Maciej Górecki

„Otwarta, bezpieczna i chroniona cyberprzestrzeń" – nowa jakość internetowej komunikacji czy poważny spór wokół nowej dyrektywy Komisji Europejskiej?

Dynamicznie zmieniająca się dzięki rozwoju technicznemu przestrzeń społeczna na przełomie XX/XXI w. determinowała pojawienie się nowych mediów sieciowych[1], które wytwarzały i dystrybuowały nowe rodzaje komunikacji. Na oczach konsumentów kultury dokonało się gwałtowne przejście od transmisji do dialogu, przy jednoczesnym umasowieniu zarówno odbiorcy, jak i nadawcy przekazu[2]. Powszechna digitalizacja i cyfryzacja przyniosły nowy wymiar samookreślenia swej egzystencji – stan bycia cyfrowym[3]. Wykształ-

[1] Zdaniem Sonii Livingostone nowe media tworzą trzy grupy podmiotów: a) fizyczne przedmioty lub urządzenia, które tworzą możliwość komunikowania znaczeń i dzielenia się nimi, b) działania lub praktyki komunikacyjne realizowane podczas opracowywania tych urządzeń, c) szersze ustalenia społeczne oraz formy organizacyjne. L.A. Lievrouw, *Media alternatywne i zaangażowane społecznie*, Warszawa 2012, s. 17.

[2] A. Przybylska, *Internet i komunikowanie we wspólnocie lokalnej*, Warszawa 2010, s. 82–83.

[3] W. Krzemińska, *Co z tą cyfryzacją?*, [w:] *Cyfryzacja w procesach komunikowania*, red. W. Krzemińska, P. Nowak, Poznań 2004, s. 13.

ciło to w użytkowniku „e-tożsamość hybrydową", która wpływa na tworzenie się własnego, osobistego języka – a co za tym idzie technik komunikowania[4]. Miało do daleko idące konsekwencje, które zdaniem Beaty Maj wyrażały się w przeniesieniu do internetu życia gospodarczego, rodzinnego, religijnego, a także politycznego[5].

Aktywność w każdej z tych sfer starała się skodyfikować szereg bytów politycznych[6], z państwami na czele. Dynamicznie zmieniająca się rzeczywistość narodowa ujawniła ukierunkowane na zarządzanie siecią aspiracje innych podmiotów stosunków międzynarodowym, zwłaszcza organizacji międzynarodowych. Konieczność odgórnego administrowania powstałą technokomunikacją (tzn. komunikacją usieciowioną i sprogramatyzowaną – sterowaną odgórnie za pośrednictwem programów – mechanizmów przez trudne do zdefiniowania ośrodki decyzyjne[7]) wzrosła, gdy okazało się, że transnarodowa sieć internetowa nie może być miejscem nieskrępowanej wymiany informacji. Oparcie funkcjonowania wszystkich instytucji państwowych na komputerowych systemach zarządzania stworzyło pole dla organizacji pragnących wykraść poufne, często tajne dane z zabezpieczonych serwerów hakerów[8].

Przykładem organizacji międzynarodowej chcącej ściśle kontrolować nielegalne praktyki w internecie jest Unia Europejska. Jednym z jej priorytetów komunikacyjnych na 2013 r. było wdrożenie strategii Komisji Europejskiej i Wysokiego Przedstawiciela Unii do Spraw

---

[4] B. Olivier, *Nauki o komunikacji*, Warszawa 2010, s. 290–291.

[5] B. Maj, *Media elektroniczne jako środowisko komunikacyjne współczesnego człowieka*, [w:] *Komunikacja wobec wyzwań współczesności*, red. M. Wawrzak-Chodaczek, I. Jagoszewska, Toruń 2011, s. 118–119.

[6] W niniejszej pracy przez politykę będzie rozumiane ogół działań służących kreacji, dystrybucji i ochronie dóbr publicznych.

[7] W. Chyła, *Technokomunikacja – instrument globalizacji*, [w:] *Studia nad komunikacją popularną, międzykulturową, sieciową i edukacyjną*, red. J. Fras, Toruń 2007, s. 267.

[8] W niniejszej pracy za hakera będzie uważana osoba, której „wiedza i umiejętności pozwalają na uzyskanie nieautoryzowanego dostępu do zasobów komputera, poprzez ominięcie systemów zabezpieczających przed takim dostępem". *Ustawa podatkowa* (online), http://www.ustawa-podatkowa.pl/szkolenie-prawne/haker, *Definicja Haker*, 21.05.2013.

Zagranicznych i Bezpieczeństwa „Otwarta, bezpieczna i chroniona cyberprzestrzeń". W niniejszym artykule zostaną przedstawione: charakterystyka głównych założeń powyższego dokumentu, ocena stanu zagrożeń, jakie potencjalnie może wywołać, kontrowersje, jakie wzbudza w środowisku firm sektora prywatnego, oraz prognozy dotyczące dalszych unijnych kodyfikacji w sferze e-bezpieczeństwa.

We wstępie dokumentu podano powody, które legły u podstaw zainteresowania się Unii sferą internetu. „Nasza wolność i nasz dobrobyt w coraz większym stopniu uzależnione są od sprawnego i innowacyjnego internetu (...). Wolność w środowisku internetowym wymaga jednak również bezpieczeństwa i ochrony. Cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami (...)[9]. Analizując treść art. 1.1, można dokonać ich klasyfikacji na poszczególne kategorie:

- wykradanie danych o konsumentach i zwracanie się do korporacji z propozycjami okupów;
- ingerencje w struktury systemów informatycznych, w tym tych odpowiedzialnych za obsługę świadczenia podstawowych usług (wody, usług opieki zdrowotnej, dostaw energii elektrycznej i usług telefonii komórkowej);
- inwigilowanie i kontrolowanie obywateli przez rządy państwowe.

W celu przeciwdziałania tym praktykom Unia proponuje dwa rodzaje inicjatyw – przestrzeganie opracowanych zasad bezpieczeństwa cybernetycznego[10] oraz strategicznych priorytetów i działań.

Do pierwszej (wskazującej konieczne do bezpiecznego użytkowania internetu normy etyczne) grupy należą:

- przestrzeganie podstawowych wartości, jakimi kieruje się UE zarówno w świecie fizycznym, jak i cyfrowym;

---

[9] *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń*, art. 1.1, https://mac.gov.pl/wp-content/uploads/2013/03/JOIN2013-1-2.pdf, 28.11.2013.

[10] W świetle dokumentu: „Bezpieczeństwo cybernetyczne polega na działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury oraz zachowanie poufności zawartych w nich informacji". *Strategia bezpieczeństwa cybernetycznego...*

- ochrona praw podstawowych, wolności wypowiedzi, danych osobowych i prywatności. W tym celu proponuje się tworzenie bezpiecznych sieci i systemów, opartych na przestrzeganiu unijnych przepisów dotyczących ochrony danych;
- swobodny dostęp do internetu dla wszystkich obywateli. Zdaniem Wspólnoty każdy powinien mieć możliwość dostępu do internetu oraz do niezakłóconego przepływu informacji. Pozwoli to stopniowo eliminować jednostki wykluczone społecznie;
- demokratyczne i efektywne zarządzanie wielostronne. Odgórne i wielostronne koordynowanie internetu przez zainteresowane podmioty komercyjne i pozarządowe;
- wspólna odpowiedzialność za zapewnienie bezpieczeństwa. Wszystkie zainteresowane podmioty powinny utworzyć mechanizmy reagowania w przypadku ingerencji w bezpieczeństwo cybernetyczne.

Do drugiej grupy (której szczegółowe założenia poszczególnych priorytetów rozpatrzone zostaną w dalszej części artykułu) należą[11]:

- osiągnięcie odporności na zagrożenia cybernetyczne;
- radykalne ograniczenie cyberprzestępczości;
- opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO);
- rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego;
- ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE.

Instrumenty pierwszej z powyższych grup skupiają się wokół utworzenia takiego stanu rzeczy, który gwarantowałby rozwój wzajemnej współpracy publiczno-prywatnej. Ma ona dać możliwość szybszego, skoordynowanego reagowania na sytuacje awaryjne

[11] *Bezpieczny, otwarty internet*, Komisja Europejska. Przedstawicielstwo w Polsce (online), http://ec.europa.eu/polska/news/130207_bezpieczny_internet_pl.htm, 21.05.2013.

w sferze zagrożeń cybernetycznych oraz efektywnego wsparcia dla ustanowionej w 2004 r. Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA). Postanowienia niniejszej dyrektywy w tym zakresie korespondować mają z zapisami Dyrektywy ramowej w sprawie usług łączności elektronicznej. Nakłada ona na dostawców sieci elektronicznej obowiązek informowania o poważnych naruszeniach bezpieczeństwa[12]. Wzmacniają ją postanowienia art. 17 dyrektywy 95/46/WE oraz art. 4 dyrektywy 2002/58/WE, mówiące o zgłaszaniu właściwym organom krajowym informacji o naruszaniu danych osobowych.

Omawiane rozwiązania instytucjonalne nie zdawały zdaniem Unii egzaminu, gdyż „wciąż istnieją braki (...) zwłaszcza w zakresie zdolności krajowych, możliwości koordynacji w przypadku incydentów obejmujących więcej niż jedno państwo, jak również pod względem zaangażowania i gotowości sektora prywatnego"[13]. Dlatego też proponuje się następujące inicjatywy:

- wyznaczenie odpowiednich, mających dbać o bezpieczeństwo cybernetyczne na poziomie państwowym organów krajowych, a co za tym idzie – krajowych strategii przeciwdziałania;
- ustanowienie państwowych, współpracujących ściśle z UE, stałych zespołów reagowania (CERT) – Computer Emergency Response Team[14] w celu zwalczania nielegalnych praktyk oraz aktywne uczestnictwo w europejskim forum państw członkowskich (EFMS)[15];
- poczynienie starań w celu zaangażowania sektora prywatnego. UE krytycznie stwierdza w dokumencie, że: „W przypadku podmiotów prywatnych nadal brakuje jednak skutecznych zachęt do dostarczania wiarygodnych danych na temat incy-

[12] Art. 13a i art. 13b dyrektywy 2002/21/WE.

[13] *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń*, art. 2.1, https://mac.gov.pl/wp-content/uploads/2013/03/JOIN2013-1-2.pdf, 28.11.2013.

[14] Swój lokalny CERT ma również Polska. Wszystkie informacje dotyczącego jego działalności dostępne są na stronie: http://www.cert.pl/, 28.11.2013.

[15] Utworzone na podstawie dokumentu COM(2009) 149 jako forum współpracy w zakresie bezpieczeństwa i odporności infrastruktury informatycznej.

dentów w zakresie bezpieczeństwa sieci informacji oraz ich skutków, do systemowego przeciwdziałania zagrożeniom i do inwestowania w rozwiązania w dziedzinie bezpieczeństwa"[16]. Te z nich, które będą opracowywać precyzyjne oceny zagrożeń atakiem cybernetycznych, stosować odpowiednie strategie obrony oraz wymieniać się informacjami z właściwymi organami krajowymi, będą uznawane za bezpieczne, zdolne do ochrony umieszczonych na firmowych serwerach danych;

- dlatego też wszystkie przedsiębiorstwa prywatne „będą zobowiązane do zgłaszania właściwym organom krajowym ds. bezpieczeństwa sieci i informacji incydentów mających znaczący wpływ na ciągłość podstawowych usług i na dostawy towarów uzależnione od sieci i systemów informatycznych"[17]. Konkretne informacje dotyczące powstałych „incydentów" (lub prognoz takowych) mają być nieobjęte klauzulą tajności, publikowane na stronach krajowych organizacji ds. zwalczania cyberprzestępstw. Efektywna współpraca pomiędzy Unią a sektorem prywatnym ma być realizowana w ramach Partnerstwa publiczno-prywatnego na rzecz odporności (EP3R[18]), inicjatywy „Łącząc Europę"[19] oraz corocznych ćwiczeń z cyklu Cyber Europe i Cyber Atlantic;
- konieczność opracowywania różnorodnych działań informacyjnych. Należą do nich: a) publikowanie sprawozdań i warsztatów przez ENISA, b) wprowadzenie „prawa jazdy w dziedzinie bezpieczeństwa sieci i informacji", które stanowiłoby system certyfikacji rozwoju umiejętności administratorów stron internetowych, c) organizowanie corocznego „miesiąca

[16] *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń*, art. 2.1, https://mac.gov.pl/wp-content/uploads/2013/03/JOIN2013-1-2.pdf, 28.11.2013.

[17] Tamże.

[18] Europejskie partnerstwo publiczno-prywatne na rzecz odporności zostało zainicjowane na podstawie dokumentu COM(2009) 149.

[19] Ma ona za zadanie zapewnić wsparcie finansowe dla budowy interoperacyjności krajowych sieci online. Więcej informacji można uzyskać na stronie: https://ec.europa.eu/digital-agenda/en/connecting-europe-facility, 28.11.2013.

bezpieczeństwa informacyjnego", d) wprowadzenie od 2014 r. szkoleń związanych z bezpieczeństwem sieci i informacji w placówkach edukacyjnych, e) prowadzenie przez przedstawicieli sektora prywatnego działań informacyjnych odnośnie do bezpieczeństwa cybernetycznego, także w rozmowach z klientami.

Kolejny podjęty w Dyrektywie („Radykalne ograniczenie cyberprzestępczości") obszar przeprowadzenia koniecznych zmian dotyczy wprowadzenia rygorystycznych przepisów ochrony bezpieczeństwa w sieci. Mają być one wprowadzone w ścisłej korespondencji z zapisami konwencji budapesztańskiej (Konwencji Rady Europy o cyberprzestępczości) i Dyrektywy w sprawie zwalczania wykorzystywania seksualnego dzieci w internecie oraz pornografii dziecięcej.

Unia Europejska – zauważając, iż rozwój technik cyberprzemocy wzrasta niewspółmiernie do metod zwalczania go – proponuje tworzenie krajowych jednostek ścigania omawianych przestępstw. Komisja Europejska będzie je wspierała poprzez różnorodne instrumenty finansowania[20]. Mają one ściśle współpracować z Eurojustem oraz utworzonym przez Europol Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3[21]).

Następne postulaty oscylują wokół kwestii budowy polityki obronnej i rozbudowania zdolności w dziedzinie bezpieczeństwa cybernetycznego, w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO). W tym celu UE kładzie nacisk na rozwijanie synergii między wojskowymi a cywilnymi praktykami dotyczącymi ochrony danych w internecie. Nie chodzi jednak o powielanie działań, ale o ich koordynacje i budowę dialogu. Ma ona skupiać się na

[20] W 2013 r. będzie ona kształtowana w ramach programu „Zapobieganie i walka z przestępczością" (ISEC), w latach następnych – w ramach Funduszu Bezpieczeństwa Wewnętrznego.

[21] W komunikacie pt. „Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością" UE stwierdziła, iż do jego zadań będzie należało dostarczanie analiz i danych, wspieranie dochodzeń, zapewnianie analizy kryminalistycznej, tworzenie kanałów wymiany informacji między organami publicznymi a sektorem prywatnym.

opracowywaniu wspólnych metod zarządzania, organizacji, szkoleń, technologii, infrastruktury, logistyki[22].

Aby wszystkie powyższe idee zostały wcielone w życie, konieczna jest rozbudowa technologii informacyjno-komunikacyjnych. Mają one nie tylko lepiej chronić dane osobowe, ale przede wszystkim – nadążać za wykorzystywanymi przez hakerów nowinkami technicznymi. Dalszą konsekwencją takiej postawy jest nadzór nad wyprodukowanymi w UE i krajach trzecich sprzętem i oprogramowaniem. Będzie ono kontrolowane pod kątem spełniania standardów bezpieczeństwa i ochrony danych.

Wspomniane we wcześniejszych paragrafach zaangażowanie sektora prywatnego musi być związane ze wspieraniem produktów związanych z bezpieczeństwem cybernetycznym. W niniejszym artykule proponuje się w tym zakresie: a) stosowanie etykiet świadczących o właściwym poziomie zabezpieczenia produktów lub znaków typu „kite mark", b) wspieranie i stymulowanie popytu na produkty tego typu, c) utworzenie platformy publiczno-prywatnej, która miałaby na celu wykształcenie dobrych praktyk wspólnego zwalczania nielegalnych procederów w internecie oraz zachęcanie przedsiębiorców do wdrażania bezpiecznych cybertechnologii, d) pomoc UE w tworzeniu krajowych systemów certyfikacji, e) tworzenie bezpiecznych łańcuchów dostaw w sektorach energetyki i transportu, f) wykorzystywanie programów wspierających badania naukowe w dziedzinie bezpieczeństwa, w tym „Horyzont 2020"[23].

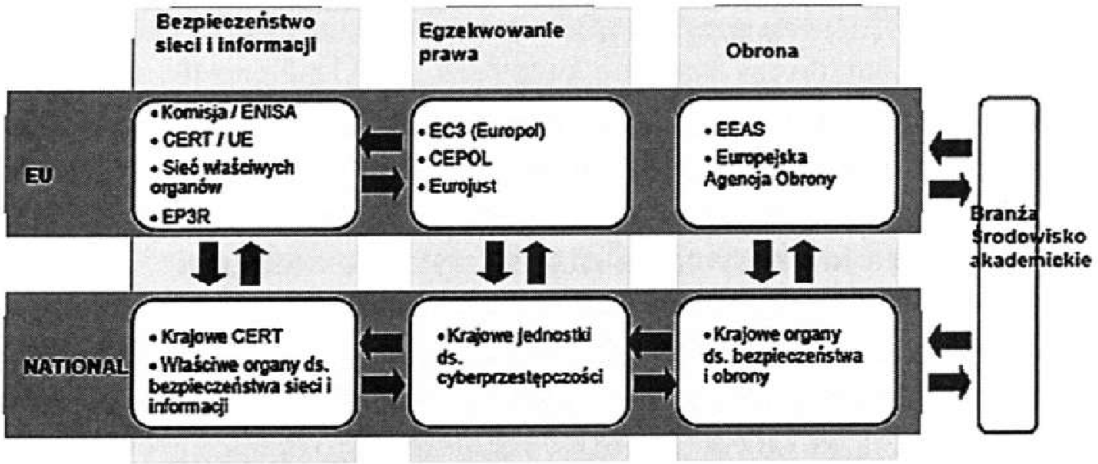
Ostatni, piąty paragraf dotyczy ustanowienia spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE. Wspólnota będzie podejmować wszelkie działania w celu likwidacji przepaści cyfrowej i wolnego, a zarazem bezpiecznego internetu, w którym przestrzegane są prawa podstawowe (należą do nich: a) opracowanie nowych,

[22] *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń*, art. 2.3, https://mac.gov.pl/wp-content/uploads/2013/03/JOIN2013-1-2.pdf, 28.11.2013.

[23] *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń*, art. 2.4, https://mac.gov.pl/wp-content/uploads/2013/03/JOIN2013-1-2.pdf, 28.11.2013.

dotyczących wolności w internecie wytycznych jurysdykcjonalnych, b) monitorowanie eksportu produktów i usług, c) przeciwdziałanie cenzurze lub masowej inwigilacji przy pomocy technik teleinformatycznych, d) stosowanie technologii teleinformatycznych w celu propagowania niniejszych praw)[24]. W związku z tym kształtowana będzie ścisła współpraca z Radą Europy, OECD, ONZ, OBWE, NATO, Unią Afrykańską, ASEAN i OPA. Jednocześnie Unia podkreśla, że odpowiedzialność za bezpieczeństwo cybernetyczne ponoszą różnorodne podmioty, w tym: administracje rządowe, krajowe CERT i organy ścigania, ale także obywatele.

Koordynacja wszystkich powyższych działań ma się odbywać na trzech szczeblach – krajowym, unijnym i międzynarodowym. Szczegółowo mechanizmy reagowania opisuje schemat 1.



Schemat 1. Bezpieczeństwo cybernetyczne – koordynacja w 3 sferach („bezpieczeństwo sieci i informacji"; „egzekwowanie prawa"; „obrona")

Źródło: *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń*, art. 4, https://mac.gov.pl/wp-content/uploads/2013/03/JOIN2013-1-2.pdf, 28.11.2013.

[24] Jednocześnie Unia podkreśla, że jej celem nie jest tworzenie nowych regulacji prawnych, a oparcie się na Międzynarodowym Pakcie Praw Obywatelskich i Politycznych, Karcie Praw Podstawowych UE, Europejskiej Konwencji Praw Człowieka oraz konwencji budapesztańskiej.

W części „Wnioski i dalsze działania" zapisano, iż niniejsze idee zostaną zrealizowane tylko w przypadku efektywnie rozwijanego partnerstwa pomiędzy wszystkimi podmiotami. Kluczowa będzie w tym wola współdecydowania o własnym bezpieczeństwie sektora obywatelskiego oraz społeczeństwa obywatelskiego.

Powyższe zapisy nie spowodowały jednak oczekiwanej przez instytucje europejskie współpracy i konsolidacji, a rozpętały „cyberburzę". Kontrowersje dotyczyły zwłaszcza zaangażowania, wielokrotnie wspominanego, sektora prywatnego. Wielu jego przedstawicieli (szacuje się, że zmiany objęłyby ok. 40 tys. zarejestrowanych w UE podmiotów) – w tym banki, sieci transportowe, administrację publiczną i sieci społecznościowe – zobligowanych w Artykule 2.1 do przekazywania informacji o atakach na ich systemy informacyjne stanowczo zaprotestowało. Ich głos wyraziło Forum Bezpieczeństwa Informacji (ISF) zrzeszające takie koncerny jak IBM, Nokia, Procter & Gamble.

Wiceprezes instytucji Steve Durbin oświadczył: „(...) publikacja informacji o incydencie może mieć znaczący wpływ nie tylko na reputację, ale i wartość firmy, a w skrajnym przypadku może nieść poważniejsze konsekwencje niż rzeczywiste zdarzenie"[25]. Innymi słowy – największym europejskim potentatom biznesowym nie zależało na powiększeniu cyberbezpieczeństwa kosztem straty zysków, spowodowanych informacją o nieszczelności ochrony ich serwerów.

Słowa krytyki nowej inicjatywy Komisji Europejskiej i Komisarz ds. Agendy Cyfrowej Neelie Kroes wyraziły także wyspecjalizowane firmy zajmującej się analizą i wykrywaniem cyberataków, z SophosLabs na czele. Przedstawiciel firmy, James Lane, stwierdził, że Wspólnota wyważa już otwarte drzwi, nie dostrzegając roli i skuteczności Komputerowych Zespołów Reagowania Kryzysowego. Wskazuje on, iż w świecie, w którym hakerzy stosują coraz to nowe metody przywłaszczania sobie osobistych danych, Unia musiałaby stworzyć bardzo szerokie, wykraczające poza omawianą dyrektywę mechanizmy. W praktyce ich akceptacja byłaby niemożliwa do

[25] A. Kaźmierska, *Spór o cyberprzestrzeń w Unii*, „Rzeczpospolita" (online), http://www.rp.pl/ artykul/984323.html, 30.05.2013.

ratyfikowania przez państwa członkowskie. Dlatego też J. Lane, podając przykład skuteczności działania brytyjskiej agencji zwalczającej internetowe procedery, optuje za wspieraniem państwowych jednostek tego typu[26]. Poszczególne zapisy wywołały też konsternacje przedstawicieli sektora finansowego, odpowiedzialnych już wcześniej za wdrażanie poszczególnych, wewnętrznych przepisów. Powstała niejasność (przepisy branżowe – wdrażanie dyrektywy) spowodowała jednoznaczną reakcję Brytyjskiego Centrum Ochrony Narodowej Infrastruktury. Instytucja wyraziła obawę, iż implementacja poszczególnych zapisów może być aktem zabłacania „dotąd czystej wody" – tzn. komplikowania jasnych przepisów prawnych z zakresu ochrony cyfrowych informacji w państwach członkowskich Wspólnoty[27].

Założenia Dyrektywy stwarzają pole do podejmowania rozmaitych dotyczących jej przyszłości prognoz. Niezależnie od nich w dokumencie „Table on the Implementation of the *Cybersecurity Stra tegy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1)" (z 28 lutego 2014 r.) opublikowany został wykaz implementacji najważniejszych założeń dokumentu. Należały do nich:

- szeroka aktywność Wspólnego Centrum Badawczego Komisji Europejskiej oraz tzw. Grupy Zadaniowej ds. Inteligentnych Sieci mających za zadanie ochronę szeroko pojętej cyberprzestrzeni;
- powołanie przez KE w 2013 r. Zaawansowanego Centrum Cyber Obrony, powołanego do walki ze złośliwym oprogramowaniem typu Malware i Botnets;
- wspólne prace ENISY oraz ekspertów nad opracowaniem projektu mapy drogowej dla budowy systemu bezpiecznej sieci i chronionej informacji. Powołanie w Strategii Cyberbezpieczeństwa Unii Europejskiej skoordynowanej platformy publiczno-prywatnej NIS (Network and Information Security);
- Przyjęcie zapisów dwóch kluczowych dyrektyw: 2011/93/EU z 13 grudnia 2011 r. w sprawie zwalczania wykorzystywania

[26] Tamże.

[27] *Mixed reaction to EC's cyber security plan*, http://www.computerweekly.com/news/2240177685/Mixed-reaction-to-ECs-cyber-security-plan, 19.05.2014.

seksualnego dzieci i pornografii dziecięcej oraz 2013/40/EU z 12 sierpnia 2013 r. w sprawie ataków na systemu informacyjne;

- efektywne działanie Europejskiej Grupy Szkoleniowej ds. Cyberprzęstępczości i Edukacji, mającej na celu koordynacje organów ścigania z poszczególnych państw Wspólnoty;
- uruchomienie działalności następujących instytucji: Globalnego Sojuszu Przeciw Wykorzystywaniu Seksualnego Dzieci, Europejskiego Centrum Cyberprzemocy (współpracującego z Europolem i Eurojustem).

Każda jurysdykcyjna ochrona prowokuje pytania o wolność i suwerenność. Być może opór opinii publicznej wobec inicjatywy KE intensyfikował charakter poszczególnych artykułów – idealistyczny, życzeniowy, koncyliacyjny, nawołujący wszystkie podmioty do współpracy, niezastanawiający się nad oczekiwaniami i interesami zainteresowanych. W efekcie większa część podmiotów prywatnych odwróciła się od niego. Należy zatem zadać pytanie – czy zarysowanie jeszcze bardziej szczegółowej, trwałej, tworzącej sieć wzajemnych korzyści platformy współpracy zmieniłoby optykę sektora prywatnego? I wreszcie – czy próba szerokiej kodyfikacji ochrony sieci nie wzbudziłaby kontrowersji społecznych, podobnych do tych ratyfikacji ACTA?

Zauważalny impas na linii Unia–sektor prywatny prowokuje pytania o możliwe alternatywy Dyrektywy. Wydaje się, że z którąś z zasygnalizowanych powyżej będzie się musiała Komisja zmierzyć. Europa ma do wyboru: pozostawienie istniejącego *status quo* z niedoregulowaną strefą e-ochrony i głośnym sprzeciwem korporacji transnarodowych albo stanowcze dążenie do ratyfikacji nowych i surowych przepisów. Dałyby one bezpieczeństwo, ale także sprzeciw użytkowników portali społecznościowych i innych „konsumentów" internetu. Obserwacja wygranej którejś z opcji będzie niezwykle interesująca.

Wygrana opcji nastawionej na poszerzanie zakresu ochrony informacji w internecie będzie świadczyć o zgodności 28 państw w czasach kryzysu (o której braku rozpisują się poszczególne media), ale i stopniowym ograniczaniu całkowitej wolności w sieci. Wygrana

pierwszej – triumf wielkich pieniędzy nad szczytnymi ideami. Warto śledzić rozwój spraw w niniejszej tematyce (Dyrektywa została opublikowana w lutym 2013 r.) – gdyż wskazuje on, w którą stronę zmierza Europa i świat. Odpowiedź na zawarte w tytule pytanie: czy analizowana Dyrektywa jest wyrazem nowej jakości internetowej komunikacji czy zarzewiem trudnego do rozwiązania sporu, jest niejednoznaczna. To, czy stanie się ona efektywnym narzędziem, zależy od woli współpracy obu mających sprzeczne interesy środowisk. Dopóki wielkie koncerny nie przyjmą forowanej przez UE wizji bezpieczeństwa, trudno będzie ją egzekwować.

Maciej Górecki

"Open, safe and secure cyberspace" – a new quality of web communication or a serious dispute over the new directive of the European Commission?

The article aims to present the controversy among the representatives of the European private sector that has raised because of one of the priorities of the European Commission communication in 2013 – "Directive open, safe and secure cyberspace". Its legal articles (concerning the need to inform about hacker attacks on private servers) divided opinion on the Old Continent. This paper presents the main assumptions of the document, the analysis of the disputed wording, and forecasts of possible solutions concerning analysis of the so called "cyber-stalemate".