POLITYKA BEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ WOBEC ZAGROŻEŃ CYBERTERRORYZMU

Aleksandra Kogut

Uniwersytet Rzeszowski

Streszczenie. Gwałtowny rozwój technologiczny spowodował tworzenie się nowych form terroryzmu. Cyberterroryzm jest nowym problemem, z którym borykają się wszystkie państwa. Celem działalności cyberterrorystycznej jest wprowadzenie chaosu w systemach informatycznych, na których bazuje działalność wszystkich instytucji państwowych. Polska, podobnie jak inne kraje, stoi przed koniecznością stałego ulepszania systemów ochronnych, aby zapobiegać potencjalnym zagrożeniom. Polityka bezpieczeństwa RP w tej dziedzinie musi podążać za nowymi wyzwaniami i dostosowywać się do istniejącej rzeczywistości. Usprawniając swoje działania i współpracując z całą społecznością międzynarodową, zapewni bezpieczeństwo swoim obywatelom i zagwarantuje kontynuację swojego sprawnego funkcjonowania.

Zjawisko terroryzmu, w szczególności międzynarodowego, stanowi obecnie problem o charakterze globalnym[1]. Wszystkie państwa wchodzące w skład społeczności międzynarodowej są w równym stopniu narażone na ataki terrorystyczne. Co więcej, globalny charakter współczesnego terroryzmu sprawia, że jest on jako zjawisko coraz bardziej niebezpieczny, trudny do zapobieżenia i pociąga za sobą niejednokrotnie tragiczne w skutkach konsekwencje. Sprzymierzeńcem terrorystów staje się zarówno postęp techniczny, jak i społeczny, niosący ze sobą takie wartości jak wolność osobista, swoboda podróżowania czy posiadania broni. Z kolei osiągnięcia w dziedzinie techniki, w szczególności w sferze środków transportu i łączności, są skutecznie wykorzystywane przez organizacje terrorystyczne[2].

Współczesny terroryzm ulega ciągłym przeobrażeniom, przybiera nowe, dotąd niespotykane formy, przez co wymyka się wszelkim uogólnieniom. Trudności ze zdefiniowaniem tego pojęcia wynikają również z różnic polityczno-ideologicznych i interpretacyjnych, bowiem czyn dla jednych wypełniający przesłanki aktu terrorystycznego, inni uznają za metodę walki wyzwoleńczej. W niektórych kręgach sprawca zamachu postrzegany będzie jako terrorysta, w innych natomiast zostanie uznany za bohatera[3].

---

1 Z. Mendrala, *Polska wobec zagrożeń terrorystycznych XXI w. Aspekty militarne*, (w:) K. Kowalczyk, W. Wróblewski (red.), *Terroryzm – globalne wyzwanie*, Toruń 2006, s. 173.

2 J. Konieczny, *Próba prognozy rozwoju współczesnego terroryzmu*, (w:) K. Sławik, *Terroryzm: aspekty prawno-międzynarodowe, kryminalistyczne i policyjne: materiały sympozjum zorganizowanego przez Wydział Prawa Uniwersytetu Szczecińskiego*, Poznań 1993, s. 107.

3 Z. Mendrala, op. cit.

Brak jednolitej i uniwersalnej definicji terroryzmu w prawie międzynarodowym jest spowodowany także różnicami politycznymi i prawnymi występującymi pomiędzy państwami. Z pewnością fakt ten stanowi istotną przeszkodę dla skutecznego zwalczania tego zjawiska, utrudnia kwalifikację niektórych czynów, a także znacząco komplikuje sytuację prawną osób zatrzymanych jako podejrzane o działania terrorystyczne[4].

Wśród licznie sformułowanych definicji terroryzmu dla przykładu wyróżnić można stanowisko Departamentu Obrony Narodowej Stanów Zjednoczonych, zgodnie z którym pod pojęciem terroryzmu rozumieć należy „bezprawne użycie bądź groźbę użycia siły lub przemocy wobec osoby lub mienia, by wymuszać lub zastraszać rządy czy społeczeństwa". Natomiast zdaniem NATO terroryzm to „bezprawne użycie lub zagrożenie użycia siły lub przemocy przeciwko jednostce lub własności w zamiarze wymuszenia lub zastraszenia rządów lub społeczeństw dla osiągnięcia celów politycznych, religijnych lub ideologicznych"[5].

W literaturze polskiej M. Madej stwierdza, że terroryzm to „służąca realizacji określonego programu politycznego przemoc lub groźba jej użycia, która ma wzbudzić strach w grupie (społeczeństwie) i w ten sposób doprowadzić do zniszczenia dotychczasowego porządku politycznego"[6].

Z kolei w polskim ustawodawstwie brakuje jednoznacznej legalnej definicji terroryzmu. W art. 2 pkt 7 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu brudnych pieniędzy określony został zamknięty katalog przestępstw stanowiących akt terrorystyczny. Zgodnie z ustawą są to przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne, przestępstwa przeciwko bezpieczeństwu powszechnemu oraz przestępstwa z art. 134-136 kodeksu karnego, tj. zamach na prezydenta RP, czynna napaść na prezydenta RP, znieważenie, czynna napaść oraz znieważenie prezydenta obcego kraju. Natomiast zgodnie z postanowieniami art. 115 § 20 kodeksu karnego za przestępstwo o charakterze terrorystycznym uznaje się czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej pięć lat, popełniony w celu:

1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy publicznej RP lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,

[4] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 176.

[5] *NATO and the fight against terrorism*; Tekst dostępny na stronie internetowej: www.nato.int/issues/terrorism/index.html (dostęp: 4.10.2012)

[6] M. Lasoń, *Kształtowanie się nowego ładu międzynarodowego w XXI w*., (w:) E. Cziomer (red.), *Międzynarodowe stosunki polityczne*, Kraków 2008, s. 381.

3) wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej, a także groźba popełnienia takiego czynu.

Poza problemami definicyjnymi zjawisko terroryzmu charakteryzuje także znaczący dynamizm, czego odzwierciedleniem jest mnogość klasyfikacji terroryzmu. Dla przykładu według kryterium podmiotowego wyróżniamy terroryzm niepaństwowy, sponsorowany przez państwa oraz państwowy. Z kolei kryterium przedmiotowe pozwala wyszczególnić terroryzm indywidualny, zbiorowy i ekonomiczny. Wśród innych podziałów wyróżnia się także terroryzm międzynarodowy, wewnętrzny, nacjonalistyczny, religijny czy ekoterroryzm[7].

W dobie globalizacji szczególnie interesującym i jeszcze nie do końca zbadanym zagadnieniem jest cyberterroryzm, będący aktem terrorystycznym stosowanym w tzw. cyberprzestrzeni. Geneza pojęcia „cyberprzestrzeń" wywodzi się z politycznej koncepcji „autostrad informacyjnych", stworzonej przy okazji kampanii prezydenckiej Billa Clintona z 1992 r. Zakładała ona, że wszelkiego rodzaju informacje zawierające tekst, dźwięk i obraz będą mogły być przesyłane na duże odległości szybko i bez przeszkód[8].

Mimo iż zagadnienie cyberterroryzmu znane jest od lat 70. XX w., nie doczekało się jeszcze uniwersalnej definicji. Jedna z najpopularniejszych i szeroko stosowanych definicji została sformułowana w 1998 r. przez Marka Pollitta, funkcjonariusza FBI. Jego zdaniem, cyberterroryzm „jest skrytym, politycznie motywowanym atakiem przeciwko informacji, systemom lub programom komputerowym, bazom danych, których efektem jest przemoc przeciwko celom niewojskowym realizowanym przez grupy ponadnarodowe"[9]. Z kolei w 2002 r. Ron Dick, ówczesny szef Departamentu Bezpieczeństwa Narodowego, stwierdził, iż cyberterroryzm stanowi „czyn przestępczy dokonywany za pośrednictwem komputera, którego rezultatem jest agresja, śmierć i/lub zniszczenie celem zmuszenia rządu do zmiany prowadzonej polityki"[10].

Brak jednoznacznej definicji cyberterroryzmu sprawia, iż często za akt terroru uznawany jest każdy umotywowany atak przeprowadzony za pośrednictwem Internetu[11]. D.E. Denning, specjalista w tej dziedzinie, stwierdza, że za atak cyberterrorystyczny można uznać tylko taki akt, który powoduje bezpośrednie szkody dla

---

[7] M. Lasoń, *Bezpieczeństwo w stosunkach międzynarodowych*, (w:) E. Cziomer (red.), *Bezpieczeństwo w XXI w. Wybrane problemy*, Kraków 2010, s. 24.

[8] A. Janowska, *Cyberterroryzm – rzeczywistość czy fikcja*?, Artykuł dostępny na stronie internetowej: http://winntbg.bg.agh.edu.pl/skrypty2/0095/445-450.pdf (dostęp: 4.10.2012).

[9] M.M. Pollitt, *Cyberterrorism: Fact or Fancy?*, (w:) Computer Fraud & Security, vol. 1998, no. 2, February 1998, s. 9.

[10] J. Mehan, *Cyberwar, Cyberterror, Cybercrime*, Cambs 2008, s. 32.

[11] A. Suchorzewska, op. cit., s. 64.

człowieka i jego mienia lub przynajmniej jest na tyle znaczący, że budzi strach[12]. Istotne zatem jest rozróżnienie pojęcia cyberterroryzm od dwóch innych zjawisk: aktywizmu i haktywizmu.

Przez aktywizm należy rozumieć normalne, niedestrukcyjne wykorzystanie Internetu dla wspierania prowadzonych działań, głównie przez zbieranie informacji, publikacji i prezentacji własnych poglądów oraz publikowanie tekstów czy zakładanie witryn internetowych[13]. Z kolei połączeniem aktywizmu z hakerstwem jest haktywizm. Haktywiści wykorzystują metody hakerskie celem zakłócenia normalnego funkcjonowania Internetu w danym obrębie, jednak nie powodują przy tym poważnych strat. Przykładem haktywizmu jest np. blokowanie rządowych witryn internetowych w różnego rodzaju protestach[14]. Powyższe rozróżnienie terminologiczne ma szczególne znaczenie dla właściwego osądzenia sprawcy i ewentualnego pociągnięcia go do odpowiedzialności.

Cyberterroryzm, będący co do zasady aktem nastawionym na wyrządzenie dotkliwej szkody, skierowany jest przede wszystkim przeciwko szeroko pojętej administracji państwowej i ma na celu sparaliżowanie systemu odpowiedzialnego za prawidłowe funkcjonowanie państwa. Podstawowym celem ataków cyberterrorystycznych mogą być systemy zarządzające bezpieczeństwem wewnętrznym, obroną narodową, łącznością i telekomunikacją, zaopatrzeniem w energię i wodę, a także sieciami finansowymi i ratownictwa[15]. Cyberterroryzm opiera się na różnorakich technikach i metodach, które stale ulegają przekształceniom wraz z rozwojem rynku zabezpieczeń. Wśród działań najczęściej stosowanych przez cyberterrorystów wyróżnia się:

- DDoS (Distributed Denial of Service) – sztucznie wytworzony natężony ruch powodujący blokadę systemu,
- flooding – skierowanie do danego systemu zbyt dużej ilości danych,
- phishing – wyłudzanie poufnych danych od nieświadomych użytkowników,
- włamanie do systemu wykorzystujące luki w oprogramowaniu zabezpieczającym bądź inżynierię społeczną, dzięki której można pozyskać hasła, a co za tym idzie, dostęp do utajnionych danych[16].

[12] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych 2003, s. 65.

[13] A. Suchorzewska, op. cit., s. 64.

[14] Ibidem, s. 65.

[15] Dane za stroną internetową: http://www.abw.gov.pl/portal/pl/89/307/Cele_atakow.html (dostęp: 4.10.2012).

[16] P. Borkowski, *Polska wobec zjawiska cyberterroryzmu. Stan bezpieczeństwa teleinformatycznego RP a współczesne zagrożenia* 23.03.2010; Artykuł dostępny na stronie internetowej: http://www.psz.pl/Piotr-Borkowski-Polska-wobec-zjawiska-cyberterroryzmu (dostęp: 4.10.2012).

Podobnie jak w przypadku terroryzmu, prawodawstwo polskie nie definiuje pojęcia cyberterroryzmu. Brak legalnej definicji oraz prawnego określenia znamion cyberterroryzmu powoduje znaczące utrudnienia w budowaniu strategii prewencyjnej, a także uniemożliwia skuteczne pociągnięcie do odpowiedzialności sprawców tych czynów[17].

Jedną z bardziej precyzyjnych definicji doktrynalnych, mogącą posłużyć za wzorzec dla prób prawnego uregulowania cyberterroryzmu, jest definicja zaproponowana przez K. Liedla, zgodnie z którą pod pojęciem cyberterroryzm należy rozumieć „politycznie umotywowany atak lub groźbę ataku na komputery, sieci lub systemy informatyczne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów"[18].

Istotne znaczenie dla rozwoju ustawodawstwa polskiego w zakresie problematyki cyberterroryzmu miał sporządzony w marcu 2009 r. *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011*. Program ten był pierwszym rządowym dokumentem całościowo obejmującym kwestie bezpieczeństwa przestrzeni cybernetycznej państwa, mającym na celu podniesienie bezpieczeństwa krytycznej dla państwa infrastruktury teleinformatycznej. Wskazuje on „propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania cyberterroryzmu oraz innych pochodzących z publicznych sieci teleinformatycznych zagrożeń dla państwa". Syntezuje, wyznacza kierunki i zadania dla poszczególnych podmiotów uczestniczących w ochronie cyberprzestrzeni kraju[19].

Dokument określił zakres pojęcia cyberprzestrzeni RP, stwierdzając, że „obejmuje ona między innymi systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne"[20]. Ponadto autorzy *Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011* akcentują konieczność stworzenia

---

[17] J. Świątkowska, I. Bunsch, *Cyberterroryzm – nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI w.*, brief programowy Instytutu Kościuszki, s. 4; Artykuł dostępny na stronie internetowej: http://ik.org.pl/cms/wp-content/uploads/2011/03/Cyberterroryzm-Brief-Programowy.pdf (dostęp: 4.10.2012).

[18] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005, s. 36.

[19] *Czy Polsce jest potrzeba narodowa strategia obrony przed terroryzmem?*, Biuro Bezpieczeństwa Narodowego, Warszawa, kwiecień 2009 r., s. 39.

[20] Rządowy Zespół Reagowania na Incydenty Komputerowe, *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*, s. 4; Dokument dostępny na stronie internetowej: http://www.cert.

legalnej definicji cyberterroryzmu, albowiem jest to „terroryzm wymierzony w newralgiczne dla państwa systemy, sieci i usługi teleinformatyczne", mogący zakłócić jego prawidłowe funkcjonowanie.

W czerwcu 2010 roku Ministerstwo Spraw Wewnętrznych i Administracji sformułowało nowy RZĄDOWY PROGRAM OCHRONY CYBERPRZESTRZENI RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2011-2016. Celem dokumentu jest zapewnienie stałego bezpieczeństwa cyberprzestrzeni RP poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy administracją publiczną oraz innymi podmiotami i użytkownikami cyberprzestrzeni RP, w tym przedsiębiorcami. Rządowy program z 2010 r. stanowi kontynuację działań podjętych na podstawie poprzedniego programu, przy czym ustala hierarchię priorytetów realizacji założeń programu, podkreślając konieczność kontynuowania działań legislacyjnych. Co więcej, program bezpośrednio wskazuje podmioty odpowiedzialne za ochronę cyberprzestrzeni RP, a także przedstawia podejmowane obecnie inicjatywy w tym zakresie[21].

Stan bezpieczeństwa informatycznego Polski jest zależny od licznych instytucji, organizacji, a także prywatnych firm. Ponieważ zjawisko to może wystąpić w wielu obszarach gospodarczych, militarnych czy państwowych, wiele podmiotów bierze na siebie odpowiedzialność za działania w tej dziedzinie[22].

Głównymi instytucjami państwowymi odpowiedzialnymi za bezpieczeństwo RP w tym zakresie są:

- Ministerstwo Spraw Wewnętrznych i Administracji,
- Agencja Bezpieczeństwa Wewnętrznego,
- Ministerstwo Obrony Narodowej,
- Służba Kontrwywiadu Wojskowego[23].

Ponadto w działania na rzecz ochrony CRP zaangażowane są takie podmioty jak Kancelaria Prezesa Rady Ministrów, Ministerstwo Edukacji Narodowej czy Komenda Główna Policji. Poza współpracą głównych instytucji państwowych, ochrona CRP ma opierać się także na działalności podmiotów wyspecjalizowanych w tej dziedzinie.

1 lutego 2008 r. powołany do życia został Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, który stanowi integralną część Agencji Bezpieczeństwa Wewnętrznego (Departamentu Bezpieczeństwa Teleinformatycznego). Do jego

gov.pl/portal/cer/30/23/Rzadowy_program_ ochrony_cyberprzestrzeni_RP_na_lata_20092011__zalozenia.html (dostęp: 4.10.2012).

[21] Rządowy Zespół Reagowania na Incydenty Komputerowe, *Rządowy program ochrony cyberprzestrzeni RP na lata 2010-2016 – założenia*, Dokument dostępny na stronie internetowej: http://bip.msw.gov.pl/download/4/7445/RPOC__24_09_2010.pdf (dostęp: 4.10.2012).

[22] P. Borkowski, op. cit.; artykuł dostępny na stronie internetowej: http://www.psz.pl/Piotr-Borkowski-Polska-wobec-zjawiska-cyberterroryzmu (dostęp: 4.10.2012).

[23] Ibidem.

głównych zadań należy „zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej RP do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa"[24].

Ponadto wyróżnić należy również CERT, czyli Zespół ds. Reagowania na Przypadki Naruszenia Bezpieczeństwa Teleinformatycznego. Pod tą nazwą w większości krajów Unii Europejskiej, Szwajcarii oraz w Stanach Zjednoczonych funkcjonują jednostki powołane do zwalczania incydentów komputerowych. Są to zazwyczaj ośrodki działające przy uczelniach technicznych lub firmach informatycznych[25].

CERT Polska funkcjonuje w ramach NASK, który jest instytucją badawczą i pełni funkcję krajowego rejestru nazw internetowych w domenie „.pl"[26]. W ramach swoich funkcji CERT zajmuje się:

- proaktywnym działaniem w celu zapobiegania zagrożeniom poprzez szerzenie informacji dotyczących potencjalnych zagrożeń,
- wspieraniem instytucji dotkniętych incydentem przez określenie przyczyny incydentu komputerowego, odnalezienie rozwiązania, poinformowanie innych potencjalnie zagrożonych instytucji[27].

Jako że Polska jest aktywnym członkiem społeczności międzynarodowej, prowadzona przez nią polityka bezpieczeństwa wobec cyberterroryzmu całkowicie pokrywa się z systemami przyjętymi w ramach Unii Europejskiej, Organizacji Narodów Zjednoczonych oraz Sojuszu Północnoatlantyckiego. Ponadto Polska wchodzi w skład organizacji IMPACT[28], będącej organizacją typu non-profit, powołanej celem wzmożenia współpracy państw w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni i udzielania wsparcia innym organizacjom działającym w tej dziedzinie. IMPACT udziela wsparcia m.in. wyspecjalizowanej agencji ds. cyberbezpieczeństwa – ITU (International Telecommunications Union)[29], powołanej w ramach Organizacji Narodów Zjednoczonych[30].

---

[24] CERT.GOV.PL, http://www.cert.gov.pl (dostęp: 4.10.2012).

[25] J. Świątkowska, I. Bunsch, op. cit., s. 8; Artykuł dostępny na stronie internetowej: http://ik.org.pl/cms/wp-content/uploads/2011/03/Cyberterroryzm-Brief-Programowy.pdf (dostęp: 4.10.2012).

[26] NASK http://www.nask.pl (dostęp: 4.10.2012).

[27] CERT.GOV.PL http://www.cert.pl/ (dostęp: 4.10.2012).

[28] IMPACT – International Multilateral Partnership Against Cyber Threats http://www.impact-alliance.org (dostęp: 4.10.2012).

[29] ITU: Committed to connecting the world http://www.itu.int (dostęp: 4.10.2012).

[30] J. Świątkowska, I. Bunsch, ibidem; Artykuł dostępny na stronie internetowej: http://ik.org.pl/cms/wp-content/uploads/2011/03/Cyberterroryzm-Brief-Programowy.pdf (dostęp: 4.10.2012).

Ostatnia dekada XX wieku przyniosła poważny postęp cywilizacyjny. Obejmuje on zmiany technologiczne, polityczne, społeczne i kulturowe. Postęp w globalnych procesach wytwarzania, przetwarzania i przekazywania informacji jest jednym z kluczowych elementów zachodzących zmian[31]. Gwałtowny rozwój techniczny usprawnia funkcjonowanie gospodarki, polepsza życie obywateli, równocześnie powodując postępujące uzależnienie od technologii informatycznych w każdej dziedzinie. Cyberprzestrzeń jest wyjątkowo rozbudowana, a co za tym idzie, coraz trudniejsze staje się jej kontrolowanie i zapewnienie bezpieczeństwa jej użytkownikom. Polska nigdy nie była przedmiotem typowego ataku cyberterrorystycznego, jednak nie można wykluczać takiego zagrożenia. Polityka Bezpieczeństwa RP zdołała wypracować w tym zakresie pewne mechanizmy obronne i zapobiegawcze, aczkolwiek z uwagi na ciągły rozwój i rozprzestrzenianie się cyberprzestępczości konieczne jest ich stałe aktualizowanie i usprawnianie.

LITERATURA:

1. P. Borkowski, *Polska wobec zjawiska cyberterroryzmu. Stan bezpieczeństwa teleinformatycznego RP a współczesne zagrożenia*, 23.03.2010, Aartykuł dostępny na stronie internetowej: http://www.psz.pl/Piotr-Borkowski-Polska-wobec-zjawiska-cyberterroryzmu (dostęp: 4.10.2012).
2. A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych 2003.
3. A. Janowska, *Cyberterroryzm – rzeczywistość czy fikcja*?, artykuł dostępny na stronie internetowej: http://winntbg.bg.agh.edu.pl/skrypty2/0095/445-450.pdf (dostęp: 4.10.2012).
4. J. Konieczny, *Próba prognozy rozwoju współczesnego terroryzmu*, (w:) K. Sławik, *Terroryzm: aspekty prawno-międzynarodowe, kryminalistyczne i policyjne: materiały sympozjum zorganizowanego przez Wydział Prawa Uniwersytetu Szczecińskiego*, Poznań 1993.
5. M. Lasoń, *Bezpieczeństwo w stosunkach międzynarodowych*, (w:) E. Cziomer (red.), *Bezpieczeństwo w XXI w. Wybrane problemy*, Kraków 2010.
6. M. Lasoń, *Kształtowanie się nowego ładu międzynarodowego w XXI w*., (w:) E. Cziomer (red.), *Międzynarodowe stosunki polityczne*, Kraków 2008.
7. K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005.
8. J. Mehan, *Cyberwar, Cyberterror, Cybercrime*, Cambs 2008.
9. Z. Mendrala, *Polska wobec zagrożeń terrorystycznych XXI w. Aspekty militarne*, (w:) K. Kowalczyk, W. Wróblewski (red.) *Terroryzm – globalne wyzwanie*, Toruń 2006.

[31] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Marynarki Wojennej", ROK XLVI NR 1 (160) 2005, s. 174; Artykuł dostepny na stronie internetowej: http://www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2005/Szubrycht_T.pdf (dostęp: 4.10.2012).

10. M.M. Pollitt, *Cyberterrorism: Fact or Fancy?*, (w:) Computer Fraud & Security, vol. 1998, no. 2, February 1998.
11. A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.
12. J. Świątkowska, I. Bunsch, *Cyberterroryzm – nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI w.*, brief programowy Instytutu Kościuszki, s. 4; Artykuł dostępny na stronie internetowej: http://ik.org.pl/cms/wp-content/uploads/2011/03/Cyberterroryzm-Brief-Programowy.pdf (dostęp: 4.10.2012).

Dokumenty:

1. *NATO and the fight against terrorism*; Tekst dostępny na stronie internetowej: http://www.nato.int/issues/terrorism/index.html (dostęp: 4.10.2012).
2. *Czy Polsce jest potrzebna narodowa strategia obrony przed terroryzmem?* Biuro Bezpieczeństwa Narodowego, Warszawa kwiecień 2009 r.
3. Rządowy Zespół Reagowania na Incydenty Komputerowe, *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia*, s. 4; dokument dostępny na stronie internetowej: http://www.cert.gov.pl/portal/cer/30/23/Rzadowy_program_ochrony_cyberprzestrzeni_RP_na_lata_20092011__zalozenia.html (dostęp: 4.10.2012).
4. Rządowy Zespół Reagowania na Incydenty Komputerowe, *Rządowy program ochrony cyberprzestrzeni RP na lata 2010-2016 – założenia*, dokument dostępny na stronie internetowej: http://bip.msw.gov.pl/download/4/7445/RPOC__24_09_2010.pdf (dostęp: 4.10.2012).

Strony internetowe:

http://www.cert.gov.pl (dostęp: 4.10.2012),

http://www.nask.pl (dostęp: 4.10.2012),

http://www.cert.pl/ (dostęp: 4.10.2012),

http://www.impact-alliance.org (dostęp: 4.10.2012),

http://www.itu.int (dostęp: 4.10.2012),

http://bip.msw.gov.pl/download/4/7445/RPOC__24_09_2010.pdf (dostęp: 4.10.2012),

http://www.cert.gov.pl/portal/cer/30/23/Rzadowy_program_ ochrony_cyberprzestrzeni_RP_na_lata_20092011__zalozenia.html (dostęp: 4.10.2012),

http://ik.org.pl/cms/wp-content/uploads/2011/03/Cyberterroryzm-Brief-Programowy.pdf (dostęp: 4.10.2012),

http://www.abw.gov.pl/portal/pl/89/307/Cele_atakow.html (dostęp: 4.10.2012),

http://www.psz.pl/Piotr-Borkowski-Polska-wobec-zjawiska-cyberterroryzmu (dostęp: 4.10.2012),

http://winntbg.bg.agh.edu.pl/skrypty2/0095/445-450.pdf (dostęp: 4.10.2012),

http:// www.nato.int/issues/terrorism/index.html (dostęp: 4.10.2012).

Security policy of the Republic of Poland towards cyberterrorism

Abstract. Rapid technological development resulted in the creation of new forms of terrorism. Cyber terrorism is a new problem faced by all countries. The aim of the cyber terrorist activity is to introduce chaos in computer systems, which are the base for all state's institutions. Poland, like other countries, faces the necessity of continuous improvement of safety systems to prevent potential hazards. RP security policy in this area must follow the new challenges and adapt to the existing reality. Streamlining its operations and cooperating with the entire international community will ensure the safety of its citizens and the continuation of its smooth functioning.