwzględniając art. 16, 67, 70, 72, 73, 75, 82, 83, 84, 85, 87 i 88 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE),

— uwzględniając art. 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 i 52 Karty praw podstawowych Unii Europejskiej,

— uwzględniając międzynarodową Konwencję o prawach dziecka z dnia 20 listopada 1989 r.,

— uwzględniając Protokół fakultatywny do Konwencji o prawach dziecka w sprawie handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii z dnia 25 maja 2000 r.,

— uwzględniając deklarację sztokholmską i plan działania przyjęte podczas Pierwszego Światowego Kongresu przeciwko Seksualnemu Wykorzystywaniu Dzieci do Celów Komercyjnych, globalne zobowiązanie przyjęte na Drugim Światowym Kongresie przeciwko Seksualnemu Wykorzystywaniu Dzieci do Celów Komercyjnych w Jokohamie, zobowiązanie i plan działania przyjęte w Budapeszcie podczas konferencji przygotowawczej do Drugiego Światowego Kongresu przeciwko Seksualnemu Wykorzystywaniu Dzieci do Celów Komercyjnych,

— uwzględniając Konwencję Rady Europy o ochronie dzieci przed wykorzystywaniem seksualnym i niegodziwym traktowaniem w celach seksualnych z dnia 25 października 2007 r.,

— uwzględniając swoją rezolucję z dnia 20 listopada 2012 r. w sprawie ochrony dzieci w świecie cyfrowym ([1]),

— uwzględniając swoją rezolucję z dnia 11 marca 2015 r. w sprawie niegodziwego traktowania dzieci w celach seksualnych w internecie ([2]),

— uwzględniając decyzję ramową Rady 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi ([3]),

— uwzględniając budapeszteńską Konwencję o cyberprzestępczości z dnia 23 listopada 2001 r. ([4]) i protokół dodatkowy do niej,

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji ([5]),

([1]) Dz.U. C 419 z 16.12.2015, s. 33.
([2]) Dz.U. C 316 z 30.8.2016, s. 109.
([3]) Dz.U. L 149 z 2.6.2001, s. 1.
([4]) Rada Europy, Seria traktatów europejskich, nr 185, z 23.11.2001.
([5]) Dz.U. L 77 z 13.3.2004, s. 1.

Wtorek, 3 października 2017 r.

— 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 dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej ([2]),

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2011/93/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 ([3]),

— uwzględniając wspólny komunikat Komisji i Wiceprzewodniczącej Komisji / Wysokiej Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 7 lutego 2013 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" (JOIN(2013)0001),

— 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 ([4]),

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych ([5]) (dyrektywę w sprawie END),

— uwzględniając wyrok Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z dnia 8 kwietnia 2014 r. ([6]) stwierdzający nieważność dyrektywy w sprawie zatrzymywania danych,

— uwzględniając rezolucję z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń ([7]),

— uwzględniając komunikat Komisji z dnia 6 maja 2015 r. pt. „Strategia jednolitego rynku cyfrowego dla Europy" (COM(2015)0192),

— uwzględniając komunikat Komisji z dnia 28 kwietnia 2015 r. zatytułowany „Europejska agenda bezpieczeństwa" (COM(2015)0185) oraz następujące po nim sprawozdania z postępów pt. „Ku rzeczywistej i skutecznej unii bezpieczeństwa",

— uwzględniając sprawozdanie z konferencji dotyczącej jurysdykcji w cyberprzestrzeni, która odbyła się w Amsterdamie w dniach 7 i 8 marca 2016 r.,

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ([8]),

([1]) Dz.U. L 345 z 23.12.2008, s. 75.
([2]) Dz.U. L 201 z 31.7.2002, s. 37.
([3]) Dz.U. L 335 z 17.12.2011, s. 1.
([4]) Dz.U. L 218 z 14.8.2013, s. 8.
([5]) Dz.U. L 130 z 1.5.2014, s. 1.
([6]) ECLI:EU:C:2014:238.
([7]) Dz.U. C 93 z 9.3.2016, s. 112.
([8]) Dz.U. L 119 z 4.5.2016, s. 1.

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW ([1]),

— uwzględniając rozporządzenie (UE) 2016/794 Parlamentu Europejskiego i Rady z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) ([2]),

— uwzględniając decyzję Komisji z dnia 5 lipca 2016 r. w sprawie podpisania umowy w sprawie partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego dla badań przemysłowych i innowacji między Unią Europejską, reprezentowaną przez Komisję, i zainteresowanymi stronami (C(2016)4400),

— uwzględniając wspólny komunikat Komisji i Wiceprzewodniczącej Komisji / Wysokiej Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwaz dnia 6 kwietnia 2016 r. do Parlamentu Europejskiego i Rady w sprawie wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej (JOIN(2016) 0018),

— uwzględniając komunikat Komisji pt. „Europejska strategia na rzecz lepszego internetu dla dzieci" (COM(2012)0196) oraz sprawozdanie Komisji z dnia 6 czerwca 2016 r. pt. „Ocena końcowa wieloletniego unijnego programu ochrony dzieci korzystających z internetu oraz innych technologii komunikacyjnych (programu Bezpieczniejszy internet)" (COM(2016)0364),

— uwzględniając wspólne oświadczenie Europolu i ENISA z dnia 20 maja 2016 r. w sprawie zgodnego z prawem dochodzenia karnego z poszanowaniem ram ochrony danych w XXI wieku,

— uwzględniając konkluzje Rady z dnia 9 czerwca 2016 r. w sprawie europejskiej sieci sądowej ds. cyberprzestępczości,

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii ([3]),

— uwzględniając dokument z grudnia 2016 r. zatytułowany „ENISA's Opinion Paper on Encryption – Strong Encryption Safeguards our Digital Identity" [Opracowanie ENISA dotyczące szyfrowania – Solidne zabezpieczenia szyfrujące gwarantują naszą tożsamość cyfrową],

— uwzględniając końcowe sprawozdanie T-CY Cloud Evidence Group Rady Europy zatytułowane „Dostęp sądownictwa karnego do dowodów elektronicznych w chmurze: zalecenia do rozważenia przez T-CY" z dnia 16 września 2016 r.,

— uwzględniając prace Wspólnej Grupy Zadaniowej ds. Przeciwdziałania Cyberprzestępczości (J-CAT),

— uwzględniając sprawozdanie Europolu poświęcone ocenie zagrożenia poważną i zorganizowaną przestępczością (EU SOCTA) z dnia 28 lutego 2017 r. oraz sprawozdanie zawierające ocenę zagrożenia przestępczością zorganizowaną w internecie (EU IOCTA) z dnia 28 września 2016 r.,

— uwzględniając wyrok TSUE w sprawie C-203/15 („TELE2") z dnia 21 grudnia 2016 r. ([4]),

---

([1]) Dz.U. L 119 z 4.5.2016, s. 89.
([2]) Dz.U. L 135 z 24.5.2016, s. 53.
([3]) Dz.U. L 194 z 19.7.2016, s. 1.
([4]) Wyrok Trybunału Sprawiedliwości z dnia 21 grudnia 2016 r., *Tele2 Sverige AB przeciwko Post- och telestyrelsen* i *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.*, C-203/15, ECLI:EU:C:2016:970.

Wtorek, 3 października 2017 r.

— uwzględniając dyrektywę (UE) 2017/541 Parlamentu Europejskiego i Rady z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW ([1]),

— uwzględniając art. 52 Regulaminu,

— uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz opinię Komisji Rynku Wewnętrznego i Ochrony Konsumentów (A8-0272/2017),

A. mając na uwadze, że cyberprzestępczość powoduje coraz większe szkody społeczne i gospodarcze, wywierając wpływ na prawa podstawowe osób fizycznych, stanowiąc zagrożenie dla rządów prawa w cyberprzestrzeni oraz zagrażając stabilności społeczeństw demokratycznych;

B. mając na uwadze, że cyberprzestępczość jest narastającym problemem w państwach członkowskich;

C. mając na uwadze, że w sprawozdaniu IOCTA z 2016 r. wykazano, że cyberprzestępczość przybiera na intensywności, złożoności i skali, że w niektórych państwach UE liczba zgłaszanych przypadków cyberprzestępczości przewyższa liczbę przypadków tradycyjnej przestępczości, że cyberprzestępczość rozszerza się na inne obszary przestępczości, takie jak handel ludźmi, wykorzystywanie narzędzi szyfrujących i służących do anonimizacji do celów przestępczych, i że ataki z użyciem oprogramowania typu ransomware przewyższają tradycyjne zagrożenia złośliwym oprogramowaniem, np. trojanami;

D. mając na uwadze, że w 2016 r. liczba ataków na serwery Komisji zwiększyła się o 20 % w porównaniu z rokiem 2015;

E. mając na uwadze, że podatność komputerów na zagrożenia wynika zarówno ze specyficznej drogi rozwoju technologii informatycznej na przestrzeni lat, dynamicznego wzrostu działalności internetowej, jak i braku działań ze strony organów rządowych;

F. mając na uwadze stale rozwijający się czarny rynek w dziedzinie zinformatyzowanych wymuszeń, wykorzystywania wynajętych botnetów oraz działalności hakerów i skradzionych towarów cyfrowych;

G. mając na uwadze, że ataki cybernetyczne wciąż skupiają się przede wszystkim na złośliwym oprogramowaniu, takim jak trojany bankowe, ale rośnie liczba i wpływ ataków na sieci i systemy kontroli przemysłowej, nastawionych na zniszczenie krytycznych struktur infrastrukturalnych i gospodarczych oraz zdestabilizowanie społeczeństwa, tak jak to miało miejsce w przypadku atak oprogramowania typu ransomware o nazwie „WannaCry" z maja 2017 r., przez co stanowią one coraz większe zagrożenie dla bezpieczeństwa, obrony i innych ważnych sektorów; mając na uwadze, że większość międzynarodowych wniosków organów ścigania o dane odnosi się do oszustw i przestępstw finansowych, a następnie brutalnych i groźnych przestępstw;

H. mając na uwadze, że chociaż coraz większe wzajemne powiązanie ludzi, miejsc i rzeczy przynosi wiele korzyści, to jednocześnie zwiększa ryzyko cyberprzestępczości; mając na uwadze, że urządzenia związane z internetem rzeczy, w tym inteligentne sieci, lodówki, samochody, narzędzia medyczne lub aparaty pomocnicze, często nie są tak dobrze chronione jak tradycyjne narzędzia internetowe, przez co są idealnym celem cyberprzestępców, zwłaszcza że aktualizacja systemu bezpieczeństwa urządzeń podłączonych jest często przypadkowa lub w ogóle nie przeprowadzana; mając na uwadze, zhakowane urządzenia związane z internetem rzeczy, które posiadają fizyczne urządzenia uruchamiające lub mają możliwość sterowania, mogą stanowić faktyczne zagrożenie dla ludzkiego życia;

I. mając na uwadze, że skuteczne ramy prawne w zakresie ochrony danych mają kluczowe znaczenie dla budowania zaufania i pewności w świecie internetu, umożliwią konsumentom i przedsiębiorstwom czerpanie w pełni korzyści z jednolitego rynku cyfrowego, a jednocześnie pozwolą na walkę z cyberprzestępczością;

J. mając na uwadze, że same przedsiębiorstwa nie są w stanie sprostać wyzwaniu zapewnienia większego bezpieczeństwa w świecie wzajemnych połączeń, a rząd powinien przyczyniać się do bezpieczeństwa cybernetycznego przez tworzenie przepisów i bodźców zachęcających użytkowników do zachowywania się w sposób bezpieczny;

([1]) Dz.U. L 88 z 31.3.2017, s. 6.

K. mając na uwadze, że granice między cyberprzestępczością, szpiegostwem cybernetycznym, wojną cybernetyczną, sabotażem cybernetycznym i cyberterroryzmem stają się coraz mniej wyraźne; mając na uwadze, że cyberprzestępczość może być wymierzona przeciwko osobom fizycznym, podmiotom publicznym lub prywatnym, i że obejmuje szeroki zakres przestępstw, w tym naruszenia prywatności, niegodziwe traktowanie dzieci w celach seksualnych w internecie, publiczne nawoływanie do przemocy i nienawiści, sabotaż, szpiegostwo, przestępstwa finansowe i oszustwa, w tym oszustwa płatnicze, kradzież i kradzież tożsamości, a także nielegalne ingerowanie w system;

L. mając na uwadze, że w sprawozdaniu dotyczącym globalnych zagrożeń przedstawionym na Światowym Forum Ekonomicznym w 2017 r. wskazano masowe zjawisko kradzieży i nadużyć danych jako jedno z pięciu najważniejszych światowych zagrożeń pod względem prawdopodobieństwa wystąpienia;

M. mając na uwadze, że znaczna liczba cyberprzestępstw nie jest ścigana i pozostaje bezkarna; mając na uwadze wciąż niski poziom zgłaszania, długie okresy wykrywania umożliwiające cyberprzestępcom opracowanie wielu wejść/wyjść lub luk typu backdoor, trudny dostęp do e-dowodów, problemy z ich uzyskaniem i z ich dopuszczalnością w sądzie, a także skomplikowane procedury oraz kwestie właściwości sądu związane z transgranicznym charakterem cyberprzestępczości;

N. mając na uwadze, że w swoich konkluzjach z czerwca 2016 r. Rada podkreśliła, że ze względu na transgraniczny charakter cyberprzestępczości, a także wspólne zagrożenia dla bezpieczeństwa cybernetycznego, przed którymi stoi UE, zasadnicze znaczenie dla prowadzenia skutecznych dochodzeń w cyberprzestrzeni i uzyskiwania dowodów elektronicznych mają wzmocniona współpraca i wymiana informacji pomiędzy organami policyjnymi, sądowniczymi i ekspertami ds. cyberprzestępczości;

O. mając na uwadze, że unieważnienie przez TSUE dyrektywy w sprawie zatrzymywania danych w wyroku z dnia 8 kwietnia 2014 r. oraz zakaz ogólnego, nieograniczonego i nieukierunkowanego zatrzymywania danych potwierdzony wyrokiem TSUE w sprawie TELE2 z dnia 21 grudnia 2016 r. powoduje surowe ograniczenia odnośnie do przetwarzania masowych danych telekomunikacyjnych oraz dostępu właściwych organów do danych;

P. mając na uwadze, że w wyroku TSUE w sprawie Maximilliana Schremsa ([1]) wskazano, że masowa inwigilacja stanowi naruszenie praw podstawowych;

Q. mając na uwadze, że walka z cyberprzestępczością musi być prowadzona przy jednoczesnym poszanowaniu tych samych gwarancji proceduralnych i materialnych oraz praw podstawowych, w szczególności w odniesieniu do ochrony danych i swobody wypowiedzi, co w przypadku walki z wszelkimi innymi dziedzinami przestępczości;

R. mając na uwadze, że dzieci korzystają z Internetu w coraz młodszym wieku i są szczególnie narażone na uwodzenie i inne formy wykorzystywania seksualnego w internecie (cyberprzemoc, niegodziwe traktowanie w celach seksualnych, zmuszanie do czynności seksualnych i wymuszenie), sprzeniewierzenia danych osobowych, jak również niebezpieczne kampanie mające na celu promowanie różnego rodzaju samookaleczania się, jak w przypadku gry „Niebieski wieloryb”, i w związku z tym wymagają szczególnej ochrony; mając na uwadze, że w cyberprzestrzeni sprawcy przestępstw internetowych mogą szybciej znajdować i nagabywać ofiary za pomocą czatów, poczty elektronicznej, gier internetowych i portali społecznościowych, a ukryte sieci peer-to-peer (P2P) w dalszym ciągu stanowią główną platformę służącą sprawcom przestępstw seksualnych wobec dzieci do zdobywania, przekazywania, przechowywania i udostępniania innym materiałów związanych z wykorzystywaniem seksualnym dzieci, a także do wyszukiwania nowych ofiar bez obaw o wykrycie;

S. mając na uwadze, że coraz silniejsza tendencja zmuszanie do czynności seksualnych i wymuszania nadal nie jest dostatecznie zbadana ani zgłaszana, głównie z uwagi na charakter przestępstwa, który wywołuje u ofiar poczucie wstydu i winy;

T. mając na uwadze, że wykorzystywanie dzieci na odległość w czasie rzeczywistym jest zgłaszane jako rosnące zagrożenie; mając na uwadze, że wykorzystywanie dzieci na odległość w czasie rzeczywistym jest w najbardziej oczywisty sposób powiązane z komercyjnym rozpowszechnianiem materiałów prezentujących seksualne wykorzystywanie dziecka;

([1]) ECLI:EU:C:2015:650.

U. mając na uwadze, że w przeprowadzonym niedawno badaniu Krajowej Agencji ds. Przestępczości w Zjednoczonym Królestwie stwierdzono, że dla młodszych osób podejmujących działania hakerskie pieniądze stanowią mniej znaczące źródło motywacji, a przyczyną ataków na sieci komputerowe jest często chęć zaimponowania przyjaciołom lub walki z danym systemem politycznym;

V. mając na uwadze, że świadomość zagrożeń wynikających z cyberprzestępczości wzrosła, ale środki ostrożności ze strony indywidualnych użytkowników, publicznych instytucji oraz przedsiębiorstw nadal pozostają niewystarczające, głównie ze względu na brak wiedzy i środków;

W. mając na uwadze, że zwalczanie cyberprzestępczości i nielegalnej działalności nie powinno przysłaniać pozytywnych aspektów wolnej i otwartej cyberprzestrzeni oferującej nowe możliwości w zakresie wymiany wiedzy i wspierania włączenia politycznego i społecznego na całym świecie;

Uwagi ogólne

1. podkreśla, że gwałtowny wzrost liczby oprogramowania typu ransomware, botnetów i przypadków nieuprawnionego naruszenia systemów komputerowych ma wpływ nie tylko na bezpieczeństwo osób, dostępność i integralność ich danych osobowych, ochronę prywatności oraz podstawowych wolności, ale także na integralność infrastruktury krytycznej, w tym między innymi infrastruktury zapewniającej dostawę energii i energii elektrycznej oraz struktur finansowych, takich jak giełdy papierów wartościowych; przypomina w tym kontekście, że walkę z cyberprzestępczością uznano za działanie priorytetowe w ramach Europejskiej agendy bezpieczeństwa z dnia 28 kwietnia 2015 r.;

2. podkreśla potrzebę ulepszenia definicji cyberprzestępczości, wojny cybernetycznej, cyberbezpieczeństwa, nękania w internecie i ataków cybernetycznych, tak aby zapewnić, że instytucje UE i państwa członkowskie stosują wspólną definicję prawną tych zjawisk;

3. podkreśla, że walka z cyberprzestępczością w pierwszej kolejności powinna polegać na zabezpieczeniu i wzmocnieniu infrastruktury krytycznej i innych urządzeń połączonych w ramach sieci, a nie tylko na stosowaniu środków represji;

4. ponownie podkreśla znaczenie środków prawnych podjętych na szczeblu europejskim w celu zharmonizowania definicji przestępstw związanych z atakami na systemy informatyczne, a także z niegodziwym traktowaniem dzieci w celach seksualnych i wykorzystywaniem seksualnym dzieci w internecie oraz w celu zobowiązania państw członkowskich do stworzenia systemu rejestrowania, wytwarzania i dostarczania danych statystycznych dotyczących tych przestępstw z myślą o skuteczniejszym zwalczaniu tego rodzaju przestępstw;

5. z całą mocą wzywa państwa członkowskie, które jeszcze tego nie uczyniły, do szybkiej i prawidłowej transpozycji oraz wdrożenia dyrektywy 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej; wzywa Komisję do ścisłego zagwarantowania i monitorowania pełnego i skutecznego wdrożenia tej dyrektywy zastępującej decyzję ramową Rady 2004/68/WSiSW oraz do terminowego przedstawienia Parlamentowi i jego właściwej komisji wyciągniętych wniosków; podkreśla, że Eurojust i Europol powinny uzyskać odpowiednie zasoby w celu usprawnienia identyfikacji ofiar, zwalczania zorganizowanych siatek sprawców wykorzystywania seksualnego oraz przyspieszenia wykrywania, analizy i zgłaszania treści dotyczących wykorzystywania dzieci zarówno online, jak i offline;

6. wyraża ubolewanie nad faktem, że 80 % europejskich przedsiębiorstw doświadczyło przynajmniej jednego incydentu w zakresie bezpieczeństwa cybernetycznego i że ataki cybernetyczne wymierzone w przedsiębiorstwa często pozostają niewykryte lub nie są zgłaszane; przypomina, że z różnych badań wynika, iż roczny koszt ataków cybernetycznych dla gospodarki światowej to znacząca liczba; jest zdania, że obowiązek ujawniania przypadków naruszenia bezpieczeństwa oraz wymiany informacji o ryzyku, wprowadzony na mocy rozporządzenia (UE) 2016/679 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) oraz dyrektywy (UE) 2016/1148 w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (dyrektywa w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS), przyczyni się do rozwiązania tego problemu poprzez zapewnienie wsparcia dla przedsiębiorstw, w szczególności MŚP;

7. podkreśla, że zmieniający się stale charakter krajobrazu zagrożeń cybernetycznych stawia przed wszystkimi zainteresowanymi stronami poważne wyzwania prawne i technologiczne; jest przekonany, że nowe technologie nie powinny być postrzegane jako zagrożenie, oraz stwierdza, że postęp technologiczny w zakresie szyfrowania poprawi ogólne bezpieczeństwo naszych systemów informacyjnych, między innymi poprzez umożliwienie użytkownikom końcowym lepszej ochrony danych i połączeń; wskazuje jednak, że nadal istnieją znaczne luki w zapewnianiu bezpieczeństwa łączności oraz że techniki, takie jak trasowanie cebulowe i ukryte sieci, mogą być wykorzystywane przez

użytkowników działających w złych zamiarach, w tym terrorystów i sprawców przestępstw seksualnych wobec dzieci, wrogie obce państwa lub ekstremistyczne organizacje polityczne lub religijne do celów przestępczych, w szczególności, aby ukryć ich działalność przestępczą lub tożsamość, powodując poważne wyzwanie dla prowadzenia dochodzeń;

8. wyraża głębokie zaniepokojenie niedawnym globalnym atakiem oprogramowania typu ransomware, które zainfekowało dziesiątki tysięcy komputerów w niemal 100 państwach i licznych organizacjach, między innymi w państwowej służbie zdrowia (National Health Service) w Zjednoczonym Królestwie, będącej najważniejszą ofiarą tego masowego ataku złośliwego oprogramowania; w tym kontekście uznaje istotny wysiłek w ramach inicjatywy „No More Ransom", która zapewnia ponad 40 darmowych narzędzi do deszyfrowania, umożliwiających ofiarom ataków oprogramowania typu ransomware na całym świecie odszyfrowanie zainfekowanych urządzeń;

9. podkreśla, że ukryte sieci i trasowanie cebulowe zapewniają również wolną przestrzeń dla dziennikarzy, działaczy kampanii politycznych i obrońców praw człowieka w określonych państwach, aby uniemożliwić wykrycie tych osób przez represyjne władze państwowe;

10. zauważa, że korzystanie z narzędzi i usług cyberprzestępczych przez sieci przestępcze i terrorystyczne jest wciąż ograniczone; podkreśla jednak, że może to prawdopodobnie ulec zmianie w świetle coraz silniejszych powiązań między terroryzmem a przestępczością zorganizowaną oraz powszechnej dostępności broni palnej i prekursorów materiałów wybuchowych w ukrytych sieciach;

11. zdecydowanie potępia wszelką ingerencję w system informatyczny podjętą lub prowadzoną przez obce państwo lub jego agentów w celu zakłócenia demokratycznych procesów w innym państwie;

12. podkreśla, że transgraniczne wnioski o zajęcie domeny, usunięcie treści i dostęp do danych użytkowników stanowią poważne wyzwania wymagające podjęcia pilnych działań, ponieważ stawka jest wysoka; w tym kontekście zaznacza, że międzynarodowe ramy dotyczące praw człowieka, mające zastosowanie zarówno w internecie, jak i poza nim, stanowią istotny punkt odniesienia na szczeblu globalnym;

13. wzywa państwa członkowskie do zapewnienia ofiarom ataków cybernetycznych pełnego korzystania ze wszystkich praw zapisanych w dyrektywie 2012/29/UE oraz do wzmożenia wysiłków w celu identyfikacji ofiar i stworzenia przeznaczonych dla nich usług, w tym poprzez trwałe wsparcie Grupy Zadaniowej Europolu ds. identyfikacji ofiar; wzywa państwa członkowskie, aby we współpracy z Europolem pilnie utworzyły odnośne platformy w celu zagwarantowania, że wszyscy użytkownicy internetu wiedzą, gdzie zwrócić się o pomoc, w przypadku gdy są niezgodnie z prawem atakowani w internecie; wzywa Komisję do opracowania badania na temat skutków transgranicznej cyberprzestępczości w oparciu o dyrektywę 2012/29/UE;

14. podkreśla, że w ocenie zagrożenia wykorzystania internetu przez zorganizowane grupy przestępcze (IOCTA) opracowanej przez Europol w 2014 r. odniesiono się do potrzeby zapewnienia wydajniejszych i skuteczniejszych narzędzi prawnych z uwzględnieniem obecnych ograniczeń procesu dotyczącego traktatu o pomocy prawnej, a także, w stosownych przypadkach, podkreślono potrzebę dalszej harmonizacji prawodawstwa w całej UE;

15. podkreśla, że cyberprzestępczość poważnie zakłóca funkcjonowanie jednolitego rynku cyfrowego, ponieważ ogranicza zaufanie do dostawców usług cyfrowych, wywiera negatywny wpływ na transakcje transgraniczne i poważnie szkodzi interesom konsumentów korzystających z usług cyfrowych.

16. podkreśla, że solidne i skuteczne strategie i środki w zakresie cyberbezpieczeństwa można osiągnąć tylko wówczas, gdy będą one oparte na podstawowych prawach i wolnościach zgodnie z Kartą praw podstawowych Unii Europejskiej, oraz na podstawowych wartościach UE;

17. podkreśla, że istnieje wielka i uzasadniona potrzeba ochrony komunikacji między osobami fizycznymi oraz między tymi osobami a publicznymi i prywatnymi organizacjami w celu zapobiegania cyberprzestępczości; podkreśla, że może w tym pomóc dobra kryptografia; zaznacza ponadto, że ograniczenie korzystania z narzędzi kryptograficznych lub osłabienie ich siły doprowadzi do powstania luk, które mogą zostać wykorzystane do celów przestępczych, a także do obniżenia zaufania do usług elektronicznych, co z kolei przyniesie szkody zarówno społeczeństwu obywatelskiemu, jak i branży;

18. apeluje o opracowanie planu działań w kwestii ochrony praw dzieci w cyberprzestrzeni w trybie online i offline oraz przypomina, że w walce organów ścigania z cyberprzestępczością szczególną uwagę należy poświęcać przestępstwom popełnianym na dzieciach; podkreśla w związku z tym potrzebę zacieśnienia współpracy wymiarów sprawiedliwości i policji państw członkowskich oraz współpracy z Europolem i Europejskim Centrum ds. Walki z Cyberprzestępczością

(EC3) w celu zapobiegania cyberprzestępczości i jej zwalczania, w szczególności wykorzystywania seksualnego dzieci w internecie;

19. apeluje do Komisji i państw członkowskich o wdrożenie wszelkich środków sądowych do zwalczania zjawiska przemocy wobec kobiet w internecie i cyberprzemocy; zwraca się w szczególności do UE i państw członkowskich o połączenie sił w celu opracowania ram dotyczących przestępstw kryminalnych, zgodnie z którymi przedsiębiorstwa internetowe będą zobowiązane do usuwania albo powstrzymania przed rozprzestrzenianiem treści poniżających, obraźliwych i upokarzających; ponadto zwraca się o zapewnienie wsparcia psychologicznego dla kobiet będących ofiarami przemocy w internecie i dziewcząt, które padły ofiarą cyberprzemocy;

20. podkreśla, że nielegalne treści w internecie powinny być bezzwłocznie usuwane na mocy odpowiedniej procedury prawnej; podkreśla rolę dostawców technologii informacyjnych i komunikacyjnych, usług internetowych i hostingowych w zapewnieniu szybkiego i skutecznego usuwania nielegalnych treści w internecie na wniosek właściwego organu ścigania;

Zapobieganie

21. wzywa Komisję, aby w kontekście przeglądu europejskiej strategii bezpieczeństwa cybernetycznego w dalszym ciągu wskazywała podatności europejskiej infrastruktury krytycznej na zagrożenia dotyczące bezpieczeństwa sieci i informacji oraz zachęcała do opracowania odpornych systemów, a także oceniła stan walki z cyberprzestępczością w UE i państwach członkowskich, tak by zyskać lepszą orientację co do tendencji i nowych zjawisk w odniesieniu do przestępstw w cyberprzestrzeni;

22. podkreśla, że odporność na zagrożenia cybernetyczne ma kluczowe znaczenie w zapobieganiu cyberprzestępczości i dlatego należy nadać jej najwyższy priorytet; wzywa państwa członkowskie do przyjęcia proaktywnych strategii politycznych i działań na rzecz obrony sieci i infrastruktury krytycznej; wzywa do opracowania kompleksowego europejskiego podejścia w sprawie walki z cyberprzestępczością, które będzie zgodne z prawami podstawowymi, ochroną danych, bezpieczeństwem cybernetycznym, ochroną konsumenta i handlem elektronicznym;

23. z zadowoleniem przyjmuje w tym kontekście inwestowanie środków UE w projekty badawcze, takie jak partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego, aby zwiększyć europejską odporność na zagrożenia cybernetyczne dzięki innowacjom i budowaniu zdolności; uznaje w szczególności wysiłki partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego na rzecz opracowania odpowiednich reakcji na zagrożenia typu zero day;

24. w związku z tym podkreśla znaczenie wolnego i otwartego oprogramowania; apeluje, aby przeznaczyć więcej środków UE szczególnie na cele badań w zakresie bezpieczeństwa informatycznego w oparciu o wolne i otwarte oprogramowanie;

25. z zaniepokojeniem zauważa brak wykwalifikowanych specjalistów z dziedziny IT zajmujących się kwestiami cyberbezpieczeństwa; wzywa państwa członkowskie do inwestowania w edukację;

26. uważa, że przepisy powinny odgrywać większą rolę w zarządzaniu zagrożeniami w zakresie cyberbezpieczeństwa dzięki udoskonalonym standardom dotyczącym produktów i oprogramowania w fazie projektu oraz w odniesieniu do kolejnych aktualizacji, a także minimalnym standardom w zakresie domyślnych nazw użytkowników i haseł;

27. wzywa państwa członkowskie do zwiększenia wymiany informacji za pośrednictwem Eurojustu, Europolu i ENISA, a także do wymiany najlepszych praktyk za pośrednictwem europejskiej sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) i zespołów reagowania na incydenty komputerowe (CERT) na temat wyzwań, z którymi borykają się one w ramach walki z cyberprzestępczością, a także informacji o konkretnych rozwiązaniach prawnych i technicznych służących rozwiązaniu tych problemów i zwiększeniu odporność na zagrożenia cybernetyczne; w tym kontekście wzywa Komisję do wspierania skutecznej współpracy i ułatwiania wymiany informacji, tak aby przewidzieć potencjalne zagrożenia i zarządzać nimi zgodnie dyrektywą dotyczącą bezpieczeństwa cybernetycznego;

28. jest zaniepokojony stwierdzeniem przez Europol, że większość udanych ataków na osoby fizyczne wynika z nieprzestrzegania przez nie właściwych zachowań w internecie oraz z braku świadomości, a także z niezwracania wystarczającej uwagi na techniczne środki bezpieczeństwa, takie jak uwzględnienie bezpieczeństwa już w fazie projektowania; podkreśla, że użytkownicy są pierwszymi ofiarami niewłaściwie zabezpieczonego sprzętu i oprogramowania komputerowego;

29. wzywa Komisję i państwa członkowskie do rozpoczęcia kampanii informacyjnej z udziałem wszystkich zainteresowanych podmiotów i stron, aby wzmocnić pozycję dzieci, wspomóc rodziców, opiekunów i wychowawców w rozumieniu niebezpieczeństw istniejących w sieci i reagowaniu na nie oraz chronić bezpieczeństwo dzieci w internecie, a także do wspierania państw członkowskich w tworzeniu programów zapobiegania przypadkom niegodziwego traktowania dzieci w internecie w celach seksualnych, do promowania kampanii informacyjnych o odpowiedzialnym zachowaniu w mediach społecznościowych oraz do zachęcania najpopularniejszych wyszukiwarek i portali społecznościowych do aktywnego podejścia do ochrony bezpieczeństwa dzieci w internecie;

30. wzywa Komisję i państwa członkowskie do rozpoczęcia zwiększających świadomość kampanii informacyjnych i prewencyjnych oraz do promowania dobrych praktyk, aby zapewnić, że obywatele, a zwłaszcza dzieci i inni szczególnie narażeni użytkownicy, ale również rządy centralne i samorządy terytorialne, operatorzy o zasadniczym znaczeniu oraz podmioty sektora prywatnego są świadomi zagrożeń związanych z cyberprzestępczością, a także wiedzą, jak zachować bezpieczeństwo w internecie i jak chronić wykorzystywane urządzenia; ponadto wzywa Komisję i państwa członkowskie, aby wspierały praktyczne środki ochrony, takie jak szyfrowanie lub inne technologie służące zwiększeniu ochrony prywatności i bezpieczeństwa oraz narzędzia anonimizacji;

31. podkreśla, że kampaniom na rzecz zwiększania świadomości powinny towarzyszyć kampanie edukacyjne dotyczące „świadomego korzystania" z narzędzi technologii ICT; zachęca państwa członkowskie do uwzględnienia bezpieczeństwa cybernetycznego, jak również zagrożeń i skutków wykorzystania danych osobowych w internecie w programach edukacji informatycznej w szkołach; podkreśla w tym kontekście starania czynione w ramach europejskiej strategii na rzecz lepszego internetu dla dzieci (strategia „Bezpieczniejszy internet dla dzieci" z 2012);

32. podkreśla pilną potrzebę zapewnienia, by walka z cyberprzestępczością obejmowała wzmożone wysiłki w dziedzinie edukacji i szkoleń związanych z bezpieczeństwem sieci i informacji przez wprowadzenie szkoleń w tym zakresie, szkoleń dla studentów informatyki w zakresie bezpieczeństwa sieci i informacji, bezpiecznego oprogramowania oraz ochrony danych osobowych oraz podstawowych szkoleń w zakresie bezpieczeństwa sieci i informacji dla pracowników administracji publicznej;

33. uważa, że ubezpieczenie od ataków hakerów internetowych mogłoby stać się jednym z narzędzi pobudzających do działania w dziedzinie bezpieczeństwa zarówno przedsiębiorstwa odpowiedzialne za zaprojektowanie oprogramowania, jak i użytkowników zachęcanych do prawidłowego korzystania z oprogramowania;

34. podkreśla, że przedsiębiorstwa powinny identyfikować słabe punkty i zagrożenia dzięki regularnym ocenom, chronić swe produkty i usługi poprzez niezwłocznie usuwanie niedoskonałości, w tym poprzez politykę zarządzania zabezpieczeniami i aktualizację ochrony danych, złagodzić skutki ataków oprogramowania typu ransomware dzięki tworzeniu solidnych systemów tworzenia kopii zapasowych, a także konsekwentnie zgłaszać ataki cybernetyczne;

35. wzywa państwa członkowskie do powołania CERT-ów, do których przedsiębiorstwa i konsumenci mogą zgłaszać zawirusowane wiadomości e-mail i strony internetowe, jak przewidziano w dyrektywie w sprawie bezpieczeństwa sieci i informacji, tak aby państwa członkowskie były regularnie informowane o incydentach związanych z bezpieczeństwem oraz o środkach zwalczania i ograniczenia ryzyka w stosunku do ich własnych systemów; zachęca państwa członkowskie do rozważenia ustanowienia bazy danych służącej rejestrowaniu wszystkich rodzajów cyberprzestępczości oraz do monitorowania zmian w zakresie odnośnych zjawisk;

36. wzywa państwa członkowskie do inwestowania w infrastrukturę krytyczną i większe bezpieczeństwo związanych z nią danych, aby móc odeprzeć ataki cybernetyczne;

Wtorek, 3 października 2017 r.

Zwiększenie kompetencji i odpowiedzialności dostawców usług

37. uważa, że zacieśniona współpraca między właściwymi organami a dostawcami usług jest kluczowym czynnikiem służącym przyspieszeniu i usprawnieniu wzajemnej pomocy prawnej i procedur wzajemnego uznawania, w granicach ustanowionych w europejskim prawodawstwie; wzywa dostawców usług łączności elektronicznej niemających siedziby w Unii do wyznaczenia na piśmie swoich przedstawicieli w Unii;

38. podkreśla, że w odniesieniu do internetu rzeczy producenci są kluczowym punktem startowym dla zaostrzania systemów odpowiedzialności, czego skutkiem będzie lepsza jakość produktów i bezpieczniejsze otoczenie pod względem dostępu z zewnątrz oraz udokumentowanej możliwości aktualizacji;

39. uważa, że w kontekście tendencji w zakresie innowacji oraz coraz większej dostępności urządzeń związanych z internetem rzeczy należy zwrócić szczególną uwagę na bezpieczeństwo wszystkich, nawet najprostszych urządzeń; uważa, że w interesie producentów sprzętu komputerowego i twórców innowacyjnego oprogramowania leży inwestowanie rozwiązania służące zapobieganiu cyberprzestępczości oraz wymiana informacji na temat zagrożeń dla bezpieczeństwa cybernetycznego; wzywa Komisję i państwa członkowskie, by promowały podejście polegające na uwzględnieniu bezpieczeństwa już w fazie projektowania, i apeluje do sektora o włączenie rozwiązań w zakresie bezpieczeństwa już w fazie projektowania do wszystkich takich urządzeń; zachęca w tym kontekście sektor prywatny do wdrażania dobrowolnych środków opracowanych na mocy odnośnego prawodawstwa UE, takiego jak dyrektywa w sprawie bezpieczeństwa sieci i informacji, i zgodnych z normami uznawanymi w skali międzynarodowej, mających na celu zwiększenie zaufania do bezpieczeństwa oprogramowania i urządzeń, takich jak znak zaufania internetu rzeczy;

40. zachęca dostawców usług, aby przyjęli kodeks postępowania w dziedzinie zwalczania nielegalnej mowy nienawiści w internecie oraz wzywa Komisję i uczestniczące przedsiębiorstwa do dalszej współpracy w tym zakresie;

41. przypomina, że dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego ([1]) (dyrektywa w sprawie handlu elektronicznego) zwalnia pośredników z odpowiedzialności za treści pod warunkiem że odgrywają oni neutralną lub bierną rolę w odniesieniu do przekazanych lub udostępnionych w ramach hostingu treści, wymaga też jednak natychmiastowej reakcji w postaci usunięcia lub uniemożliwienia dostępu do treści w sytuacji, gdy pośrednik poweźmie wiedzę o naruszeniu prawa, bezprawnej działalności lub nielegalnych informacjach;

42. podkreśla bezwzględną potrzebę ochrony baz danych organów ścigania przed incydentami bezpieczeństwa i bezprawnym dostępem, gdyż jest to przedmiotem obaw obywateli; wyraża zaniepokojenie w związku z eksterytorialnym zasięgiem działania organów ścigania w zakresie dostępu do danych w kontekście dochodzenia w sprawie przestępstw, oraz podkreśla potrzebę wdrożenia surowych przepisów w tej sprawie;

43. uważa, że problemy związane z nielegalną działalnością w internecie należy rozwiązywać szybko i skutecznie, w tym poprzez procedury powiadamiania, jeżeli treść i usuwania treści, jeżeli nie są już potrzebne do wykrywania, dochodzenia i ścigania; przypomina, jeżeli usunięcie nie jest możliwe, że państwa członkowskie mogą podjąć niezbędne i proporcjonalne środki w celu zablokowania dostępu do takich treści z terytorium Unii; podkreśla, że takie środki muszą być zgodne z obowiązującymi procedurami ustawowymi i sądowymi, jak również z Kartą, i muszą być również podlegać odpowiednim zabezpieczeniom, w tym możliwości dochodzenia roszczeń na drodze sądowej;

44. podkreśla rolę podmiotów świadczących usługi społeczeństwa informacyjnego cyfrowego w zapewnianiu szybkiego i skutecznego usuwania nielegalnych treści z internetu na żądanie właściwego organu ścigania, i z zadowoleniem przyjmuje postępy poczynione w tym zakresie, również w ramach wkładu unijnego forum internetowego; podkreśla potrzebę większego zaangażowania i współpracy ze strony właściwych organów i dostawców usług społeczeństwa informacyjnego w celu szybkiego i skutecznego usuwania treści przez branżę i uniknięcia blokowania nielegalnych treści w drodze środków rządowych; apeluje do państw członkowskich o pociągnięcie do odpowiedzialności prawnej platform niezgodnych z prawem; ponownie zaznacza, że wszelkie środki usuwania nielegalnych treści w internecie oparte na warunkach użytkowania powinny być dozwolone jedynie wówczas, jeżeli krajowe przepisy postępowania zapewniają użytkownikom możliwość dochodzenia ich praw przed sądem po powzięciu wiedzy o takich środkach;

45. podkreśla, że zgodnie ze swoją rezolucją z dnia 19 stycznia 2016 r. zatytułowaną „W kierunku aktu o jednolitym rynku cyfrowym" ([2]) ograniczona odpowiedzialność pośredników ma istotne znaczenie dla ochrony otwartości internetu, praw podstawowych, pewności prawa i innowacyjności; przyjmuje z zadowoleniem zamiar Komisji, by przedstawić wytyczne dotyczące procedur zgłaszania i usuwania, aby wesprzeć platformy internetowe w wypełnianiu ich obowiązków

([1]) Dz.U. L 178 z 17.7.2000, s. 1.
([2]) Teksty przyjęte, P8_TA(2016)0009.

i przestrzeganiu przepisów dotyczących odpowiedzialności zawartych w dyrektywie o handlu elektronicznym (2000/31/WE), aby zwiększyć pewność prawa i zaufanie użytkowników; wzywa Komisję do przedstawienia wniosku ustawodawczego w tej sprawie;

46. wzywa do stosowania podejścia polegającego na podążaniu śladem pieniądza, o którym jest mowa w rezolucji Parlamentu z dnia 9 czerwca 2015 r. w sprawie dążenia do odnowy konsensusu w sprawie egzekwowania praw własności intelektualnej: plan działania UE ([1]), w oparciu o ramy regulacyjne dyrektywy w sprawie handlu elektronicznego oraz dyrektywy w sprawie egzekwowania praw własności intelektualnej;

47. podkreśla zasadnicze znaczenie zapewniania stałych i szczegółowych szkoleń oraz wsparcia psychologicznego dla moderatorów treści w podmiotach prywatnych i publicznych, które są odpowiedzialne za ocenę treści budzących wątpliwości lub nielegalnych, ponieważ powinni oni być uznawani za pierwszy poziom reakcji w tym zakresie;

48. wzywa usługodawców, aby wprowadzili jednoznaczne kategorie zgłaszania, a także utworzyli wyraźne zaplecze administracyjne, gwarantujące szybkie i odpowiednie działania następcze;

49. wzywa usługodawców do pracy nad wzmożeniem działań mających na celu informowanie o zagrożeniach internetowych, w szczególności na rzecz dzieci, przez opracowanie narzędzi interaktywnych i materiałów informacyjnych;

Zacieśnienie współpracy policyjnej i sądowej

50. wyraża zaniepokojenie faktem, że wielu sprawców cyberprzestępstw pozostaje bezkarnych; ubolewa nad stosowaniem przez dostawców usług internetowych technologii takich jak NAT CGN, które w znacznym stopniu utrudniają dochodzenia, uniemożliwiając pod względem technicznym dokładną identyfikację użytkownika adresu IP, czyli sprawstwa przestępstw internetowych; podkreśla, że należy umożliwić organom ścigania legalny dostęp do istotnych informacji w ściśle określonych okolicznościach, w których taki dostęp jest konieczny i proporcjonalny ze względów bezpieczeństwa i wymiaru sprawiedliwości; podkreśla, że organy sądowe i organy ścigania muszą zostać wyposażone w wystarczające zdolności, aby skutecznie prowadzić czynności dochodzeniowe;

51. wzywa państwa członkowskie do nienakładania na dostawców szyfrowania obowiązków, które prowadziłyby do osłabienia lub naruszenia bezpieczeństwa ich sieci i usług w wyniku stworzenia lub ułatwienia tworzenia luk w zabezpieczeniach typu backdoor; podkreśla, że wykonalne rozwiązania muszą być przewidziane zarówno w prawodawstwie, jak i wypracowane w drodze ciągłego postępu technologicznego, o ile są one konieczne dla wymiaru sprawiedliwości i bezpieczeństwa; wzywa państwa członkowskie do współpracy, w porozumieniu z przedstawicielami wymiaru sprawiedliwości i z Europolem, w drodze dostosowania warunków legalnego korzystania z narzędzi dochodzeniowych w internecie;

52. podkreśla, że zgodne z prawem przechwycenie może być bardzo skutecznym środkiem zwalczania bezprawnego hakowania, pod warunkiem że jest to środek konieczny, proporcjonalny, oparty na odpowiedniej procedurze prawnej i w pełni zgodny z prawami podstawowymi, a także z unijnymi przepisami o ochronie danych oraz z orzecznictwem; wzywa państwa członkowskie do korzystania z prawnego przechwytywania wobec podejrzanych osób, do ustanowienia przejrzystych zasad dotyczących procesu udzielania uprzedniego zezwolenia sądowego na zgodne z prawem praktyki przechwytywania, w tym ograniczeń dotyczących stosowania i trwania zgodnych z prawem narzędzi praktyk hakerskich, w celu utworzenia mechanizmu nadzoru, a także do zapewnienia skutecznych środków odwoławczych dla ofiar tych działań hakerskich;

53. namawia państwa członkowskie do współpracy ze społecznością działającą na rzecz bezpieczeństwa ICT oraz do zachęcania jej, by odgrywała czynniejszą rolę w zakresie etycznego hakerstwa i zgłaszania nielegalnych treści, takich jak materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych;

54. zachęca Europol do ustanowienia anonimowego systemu zgłaszania z ukrytych sieci, który umożliwiłby osobom fizycznym zgłaszanie właściwym organom nielegalnych treści, takich jak materiały przedstawiające wykorzystywanie seksualne dzieci, z wykorzystaniem takich samych zabezpieczeń technicznych jak te stosowane w wielu organizacjach prasowych, które korzystają z podobnych systemów, aby ułatwiać wymianę wrażliwych danych z dziennikarzami w sposób umożliwiający większą anonimowość i bezpieczeństwo niż konwencjonalne wiadomości e-mail;

([1]) Dz.U. C 407 z 4.11.2016, s. 25.

55. podkreśla, że należy zminimalizować zagrożenia dla prywatności użytkowników internetu na skutek wycieków lub z powodu narzędzi wykorzystywanych przez organy ścigania podczas dochodzeń;

56. podkreśla, że organy sądowe i organy ścigania muszą zostać wyposażone w wystarczające zdolności i środki, aby mogły skutecznie reagować na cyberprzestępczość;

57. podkreśla, że różnorodność krajowych, terytorialnych systemów prawnych utrudnia określenie prawa właściwego w transgranicznych interakcjach i przyczynia się do braku pewności prawnej, co z kolei uniemożliwia współpracę transgraniczną niezbędną do skutecznego przeciwdziałania cyberprzestępczości;

58. podkreśla konieczność opracowania konkretnych elementów na potrzeby wspólnego unijnego podejścia w dziedzinie wymiaru sprawiedliwości w cyberprzestrzeni, zgodnie z ustaleniami nieformalnego spotkania ministrów sprawiedliwości i spraw wewnętrznych z dnia 26 stycznia 2016 r.;

59. podkreśla w tym zakresie potrzebę opracowania wspólnych norm proceduralnych umożliwiających określenie czynników terytorialnych, które stanowią podstawę dla ustalenia prawa właściwego w odniesieniu do cyberprzestrzeni, oraz określenia środków dochodzeniowych, które można stosować bez względu na granice geograficzne;

60. przyznaje, że takie wspólne podejście europejskie, wymagające poszanowania praw podstawowych i prywatności, zbudowałoby zaufanie wśród zainteresowanych stron, ograniczyło opóźnienia w przetwarzaniu wniosków transgranicznych, wprowadziło interoperacyjność wśród jednolitych podmiotów i stworzyło szansę na włączenie zasad sprawiedliwego procesu do ram operacyjnych;

61. uważa, że w perspektywie długoterminowej, wspólne standardy proceduralne jurysdykcji w zakresie egzekwowania przepisów w cyberprzestrzeni należy również opracować na szczeblu globalnym; w związku z tym z zadowoleniem przyjmuje prace grupy Rady Europy zajmującej się materiałem dowodowym w chmurze;

Dowód elektroniczny

62. podkreśla, że wspólne europejskie podejście do wymiaru sprawiedliwości w sprawach karnych dotyczących cyberprzestrzeni jest kwestią priorytetową, ponieważ przyczyni się do poprawy egzekwowania praworządności w cyberprzestrzeni oraz ułatwi pozyskiwanie dowodów elektronicznych w postępowaniach karnych i przyczyni się do rozstrzygania spraw szybciej niż obecnie;

63. podkreśla potrzebę znalezienia sposobów szybszego zabezpieczania i uzyskiwania dowodów elektronicznych, a także znaczenie ścisłej współpracy między organami ścigania, w tym poprzez większe wykorzystanie wspólnych zespołów dochodzeniowo-śledczych, państwami trzecimi i dostawcami usług działającymi na terytorium europejskim, zgodnie z ogólnym rozporządzeniem o ochronie danych ((UE) 2016/679), dyrektywą (UE) 2016/680 (dyrektywa w sprawie policji) oraz obowiązującymi umowami o wzajemnej pomocy prawnej; podkreśla potrzebę utworzenia pojedynczych punktów kontaktowych we wszystkich państwach członkowskich oraz optymalnego wykorzystania istniejących punktów kontaktowych, ponieważ ułatwi to dostęp do dowodów elektronicznych, jak również wymianę informacji, lepszą współpracę z dostawcami usług oraz przyspieszy procedurę wzajemnej pomocy prawnej;

64. uznaje, że obecnie fragmentaryczne ramy prawne mogą utrudniać dostawcom wykonanie żądań organów ścigania; wzywa Komisję, by zaproponowała europejskie ramy prawne dotyczące dowodów elektronicznych, w tym zharmonizowane zasady określania statusu dostawcy krajowego lub zagranicznego, a także by nałożyła na dostawców usług obowiązek odpowiadania na wnioski z państw trzecich, które są oparte na należytej procedurze prawnej i są zgodne z europejskim nakazem dochodzeniowym (END), przy jednoczesnym uwzględnieniu zasady proporcjonalności w celu uniknięcia szkodliwego wpływu na korzystanie ze swobody przedsiębiorczości, swobody świadczenia usług i zapewnienia odpowiednich zabezpieczeń, z myślą o stworzeniu pewności prawnej, a także o zwiększeniu zdolności usługodawców i pośredników do reagowania na wnioski organów ścigania;

65. podkreśla, że wszelkie ramy w zakresie dowodów elektronicznych powinny obejmować wystarczające zabezpieczenia praw i wolności wszystkich zaangażowanych podmiotów; podkreśla, że powinno to obejmować wymóg, aby wnioski o dowody elektroniczne były w pierwszej kolejności kierowane do administratorów lub właścicieli danych, aby zapewnić poszanowanie praw przysługujących im i osobom, których dane dotyczą (np. prawa do poufności wymiany informacji lub do sądowego dochodzenia roszczeń w przypadku nieproporcjonalnego lub nieuprawnionego dostępu);

podkreśla także potrzebę zapewnienia, by wszelkie przyjęte ramy prawne chroniły usługodawców i wszystkie inne strony przed żądaniami, które prowadziłyby do kolizji przepisów prawa lub w inny sposób naruszały suwerenność innych państw;

66. wzywa państwa członkowskie do pełnego wdrożenia dyrektywy 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych w celu skutecznego zabezpieczania i uzyskiwania dowodów elektronicznych w UE (dyrektywa w sprawie END), a także do włączenia przepisów szczególnych dotyczących cyberprzestrzeni do krajowych kodeksów karnych w celu ułatwienia dopuszczalności dowodów elektronicznych w sądzie oraz wydania jaśniejszych wytycznych dla sędziów w kwestii kar za cyberprzestępczość;

67. z zadowoleniem przyjmuje trwające w Komisji prace nad platformą współpracy obejmującą bezpieczny kanał komunikacji dla cyfrowych wymian informacji w sprawie europejskich nakazów dochodzeniowych (END) w celu gromadzenia dowodów elektronicznych i odpowiedzi między unijnymi organami sądowymi; zachęca Komisję, aby we współpracy z państwami członkowskimi, Eurojustem i dostawcami usług zbadała i ujednoliciła formularze, narzędzi i procedury służące uzyskaniu zabezpieczenia i pozyskaniu dowodów elektronicznych w celu ułatwienia procesu uwierzytelniania, przyspieszenia procedur oraz zwiększenia przejrzystości i odpowiedzialności w procesie zabezpieczania i pozyskiwania dowodów elektronicznych; wzywa Agencję Unii Europejskiej ds. Szkolenia w Dziedzinie Egzekwowania Prawa (CEPOL) do opracowania modułów szkoleniowych dotyczących skutecznego wykorzystywania obecnych ram zabezpieczenia i pozyskiwania dowodów elektronicznych; podkreśla w związku z tym, że usprawnienie polityk dostawców usług pomogłoby ograniczyć niejednolitość podejść, zwłaszcza w zakresie procedur i warunków przyznawania dostępu do danych będących przedmiotem żądania;

Budowanie potencjału na szczeblu europejskim

68. wskazuje, że ostatnie zdarzenia wyraźnie świadczą o dużej podatności UE, a zwłaszcza instytucji UE, rządów krajowych i parlamentów narodowych, dużych przedsiębiorstw europejskich, europejskich infrastruktur i sieci informatycznych na zaawansowane ataki, w których wykorzystuje się złożone i złośliwe oprogramowanie; wzywa Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) do ciągłej oceny poziomu zagrożenia, a także wzywa Komisję do inwestowania w infrastrukturę informatyczną oraz ochronę i odporność infrastruktury krytycznej instytucji UE w celu zmniejszenia podatności UE na poważne ataki cybernetyczne ze strony dużych organizacji przestępczych, grup terrorystycznych lub państw;

69. uznaje istotny wkład Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3) Europolu, Eurojustu oraz ENISA w walkę z cyberprzestępczością;

70. wzywa Europol do wspierania krajowych organów ścigania w tworzeniu bezpiecznych i odpowiednich kanałów nadawczych;

71. ubolewa nad obecnym brakiem unijnych norm w zakresie szkoleń i certyfikacji; przyznaje, że przyszłe tendencje w dziedzinie cyberprzestępczości wymagają coraz większej wiedzy od osób odpowiedzialnych za jej zwalczanie; z zadowoleniem przyjmuje istniejące inicjatywy, takie jak europejska grupa ds. szkolenia i edukacji w zakresie cyberprzestępczości (ECTEG), projekt szkolenia instruktorów (TOT) i działania szkoleniowe w ramach unijnego cyklu polityki, które już obecnie torują drogę do eliminacji luk wiedzy na szczeblu unijnym;

72. wzywa CEPOL oraz europejską sieć szkolenia kadr wymiaru sprawiedliwości do rozszerzenia oferty szkoleń poświęconych zagadnieniom cyberprzestępczości przeznaczonych dla właściwych organów ścigania i organów sądowych w całej Unii;

73. podkreśla, że liczba cyberprzestępstw zgłaszanych Eurojustowi wzrosła o 30 %; wzywa do przydzielenia wystarczających środków i utworzenia w razie potrzeby dodatkowych stanowisk, aby Eurojust mógł sprostać rosnącemu obciążeniu pracą związaną z cyberprzestępczością, a także do dalszego rozwijania i umocnienia wsparcia dla prokuratorów krajowych zaangażowanych w walkę z cyberprzestępczością w sprawach transgranicznych, w tym za pośrednictwem ustanowionej niedawno europejskiej sieci sądowej ds. cyberprzestępczości;

74. zwraca się o dokonanie przeglądu mandatu ENISA i wzmocnienie krajowych agencji bezpieczeństwa cybernetycznego; wzywa do umocnienia agencji ENISA w zakresie jej zadań, personelu i zasobów; podkreśla, że nowy mandat powinien obejmować również silniejsze powiązania z Europolem oraz z zainteresowanymi stronami z branży, tak aby agencja mogła udzielać właściwym organom lepszego wsparcia w walce z cyberprzestępczością;

75. zwraca się do Agencji Praw Podstawowych (FRA) o sporządzenie praktycznego i szczegółowego podręcznika zawierającego wytyczne w sprawie nadzoru i kontroli dla państw członkowskich;

Zacieśnienie współpracy z państwami trzecimi

76. podkreśla znaczenie współpracy z państwami trzecimi w walce z cyberprzestępczością, w tym poprzez wymianę najlepszych praktyk, wspólne dochodzenia, budowania zdolności i wzajemną pomoc prawną;

77. wzywa państwa członkowskie, które tego jeszcze nie uczyniły, do ratyfikacji i pełnego wdrożenia Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. (konwencja budapeszteńska) wraz z jej protokołami dodatkowymi, oraz do jej promowania na stosownych forach międzynarodowych we współpracy z Komisją Europejską;

78. podkreśla głębokie zaniepokojenie pracami działającej przy Radzie Europy komisji na rzecz Konwencji o cyberprzestępczości związanymi z wykładnią art. 32 konwencji budapeszteńskiej, dotyczącego ponadgranicznego dostępu do przechowywanych danych („dowody w chmurze"), i sprzeciwia się zawarciu wszelkich protokołów dodatkowych lub wytycznych, które miałyby na celu rozszerzenie zakresu postanowień tego artykułu poza obecny system ustanowiony przez konwencję, który już teraz stanowi istotny wyjątek od zasady terytorialności, ponieważ mogłoby to prowadzić do nieograniczonego, zdalnego dostępu organów ścigania do serwerów i komputerów znajdujących się w innych jurysdykcjach bez stosowania porozumień o wzajemnej pomocy prawnej ani innych instrumentów współpracy sądowej wprowadzonych dla zagwarantowania poszanowania praw podstawowych jednostki, w tym ochrony danych osobowych i prawa do sprawiedliwego procesu, zwłaszcza tych przewidzianych w Konwencji Rady Europy nr 108;

79. ubolewa nad brakiem wiążącego prawa międzynarodowego w zakresie zwalczania cyberprzestępczości oraz wzywa państwa członkowskie i instytucje europejskie do działania na rzecz przyjęcia konwencji w tym zakresie;

80. wzywa Komisję do wystąpienia z wnioskiem w sprawie możliwych inicjatyw na rzecz poprawy wydajności i promowania stosowania traktatów o pomocy prawnej w celu zwalczania zjawiska przyjmowania przez państwa trzecie założenia dotyczącego jurysdykcji eksterytorialnej;

81. wzywa państwa członkowskie do zapewnienia wystarczającego budowania zdolności w związku z przetwarzaniem wniosków o wzajemną pomoc prawną w ramach dochodzeń dotyczących cyberprzestrzeni oraz do opracowania stosownych programów szkoleniowych dla pracowników odpowiedzialnych za rozpatrywanie takich wniosków;

82. podkreśla, że porozumienia o współpracy strategicznej i operacyjnej między Europolem a państwami trzecimi ułatwiają zarówno wymianę informacji, jak i współpracę w praktyce;

83. odnotowuje fakt, że największa liczba wniosków organów ścigania jest wysyłana do USA i Kanady; jest zaniepokojony tym, że wskaźnik ujawniania dokumentów dużych amerykańskich dostawców usług w odpowiedzi na wnioski ze strony europejskich organów wymiaru sprawiedliwości w sprawach karnych nie osiąga 60 %, i przypomina, że zgodnie z rozdziałem V rozporządzenia ogólnego traktaty o pomocy prawnej i inne umowy międzynarodowe są preferowanym mechanizmem umożliwiającym dostęp do danych osobowych przechowywanych za granicą;

84. wzywa Komisję do przedstawienia konkretnych środków w celu ochrony praw podstawowych osób podejrzanych lub oskarżonych w przypadku wymiany informacji między europejskimi organami ścigania a państwami trzecimi, zwłaszcza zabezpieczeń związanych z szybkim uzyskaniem – na wniosek sądu – stosownych dowodów, informacji dotyczących abonenta, szczegółowych metadanych oraz danych o treści (o ile nie są zaszyfrowane) od organów ścigania i/lub dostawców usług w celu poprawy wzajemnej pomocy prawnej;

85. wzywa Komisję, aby we współpracy z państwami członkowskimi, powiązanymi organami UE i w razie potrzeby z państwami trzecimi rozważyła nowe sposoby skutecznego zabezpieczania i uzyskiwania dowodów elektronicznych przechowywanych na serwerach w państwach trzecich, przy pełnym poszanowaniu praw podstawowych i unijnych przepisów o ochronie danych osobowych, przez przyspieszenie i usprawnienie wykorzystania procedur wzajemnej pomocy prawnej i, w razie potrzeby, wzajemnego uznawania;

86. podkreśla znaczenie Centrum Reagowania na Incydenty Komputerowe NATO (NCIRC);

87. wzywa państwa członkowskie do uczestnictwa w Globalnym Forum Wiedzy Cyfrowej (GFCE), aby ułatwić nawiązywanie współpracy i budowanie zdolności;

88. popiera pomoc UE w zakresie budowania potencjału w krajach Partnerstwa Wschodniego ze względu na to, że wiele ataków cybernetycznych pochodzi właśnie z tych państw;

o

o o

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