MIRON LAKOMY
Katowice

Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego – zarys problemu

Wstęp

Upowszechnienie komputerów oraz dostępu do Internetu od początku lat 90. XX wieku doprowadziło do dynamicznego rozwoju procesów digitalizacji. Stało się to szczególnie widoczne w XXI wieku, kiedy Internet zaczął odgrywać rosnącą rolę w życiu politycznym, gospodarczym oraz społecznym. Jak zauważyli Krzysztof Liedel i Michał Grzelak, globalna sieć, dostępna nie tylko za pomocą komputerów i telefonów komórkowych, ale także tabletów czy przedmiotów codziennego użytku, stała się jednym z podstawowych mediów oraz synonimem wolności słowa, nieskrępowanego przepływu informacji, a w pewnych przypadkach, nawet narzędziem rewolucji i zmian społecznych (Liedel, Grzelak, 2012, s. 126). Cyberprzestrzeń rozumiana za Pierrem Delvy jako „przestrzeń otwartego komunikowania za pośrednictwem połączonych komputerów i pamięci informatycznych, pracujących na całym świecie" (*Cyberprzestrzeń – definicje*), jednocześnie stała się jednak również wymiarem, w którym zaczęły pojawiać się poważne zagrożenia tak dla bezpieczeństwa narodowego[1], jak i międzynarodowego. Według Alexisa Bautzmanna, sprawiło to, iż coraz więcej państw zaczęło się interesować tą problematyką, dostrzegając między innymi rosnącą użyteczność Internetu do działań o charakterze militarnym. Jego zdaniem, nawet w strukturach Rady Bezpieczeństwa ONZ można obecnie zauważyć swoisty „powiew" zimnej wojny, tym razem o charakterze elektronicznym (Bautzmann, 2012, s. 80–81). Poważne ataki teleinformatyczne stały się bowiem przykrą codziennością stosunków międzynarodowych przełomu pierwszej i drugiej dekady XXI wieku.

Zasadniczym impulsem, który uświadomił społeczności międzynarodowej wagę tych zagadnień były z pewnością wydarzenia w Estonii oraz w Gruzji. W tym pierwszym przypadku, w kwietniu 2007 roku w wyniku sporu politycznego na linii Tallin–Moskwa, doszło do bezprecedensowych ataków teleinformatycznych na estoński Internet. Rosyjscy hakerzy zdołali nie tylko włamać się do szeregu najważniejszych portali sektora tak publicznego, jak i prywatnego, ale także m.in. sparaliżować bankowość internetową. Był to pierwszy przypadek w historii, kiedy suwerenne państwo zostało na taką skalę zaatakowane w cyberprzestrzeni. Już rok później, w sierpniu 2008 roku, podczas konfliktu zbrojnego w Osetii Południowej, rosyjscy hakerzy ponownie

[1] Warto zauważyć, iż już w amerykańskiej *National Security Strategy* z 2010 roku stwierdzono, iż cyberzagrożenia stanowią jedne z najpoważniejszych wyzwań dla bezpieczeństwa narodowego, bezpieczeństwa publicznego oraz rozwoju gospodarczego (*National Security Strategy*).

przeprowadzili masowe cyberataki, tym razem przeciwko gruzińskim stronom internetowym. Oba te wydarzenia uświadomiły elitom politycznym potrzebę wypracowania skutecznych rozwiązań w dziedzinie bezpieczeństwa teleinformatycznego. Niektóre państwa, takie jak Stany Zjednoczone, Izrael, Rosja czy Chiny już od dawna prowadziły prace nad uzyskaniem odpowiedniego potencjału w cyberprzestrzeni. Zdecydowaną większość tego typu działań podjęto jednak dopiero w drugiej połowie pierwszej dekady XXI wieku (Lakomy, 2010, s. 61–65). Warto zauważyć, iż „pierwsza cyberwojna" z Estonii ujawniła także zasadnicze nieprzygotowanie organizacji międzynarodowych do reagowania na tego typu incydenty. W środowisku międzynarodowym nie wypracowano bowiem dotychczas spójnego *modus operandi* w tej dziedzinie, tak z punktu widzenia prawa międzynarodowego publicznego, jak i bieżącej współpracy politycznej oraz wojskowej[2]. Stosunkowo najszybciej na wyzwania te zareagował Sojusz Północnoatlantycki, który w ciągu kilku lat przygotował w miarę spójną i, jak na razie, skuteczną strategię cyberbezpieczeństwa (Myrli). W tym kontekście, warto więc postawić pytanie, jaki stosunek do tych nowych zagrożeń dla bezpieczeństwa międzynarodowego ma Unia Europejska. Biorąc pod uwagę coraz wyraźniejszy rozwój wyzwań w cyberprzestrzeni, odpowiednia nań reakcja staje się warunkiem *sine qua non* nie tylko zapewnienia Europie odpowiedniego poziomu bezpieczeństwa, ale także umocnienia jej pozycji międzynarodowej (Dziwisz, 2011). Jest to tym istotniejsze, iż od dawna jednocząca się Europa formułuje rosnące ambicje odgrywania ważnej roli w nowej architekturze ładu międzynarodowego (Rewizorski, 2010, s. 137–153).

Zagrożenia teleinformatyczne

Podejmując próbę analizy polityki cyberbezpieczeństwa Unii Europejskiej, warto na wstępie dokonać krótkiej charakterystyki najważniejszych zagrożeń teleinformatycznych. Jest to zadanie stosunkowo trudne, gdyż nie ma zgody badaczy tak co do typologii, jak i definicji wyzwań pojawiających się w cyberprzestrzeni. Jednym z najczęściej wykorzystywanych terminów jest z pewnością cyberprzestępczość, która sprawia jednak poważne problemy natury identyfikacyjnej i interpretacyjnej. Amerykańskie Internet Crime Complaint Center zdefiniowało ją jako „oszustwo *online* w wielu formach, obejmujące kwestie praw własności intelektualnej, włamań komputerowych (haking), szpiegostwa gospodarczego, wymuszania *online*, międzynarodowego prania pieniędzy, kradzieży tożsamości oraz rosnącej listy przestępstw ułatwianych dzięki Internetowi". Natomiast według Konwencji Rady Europy o Cyberprzestępczości w skład tego procederu można zaliczyć cztery kategorie działań wykonywanych przy pomocy komputerów: szeroko rozumiane naruszenia bezpieczeństwa takie jak haking czy nielegalne uzyskanie danych, oszustwa i fałszerstwa, pornografia dziecięca oraz naruszenia praw autorskich. Jak jednak słusznie stwierdziły Kristin M. Finklea oraz Catherine A. Theohary, rozumienie zjawiska cyberprzestępczości może być zdecy-

[2] Do najważniejszych problemów można tu zaliczyć m.in. dezaktualizację prawa wojny, wyzwania związane z identyfikacją sprawców oraz interpretacją umów międzypaństwowych i traktatów sojuszniczych, w tym np. traktatu waszyngtońskiego (Ellis, 2011).

dowanie szersze i obejmować wykorzystanie komputerów do wszelkich tradycyjnych aktów łamania prawa. Ponadto ich zdaniem, czynnikiem, który odróżnia cyberprzestępczość od innych rodzajów szkodliwej działalności w Internecie jest przede wszystkim odmienna motywacja. Tym samym, przykładowo cyberszpiegostwo w zależności od motywacji, może być uznane albo za cyberprzestępczość, albo za akt inspirowany państwowo. Jest to o tyle istotne, iż w obu przypadkach może to skutkować odmiennymi reperkusjami o charakterze prawnym lub politycznym (Finklea, Theohary, 2012; *Konwencja Rady Europy*). Warto wyodrębnić jeszcze dwa rodzaje szkodliwej aktywności cyberprzestrzennej o charakterze pozapaństwowym. Pierwszą z nich jest haking, który można zdefiniować jako szkodliwą działalnością w sieci, której celem samym w sobie jest sam akt udanego cyberataku, bez politycznego, społecznego lub ekonomicznego podtekstu. Drugim jest natomiast haktywizm, który bywa często utożsamiany z wykorzystaniem Internetu do manifestacji określonego stanowiska wobec szeroko rozumianych kwestii politycznych, społecznych lub gospodarczych za pomocą technik hakerskich. Łączy się on więc poniekąd z zagadnieniem obywatelskiego nieposłuszeństwa, wyrażanego jednak za pomocą sieci (Terlikowski, 2008; *Electronic Civil Disobedience*).

Z zagadnieniem tym wiąże się poniekąd zjawisko cyberterroryzmu, który to termin podobnie jak cyberprzestępczość, jest często swobodnie wykorzystywany w debacie publicznej. Tak jak w przypadku haktywizmu, u podstaw cyberterroryzmu leży motywacja o charakterze politycznym lub społecznym. Tu jednak podobieństwa się kończą, gdyż podmiotami dokonującymi tego rodzaju cyberataków mogą być tak jednostki, ich grupy (np. organizacje terrorystyczne), jak również państwa. Inną cechą, która odróżnia go od haktywizmu jest także typowe dla terroryzmu dążenie do wyrządzenia poważnych szkód np. infrastrukturze krytycznej państwa, a co za tym idzie, wywarcia wpływu na poczucie bezpieczeństwa ludności (Bógdał-Brzezińska, Gawrycki, 2003; Lakomy, 2010; Gordon, Ford, 2003). Kolejnym typem szkodliwej działalności w sieciach teleinformatycznych jest z pewnością cyberszpiegostwo, które może być zdefiniowane jako próba uzyskania niejawnych informacji w cyberprzestrzeni. Od początku XXI wieku ta forma zagrożeń teleinformatycznych przeżywa dynamiczny rozwój. Jest to szczególnie widoczne w przypadku hakerów chińskich, którzy wielokrotnie w ostatnich latach skutecznie wyprowadzali niejawne dane i technologie z komputerów należących nie tylko do zachodnich instytucji państwowych, ale także wielkich korporacji (Rohozinski, Deibert, 2009; Adair, Deibert, Walton, 2010). Wreszcie, można także zauważyć rosnącą rolę cyberprzestrzeni jako kolejnego teatru wojny. Potencjał militarnego wykorzystania sieci teleinformatycznych potwierdziła w ostatnich latach m.in. izraelska operacja wojskowa *Orchard*, przeprowadzona w 2007 roku przeciwko instalacjom atomowym w Syrii (Clarke, Knake, 2010; Lakomy, 2011, s. 151; *Department of Defense Strategy*).

Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego

W świetle omówionych powyżej zagrożeń, warto więc zwrócić uwagę, w jaki sposób do tej problematyki ustosunkowała się Unia Europejska. Jak wspomniano

wcześniej, wydarzenia w Estonii oraz Gruzji w zasadniczym stopniu uświadomiły elitom politycznym państw zachodnich potrzebę wypracowania skutecznych rozwiązań w tej dziedzinie. Udowodniły także nieprzygotowanie do walki z tymi zagrożeniami Sojuszu Północnoatlantyckiego. W tym kontekście, należy zauważyć, iż reakcja Unii Europejskiej nie mogła jednak podążyć ścieżką wytyczoną przez NATO (Healey, van Bochoven, 2012). Polityka UE wobec wyzwań teleinformatycznych musiała bowiem wziąć pod uwagę szereg dylematów natury instytucjonalnej, prawnej i politycznej. Przede wszystkim, podstawowa wątpliwość dotyczyła tego, w jaki sposób Europa powinna zareagować na te zagrożenia, nie powielając zarazem rozwiązań przyjętych przez Pakt Północnoatlantycki. Tym samym powstało też pytanie, które organy Unii Europejskiej powinny tą problematyką się zainteresować: te właściwe Wspólnej Polityce Bezpieczeństwa i Obrony, czy też te obejmujące wymiar sprawiedliwości i spraw wewnętrznych. Był to problem o tyle poważny, iż jak wskazano wcześniej, cyberzagrożenia mogą przybierać formę działalności tak o charakterze kryminalnym, jak i inspirowanym przez rządy państw. Co więcej, wykorzystanie mechanizmów WPBiO mogłoby sugerować chęć dublowania procedur wypracowanych w ramach NATO. Byłoby to o tyle problematyczne, iż stałoby to w sprzeczności z koncepcją nowego podziału obowiązków między UE a Sojusz Północnoatlantycki, sformułowaną przez prezydenta Francji Nicolasa Sarkozy (*Conférence sur la sécurité*). Po drugie, pojawiła się wątpliwość, w jakim zakresie UE mogła ingerować w polityki cyberbezpieczeństwa państw członkowskich? Po trzecie, jak zauważyła Annegret Bendiek, priorytetem Unii Europejskiej jest stworzenie przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W tym kontekście, powstała wątpliwość, czy decyzje podejmowane przez instytucje UE nie zaprzepaściłyby tego celu, nadając priorytet bezpieczeństwu kosztem wartości, jaką jest wolność. Wreszcie, Unia Europejska musiała podjąć decyzję, czy polityka cyberbezpieczeństwa powinna objąć także sektor prywatny oraz szeroko pojęte środowisko międzynarodowe (Bendiek 2012).

Jedną z pierwszych inicjatyw Unii Europejskiej w dziedzinie cyberbezpieczeństwa była z pewnością decyzja o utworzeniu w 2004 roku Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency), na mocy dyrektywy nr 460/2004. Stwierdzono w niej, iż „systemy komunikacji i informacji stały się zasadniczym czynnikiem w rozwoju społecznym i gospodarczym. Komputery oraz sieć stają się wszechobecnym dobrem, na takiej samej zasadzie jak elektryczność czy dostęp do wody. Bezpieczeństwo sieci komunikacyjnych i systemów informacyjnych, a w szczególności ich dostępność, jest zatem obiektem rosnącej troski społeczeństwa". Dyrektywa przewidziała cztery zadania dla agencji. Przede wszystkim, miała ona być odpowiedzialna za wzmocnienie zdolności Unii Europejskiej, jej państw członkowskich, a także środowiska biznesowego do zapobiegania i zwalczania wyzwań w dziedzinie bezpieczeństwa informacyjnego. Po drugie, agencja miała być organem pomocniczym oraz doradczym dla Komisji Europejskiej oraz państw członkowskich w kwestiach dotyczących bezpieczeństwa teleinformatycznego, ale tylko w zakresie określonym przez regulamin. Po trzecie, miała stymulować współpracę między sektorami publicznym a prywatnym. Wreszcie po czwarte, miała także pomagać Komisji Europejskiej w rozwoju *acquis communautaire* w dziedzinie bezpieczeństwa teleinformatycznego (*Regulation (EC) No 460/2004*).

Powołanie wyspecjalizowanego organu zajmującego się cyberbezpieczeństwem już w 2004 roku mogło świadczyć o dużym znaczeniu tej problematyki dla instytucji unijnych. Mimo to, przez pierwsze trzy lata funkcjonowania, ENISA w zasadzie nie osiągnęła znaczących sukcesów. Wydaje się, iż stało się tak z dwóch powodów. Przede wszystkim, Unia Europejska, mimo zapisów dyrektywy nr 460, w rzeczywistości nie dostrzegała jeszcze rosnącego znaczenia wyzwań na tym obszarze. Było to tym widoczniejsze, iż również Sojusz Północnoatlantycki oraz poszczególne państwa członkowskie także nie były wówczas zainteresowane opracowaniem strategii bezpieczeństwa teleinformatycznego (Myrli). Po drugie, UE nie dysponowała także odpowiednimi mechanizmami i procedurami, które pozwoliłyby na rozwinięcie współpracy w tej dziedzinie. Kwestie te uznano bowiem przede wszystkim za obszar bezpośrednich prerogatyw państwowych oraz zakres kompetencji Sojuszu Północnoatlantyckiego. Ponadto, trwały wówczas prace nad reformą instytucjonalną Unii, co w pewnym sensie mogło paraliżować nowe inicjatywy w zakresie cyberbezpieczeństwa. Jednocześnie jednak, należy zauważyć, iż UE mimo wszystko dysponowała wówczas wyjątkowymi instrumentami wpływania na porządek prawny krajów członkowskich, czego jednak należycie nie wykorzystano.

O tendencjach tych świadczył fakt, iż kolejna inicjatywa dotycząca zagrożeń pojawiających się w Internecie, miała miejsce dopiero w dwa lata po powołaniu ENISA. W maju 2006 roku Komisja Europejska wydała komunikat: *A strategy for a Secure Information Society – „Dialogue, partnership and empowerment"*. W dokumencie tym stwierdzono, iż powstała potrzeba zbudowania jednolitej i bezpiecznej przestrzeni informacyjnej Unii Europejskiej. Podkreślono ambicję budowy „dynamicznej, globalnej strategii dla Europy, bazującej na kulturze bezpieczeństwa" oraz dialogu i partnerstwie. Co ciekawe, zauważono, iż szkodliwa działalność w cyberprzestrzeni nie stanowi zagrożenia jedynie dla administracji publicznej, ale także dla sektora prywatnego oraz pojedynczych użytkowników. Tym samym, wskazano na fundamentalne znaczenie sektora ICT dla gospodarki i rozwoju społecznego Unii Europejskiej. Zawarte w tym dokumencie nowe podejście do cyberbezpieczeństwa obejmowało więc trzy główne kierunki działań: wprowadzenie nowych zabezpieczeń teleinformatycznych, zaktualizowanie ustawodawstwa dotyczącego komunikacji elektronicznej oraz walkę z cyberprzestępczością. W tym kontekście, Komisja Europejska zapowiedziała działania mające na celu m.in. zwalczanie spamu oraz szkodliwego oprogramowania (szczególnie szpiegowskiego), a także wspieranie rozwoju współpracy w tej dziedzinie odpowiednich służb państw członkowskich. Zauważono również potrzebę stworzenia wspólnego, europejskiego systemu wymiany informacji i ostrzegania oraz osiągnięcia dialogu i partnerstwa między wszystkimi zainteresowanymi stronami. Szczególny nacisk położono tu na współpracę UE nie tylko z państwami członkowskimi, ale także sektorem prywatnym (*Communication from the Commission to the Council*, 2006). Zapisy te należy uznać za ciekawe z trzech powodów. Przede wszystkim, inicjatywa ta była o tyle istotna, iż podjęto ją jeszcze przed „pierwszą cyberwojną" w Estonii. Tym samym, decydenci Unii Europejskiej, przynajmniej oficjalnie, już wcześniej dostrzegli rosnące wyzwania dla bezpieczeństwa teleinformatycznego Europy. Po drugie, innym pozytywnym aspektem tego komunikatu było uznanie, iż skuteczne przeciwdziałanie zagrożeniom w Internecie, nie może się opierać wyłącznie na instytucjach sektora pu-

blicznego. Współpraca organów państwowych i międzynarodowych z podmiotami gospodarczymi, organizacjami pozarządowymi czy środowiskiem naukowym wydaje się być bowiem jedną z podstawowych zasad przeciwdziałania wyzwaniom teleinformatycznym. Wreszcie po trzecie, warto zwrócić uwagę na fakt, iż dokument UE został poświęcony przede wszystkim walce z cyberprzestępczością, pomijając inne, omówione wyżej przykłady szkodliwej działalności w sieci. Tym samym, sugerowało to, Bruksela nie przewidywała uwzględnienia tych zagadnień w ramach projektu „Europy obrony". Tak więc, należy podkreślić, iż Unia Europejska stosunkowo wcześnie zainteresowała się problematyką cyberprzestępczości. Niestety, w dużej mierze miało to charakter raczej pozorny, gdyż deklaracjom politycznym nie towarzyszyły istotniejsze inicjatywy w wymiarze praktycznym.

Jak wspomniano wcześniej, pewien przełom nastąpił dopiero w kwietniu 2007 roku, kiedy europejskie elity polityczne uświadomiły sobie wagę zagrożeń pojawiających się w cyberprzestrzeni. W reakcji na wydarzenia w Estonii, już w maju Komisja Europejska wydała komunikat, w którym zwracała się do innych instytucji unijnych z prośbą o wypracowanie nowej strategii walki z cyberprzestępczością. Stwierdzono w nim: „W świetle tego zmieniającego się środowiska, pojawiła się paląca potrzeba podjęcia działań – tak na narodowym, jak i europejskim poziomie – przeciwko wszelkim formom cyberprzestępczości, które stanowią coraz poważniejsze zagrożenie dla infrastruktury krytycznej, społeczności, biznesu oraz obywateli". Zauważono, iż walka z tego typu wyzwaniami jest w dużej mierze utrudniona wątpliwościami natury prawnej, jurysdykcyjnej oraz czysto technicznej, związanej z identyfikacją sprawcy ataku. Komisja podkreśliła potrzebę promowania europejskiej i międzynarodowej współpracy w tej dziedzinie. Do głównych jej założeń zaliczono m.in. walkę z cyberprzestępczością na poziomie narodowym, europejskim i międzynarodowym oraz przygotowanie unijnej strategii w tej dziedzinie. Potwierdzono tym samym, iż to kwestie kryminalne stały się głównym obiektem zainteresowania instytucji UE. Wśród innych priorytetów KE wymieniono również pracę na rzecz zwiększenia świadomości na temat zagrożeń pojawiających się w Internecie. Do zadań na przyszłość zaliczono natomiast: rozwój współpracy operacyjnej służb, organizację wspólnych ćwiczeń w zakresie bezpieczeństwa teleinformatycznego, wzmocnienie dialogu z sektorem przemysłowym, harmonizację narodowych regulacji prawnych oraz stworzenie instrumentów służących gromadzeniu danych i statystyk dotyczących cyberprzestępczości. Wreszcie, w dokumencie tym podkreślono znaczenie dotychczasowej aktywności Komisji Europejskiej na arenie międzynarodowej, w ramach takich struktur G-8 Lyon-Roma High-Tech Crime Group lub Interpol (*Communication*, 2007). Warto zauważyć, iż Unia Europejska zareagowała stosunkowo szybko na wydarzenia z Estonii, proponując pewien wachlarz rozwiązań, które miały stać się fundamentem unijnej polityki cyberbezpieczeństwa. Na szczególną uwagę zasługuje fakt, iż Komisja Europejska skupiła się na tych wyzwaniach, które miały związek z szeroko rozumianą cyberprzestępczością. Tym samym, szkodliwą działalność w sieci inspirowaną przez państwa pozostawiono w gestii państw członkowskich oraz Sojuszu Północnoatlantyckiego. Jednocześnie warto zauważyć, iż rozwiązania w tej dziedzinie były znacznie utrudnione ze względu na brak zgody wszystkich państw członkowskich na ratyfikację Konwencji Rady Europy o Cyberprzestępczości (*The Growing Pains*).

Wbrew oczekiwaniom, komunikat KE z maja 2007 roku spotkał się jednak tylko z ograniczonym zainteresowaniem innych organów i państw członkowskich UE. Świadczył o tym fakt, iż dopiero w czerwcu 2008 roku podjęto działania na rzecz wdrożenia jego niektórych założeń. Rozpoczęto wówczas program *Safer Internet Plus*, który przewidywał cztery rodzaje działań podejmowanych przez UE: walkę z nielegalną zawartością sieci, powstrzymywanie szkodliwej działalności (np. spamu za pomocą specjalnych filtrów *online*), promocję bezpieczniejszego środowiska sieciowego oraz wzmocnienie świadomości użytkowników. Na realizację tych celów w latach 2009–2013 przeznaczono w sumie 55 milionów euro (*Making the Internet*). Na uwagę zasługują także podjęte w 2008 roku publiczne konsultacje na temat bezpieczeństwa teleinformatycznego: *Towards a Strengthened Network and Information Security in Europe*. Komisja Europejska stwierdziła wówczas, iż systemy komunikacyjne i informacyjne „stają się systemem nerwowym naszego nowoczesnego społeczeństwa. Wiele usług i procesów w ramach naszej gospodarki i społeczeństwa jest zależnych od ich dobrego funkcjonowania" (*Commission launches*, 2008). Inicjatywy te można oceniać z dwóch perspektyw. Z jednej strony, należy zauważyć, iż w tym okresie to KE stała się głównym promotorem europejskich działań na rzecz budowy wspólnej strategii przeciwdziałania cyberprzestępczości. Z drugiej jednak, wysiłki UE nadal nie przystawały do wagi stale ewoluujących zagrożeń teleinformatycznych. Wydaje się, iż w dużej mierze mogło to wynikać z niepewnego statusu traktatu reformującego UE.

Do pewnej intensyfikacji działań w tej dziedzinie doszło dopiero w marcu 2009 roku, kiedy KE przyjęła kolejny komunikat, tym razem w sprawie ochrony infrastruktury krytycznej. Sugerowało to, iż UE poszerzyła zakres problemowy polityki bezpieczeństwa teleinformatycznego pod wpływem doświadczeń wojny na Kaukazie w sierpniu 2008 roku. Był to wstęp do realizacji europejskiego programu ochrony infrastruktury krytycznej (*An European Programme for Critical Infrastructure Protection*). Jego zasadniczym przesłaniem było stwierdzenie, iż sektor ICT powinien być w przyszłości dla Europy priorytetową gałęzią gospodarki. W komunikacie podkreślono potrzebę wyznaczenia najważniejszych części składowych europejskiej infrastruktury krytycznej. Wynikało to ze świadomości Brukseli, iż ataki na tego typu cele mogą stanowić poważne zagrożenie tak dla gospodarki, jak i bezpieczeństwa ludności Unii Europejskiej. W tym kontekście, zaakcentowano ponownie potrzebę osiągnięcia lepszej koordynacji narodowych wysiłków w zakresie cyberbezpieczeństwa. Ponadto, zauważono także konieczność rozwoju współpracy na arenie międzynarodowej, przede wszystkim ze względu na transnarodowy i globalny charakter Internetu. Nowy plan zwiększenia odporności krytycznej infrastruktury UE na cyberataki został więc oparty na pięciu filarach:

– gotowości i zapobieganiu, które obejmowały m.in. osiągnięcie ogólnoeuropejskiego porozumienia w sprawie minimalnych standardów zabezpieczeń oraz powołania krajowych zespołów CERT we wszystkich państwach członkowskich[3];

[3] Zestaw tych wymagań został przyjęty w grudniu 2009 roku przez ENISĘ, przy współpracy z europejskim środowiskiem zespołów CERT. W 2010 roku, zostały one przekształcone w zestaw rekomendacji polityki cyberbezpieczeństwa dla państw członkowskich (*Baseline capabilities*).

– wykrywaniu i reagowaniu, polegających m.in. na budowie europejskiego systemu wymiany informacji o zagrożeniach teleinformatycznych (European Information Sharing and Alert System – EISAS);
– łagodzeniu skutków i przywracaniu sprawności operacyjnej, mających na celu opracowanie krajowych planów awaryjnych oraz organizację regularnych ćwiczeń w zakresie reagowania na cyberataki przeciwko infrastrukturze sieciowej. Co ciekawe, europejskie ćwiczenia miały być wzorowane na amerykańskich *Cyber Storm*;
– współpracy międzynarodowej obejmującej przygotowanie m.in. mapy drogowej dla globalnej kooperacji w dziedzinie bezpieczeństwa teleinformatycznego;
– opracowaniu standardów zabezpieczeń dla sektora ICT oraz wyznaczeniu elementów europejskiej krytycznej infrastruktury teleinformatycznej (*Communication*, 2009).

Przyjęty po 2007 r. kierunek rozwoju europejskiej polityki cyberbezpieczeństwa został potwierdzony w maju 2010 roku, kiedy Unia Europejska przyjęła kolejny istotny dokument: Agendę Cyfrową dla Europy (*A Digital Agenda for Europe*). Podkreślono w nim zasadniczy związek między bezpieczeństwem teleinformatycznym a długotrwałym rozwojem gospodarczym i społecznym Europy, opartym o wolny rynek i technologie cyfrowe. Zauważono, iż zabezpieczenie Unii przed tego typu wyzwaniami jest warunkiem *sine qua non* realizacji przedstawionej przez Komisję Europejską strategii *Europa 2020*. Ponadto, rozwój gospodarki cyfrowej, a co za tym idzie, przezwyciężenie kryzysu gospodarczego w UE byłoby, według autorów, możliwe tylko po przezwyciężeniu siedmiu zasadniczych przeszkód, do których zaliczono cyberprzestępczość. W dokumencie stwierdzono: „Europejczycy nie będą chcieli angażować się w coraz bardziej złożoną działalność internetową o ile nie będą mieli pewności, że oni sami lub ich dzieci mogą w pełni polegać na sieci. Dlatego Europa musi zająć się nową formą działalności kryminalnej – „cyberprzestępczością" – obejmującą między innymi wykorzystywanie dzieci, kradzież tożsamości i ataki cybernetyczne oraz musi opracować odpowiednie mechanizmy reakcji. Jednocześnie powstawanie nowych baz danych i nowych technologii zezwalających na zdalną kontrolę osób stanowi nowe wyzwanie dla ochrony podstawowych praw Europejczyków w zakresie danych osobistych i prywatności. Internet stał się tak nieodzowną częścią infrastruktury informacyjnej zarówno dla osób prywatnych, jak i dla gospodarki europejskiej, że musimy zapewnić odporność systemów informatycznych i sieci na wszelkiego rodzaju nowe zagrożenia". W celu realizacji tych założeń, Komisja Europejska zadeklarowała m.in. unowocześnienie ENISA, rozbudowę europejskich zespołów reagowania na incydenty komputerowe, przygotowanie do 2012 roku europejskiej platformy walki z cyberprzestępczością, wypracowanie nowych przepisów i procedur reagowania na cyberataki oraz przeprowadzenie analizy możliwości powołania centrum ds. walki z przestępczością internetową (*Communication*, 2010).

Potwierdzeniem obranego kierunku rozwoju polityki cyberbezpieczeństwa był kolejny komunikat Komisji Europejskiej z marca 2011 roku. Został on w pełni poświęcony ochronie krytycznej infrastruktury teleinformatycznej UE. W dokumencie tym podkreślono świadomość dynamicznego rozwoju wyzwań rodzących się w sieci. Po raz kolejny stwierdzono, iż nie są one właściwe jedynie dla Unii, przez co walka z nimi nie powinna mieć wymiaru wyłącznie europejskiego. Do najważniejszych, dotychcza-

sowych osiągnięć polityki cyberbezpieczeństwa zaliczono: wymianę doświadczeń w ramach Europejskiego Forum Państw Członkowskich (European Forum of Member States), powołanie europejskiego partnerstwa publiczno-prywatnego (European Public-Private Partnership for Resilience), ustalenie minimalnych wymogów oraz rekomendacji dla państw członkowskich, stworzenie mapy drogowej rozwoju europejskiego systemu wymiany informacji oraz alarmów w ramach ENISA oraz przeprowadzenie pierwszych paneuropejskich ćwiczeń w tej dziedzinie, które miały miejsce 4 listopada 2010 roku. Wzięło w nich aktywny udział 19 państw członkowskich UE wraz ze Szwajcarią, Norwegią oraz Islandią. Wśród sukcesów, dokument KE wymienił także aktywność Unii Europejskiej na arenie międzynarodowej, w tym współpracę ze Stanami Zjednoczonymi, OECD, ITU, NATO czy grupą G-8. Ponadto, za istotne osiągnięcie uznano wyznaczenie najważniejszych elementów krytycznej infrastruktury teleinformatycznej. Wreszcie, KE ustanowiła kilka zadań na przyszłość:

- promocję elastyczności oraz stabilności funkcjonowania Internetu, poprzez aktywną współpracę UE z innymi partnerami na arenie międzynarodowej;
- budowę strategicznych partnerstw, obejmujących z jednej strony współpracę narodowych zespołów reagowania na incydenty komputerowe (CERT), z drugiej natomiast, funkcjonowanie powołanej w 2010 roku europejsko-amerykańskiej grupy roboczej ds. cyberbezpieczeństwa i cyberprzestępczości (EU-U.S. Working Group on Cyber-Security and Cyber-Crime);
- rozwój zaufania w sieciowej „chmurze", obejmujący dynamiczne dostosowywanie się do stale rozwijających się technologii;
- wzmocnienie przygotowania Unii Europejskiej do obrony przed cyberatakami, przede wszystkim dzięki stworzeniu sieci dobrze działających narodowych zespołów reagowania na incydenty komputerowe do końca 2012 roku;
- opracowanie do 2012 r. planów UE na wypadek wystąpienia poważnych cyberataków oraz przeprowadzanie regularnych, paneuropejskich ćwiczeń w przestrzeni teleinformatycznej;
- koordynacja wysiłków państw członkowskich oraz Komisji Europejskiej w celu promocji norm i rozwiązań w zakresie globalnej „stabilności oraz elastyczności" Internetu.

Co ważne, w dokumencie stwierdzono, iż celem Unii Europejskiej jest zrównoważenie dotychczasowej dyskusji na temat cyberbezpieczeństwa, która w zbyt dużym stopniu skupia się na kwestiach militarnych oraz bezpieczeństwie narodowym (*Communication*, 2011). Wydaje się, iż było to bardzo znamienne sformułowanie. Potwierdziło bowiem odmienny charakter polityki cyberbezpieczeństwa UE, skupionej na walce z cyberprzestępczością i wypracowaniu odpowiednich norm i procedur, tak w ramach partnerstwa publiczno-prywatnego, jak i współpracy międzynarodowej. Tym samym, Unia Europejska nie podejmowała prób dublowania narodowych bądź natowskich kompetencji w tej dziedzinie.

Bez względu na powyższe deklaracje, jednak nie ulega wątpliwości, iż rzeczywiste osiągnięcia Unii Europejskiej w dziedzinie bezpieczeństwa teleinformatycznego były do 2011 roku dość ograniczone. Tak przed jak i po 2007 roku opracowano co prawda szereg dokumentów o charakterze koncepcyjnym, jednak ich praktyczne znaczenie okazało się niewielkie. Także funkcjonująca od lat ENISA była w dużej mierze nie-

przystosowana do wyzwań, które ujawniły się w cyberprzestrzeni. Tym samym, sukcesy wymienione przez Komisję Europejską odegrały raczej niewielką rolę. Pewne sygnały zmian pojawiły się dopiero w 2012 roku. Już w marcu bowiem powołano nową komórkę w ramach Europolu: Europejskie Centrum Cyberprzestępczości (European Cybercrime Center). Do głównych obszarów zainteresowania ECC, przy poszanowaniu zasady subsydiarności, zaliczono przede wszystkim: zorganizowaną cyberprzestępczość, najbardziej szkodliwe akty przestępcze w sieci, np. na tle seksualnym oraz ataki przeciwko infrastrukturze krytycznej. ECC ma pełnić następujące funkcje:

– centralnego punktu wymiany informacji na temat cyberprzestępczości w ramach Unii Europejskiej, tak dla zespołów CERT, jak i sektora prywatnego;
– wspomagania państw członkowskich w zakresie sporządzania ekspertyz oraz prowadzania ćwiczeń;
– wspierania dochodzeń prowadzonych przez służby państw członkowskich w zakresie przestępczości teleinformatycznej;
– reprezentowania europejskiego punktu widzenia w debatach na temat cyberprzestępczości z sektorem prywatnym, środowiskiem naukowym czy organizacjami pozarządowymi.

Szczególnie ciekawy wydaje się ten ostatni punkt. Odpowiednie zwalczanie zagrożeń pojawiających się w cyberprzestrzeni nie jest bowiem możliwe jedynie przy wykorzystaniu środków i służb publicznych. Zgodnie z zapowiedziami, ECC powinno osiągnąć pełną gotowość operacyjną do 2013 roku. W komunikacie Komisji Europejskiej na ten temat potwierdzono, iż to właśnie działalność kryminalna w Internecie została uznana za jedno z najpoważniejszych wyzwań stojących tak przed UE, jak i całą społecznością międzynarodową. Ponadto, Europol zintensyfikował swoją aktywność w cyberprzestrzeni, czego wyrazem była m.in. operacja *Rescue*, w ramach której ujęto niemal 200 przestępców na tle seksualnym (*Communication*, 2012). Wyrazem realizacji wcześniejszych założeń były także nowe inicjatywy podejmowane przez ENISA. Przykładowo w październiku 2012 roku ogłosiła ona europejski miesiąc cyberbezpieczeństwa. Głównym założeniem tego projektu było zwiększenie świadomości społeczeństw oraz elit politycznych tą problematyką. Warto dodać, iż stanowił on pewną formę uzupełnienia podobnych działań w ramach EU-U.S. Working Group on Cyber-Security and Cyber-Crime (*European Cyber Security Month*).

Innym przejawem wdrażania założeń polityki cyberbezpieczeństwa Unii Europejskiej w 2012 było z pewnością wsparcie badań w tej dziedzinie. W listopadzie, Komisja Europejska zadeklarowała bowiem, iż mając świadomość wyzwań stojących na drodze realizacji agendy cyfrowej, zdecydowano się zintensyfikować działalność naukową na tym obszarze. W latach 2007–2013 KE przeznaczyła na ten cel ok. 350 mln euro. Natomiast w budżecie na lata 2013–2020 przewidziano aż 400 mln euro, wraz z kolejnymi 450 mln euro z projektu *Secure Societies*. Wśród najistotniejszych inicjatyw naukowych, KE wymieniła: Syssec, Nessos, TECOM oraz projekty rozwijające techniki kryptograficzne (*Digital Agenda*). Wzrost środków na badania o 14% był więc kolejnym sygnałem priorytetyzacji polityki cyberbezpieczeństwa UE (Baker, 2012).

Warto zauważyć, iż na przełomie pierwszej i drugiej dekady XXI wieku, równolegle z działaniami podejmowanymi przez KE, kwestie te znalazły się również w obszarze zainteresowań europejskiej dyplomacji. Na konferencji w Budapeszcie 4 października

2012 roku Catherine Ashton stwierdziła bowiem wyraźnie, iż Internet ma ogromne znaczenie, nie tylko dla rozwoju gospodarczego Europy, ale także przemian politycznych i społecznych, co najlepiej udowodniła arabska wiosna. W związku z tym, wolność słowa, wolność zrzeszania się czy prawo dostępu do informacji powinny być respektowane również w cyberprzestrzeni. Jej zdaniem, Internet nie może stać się „ofiarą własnego sukcesu". Zadeklarowała więc, iż „Unia Europejska jest zdeterminowana, aby promować i bronić swoich wartości *online*". Według Ashton, kwestia ta stała się jednym z fundamentalnych celów dyplomacji Unii Europejskiej (Ashton 2012).

W 2012 roku, wyzwaniami w cyberprzestrzeni zainteresował się również Parlament Europejski. W tym kontekście, najistotniejsze znaczenie miał raport z listopada sporządzony przez eurodeputowanego Tunne Kelama. Stwierdzono w nim rażącą nieskuteczność dotychczasowych wysiłków UE na rzecz cyberbezpieczeństwa. T. Kelam zauważył, iż w ramach UE brakuje jednoznacznych rozwiązań koncepcyjnych i proceduralnych w tej dziedzinie. Jego zdaniem, Unia Europejska zbyt późno zareagowała na zagrożenia komputerowe, co wynika między innymi z braku dostatecznej koordynacji na szczeblu europejskim oraz braku spójności pomiędzy strategiami cyberbezpieczeństwa poszczególnych państw członkowskich. W związku z tym, raport zaakcentował potrzebę budowy wzajemnego zaufania między sektorami publicznym i prywatnym oraz przygotowania i implementacji narodowych strategii cyberbezpieczeństwa. Co więcej, w raporcie zaznaczono, iż problematyka ta powinna być nie tylko obiektem zainteresowania ENISA ale także Europejskiej Agencji Obrony, co sugerowało otworzenie się na militarny wymiar cyberprzestrzeni. Wreszcie, zaapelował do Europejskiej Służby Działań Zewnętrznych, aby w większym stopniu niż dotychczas, położyła nacisk na współpracę z innymi podmiotami międzynarodowymi, w tym przede wszystkim z USA (*EU Cyber Security and Defense*). Na problem ten zwrócili uwagę również inni członkowie Parlamentu Europejskiego. W listopadzie 2012 roku na spotkaniu poświęconym bezpieczeństwu teleinformatycznemu, po raz kolejny krytycznie odnieśli się oni do dotychczasowych działań Unii. Zauważono wówczas, iż UE powinna skończyć z tendencją do „delegowania problemów bezpieczeństwa na innych". Przestrzegano przed redukowaniem budżetów obronnych oraz zaakcentowano potrzebę budowy strategii cyberbezpieczeństwa na poziomie unijnym. Stwierdzono bowiem, iż rozwój sieci teleinformatycznych wiąże się z zagrożeniami dla „bezpieczeństwa, obronności, stabilności i konkurencyjności UE" (Smith, 2012).

Wreszcie, o pewnych osiągnięciach Unii Europejskiej na obszarze bezpieczeństwa teleinformatycznego świadczy także fakt powołania 1 września 2012 roku Zespołu Reagowania na Incydenty Komputerowe Unii Europejskiej (Computer Emergency Response Team – CERT-UE). Składa się on z ekspertów komputerowych pochodzących z najważniejszych instytucji Unii Europejskiej: Komisji Europejskiej, Parlamentu Europejskiego czy Komitetu Regionów. Głównym zadaniem CERT-EU jest wspieranie innych instytucji Unii w ochronie przeciwko „intencjonalnym i złośliwym atakom, które zaszkodziłyby integralności ich aktywów teleinformatycznych oraz szkodziłyby interesom Unii Europejskiej". Nowy organ pełni więc cztery funkcje: wykrywania, prewencji, odpowiedzi oraz regeneracji uszkodzonej infrastruktury (*RFC 2350*). Powołanie tego zespołu było przede wszystkim realizacją jednego z najważniejszych zapisów Agendy Cyfrowej dla Europy. Z drugiej jednak strony, porównując działania

UE do reform, które po 2007 roku przeprowadził Sojusz Północnoatlantycki, może dziwić tak długi okres jego tworzenia. Jest to tym ciekawsze, iż w tym samym okresie, Unia Europejska kładła duży nacisk na wypracowanie narodowych rozwiązań na obszarze cyberbezpieczeństwa, przede wszystkim poprzez powołanie zespołów CERT we wszystkich państwach członkowskich.

Zakończenie

Szkodliwa działalność w cyberprzestrzeni, tak o charakterze przestępczym, jak i państwowym, w XXI wieku stała się poważnym wyzwaniem dla polityki wewnętrznej oraz bezpieczeństwa i obrony Unii Europejskiej. Bruksela stosunkowo wcześnie zainteresowała się problematyką bezpieczeństwa teleinformatycznego, czego wyrazem stało się powołanie European Network and Information Security Agency. Nie ulega jednak wątpliwości, iż podjęte po 2004 roku działania w dużej mierze rozminęły się z wagą wyzwań teleinformatycznych. Nowy rozdział polityki cyberbezpieczeństwa UE został otworzony dopiero w 2007 roku, kiedy w wyniku pierwszej cyberwojny w Estonii, europejscy decydenci uświadomili sobie częściowo potrzebę wypracowania kompleksowych rozwiązań w tej dziedzinie. W przeciwieństwie jednak do niektórych państw członkowskich, np. Francji (*Information systems defence and security*), Niemiec (*Cyber Security Strategy for Germany*), Wielkiej Brytanii, Polski czy Sojuszu Północnoatlantyckiego, początkowe prace nad polityką cyberbezpieczeństwa miały charakter niemal wyłącznie koncepcyjny. Porównując wysiłki poczynione przez NATO (Healey, von. Bochoven, 2012) i UE po 2007 roku, w oczy rzuca się niewielkie zainteresowanie Brukseli wypracowaniem praktycznych ram współpracy w cyberprzestrzeni. Można wskazać na trzy grupy powodów tego stanu rzeczy. Przede wszystkim, europejscy decydenci nie chcieli dublować struktur i rozwiązań z zakresu „twardego bezpieczeństwa" poczynionych przez Sojusz Północnoatlantycki. Po drugie, polityka cyberbezpieczeństwa była postrzegana jako obszar kompetencji państw członkowskich. Wreszcie po trzecie, kwestie związane z rozwojem idei „Europy obrony" w okresie prac nad traktatem reformującym UE zeszły na dalszy plan. Wyrazem powyższych tendencji były kolejne dokumenty przedstawiane przez Komisję Europejską, w których wielokrotnie podkreślano, iż UE kwestie bezpieczeństwa teleinformatycznego postrzegała przede wszystkim z perspektywy cyberprzestępczości i szkód, jakie wyrządza ona rozwojowi gospodarczemu i społecznemu. Ten kierunek działań wydaje się szczególnie interesujący, ponieważ kładł on nacisk na niemilitarne i niepaństwowe aspekty szkodliwego wykorzystania sieci. Tym samym, Unia Europejska działała nieco pod prąd globalnych tendencji wyrażanych m.in. przez Stany Zjednoczone, które zaczęły postrzegać cyberprzestrzeń jako kolejny teatr konfliktu zbrojnego. Tym samym, nie dość, że UE nie dublowała funkcji i kompetencji państw członkowskich oraz NATO, to jeszcze znalazła pewną „niszę" w tej dziedzinie. Należy bowiem pamiętać, iż do 2007 roku nie udało się wypracować spójnych i efektywnych ram współpracy międzynarodowej w zakresie zwalczania przestępczości teleinformatycznej. Przykładem nieskuteczności wcześniejszych rozwiązań tego typu były poważne problemy, jakie napotkała ratyfikacja Konwencji Rady Europy o Cyberprzestępczości. O wadze

współpracy na poziomie europejskim i międzynarodowym świadczył także fakt, iż szkodliwa działalność w Internecie ma charakter transnarodowy, przez co rozwiązania na poziomie państwowym częstokroć mogły się okazywać mało efektywne.

Komisja Europejska od 2007 roku wydała szereg dokumentów, deklaracji i komunikatów, które w ciekawy sposób ujmowały problematykę cyberbezpieczeństwa, wskazując na najważniejsze zagrożenia i dylematy, ale także proponując ciekawe definicje zagrożeń oraz pewne rozwiązania praktyczne. Niestety, propozycje KE tylko w niewielkim stopniu zostały zrealizowane. Mimo wielokrotnego podkreślania, że UE dostrzega znaczenie wyzwań w cyberprzestrzeni, merytoryczna współpraca państw członkowskich oraz instytucji Unii rozwijała się bardzo powoli. Do istotnych osiągnięć Unii należy z pewnością zaliczyć m.in. wzmocnienie potencjału ENISA, budowę europejskiego systemu wymiany informacji i alarmów (EISAS), rozpoczęcie programu ochrony infrastruktury krytycznej (*An European Programme for Critical Infrastructure Protection*), czy rozwój partnerstwa publiczno-prywatnego. Były to ważne inicjatywy, które świadczyły o rosnącym zrozumieniu zagrożeń pojawiających się w cyberprzestrzeni. Na szczególną uwagę zasługuje rozwój współpracy z sektorem prywatnym, organizacjami pozarządowymi oraz środowiskiem naukowym, co jest jednym z podstawowych warunków skutecznego przeciwdziałania cyberprzestępczości. Wreszcie, należy podkreślić postępy w zakresie organizacji ćwiczeń zespołów reagowania na incydenty komputerowe. Z drugiej jednak strony, wydaje się, iż działania Unii Europejskiej w tej dziedzinie w dużej mierze rozminęły się z potrzebami oraz oczekiwaniami. Przede wszystkim, uderza bardzo długi okres formułowania podstawowych celów i założeń unijnej polityki cyberbezpieczeństwa. Co prawda, pierwsze dokumenty poświęcone temu zagadnieniu pojawiły się jeszcze przed 2007 rokiem, to jednak spójne plany opracowano dopiero 2 lata później. Najdobitniej o poważnych opóźnieniach świadczył fakt, iż dopiero w 2012 roku powołano europejski zespół reagowania na incydenty komputerowe (CERT-UE), co powinno być jednym z pierwszych posunięć UE. Intensyfikacja działań na tym kierunku dopiero w 2012 roku, czyli 5 lat po pierwszej cyberwojnie świadczyła więc o poważnych zaniedbaniach. Po drugie, należy zauważyć, iż za wieloma deklaracjami Komisji Europejskiej bądź innych instytucji Unii nie podążyły konkretne inicjatywy. Stało się to szczególnie widoczne w przypadku współpracy międzynarodowej. Poza partnerstwem europejsko-amerykańskim, trudno bowiem wskazać na inne ważne i skutecznie funkcjonujące, globalne inicjatywy w zakresie cyberbezpieczeństwa, których UE byłaby aktywnym uczestnikiem. Po trzecie wreszcie, może dziwić fakt, iż Unia Europejska do końca 2012 roku nie opracowała jednolitej i spójnej strategii cyberbezpieczeństwa. Jej rolę pełniły dotychczas kolejne komunikaty i programy (np. CIIP) Komisji Europejskiej oraz Agenda Cyfrowa dla Europy, które szeroko nawiązywały do tej problematyki.

Politykę Unii Europejskiej wobec zagrożeń teleinformatycznych na przełomie pierwszej i drugiej dekady XXI wieku można więc oceniać dwojako. Z jednej strony, należy docenić, iż UE, mimo wielu przytoczonych powyżej głosów, nie podjęła kroków zmierzających do dublowania kompetencji państw członkowskich oraz funkcji Sojuszu Północnoatlantyckiego. Skupienie się na problematyce cyberprzestępczości należy uznać za zasadne, nie tylko z powodu jej rosnącego znaczenia dla bezpieczeństwa UE, ale także dotychczas niedostatecznie wykształconych mechanizmów współpra-

cy ponadnarodowej. Mimo wieloletniego okresu formułowania polityki bezpieczeństwa teleinformatycznego UE, potencjał ten nie został jednak dostatecznie wykorzystany. Warto zauważyć, iż tymczasowe inicjatywy Brukseli były realizowane bardzo powoli, często rozmijając się z dynamiką i charakterem pojawiających się w Internecie wyzwań. Z drugiej strony, można jednak zaobserwować intensyfikację współpracy w tym zakresie, która uwidoczniła się pod koniec 2012 roku. W tym kontekście, Unia Europejska na początku drugiej dekady XXI wieku stoi przed szeregiem wyzwań w zakresie rozwoju polityki cyberbezpieczeństwa. Należy do nich zaliczyć m.in.: określenie jasnych ram współpracy w środowisku międzynarodowym oraz na poziomie europejskim, opracowanie spójnej strategii cyberbezpieczeństwa UE, rozwój zdolności w zakresie koordynacji polityk państw członkowskich, organizacja wspólnych szkoleń, ćwiczeń i manewrów, rozbudowa potencjału reagowania na incydenty komputerowe, przygotowanie odpowiednich rozwiązań legislacyjnych oraz, *last but not least*, określenie jasnego stanowiska wobec dylematów związanych z ochroną wolności i prywatności użytkowników Internetu (Bendiek, 2012). Reasumując wydaje się, iż odpowiednie ustosunkowanie się do tych wyzwań będzie jednym z czynników, które w przyszłości będą wpływały na sytuację bezpieczeństwa Unii Europejskiej, tak w wymiarze wewnętrznym, jak i międzynarodowym.

Bibliografia

About us, CERT-EU, http://cert.europa.eu/cert/plainedition/en/cert_about.html.

Adair S., Deibert R., Walton G., *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Information Warfare Monitor, Shadowserver Foundation, 6.04.2010.

Ashton C., *Speech EU High Representative Catherine Ashton on Cyber security: an open, free and secure Internet*, European Union External Action, Budapest, 4.10.2012.

Baker J., *EU's cybersecurity budget up 14%*, IT World, 26.11.2012, http://www.itworld.com/it-management/321574/eus-cybersecurity-budget-14, 12.12.2012.

Baseline capabilities for national/governmental CERTs, European Network and Information Security Agency, Version 1.0, Initial Draft, December 2009.

Bautzmann A. (2012), *Le cyberspace, nouveau champ de bataille?*, „Diplomatie", luty–marzec.

Bendiek A. (2012), *European Cyber Security Policy*, „SWP Research Paper", RP 13.

Bógdał-Brzezińska A., Gawrycki M. F. (2003), *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacjia Studiów Międzynarodowych, Warszawa.

Clarke R. A., Knake R. (2010), *Cyberwar: The Next Threat to National Security and What to Do About It*, Ecco, New York.

Commission launches public consultation on network and information society, Europe's Information Society, 7.11.2008, http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4464, 10.12.2012.

Communication from the Commission to the Council and the European Parliament –*Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre* (2012), Commission of the European Communities, COM(2012) 140 final, Brussels, 28.03.2012.

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions (2006), Commission of the European Union, COM(2006) 251 Final, Brussels, 31.05.2006.

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, *Towards the general policy on the fight against cyber crime* (2007), Commission of the European Communities, Brussels 22.05.2007.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience* (2009), Commission of the European Communities, COM(2009) 149 Final, Brussels, 30.03.2009.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – *A Digital Agenda for Europe* (2010), Commission of the European Communities, COM(2010) 245 Final, Brussels, 19.05.2010.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – *Achievements and next steps: towards global cyber-security* (2011), Commission of the European Communities, COM(2011) 163 Final, Brussels, 31.03.2011.

Conférence sur la sécurité „Wehrkunde". Allocution du Président de la République (2009), M. Nicolas Sarkozy, *Déclaration de la politique étrangères*, Munich, 7.02.2009.

Cyber Security Strategy for Germany, Federal Ministry of the Interior, February 2011.

Cyberprzestrzeń – definicje, www.techsty.art.pl, 3.12.2012.

Department of Defense Strategy for Operating in Cyberspace, U.S. Department of Defense, July 2011.

Digital Agenda: European Commission supports research on Cyber security, Europa Press Release, MEMO/12/899, 26.11.2012, http://europa.eu/rapid/press-release_MEMO-12-899_en.htm, 12.12.2012.

Dziwisz D. (2011), *Cyberbezpieczeństwo – nowy priorytet strategii obrony Stanów Zjednoczonych*, „Sprawy Międzynarodowe", nr 3.

Electronic Civil Disobedience & Hacktivism, Zapatistas: the first „postmodern" revolution, 17.10.2011.

Ellis B. W. (10.04.2011), *The International Legal Implications and Limitations of Information Warfare: What are the Options?*, „USAWC Strategy Research Project".

EU Cyber Security and Defense: time to act now! Tunne Kelam MEP, EPP Group in the European Parliament, Press Release, 22.11.2012, http://www.eppgroup.eu/press/showpr.asp?prcontroldoctypeid=1&prcontrolid=11543&prcontentid=19197&prcontentlg=en, 12.12.2012.

European Cyber Security Month, European Network and Information Security Agency, http://www.enisa.europa.eu/activities/cert/security-month, 12.12.2012.

Finklea K. M., Theohary C. A. (20.07.2012), *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, „Congressional Research Service".

Gordon S., Ford R. (2003), *Cyberterrorism?*, „Symantec Security Response White Paper", Cupertino.

Healey J., van Bochoven L. (2012), *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, „Atlantic Council Issue Brief", February.

Information systems defence and security. France's Strategy, Agence Nationale de la Sécurité des Systemes d'Information, February 2011.

Konwencja Rady Europy o Cyberprzestępczości, Rada Europy, Budapeszt, 23.11.2001.

Lakomy M. (2010), *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations", nr 3–4.

Lakomy M. (2011), *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe – International Relations", nr 3–4.

Liedel K., Grzelak M. (2012), *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo narodowe", nr 2.

Making the Internet a safer place, European Commission. Information Society and Media, June 2008, http://ec.europa.eu/information_society/doc/factsheets/018-saferinternetplus-en.pdf, 10.12.2012.

Myrli S., *NATO and Cyber Defence*, NATO Parliamentary Assembly, 173 DSCFC 09 E BIS.

National Security Strategy, The White House, Washington D.C. 2010.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) (2004), Official Journal L 077, EURLEX, 13.03.2004.

Rewizorski M. (2010), *Rola Unii Europejskiej w budowie nowego ładu międzynarodowego*, „Rocznik Integracji Europejskiej", nr 4.

RFC 2350, Computer Emergency Response Team – CERT-UE*,* 25.10.2012.

Rohozinski R., Deibert R. (29.03.2009), *Tracking Ghostnet: Investigating a Cyber Espionage Network*, „Information Warfare Monitor".

Smith T., *EU must bolster its cyber security say MEP*, CBR, 23.11.2012, http://www.cbronline.com/news/eu-must-bolster-its-cyber-security-say-meps-231112, 12.12.2012.

Terlikowski M., *Haking, haktywizm, cyberterroryzm*, Polski Instytut Spraw Międzynarodowych, 23.04.2008, www.pism.pl, 1.12.2012.

The Growing Pains in EU Cyber Security Policy, „EuroWire", Bertelsmann Foundation 2011.

Streszczenie

Szkodliwa działalność w Internecie oraz innych sieciach teleinformatycznych, w XXI wieku stanowi coraz większe wyzwanie dla bezpieczeństwa narodowego i międzynarodowego. Co za tym idzie, problematyka ta stała się istotna nie tylko dla państw, ale także organizacji międzynarodowych. Unia Europejska, zrzeszająca jedne z najbardziej zdigitalizowanych społeczeństw globu, prowadzi prace w tej dziedzinie już od 2004 roku. Nie ulega jednak wątpliwości, iż wysiłki UE w dużej mierze rozminęły się z wagą zagrożeń cyberprzestrzennych. Do pewnej zmiany doszło dopiero po 2007 roku, kiedy Bruksela w wyniku „pierwszej cyberwojny" w Estonii, dostrzegła konsekwencje braku zabezpieczeń przed atakami komputerowymi. Wysiłki Unii, inspirowane w głównej mierze przez Komisję Europejską przebiegały dwutorowo. Z jednej strony, obejmowały one prace koncepcyjne, w tym m.in. analizę zjawiska cyberprzestępczości czy wrażliwości na ataki europejskiej krytycznej infrastruktury teleinformatycznej. Z drugiej, podejmowano prace na rzecz rozwoju współpracy w zakresie cyberbezpieczeństwa między UE a państwami członkowskimi. W tym kontekście, należy zauważyć, iż działania Unii Europejskiej w dużej mierze były opóźnione w stosunku do dynamiki pojawiających się w cyberprzestrzeni wyzwań. Co prawda, od 2007 roku, UE poczyniła szereg inicjatyw, które wzmocniły jej potencjał do działania w środowisku teleinformatycznym, jednak w wielu dziedzinach nadal istniały poważne zaniedbania. Pewna oznaka zmiany pojawiła się dopiero w 2012 roku, kiedy powołano zespół CERT-EU oraz zapowiedziano zwiększenie środków finansowych przeznaczonych na cyberbezpieczeństwo. Mimo to, w przyszłości Bruksela będzie musiała ustosunkować się do szeregu wyzwań w tej dziedzinie, w tym m.in.: modelu współpracy międzynarodowej, opracowania spójnej strategii bezpieczeństwa teleinformatycznego czy kwestii ochrony praw człowieka w sieci. Odpowiednia reakcja na te problemy będzie jednym z czynników, które

w przyszłości wpłyną na sytuację bezpieczeństwa Unii Europejskiej, tak w wymiarze wewnętrznym jak i międzynarodowym.

Summary

The European Union and threats to IT security – an outline of the issue

Harmful activities on the Internet are a growing threat to national and international security in the 21st century. These issues are therefore becoming increasingly important not only for individual states, but also for international organizations such as the European Union, which combines the most digitalized societies in the world. Despite the fact that a European cyber security policy was already initiated in 2004, the EU's attempts were usually quite outdated. A major breakthrough took place in 2007, after the 'first cyber war' in Estonia. Afterwards, Brussels' efforts went in two directions. On the one hand, the European Commission's activities were aimed at finding proper political, juridical and procedural solutions to cyber threats. On the other hand, the EU was interested in developing close cooperation with member states, as well as with the international environment. Unfortunately, most of the initiatives undertaken by the European Commission were still lagging behind the global standards set by the United States or the Atlantic Alliance. This situation changed only in 2012, when the EU undertook some important actions. First of all, a CERT-EU team was finally set up. Furthermore, the Commission declared that the funding of cyber security research would be increased by 14% in the future. And finally, ENISA undertook several important projects aimed at increasing cyber security awareness in Europe. These efforts, however, are not sufficient to fight the contemporary challenges arising from cyber space. This is why, in the future, in order to secure its political, social and economic development, the European Union will need to create a proper cyber security strategy.