Sandra Tur
Państwowa Szkoła Wyższa
im. Papieża Jana Pawła II w Białej Podlaskiej

ZAGROŻENIE BEZPIECZEŃSTWA PAŃSTWA W XXI WIEKU – CYBERTERRORYZM

Streszczenie

Bezpieczeństwo jest fundamentem funkcjonowania współczesnego państwa, jak i całego świata. Obecna ekspansja Internetu w zasadniczy sposób wpływa na poziom bezpieczeństwa, który jest zmienny. Współczesny świat stoi u progu zagrożeń, które z upływem czasu, staną się realnym zagrożeniem. Historia zna już wiele przypadków wykorzystania cyberprzestrzeni do działań niezgodnych z prawem, a nawet i takich, które zagrażają bezpieczeństwu całego świata. Artykuł jest próbą przybliżenia istoty cyberterroryzmu, jako zjawiska, które udoskonala się wraz z rozwojem Internetu i możliwościami z nim związanymi. Problem ten dotyczy indywidualnych użytkowników, jak i całych państw.

Przemiany społeczno-technologiczne wpłynęły znacząco na zmianę podejścia do kwestii bezpieczeństwa. Jego stan nie jest już tylko związany z brakiem konfliktów czy wojen. Współcześnie zagrożenie bezpieczeństwa dotyka wszystkich, nawet w zaciszu własnego domu. Rozwój technologiczny, jego zaawansowanie, a przede wszystkim ekspansja Internetu, spowodowała zagrożenie atakami w cyberprzestrzeni. Dotyczy to indywidualnych użytkowników, jak i przede wszystkim całych państw. Rozwój technologiczny usprawnia zarządzanie wieloma sferami życia społecznego (banki, urzędy, szkoły, itp.) jednocześnie powoduje duże podporządkowanie się względem infrastruktury krytycznej. Zaatakowany element może powodować znaczące zakłócenia w całym systemie, poprzez wprowadzanie, modyfikowanie i przekształcanie danych oraz poprzez łamanie różnorodnych zabezpieczeń.

W XXI wieku jest to szczególnie znaczące zagrożenie w kontekście bezpieczeństwa Polski. Znaczenie granic państwa powoli zaciera się, co w konsekwencji prowadzi do swobodnego przepływu ludzi, kapitału, informacji czy wiedzy. Powoduje to zwiększenie wysiłków na rzecz utrzymania i poprawy bezpieczeństwa obywateli. Również procesy globalizacji negatywnie wpływają na poczucie bezpieczeństwa. Świat staje się otwarty, co staje się polem wielu ataków. Z analizy Centrum Badania Opinii Społecznej wynika, że większość Polaków nie czuje się bezpiecznie. „Opinie na temat bezpieczeństwa publicznego mogą wiązać się z zaufaniem do państwa i poszcze-

gólnych instytucji w kwestii radzenia sobie z problemem przestępczości. Jako jeden ze wskaźników opinii o sprawności instytucji państwa można potraktować poglądy na temat funkcjonowania demokracji w naszym kraju. Osoby niezadowolone z funkcjonowania demokracji zdecydowanie częściej wypowiadają się krytycznie o bezpieczeństwie publicznym (41% z nich uważa, że Polska nie jest krajem bezpiecznym, 55% ma odmienne zdanie), niż badani zadowoleni z obecnego systemu (odpowiednio 17% i 80%). (…) Mniej więcej połowa badanych czuje się osobiście zagrożona przestępczością (48%), ale tylko nieliczni czują silne obawy (4%). Nieco częściej ankietowani obawiają się o bezpieczeństwo swoich najbliższych (58%)"[1]. Z komunikatów dotyczących bezpieczeństwa w naszym kraju wynika, iż badani zdają sobie sprawę z zagrożeń oraz z możliwości ataków terrorystycznych. Z roku na rok rośnie liczba osób realnie obawiająca się ataku. Może mieć to oczywiście swoje podłoże w przekazie medialnym, który nieustannie informuje nas doniesieniami z Europy, jak i ze świata. „W ciągu ostatnich dwóch lat zauważalnie wzrosły też obawy związane z atakami terrorystycznymi. Wprawdzie nadal większość badanych nie obawia się ich (57%), jednak od roku 2013 grupa ta znacznie się zmniejszyła (o 15 punktów), zarazem w takim samym stopniu przybyło osób wyrażających przynajmniej umiarkowane obawy w tym zakresie (o 15 punktów, do 41%). Obecny poziom obaw jest najwyższy w ostatnich pięciu latach, ale niższy niż w latach 2003–2005, natomiast zbliżony do zarejestrowanego w roku 2001 i 2002"[2].

Istota zagrożeń w cyberprzestrzeni

Zgodnie z przyjętą definicją w *Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*:

1. „Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.
2. Cyberprzestrzeń RP (dalej jako CRP) – cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe).
3. Cyberprzestępstwo – czyn zabroniony popełniony w obszarze cyberprzestrzeni.

[1] K. Kowalczuk, *Polacy o bezpieczeństwie w kraju i miejscu zamieszkania*. *Komunikat z badań Centrum Badania Opinii Społecznej*, Warszawa 2015, s. 4-5.

[2] M. Feliksiak, *Zagrożenie terroryzmem*. *Komunikat z badań Centrum Badania Opinii Społecznej*, Warszawa 2015, s. 2.

4. Cyberterroryzm – cyberprzestępstwo o charakterze terrorystycznym.
5. Cyberatak – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników. Umożliwia ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu (…)"[3].

Cyberterroryzm jest połączeniem terroryzmu z cyberprzestrzenią. Dzięki rozbudowanej sieci technologicznej państwa są narażone na ataki ze wszystkich stron świata, bez użycia typowej broni używanej w rzeczywistości społecznej. „Terroryzm to metoda działania polegająca na przemocy wobec innych, pojedynczych ważnych osób, zbiorowisk ludzkich lub wobec przypadkowych grup ludzi znajdujących się w różnych obiektach na terenie kraju, np. w miejscach pracy, w środkach komunikacyjnych, w różnego rodzaju lokalach, itp. Terroryzm ma różne formy, między innymi są to klasyczne akty kryminalne (morderstwa, podpalenia) i inne, które polegają na celowym wywołaniu terroru, tzn. wywołaniu niepewności, paniki, zastraszenia w celu osiągnięcia zamierzeń politycznych lub zmuszenia organu władzy publicznej do podjęcia lub zaniechania określonych czynności. Wspólnymi cechami terroryzmu i cyberterroryzmu jest stosowanie przemocy w celu wywołania zamierzonych i wskazanych powyżej skutków i celów. Z uwagi na ich medialność w społeczeństwie, wspólnym składnikiem jest wywołanie lęku, niepewności i zastraszenia. Aktorami cyberterroryzmu są głównie osoby i organizacje, grupy kryminalne, wspierane przez cyberterrorystów oraz państwa stosujące terroryzm"[4].

Skala omawianego zjawiska jest tak poważna i znacząca, że w 2010 roku przez Ministerstwo Spraw Wewnętrznych i Administracji, został opracowany, wspomniany wcześniej: *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*. Program zawiera opracowanie strategiczne dotyczące bezpieczeństwa Rzeczypospolitej Polskiej i jej obywateli w cyberprzestrzeni. Wyznaczone zostały jednostki powołane do utrzymania bezpieczeństwa, wzajemna współpraca oraz ustalono hierarchię priorytetów dotyczących realizacji programu. Celem programu jest ciągła poprawa bezpieczeństwa państwa w cyberprzestrzeni, co będzie realizowane przez: „1. Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej, w tym teleinformatycznej infrastruktury krytycznej państwa; 2. Zmniejszenie skutków naruszeń bezpieczeństwa cyberprzestrzeni; 3. Zdefiniowanie kompetencji podmiotów odpowiedzialnych za

[3] *Rządowy program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016*, RCB, Warszawa 2010, s. 6

[4] J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i techniki informacyjne" 2014, nr 1-2, s. 25.

ochronę cyberprzestrzeni; 4. Stworzenie i realizacja spójnego dla wszystkich podmiotów administracji publicznej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych; 5. Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni oraz przedsiębiorcami, dostarczającymi usługi w cyberprzestrzeni i operatorami teleinformatycznej infrastruktury krytycznej; 6. Zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni"[5].

Rodzaje zagrożeń w cyberprzestrzeni

W literaturze przedmiotu opisywanych jest szereg informacji na temat rodzajów przestępstw w cyberprzestrzeni. Uściślenia kategorii podjęła się Unia Europejska, ustalając na gruncie Konwencji Rady Europy o cyberprzestępczości (ETS/STE Nr 185), iż cyberprzestępstwa dzieli się na:

1. „przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów obejmujące: nielegalny dostęp (art. 2), nielegalne przechwytywanie danych (art. 3), naruszenie integralności danych (art. 4), naruszenie integralności systemu (art. 5), niewłaściwe użycie urządzeń (art. 6);
2. przestępstwa komputerowe obejmujące: fałszerstwo komputerowe (art. 7), oszustwo komputerowe (art. 8);
3. przestępstwa ze względu na charakter zawartych informacji, w tym: przestępstwa związane z pornografią dziecięcą (art. 9) oraz dodane w protokole dodatkowym do konwencji: rozpowszechnianie materiałów o treściach rasistowskich i ksenofobicznych przez systemy komputerowe (art. 3, groźby motywowane rasizmem lub ksenofobią (art. 4), zniewaga motywowana rasizmem lub ksenofobią (art. 5), zaprzeczanie, rewidowanie albo usprawiedliwianie ludobójstwa oraz zbrodni przeciwko ludności (art. 6);
4. przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Również na forum Organizacji Narodów Zjednoczonych podejmuje się próby zdefiniowania i podziału wskazanych przestępstw. Zgodnie z definicją wypracowaną przez Organizację Narodów Zjednoczonych podczas Dziesiątego Kongresu Narodów Zjednoczonych w sprawie Zapobiegania Przestępczości i Traktowania Przestępców, który miał miejsce od 10 do 17 kwietnia 2000 r. w Wiedniu, o cyberprzestępczości można mówić w wą-

[5] *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, RCB, Warszawa 2010, s. 7.

skim i szerokim sensie. W sensie szerokim zalicza się do nich wszystkie nielegalne działania, popełnione za pomocą lub dotyczące systemów lub sieci komputerowych. Natomiast w sensie wąskim za cyberprzestepstwo uznaje się działania dokonane za pomocą operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych oraz procesowanych przez te systemy danych”[6]. Każdy obiekt znajdujący się w przestrzeni wirtualnej może stać się atakiem cyberterrorystów. „Najczęściej mogą to być ważne węzły informacyjne, teleinformatyczne oraz telekomunikacyjne, które mogą spowodować zakłócenia zasobów teleinformatycznych i telekomunikacyjnych, niepewność w społeczeństwie, strach, panikę i podobne następstwa. Jest oczywistym, że zagrożeniem szczególnym w działalności cyberterrorystycznej jest infrastruktura krytyczna państw, wspólnot i różnego rodzaju organizacji, czyli systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje w szczególności systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, bankowe i finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające funkcjonowanie administracji publicznej, produkcji, stosowania, przechowywania i składowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Elementami, które w szczególności zostały zaklasyfikowane do krytycznej infrastruktury telekomunikacyjnej są systemy i sieci telekomunikacyjne, teleinformatyczne niezbędne do wykonywania statutowych zadań organów administracji rządowej oraz wymiany informacji w siłach zbrojnych i rejestry państwowe w warstwie aplikacyjnej, a także sieci telekomunikacyjne wykorzystywane przez administrację publiczną (rządową i samorządową) i siły zbrojne w warstwie medium transmisyjnego”[7].

Wskazane przykłady miejsc zagrożonych atakami cyberterrorystycznymi w skali danego państwa, świadczą o sile tego negatywnego zjawiska. Liczne możliwości, jakie stoją przed terrorystami, którzy specjalizują się w wykorzystaniu komputera w celu ataku, wskazują doniosłą rolę organów sprawujących ochronę cyberprzestrzeni.

[6] M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo” 2012, nr 7-8, s. 247-248.
[7] J. Kowalewski, M. Kowalewski, op. cit., s. 27-28.

Zagrożenie cyberterroryzmem

O sile terroryzmu i jego wpływie na opinię publiczną, świat dowiedział się 11 września 2001 roku, po ataku na World Trade Center. Był to moment przełomowy w postrzeganiu cyberterroryzmu, jako zjawiska zagrażającemu każdemu państwu na świecie, nawet najlepiej zabezpieczonemu. Przykładem jest również tzw. estońska cyberwojna z 2007 roku, kiedy to w następstwie likwidacji pomnika żołnierzy radzieckich w Tallinie, w ciągu kilku dni zaatakowano estońskie witryny rządowe, uniwersyteckie, bankowe i prasowe, doprowadzając do zaprzestania świadczenia usług bankowości elektronicznej online, zablokowania stron internetowych partii politycznych, itp. Kulminacja ataku nastąpiła 9 maja, w rocznicę zakończenia II Wojny Światowej. Ataków dokonywano z komputerów zlokalizowanych w ponad pięćdziesięciu krajach świata, a ustały one po około trzech tygodniach. Cyberwojna cechowała się, analogicznie jak cyberterroryzm: niskimi kosztami działalności, zaniknięciem granic państwowych, możliwością dokonywania nagłych i nieprzewidzianych ataków, anonimowością atakujących, minimalnym ryzykiem wykrycia ataku oraz możliwością sparaliżowania systemu wrogiego kraju[8]. Według D. E. Denninga – amerykańskiego eksperta do spraw cyberbezpieczeństwa: „Cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien on skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczające szkody, by stwarzać strach”[9]. Natomiast zdaniem Jamesa Lewisa, cyberterroryzm to: „(...) wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań”[10].

Mimo jeszcze małego wpływu cyberterroryzmu, jego skutki są tak samo tragiczne i niebezpieczne, jak w przypadku tradycyjnego terroryzmu. Środki prewencyjne podejmowane przez poszczególne państwa mają na celu minimalizowanie niebezpieczeństwa oraz zwiększenie poczucia bezpieczeństwa wśród obywateli i wszystkich użytkowników sieci. Cyberterroryzm

[8] M. Czyżak, *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i techniki informacyjne”, 2010, nr 1-2, s. 48-49.

[9] J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Wydawnictwo Placet, Warszawa 2008, s. 69.

[10] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej” 2005, Nr 1 (160), s. 175.

jest niezwykle niebezpiecznym zagrożeniem przede wszystkim w stosunku do rządu poszczególnych państw, gdyż jego głównym celem jest wymuszenie określonych zachowań zgodnych z życzeniami terrorystów.

Podsumowanie

Dzisiejszy świat jest połączony w globalnej sieci techniczno-komunikacyjnej. Państwa istnieją i rozwijają się na zasadzie współpracy, wymiany (od handlu, po informację, wiedzę, innowacje). Swobodne przepływy, przenoszenie życia społecznego również do sieci oraz umiejętne negatywne wykorzystanie jej zasobów przez hakerów, co powoduje zwiększenie poczucia zagrożenia. Dla indywidualnych jednostek cyberprzestępstwa nie są nowością. Natomiast cyberterroryzm często nie jest uświadamiany. W końcu co złego może zrobić komputer – jedynie się zawiesić. Otóż cyberterroryści mając dostęp do sieci i swoją wiedzę mogą sparaliżować systemy bankowe, rządowe, lotnicze oraz wszystkie inne, do których mamy dostęp dzięki komputerowi. Wszyscy są zagrożeni bez względu na to, czy bezpośrednio czy tylko pośrednio korzystają z zasobów sieci. Z badań przeprowadzonych w maju 2013 roku przez Centrum Badania Opinii Społecznej wynika, że: „blisko połowa dorosłych Polaków ma stały dostęp do internetu tylko w domu, a co piąty – zarówno w domu, jak i w pracy lub szkole. Możliwość korzystania z internetu wyłącznie w miejscu pracy lub w szkole ma 1% badanych. Można zatem powiedzieć, że stałym dostępem do sieci cieszy się 71% Polaków. Zbiorowość osób nie mających w ogóle dostępu do internetu stanowi mniej niż jedną trzecią społeczeństwa (29%). (…) Zagrożenia płynące z internetu, w tym cyberterroryzm, przeważnie uważane są za realne. Co jednak ciekawe, internauci częściej dostrzegają zagrożenia dla firm, dużych korporacji i instytucji państwowych niż dla społeczeństwa lub osób prywatnych”[11].

Jak pokazuje wcześniej wspomniana sytuacja Estonii czy Stanów Zjednoczonych cyberterroryzm dotyka wszystkich obywateli, a nie tylko instytucje państwowe. Atak wymierzony jest w organizacje rządowe, w celu sparaliżowania całego społeczeństwa, w tym pojedynczych jednostek. Niemniej jednak jest to zagrożenie wynikające z obecnych czasów i tym samym nowe, co powinno być uwzględniane w polityce społecznej, aby zaczęto o tym rozmawiać i oswajać się z ewentualnymi zagrożeniami ze strony cyberterrorystów oraz aby to zagadnienie zaistniało w świadomości społecznej. Największym zagrożeniem jesteśmy często my sami, tworząc hasła bez większego zastanowienia, podając dane, których nie powinniśmy ujawniać,

[11] J. Fryłow, *Opinie o bezpieczeństwie w Internecie*, Komunikat z badań Centrum Badania Opinii Społecznej, Warszawa 2013, s. 3-6.

pisząc o sobie i tworząc profile jesteśmy podatni na ataki. „Łamałem ludzi, nie hasła". To słowa wypowiedziane przez jednego z najpotężniejszych przestępców w historii działań cyberprzestępczych. Z wykorzystaniem metod socjotechnicznych oraz przy użyciu ponadprzeciętnych umiejętności informatycznych wykradał kluczowe informacje oraz włamywał się do najważniejszych systemów teleinformatycznych, jakie istniały w okresie jego działalności. Kevin Mitnick, bo o nim mowa, przez kilkanaście lat wymykał się wymiarowi sprawiedliwości Stanów Zjednoczonych. Skazany łącznie na kilkaset lat więzienia za przestępstwa komputerowe, został zwolniony po zaledwie czterech, by pełnić rolę głównego doradcy do spraw bezpieczeństwa w Pentagonie. Według niego to „czynnik ludzki od wieków jest najsłabszym ogniwem bezpieczeństwa informacji". Te słowa na pozór wydają się niegroźne, ale zwracają uwagę na bardzo ważny aspekt, zwłaszcza teraz, gdzie informacja ma kluczowe znaczenie. Jego słowa potwierdzają, że to człowiek stanowi największe zagrożenie w wycieku oraz dostępie do informacji osób niepożądanych"[12].

Bibliografia

1. Czyżak M., *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i techniki informacyjne" 2010, nr 1-2.
2. Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, PWN, Warszawa 2002.
3. Feliksiak M., *Zagrożenie terroryzmem*, Komunikat z badań Centrum Badania Opinii Społecznej, Warszawa 2015.
4. Fryłow J., *Opinie o bezpieczeństwie w Internecie*, Komunikat z badań Centrum Badania Opinii Społecznej, Warszawa 2013.
5. Kisielnicki J., *MIS. Systemy informatyczne zarządzania*, Wydawnictwo Placet, Warszawa 2008.
6. Kowalczuk K., *Polacy o bezpieczeństwie w kraju i miejscu zamieszkania*, Komunikat z badań Centrum Badania Opinii Społecznej, Warszawa 2015.
7. Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i techniki informacyjne" 2014, nr 1-2.
8. *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, RCB, Warszawa 2010.

[12] D. Gałan, *Ataki cyberterrorystyczne jako nowe zagrożenie dla społeczeństwa informacyjnego*, http://academicon.pl/blogi_naukowe/bezpieczenstwo-w-sieci/cyberterroryzm-jako-nowe-wyzwanie spoleczenstwa-informacyjnego (dostęp: 30.06.2015).

9. Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, 7-8.
10. Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1 (160).

Liczba znaków ze spacjami: 20 363