Anna Kańciak

Bezpieczeństwo w cyberprzestrzeni i społeczeństwo informacyjne jako przedmioty analiz naukowych i debat publicznych

(Podsumowanie inicjatyw krajowych w pierwszej połowie 2013 r.)

Znaczenie bezpieczeństwa obywateli korzystających z systemów technologii informacyjno-komunikacyjnych (TIK) z każdym dniem wzrasta. Potrzeba zwiększenia świadomości użytkowników tych technologii odnośnie do tej kwestii, przy jednoczesnej intensyfikacji działań właściwych organów ścigania, i podejmowanie inicjatyw w tym zakresie przez kompetentne podmioty administracji państwowej stały się przedmiotem analiz i badań środowisk akademickich oraz tematem debat publicznych.

Zakres tematyczny inicjatyw poświęconych bezpieczeństwu w cyberprzestrzeni może wydawać się dość wąski, problematyka bezpieczeństwa cyberprzestrzeni, określanej piątym wymiarem, a potocznie sprowadzanej po prostu do bezpieczeństwa korzystania z Internetu, jest jednak wielowątkowa. Obejmuje ona różnorodne zagadnienia, m.in. z zakresu informatyki, techniki czy prawa i ma w dalszej perspektywie wpływ na wszystkie obszary ludzkiej aktywności. W rezultacie można wskazać na różne aspekty cyberprzestrzeni, uwzględniając przy tym jej wymiar ludzki (skupiający się na aktywności użytkowników) oraz wymiar techniczny.

Swobodne i bezrefleksyjne korzystanie z Internetu oraz rosnąca cyberprzestępczość są jednym z problemów organów ścigania i wymiaru sprawiedliwości, a w konsekwencji przedmiotem intensywnych prac zmierzających do wprowadzenia zmian w systemie prawnym. Zakładają one takie kwestie, jak egzekwowanie obowiązków, korzystanie z praw oraz implementację i przestrzeganie międzynarodowych regulacji. Całość tych działań powinna współgrać z postępem technologicznym, aktywnością jednostek naukowych oraz potrzebami sektora prywatnego.

Rozwój możliwości technologicznych wymusza także konieczność przeprowadzenia rewizji metod działania organów ścigania oraz wprowadzenia nowych norm prawnych. Bezpieczeństwo systemów informacyjno-komunikacyjnych tworzących krytyczną infrastrukturę informatyczną[1] (ang. *critical information infrastructures* – CII) nadaje kierunek i kształt nowym międzynarodowym inicjatywom legislacyjnym mającym wpływ na regulacje krajowe.

Znaczenie i możliwości cyberprzestrzeni są również zauważane w wymiarze ekonomicznym. Cyfryzacja działalności gospodarczej, a przez to rynku krajowego i międzynarodowego, może przyczynić się do szybszego wyjścia państw Unii Europejskiej z kryzysu ekonomicznego[2].

Trzecim aspektem zapewnienia bezpieczeństwa cyberprzestrzeni, po prawnym i ekonomicznym, jest aspekt społeczny. Podkreślane są w tym zakresie pozytywne strony cyfryzacji procesów edukacyjnych, w których ramach można wskazać naukę czytel-

[1] Zgodnie z definicją zaproponowaną w *Zielonej Księdze w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej* z 17.11.2005 r., COM(2005) 576 końcowy, s. 21.

[2] Szerzej zob. A. Kańciak, *Jednolity rynek cyfrowy*, „Prawo Europejskie w Praktyce" 2013, nr 2 (104), s. 85–92.

niczo-medialną, elektroniczne usługi biblioteczne czy edukację językową[3]. Cyfryzacja ma również swój wymiar kryminologiczny i wiktymizacyjny, których zakres zwiększa się wraz z procesem digitalizacji kolejnych sektorów gospodarki, administracji oraz życia społecznego.

Inicjatywy poświęcone przestrzeni cyfrowej, podejmowane w pierwszej połowie 2013 r., odzwierciedlają szeroki zakres wyzwań i możliwości, jakie daje cyberprzestrzeń zarówno w wymiarze ludzkim, jak i technicznym. Analizując wydarzenia na arenie krajowej poświęcone temu zagadnieniu, można wyróżnić trzy grupy podmiotów aktywnie podejmujących tę problematykę.

Zdecydowanie wiodącą grupę podmiotów, podejmujących inicjatywy poświęcone cyberprzestrzeni, stanowią ośrodki naukowe i akademickie. Również zakres tematyczny rozpatrywanych przez nie zagadnień jest odmienny. Na problem społeczny oraz wymiar ludzki cyberprzestrzeni wskazano na międzynarodowej konferencji naukowej pt. „Www. Człowiek w cyberprzestrzeni. Konteksty pedagogiczne i społeczne”[4]. Tematem przewodnim tego spotkania było funkcjonowanie człowieka w wirtualnej przestrzeni, na wszystkich etapach jego życia i rozwoju. Celem konferencji było określenie obszarów, zasad i metod korzystania z multimediów we współczesnym środowisku edukacyjnym i wychowawczym oraz przedstawienie możliwości i problemów związanych z miejscem i rolą elektronicznych mediów w społeczeństwie[5].

Spotkaniem, które z kolei zwróciło uwagę na kryminogenny aspekt cyberprzestrzeni, była trzecia ogólnopolska konferencja dotycząca problematyki cyberprzestępczości i cyberbezpieczeństwa – Ataki Sieciowe 2013[6]. Podczas tego spotkania prawnicy, informatycy, specjaliści z branży IT oraz przedstawiciele administracji państwowej dyskutowali nad zagadnieniem współczesnych zagrożeń związanych z rozwojem Internetu. Zwrócono uwagę na techniczne aspekty działania struktur typu botnet[7] oraz jego wykorzystania do popełniania cyberprzestępstw, trendy w urządzeniach mobilnych, a także na możliwości wykorzystania portali społecznościowych do zbierania materiału dowodowego. W ramach jednego z wystąpień zaprezentowano sposób wykradania danych w trakcie ataku komputerowego. W aspekcie prawnym natomiast poruszono kwestię obowiązków organów państwa oraz podmiotów prywatnych w celu zapobiegania cyberatakom o charakterze międzynarodowym, stanowiącym szkodę transgraniczną wyrządzoną przy wykorzystaniu infrastruktury informatycznej. Z kolei przedstawiciele administracji państwowej podczas tego spotkania poruszyli kwestię bezpieczeństwa polskich sieci w zestawieniu z danymi światowymi oraz temat roli Rządowego Centrum

[3] Szerzej zob. J. Bednarek, A. Andrzejewska, *Cyberświat. Możliwości i zagrożenia*, Warszawa 2009, Wydawnictwo Akademickie „Żak”.

[4] Konferencja zorganizowana przez Wyższą Szkołę Biznesu w Dąbrowie Górniczej w dniach 12–13 marca 2013 r.

[5] Szerzej zob. http://www.wsb.edu.pl/index.php?idg=mwe.

[6] Konferencja odbyła się w dniach 18–19 marca 2013 r. na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu.

[7] Pojęcie botnet oznacza *sieć komputerów zarażonych złośliwym oprogramowaniem (wirusami komputerowymi). Taka sieć zainfekowanych komputerów (tzw. zombie) może zostać aktywowana do wykonywania szczególnych zadań, takich jak ataki na systemy informatyczne (cyberataki). Owe komputery „zombie” można kontrolować – często bez wiedzy użytkowników zainfekowanych komputerów – z innego komputera* […] nazywanego również „centrum dowodzenia i kontroli” (ang. *command-and-control centre*). Szerzej zob. *Wniosek. Dyrektywa Parlamentu Europejskiego i Rady dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW*, Bruksela, 30.09.2010 r., KOM(2010)517 wersja ostateczna, 2010/0273 (COD).

Bezpieczeństwa w ochronie cyberprzestrzeni[8]. Odmiennemu zagadnieniu, bo cyfryzacji i informatyzacji administracji publicznej, była z kolei poświęcona konferencja naukowa w Lublinie[9]. Podczas tej debaty poruszono takie kwestie, jak informatyzacja zamówień publicznych, funkcjonowanie e-sądów oraz automatyzacja decyzji jako przykłady tzw. e-administracji.

Przekrój tematyczny przywołanych konferencji naukowych stanowi potwierdzenie nie tylko szerokiego zakresu przedmiotowego problematyki dotyczącej cyberprzestrzeni, ze wszystkimi elementami składającymi się na jej wymiar techniczny i ludzki. Stanowi również dowód ważkości i aktualności tematu, ale też jest wyrazem większej świadomości negatywnych stron cyfryzacji ludzkiej aktywności. Proces cyfryzacji, co potwierdzają wspomniane wyżej spotkania naukowe, stanowi wyzwanie dla wymiaru sprawiedliwości, organów porządku publicznego i administracji państwowej. Piętrzące się pytania o bezpieczeństwo, o granice wolności, legalności, a w aspekcie społecznym – również moralności, stanowią asumpt do kolejnych prac na poziomie naukowym. Bezsprzecznym atutem przytoczonych spotkań jest każdorazowe angażowanie przez ośrodki naukowe przedstawicieli administracji oraz praktyków zajmujących się na co dzień ochroną systemów technologii komunikacyjno-informatycznych. Udział przedstawicieli Ministerstwa Sprawiedliwości, Rządowego Centrum Bezpieczeństwa[10], czy CERT.GOV nadaje każdej debacie akademickiej wymiar praktyczny i odrzuca zarzut pozostawania prac naukowych w sztywnych ramach pracy akademickiej.

Program wspomnianych konferencji wskazuje również na kolejny istotny aspekt bezpieczeństwa w cyberprzestrzeni, jakim jest zagadnienie ochrony danych osobowych w Internecie. Stąd wśród prelegentów wielu spotkań naukowych pojawia się Główny Inspektor Ochrony Danych Osobowych. Anonimowość, charakterystyczna cecha aktywności w cyberprzestrzeni, przez wielu ekspertów traktowana jako konieczny element definicyjny tego pojęcia, staje się największym zagrożeniem dla bezpieczeństwa w tym zakresie. Odnosi się to zarówno do ochrony użytkowników, jak i krytycznej infrastruktury informatycznej. GIODO podczas spotkań naukowych poddaje pod rozwagę kwestię granicy pomiędzy wolnością wypowiedzi, ochroną prywatności, a koniecznością zapewnienia oczekiwanego przez użytkownika minimalnego poziomu bezpieczeństwa przez kompetentne podmioty. Problematyka ochrony danych osobowych w cyberprzestrzeni stanowi, co podkreślał dr Wojciech Wiewórkowski podczas konferencji w Toruniu, aktualny temat prac na forum unijnym w gronie grupy roboczej ds. ochrony danych ustanowionej na mocy art. 29 dyrektywy 95/46/WE[11], organu skupiającego inspektorów ochrony danych osobowych, Europejskiego Inspektora Ochrony Danych oraz Komisję Europejską. W kontekście problematyki cyberbezpieczeństwa ochrona danych osobowych powinna być elementem kluczowym. Mimo to została

[8] http://www.atakisieciowe.umk.pl/ [dostęp: 18 III 2013].

[9] Konferencja odbyła się 20 maja 2013 r. z inicjatywy Koła Naukowego Studentów Administracji Katolickiego Uniwersytetu Lubelskiego.

[10] http://rcb.gov.pl/.

[11] Grupa robocza ds. ochrony danych (Article 29 Data Protection Working Party) ustanowiona na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. zajmuje się zapewnieniem wiedzy eksperckiej z poziomu krajowego dla Komisji Europejskiej w zakresie problematyki ochrony danych, promowaniem jednolitych standardów Dyrektywy 95/46 we wszystkich państwach członkowskich UE, jak również Norwegii, Lichtensteinu oraz Islandii, doradzaniem Komisji we wszystkich sprawach z zakresu prawa Unii Europejskiej, które może mieć wpływ na prawo do ochrony danych osobowych, http://www.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29 [dostęp: 20 VI 2013].

pominięta w komunikacie opracowanym wspólnie przez Komisję Europejską i Wysokiego Przedstawiciela Unii do spraw Zagranicznych i Polityki Bezpieczeństwa[12] stanowiącym kompleksową strategię na rzecz zabezpieczenia sieci w UE przed cyberprzestępczością.

W świetle toczącej się debaty na forum krajowym i międzynarodowym wydaje się, że zagadnienie ochrony danych osobowych w przestrzeni cyfrowej stanowi trudny i kontrowersyjny temat do dyskusji z uwagi na odmienne argumenty i racje zaangażowanych podmiotów. Przykładem jest wypracowana w gronie ekspertów *Polityka ochrony cyberprzestrzeni RP*[13], która chociaż jest zgodna z ustawą o ochronie danych osobowych[14], to pomija czynnik ludzki, nie tylko z zakresie jego roli w cyberprzestrzeni[15], lecz także jako przedmiotu ochrony.

Kolejną grupą, po ośrodkach naukowych, organizującą spotkania w związku ze swoją działalnością poświęconą problematyce związanej z cyberprzestrzenią są podmioty prywatne, stowarzyszenia oraz fundacje. Należy zaznaczyć, że problematyka podejmowana przez te podmioty dotyczy niemal wyłącznie technicznego wymiaru cyberprzestrzeni. Przykładem takiej inicjatywy jest konferencja CONFidence[16], podczas której uczestnicy dyskutowali m.in. na temat niewidocznych ataków wewnątrz sieci i problematyki ich wykrywania oraz omawiali wyniki badań z zakresu hackowania urządzeń wbudowanych, a w szczególności niedużych urządzeń sieciowych czy niekonwencjonalnych sposobów wyłapywania bugów[17]. Innymi, podobnych rozmiarów, spotkaniami o zbliżonej tematyce były Kongresy Bezpieczeństwa Sieci[18] oraz konferencja „Open Source Day 2013"[19]. Do listy spotkań poświęconych podobnym zagadnieniom

[12] *Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a ‚Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union*. Szerzej zob. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf [dostęp: 20 VI 2013].

[13] *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej*, Warszawa, 18 września 2012 r., http://mac.bip.gov.pl/prawo-i-prace-legislacyjne/polityka-ochrony-cyberprzestrzeni-rp-resortowe-zglaszanie-uwag-do12-10-2012.html [dostęp: 20 VI 2013].

[14] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz.U. z 2002 r. Nr 101, poz. 926, z późn. zm.

[15] J. Świątkowska, *Projekt „Polityka ochrony cyberprzestrzeni RP" Nowa jakość czy stare problemy?*, Brief programowy Instytutu Kościuszki, listopad 2012, http://ik.org.pl/cms/wp-content/uploads/2012/11/Brief_Programowy_IK_POCRP_listopad_2012.pdf [dostęp: 20 VI 2013].

[16] Konferencja poświęcona tematyce bezpieczeństwa IT – CONFidence odbyła się w dniach 28–29 maja 2013 r. w Krakowie. CONFidence powstał w 2005 r. jako projekt stworzony przez grupę entuzjastów zainteresowanych poprawą bezpieczeństwa systemów operacyjnych i aplikacji. W ciągu kilku lat przeobraził się on w największe spotkanie hackerów w Polsce. Co roku CONFidence gromadzi prawie 400 uczestników – specjalistów ds. bezpieczeństwa IT z rządu, przemysłu, sektora bankowego i środowisk akademickich, a także naukowców i twórców oprogramowania. Konferencja odbywa się dwa razy w roku: w maju w Krakowie oraz w listopadzie w innym państwie europejskim. Szerzej zob. http://2013.confidence.org.pl/about-confidence [dostęp: 20 VI 2013].

[17] Bug – błąd oprogramowania lub w żargonie informatycznym – usterka programu komputerowego powodująca jego nieprawidłowe działanie, wynikająca z błędu człowieka na jednym z etapów tworzenia oprogramowania, zwykle podczas tworzenia kodu źródłowego, choć niekiedy także na etapie projektowania, http://www.curylo.info/index.php/slownik-informatyczny-termin-bug.htm [dostęp: 21 VI 2013].

[18] 9. Kongres Bezpieczeństwa Sieci, 20 lutego 2013 r. Warszawa, szerzej zob. http://gigacon.org/kbs_2013_wawa, X Kongres Bezpieczeństwa Sieci, 21 maja 2013 r. Wrocław, szerzej zob. http://gigacon.org/kbs_wro/2013 [dostęp: 21 VI 2013].

[19] Konferencja „Open Source Day 2013", zorganizowana przez Linux Polska sp. z o. o., http://opensourceday.pl/.

należy dodać także konferencję poświęconą bezpieczeństwu i niezawodności systemów informatycznych, podczas której poruszono szeroki zakres tematyczny: od zarządzania bezpieczeństwem informacji, systemów audytu bezpieczeństwa, systemów kontroli włamań, poprzez oprogramowania i urządzenia szyfrujące, aż po zarządzanie tożsamością, kontrolę dostępu i bezpieczeństwo transakcji elektronicznych[20].

Pierwszą połowę 2013 r. zamyka druga edycja konferencji na temat bezpieczeństwa nowej generacji[21], zaliczana do grupy największych spotkań krajowych w dziedzinie problematyki bezpieczeństwa w cyberprzestrzeni. Podczas tego spotkania eksperci krajowi i zagraniczni z branży IT poruszyli m.in. takie zagadnienia, jak: ataki APT[22], cyberszpiegostwo i cyberterroryzm, ochrona danych osobowych, aktualne tematy dotyczące bezpieczeństwa danych firmowych i pracy w sieci, oceny systemów zabezpieczeń pod kątem jakości i wydajności oraz zarządzanie tożsamością[23].

Większość aspektów bezpieczeństwa w cyberprzestrzeni poruszonych podczas wymienionych spotkań nierzadko pozostaje dla zdecydowanej części użytkowników Internetu na wysokim poziomie szczegółowości i wymaga wiedzy eksperckiej. Lukę pomiędzy konferencjami naukowymi skierowanymi głównie do studentów i pracowników naukowych a inicjatywami eksperckimi ukierunkowanymi na sektor informatyczny wypełniają spotkania organizowane przez organy administracji państwowej. Ich zaletami, z perspektywy obywatela, są: wyższy poziom ogólności pozwalający zrozumieć problematykę bez konieczności odwoływania się do specjalistycznej terminologii i wiedzy eksperckiej, dostępność wynikająca z braku odpłatności za udział w spotkaniach oraz możliwość bezpośredniego kontaktu z przedstawicielami administracji państwowej.

Przykładem tego rodzaju aktywności poświęconej różnym aspektom cyberprzestrzeni są debaty publiczne organizowane pod patronatem GIODO oraz Ministra Administracji i Cyfryzacji. Obszerna lista spotkań, podczas których przedstawiciele administracji publicznej uczestniczą w rozmowach na temat bezpieczeństwa w cyberprzestrzeni oraz ochrony użytkowników Internetu, jest dostępna na stronach poszczególnych urzędów. Na uwagę zasługuje debata z udziałem ministra Michała Boniego oraz przedstawiciela Komisji Europejskiej, której tematem przewodnim była ochrona danych osobowych[24]. Spotkanie, osadzone w szerszym kontekście planowanej z inicjatywy Komisji Europejskiej kompleksowej reformy przepisów o ochronie danych, miało przybliżyć kierunek prac prowadzonych w tym zakresie i stanowisko polskiego rządu dotyczące tej kwestii. Debata publiczna nie pozwoliła na przedyskutowanie wszystkich aspektów projektów Komisji, które służą aktualizacji i modernizacji dyrektywy o ochronie da-

[20] Szerzej: http://eib.edu.pl/patronat-eib-konferencja-bezpieczenstwo-i-niezawodnosc-systemow-informatycznych-2013/ [dostęp: 20 VI 2013].

[21] Konferencja „Next Generation SECURITY Conference" odbyła się w dniach 12–13 czerwca 2013 r. w Warszawie. Szerzej zob. http://www.ubucentrum.net/2013/05/ngsec-2013-jedna-z-najwiekszych-w.html [dostęp: 20 VI 2013].

[22] Ataki typu APT (ang. *advanced persistent threats*) są złożonymi, długotrwałymi i wielostopniowymi działaniami skierowanymi przeciwko konkretnym osobom, organizacjom lub firmom. Wykorzystywane programy i narzędzia są tworzone i użytkowane w sposób minimalizujący szansę wykrycia niepożądanej aktywności przez atakowaną organizację. Więcej zob. http://www.egospodarka.pl/92420,Ocena-ryzyka-lekarstwem-na-cyberataki-typu-APT,1,12,1.html [dostęp: 20 VI 2013].

[23] Więcej zob. http://di.com.pl/news/48221,0,Next_Generation_Security_2013_-_konferencja_o_bezpieczenstwie_w_branzy_IT_juz_w_czerwcu.html [dostęp: 23 VI 2013].

[24] Debata publiczna z udziałem wiceprzewodniczącej Komisji Europejskiej Viviane Reding odbyła się 13 maja 2013 r. w Szkole Głównej Handlowej. Szerzej zob. https://mac.gov.pl/dzialania/michal-boni-zacheca-do-debaty-o-ochronie-danych-osobowych-potrzebujemy-cyfrowej-umowy-spolecznej/ [dostęp: 20.6.2013].

nych z 1995 r.[25] Przybliżono jednak najważniejsze dotychczas przygotowane inicjatywy, tj. komunikat[26] polityczny określający cele reformy oraz dwa wnioski ustawodawcze. Pierwszy z nich jest rozporządzeniem na temat unijnych ram ochrony danych. Drugi to dyrektywa w sprawie ochrony danych osobowych przetwarzanych na potrzeby zapobiegania przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania oraz powiązanych działań wymiaru sprawiedliwości w sprawach karnych[27]. Przywołana debata, mająca zapoznać jej uczestników z pracami na forum unijnym i z inicjatywami Komisji Europejskiej, a także kierunkiem działania polskiego rządu w tym zakresie, była kolejnym spotkaniem Ministerstwa Administracji i Cyfryzacji z podmiotami zainteresowanymi przedmiotowymi zmianami w ramach rozpoczętego cyklu konsultacji społecznych.

Bezpieczeństwo podmiotów aktywnie działających w cyberprzestrzeni jest, obok ochrony systemów technologii informacyjno-komunikacyjnej, czy w szerszym kontekście, krytycznej infrastruktury informatycznej, zagadnieniem coraz częściej pojawiającym się podczas debat publicznych i inicjatyw organów administracji państwowej. Obywatele nie są wyłącznie użytkownikami Internetu. Inicjatywy legislacyjne oraz pozalegislacyjne podejmowane w Unii Europejskiej, które nadają kierunek pracom na poziomie krajowym, podkreślają rosnącą rolę społeczeństwa informacyjnego. Pojęcie to, choć utożsamiane z XXI wiekiem i nadejściem ery cyfrowej, pojawiło się w literaturze już w pierwszej połowie lat 60. XX w.[28] Z kolei do unijnego ustawodawstwa weszło z początkiem lat 90.[29], stając się po dwudziestu latach jednym z priorytetów Europejskiej Agendy Cyfrowej[30].

Społeczeństwo informacyjne, jako jedno z założeń długoterminowej strategii państwa[31], jest przedmiotem dyskusji oraz wiodącym tematem spotkań organizowanych przez organy administracji państwowej. Do najważniejszych wydarzeń poświęconych temu zagadnieniu należy zaliczyć coroczne[32] obchody Światowego Dnia Społeczeństwa

---

[25] *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*, Dziennik Urzędowy L 281 z 23 listopada 1995 r. poz. 0031–0050.

[26] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:PL:PDF [dostęp: 20 VI 2013].

[27] http://europa.eu/rapid/press-release_IP-12-46_pl.htm [dostęp: 20 VI 2013].

[28] Szerzej zob. J.S. Nowak, *Społeczeństwo informacyjne – geneza i definicje*, w: *Społeczeństwo informacyjne. Doświadczenie i przyszłość*, G. Bliźniuk, J.S. Nowak (red.), Katowice 2006, Polskie Towarzystwo Informatyczne, Oddział Górnośląski, s. 15, http://www.silesia.org.pl/upload/Nowak_Jerzy_Spoleczenstwo_informacyjne-geneza_i_definicje.pdf [dostęp: 21 VI 2013].

[29] *Growth, competitiveness, employment. The challenges and ways forward into the 21st century*, White Paper, 5 December 1993COM(93) 700, Bulletin of the European Communities, Supplement 6/93. http://europa.eu/documentation/official-docs/white-papers/pdf/growth_wp_com_93_700_parts_a_b.pdf [dostęp: 20 VI 2013].

[30] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska agenda cyfrowa*, Bruksela 26.08.2010, KOM(2010) 245 wersja ostateczna/2 [dostęp: 21 VI 2013].

[31] *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*, grudzień 2008 r., MSWiA, http://szs.mac.gov.pl/portal/SZS/495/6271/Strategia_rozwoju_spoleczenstwa_informacyjnego_w_Polsce_do_roku_2013__dokument_p.html [dostęp: 21 VI 2013].

[32] Światowy Dzień Społeczeństwa Informatycznego jest obchodzony 17 maja zgodnie z rezolucją Zgromadzenia Ogólnego ONZ z dnia 27 marca 2006 r. (A/RES/60/252) http://www.unic.un.org.pl/wsis/tunis/ [dostęp: 23 VI 2013].

Informatycznego zorganizowane przez Polskie Towarzystwo Informatyczne (PTI)[33]. Do inicjatyw, które poruszają problematykę tzw. włączenia obywatela, tj. zaangażowania go do aktywnego tworzenia i kształtowania społeczeństwa informatycznego, należy zaliczyć spotkania ministra administracji i cyfryzacji w ramach debaty pt. *Państwo 2.0. Obywatele źródłem wiedzy i rozwiązań*[34].

Swój udział w rozwijaniu wiedzy na temat społeczeństwa informacyjnego mają również ośrodki naukowe, aktywnie angażujące przedstawicieli administracji państwowej. Do inicjatyw proponowanych przez nie należy zaliczyć m.in. międzynarodową konferencję naukową „Internet w społeczeństwie informacyjnym"[35], czy konferencję poświęconą problemom społeczeństwa informacyjnego[36]. Podczas każdego z tych wydarzeń podkreślono aktywną rolę człowieka w cyberprzestrzeni, który jest nieodłącznym elementem całości społeczności internetowej. Systemy informacyjno-komunikacyjne przynoszą użytkownikom znaczące korzyści (np. korzystanie z cyfryzacji sektora publicznego w ramach elektronicznych usług administracji publicznej, z digitalizacji sektora edukacyjnego czy z dużych możliwości społeczno-kulturalnych), co przekłada się na wzrost poziomu społeczeństwa oraz rozwój ekonomiczny. Należy jednak pamiętać, że cyberprzestrzeń jest również obszarem działalności kryminogennej, stwarzającej różnego rodzaju zagrożenia, często niedostrzegane przez społeczność internetową. W związku z powyższym powstaje konieczność kształtowania postaw i świadomości użytkowników systemów informacyjno-komunikacyjnych w zakresie przestępczości w przestrzeni cyfrowej, w tym pojawia się potrzeba rozpowszechniania prawnych, administracyjnych i społecznych metod ochrony systemów TIK oraz ochrony ich użytkowników.

Przegląd podejmowanych inicjatyw, zarówno naukowych, jak i organizowanych przez organy państwowe czy ośrodki niepubliczne, pokazuje szeroki zakres zagadnień wynikających z cyfryzacji życia społecznego, postępu cywilizacyjnego oraz związanych z tym potrzeb ekonomicznych. Przytoczone wydarzenia, bez względu na ich zakres tematyczny oraz charakter, nie są jednak w stanie kompleksowo objąć wszystkich aspektów cyberprzestrzeni. Z tego powodu dodatkowo podejmowane są inicjatywy poświęcone szeroko pojętemu bezpieczeństwu, organizowane zarówno w formie konferencji naukowych, jak i debat publicznych, zwoływane przez organy administracji państwowej. Wydarzenia te już jako stały punkt programu poruszają problematykę bezpieczeństwa w cyberprzestrzeni jako kluczowego aspektu bieżącej polityki bezpieczeństwa. Przykładem może być konferencja poświęcona bezpieczeństwu i ciągłości funkcjonowania organów państwa w obliczu aktualnych zagrożeń[37], nad którą patronat merytoryczny sprawowało Rządowe Centrum Bezpieczeństwa[38]. Podczas tego spotka-

[33] http://sdsi.pti.org.pl/index.php/pol/Program-obchodow [dostęp: 21.6.2013].

[34] Debata „Państwo 2.0. Obywatele źródłem wiedzy i rozwiązań" odbyła się 27 czerwca 2013 r. w Bibliotece Uniwersyteckiej w Warszawie.

[35] VIII Międzynarodowa Konferencja Naukowa „Internet w społeczeństwie informacyjnym", odbyła się w Dąbrowie Górniczej w dniach 25–26 kwietnia 2013 r. Szerzej zob. http://iwsi.pl/ [dostęp: 21 VI 2013].

[36] XVI Ogólnopolska Konferencja Naukowa z cyklu: „Problemy Społeczeństwa Informacyjnego, PSI2013, Realne przestępstwa w wirtualnym świecie" odbyła się 10 maja 2013 r. na Uniwersytecie Szczecińskim. Szerzej zob. http://infotrendy.eu/psi2013/okonferencji [dostęp: 27 VI 2013].

[37] II Konferencja Zarządzania Ciągłością Działania pt. „Zapewnienie bezpieczeństwa i ciągłości funkcjonowania organów państwa w obliczu dzisiejszych zagrożeń" odbyła się w dniach 4–5 czerwca 2013 r. w Szczytnie i była zorganizowana wspólnie przez Wyższą Szkołę Policyjną w Szczytnie oraz British Standards Institute Group Polska (BSI), http://www.bsigroup.pl/pl/KonferencjaSzczytno/ [dostęp: 26 VII 2013].

[38] http://rcb.gov.pl/?p=3314 [dostęp: 26 VII 2013].

nia jeden z paneli został poświęcony m.in. zagadnieniom związanym z infrastrukturą IT oraz rozwiązaniami technologicznymi, ale także szeroko rozumianej kulturze bezpieczeństwa. Podobną inicjatywę stanowiła konferencja dotycząca wielowymiarowości bezpieczeństwa zarówno wewnętrznego, jak i międzynarodowego[39]. W jej programie, obok takich tematów, jak bezpieczeństwo energetyczne, militarne, ekologiczne czy ekonomiczne, pojawiło się również bezpieczeństwo informacji, w tym również informatyczne i teleinformatyczne.

Cyberbezpieczeństwo stanowiło także istotny element debat publicznych oraz inicjatyw na temat bezpieczeństwa organizowanych przez administrację państwową. W ramach konferencji dotyczącej bezpieczeństwa międzynarodowego i demokracji[40] szef BBN gen. Stanisław Koziej poruszył kwestię bezpieczeństwa w cyberprzestrzeni, wskazując na potrzebę zapewnienia w tym zakresie prawidłowego działania systemów gromadzenia, monitorowania i transmisji danych.

Znaczna liczba spotkań poświęconych bezpieczeństwu w cyberprzestrzeni oraz rozwijającej się w jej ramach cyberprzestępczości niewątpliwie stanowi dowód ważkości problemu i jego pilności zarówno dla sektora prywatnego, publicznego, jak i środowisk naukowych. Wskaźnikiem oddającym poziom dalszego zainteresowania i tempa prac prowadzonych przez ekspertów oraz administrację państwową będą działania na forum unijnym. Z uwagi na priorytetowość tego tematu w agendzie unijnej, wynikającą z przeprowadzonych analiz[41], a także przygotowanych projektów legislacyjnych oraz pozalegislacyjnych[42], można spodziewać się co najmniej takiego poziomu aktywności ze strony właściwych organów administracji państwowej i wzrastającego zainteresowania sektora prywatnego oraz ośrodków naukowych.

Katalizatorem dalszych prac będą kolejne przypadki nielegalnej aktywności w Internecie. Sprawą priorytetową dla organów porządku publicznego pozostaną przypadki blokowania stron internetowych podmiotów publicznych, jak to miało miejsce w styczniu 2012 r.[43] w związku z porozumieniem ACTA[44], a także pod koniec lutego

[39] Konferencja „Wielowymiarowość bezpieczeństwa: wewnętrznego i międzynarodowego" odbyła się w dniach 11–12 kwietnia 2013 r. na Wydziale Nauk Społecznych SGGW w Warszawie, http://kmdsggw.wordpress.com/konferencja/ [dostęp: 26 VII 2013].

[40] Konferencja pt. „Bezpieczeństwo międzynarodowe a demokracja" odbyła się 11 marca 2013 r. w Grudziądzkiej Szkole Wyższej, http://www.bbn.gov.pl/pl/wydarzenia/4462,Wyklad-Szefa-BBN-o-dylematach-wspolczesnego-bezpieczenstwa.html [dostęp: 27 VII 2013].

[41] Szerzej zob. *Cyber security report, Special Eurobarometer 390*, Conducted by TNS Opinion & Social at the request of the European Commission, Directorate-General Home Affairs, July 2012, http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf [dostęp: 28 VI 2013].

[42] Szerzej zob. *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Brussels, 7.2.2013, COM(2013) 48 final 2013/0027 (COD), http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf [dostęp: 26 VI 2013].

[43] Wyciąg z analizy ataków na witryny internetowe administracji państwowej w celu pomocy dla administratorów serwerów administracji państwowej w ocenie zagrożenia przygotowany przez Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, http://www.cert.gov.pl/portal/cer/9/518/Wyciagzogolnejanalizyatakow_na_witryny_administracji_panstwowej_RP_wokresie21__2.html [dostęp: 20 VIII 2013].

[44] Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi (*Anti-Counterfeiting Trade Agreement* – ACTA) – międzynarodowa umowa mająca ustalić międzynarodowe standardy w walce z naruszeniami własności intelektualnej. Szerzej zob. *Wniosek. Decyzja Rady w sprawie zawarcia umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi między Unią Europejską i jej Państwami Członkowskimi, Australią, Kanadą, Japonią, Republiką Korei, Meksykańskimi Stanami Zjednoczonymi, Królestwem Marokańskim, Nową Zelandią, Republiką Singapuru, Konfederacją Szwajcarską i Stanami Zjednoczonymi Ameryki*, Bruksela, dnia 24.06.2011 r., KOM(2011) 380 wersja ostateczna.

2013 r., kiedy doszło do ataku na strony m.in. Kancelarii Premiera, MSZ, MON oraz Kancelarii Prezydenta. Stanowią one podstawę do debaty na temat poziomu bezpieczeństwa systemów informacyjno-komunikacyjnych organów państwowych oraz przedmiot konferencji naukowych, podczas których coraz częściej stawiane jest pytanie o bezpieczeństwo w cyberprzestrzeni.

Szczególne znaczenie dla polityki bezpieczeństwa w cyberprzestrzeni będą miały dwie kwestie. Pierwszą z nich będą wyniki prac podejmowanych przez państwa członkowskie w kontekście ochrony systemów technologii informacyjno-komunikacyjnej w ramach realizacji postanowień Europejskiej Agendy Cyfrowej. Drugą natomiast – efekty inicjatyw podjętych przez Unię Europejską w związku z ujawnieniem stosowania przez Stany Zjednoczone tajnego programu do elektronicznego pozyskiwania danych w drodze inwigilacji, o kryptonimie PRISM[45]. To z kolei przełoży się na kwestię ochrony danych i zakres praw użytkowników w cyberprzestrzeni. Nowe oczekiwania z tym związane wpłyną na działania Komisji Europejskiej nad nowymi inicjatywami dotyczącymi bezpieczeństwa danych w Internecie[46]. Potencjalne ingerencje w bezpieczne i swobodne korzystanie m.in. z Internetu, rozpoczną po raz kolejny dyskusję o granice nieskrępowanego dostępu do zasobów oraz możliwości sieci, jak to miało miejsce w przypadku umowy ACTA. W konsekwencji wydarzenia związane z rosnącą aktywnością w cyberprzestrzeni oraz wykorzystaniem systemów TIK w coraz to nowych sektorach oraz działach administracji państwowej przyczynią się do dwóch sytuacji: zwiększenia, a co najmniej utrzymania, uwagi środowisk naukowych, ekspertów ds. bezpieczeństwa i nowych technologii, którzy pozostaną głównym partnerem organów państwowych w kolejnych inicjatywach oraz, w szerszej skali, zintensyfikują prace w zakresie zwalczania cyberprzestępczości, ochrony ofiar cyberataków oraz ochrony danych osobowych w cyberprzestrzeni.

[45] PRISM – kryptonim programu US-984XN służącego Agencji Bezpieczeństwa Narodowego oraz Federalnemu Urzędowi Śledczemu do zbierania danych na temat użytkowników serwisów typu Google, Facebook, Microsoft oraz innych większych firm zajmujących się nowymi technologiami w formie meta danych oraz zawartości m.in. poczty elektronicznej, rozmów, połączeń VoIP, danych przechowywanych w chmurze. Szerzej: http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet [dostęp: 27 VIII 2013].

[46] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity [dostęp: 12 II 2013].