

Zbigniew CIEKANOWSKI¹
Krzysztof REJMAN²
Henryk WYRĘBEK³

CYBERTERRORYZM JAKO WSPÓŁCZESNA BRÓŃ MASOWEGO RAŻENIA

Wraz z rozwojem techniki komputerowej pojawiło się nowe określenie – „cyberterroryzm” jako współczesny rodzaj broni masowego rażenia, która wraz z dalszym rozwojem będzie stawać się coraz bardziej niebezpieczna. Cyberterroryzm jako specyficzna kategoria zagrożeń obejmuje działania w stosunku do systemów teleinformatycznych, podejmowane dla osiągnięcia konkretnych celów terrorystycznych. Organizacje terrorystyczne są z reguły powiązane z jakimś państwem, jego służbami specjalnymi, wyznaniem religijnym, grupami przestępczymi lub mogą funkcjonować w celu zdobycia popularności na arenie krajowej (lokalnej) czy międzynarodowej. Działania te mają specyficzne cele, które pozwalają uzyskać wpływ na decyzje socjalne, polityczne czy nawet militarne. W artykule podjęto próbę analizy istoty i uwarunkowań cyberterroryzmu. Wskazano jakie elementy warunkują łatwość rozpowszechniania się cyberagresji oraz określono co wpływa na asymetryczność konfliktu wywołanego przez niepożądaną działalność przestępców w sieci. Przedstawiono pojęcia ściśle związane z poruszaną tematyką jak m.in.: cyberprzestrzeń, cyberprzestępstwo, cyberagresja, cyberterrorysty oraz odniesiono się do ram funkcjonowania podmiotów w sieci, które ustala prawodawstwo międzynarodowe. Wskazano zatem na podstawowe regulacje zatwierdzone przez Unię Europejską, ale i państwa skupione wokół NATO. Ponieważ działalność cyberterrorystów zorientowana jest na wywołanie paraliżu płaszczyzny politycznej, społecznej, psychologicznej oraz ekonomicznej, próby monitorowania zagrożeń dotyczą bardzo szerokiego pola oddziaływania. W treści opracowania wskazano, że szcze-

¹ Dr hab. inż. Zbigniew Ciekowski, prof. nadzw., Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej, ul. Sidorska 95/97, 21-500 Biała Podlaska; e-mail: zbigniew@ciekanowski.pl.

Zbigniew Ciekowski, DSc, PhD, Eng., Associate Prof., The Pope John Paul II State School of Higher Education in Biała Podlaska, Sidorska 95/97, 21-500 Biała Podlaska; e-mail: zbigniew@ciekanowski.pl.

² Dr hab. Krzysztof Rejman, prof. nadzw., Katedra Nauk Humanistycznych, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Al. Powstańców Warszawy 12, 35-959 Rzeszów; e-mail: krejman@poczta.onet.pl (autor korespondencyjny).

Krzysztof Rejman, DSc, PhD, Associate Prof., Rzeszow University of Technology, Faculty of Management, Powstańców Warszawy 12, 35-959 Rzeszów; e-mail: krejman@poczta.onet.pl (corresponding author).

³ Dr hab. inż. Henryk Wyrębek, prof. nadzw., Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Wydział Humanistyczny, ul. Stanisława Konarskiego 2, 08-110 Siedlce; e-mail: henryk.wyrebek@uph.edu.pl.

Henryk Wyrębek, DSc, PhD, Eng., Associate Prof., Siedlce University of natural Science and Humanities, Faculty of Humanities, Stanisława Konarskiego 2, 08-110 Siedlce; e-mail: henryk.wyrebek@uph.edu.pl.

gólnie narażone na działanie cyberterrorystów są sektory, w których funkcjonują sieci telekomunikacyjne (infrastruktura telefoniczna, satelitarna oraz komputerowa), sektor finansowy i bankowy, transport, sektor energetyczny oraz instytucje władz publicznych. Autorzy opracowania snują rozważania wokół tezy, że zakłócenie działania, choć jednego z wymienionych wyżej sektorów, może doprowadzić do ogromnych, negatywnych konsekwencji dla każdego obywatela danego państwa.

Słowa kluczowe: cyberprzestrzeń, cyberprzestępstwo, cyberagresja, cyberterroryści, prawodawstwo międzynarodowe.

1. WSTĘP

Choć prace nad Internetem trwają od końca lat 60. XX wieku, to dopiero w ostatniej dekadzie ubiegłego wieku nastąpił jego niebywały rozwój i upowszechnienie. Jak wynika z ostrożnych szacunków w lipcu 2012 r. ponad 34% społeczeństwa światowego (czyli około 2,4 miliarda osób) miało stały dostęp do sieci internetowej, a w Polsce odsetek ten przekroczył 65%.

Rozwój sieci spowodował sytuację, że człowiek, posiadający odpowiedni sprzęt i umiejętności ma nieograniczony dostęp do każdej informacji. Dodatkowo coraz częściej z medium tego korzystają różne podmioty – rządy, instytucje czy przedsiębiorstwa. System WWW, poczta internetowa, a także ogólny dostęp do fizycznej infrastruktury pozwalającej na niebywale szybki transfer danych i informacji z olbrzymią prędkością stanowi nie tylko o sile, ale i o słabości Internetu. Ponieważ dostęp do sieci jest powszechny, coraz częściej jest ona wykorzystywana przeciwko społeczeństwu, które narażone jest na szereg działań określanych jako przestępczość cybernetyczna⁴.

Skutki zamachów w cyberprzestrzeni w 2007 r. odczuła Estonia, w której po atakach internetowych nastąpił całkowity paraliż stron należących do banków, mediów, przedsiębiorstw, jak i urzędów państwowych. W tym samym r. Izrael po zainfekowaniu komputerów systemu lotniczego Syrii przeprowadził atak na ośrodek wojskowy tego kraju. Rok później, w trakcie konfliktu rosyjsko-gruzińskiego, służby rosyjskie zainfekowały gruzińską sieć, wskutek czego na wiele dni wyłączone zostały państwowe strony internetowe. W 2010 r. wywiad Stanów Zjednoczonych wpuścił wirusa do irańskich komputerów kontrolujących prace nad programem atomowym, a cały świat obiegła informacja o cyberszpiegach pochodzących z Chin. Wszystkie te wydarzenia doprowadziły nie tylko do olbrzymich strat ekonomicznych, ale wykazały również jak groźny staje się cyberterroryzm⁵.

Według wielu osób cyberterroryzm powinien stać się przedmiotem zainteresowania polityków, ekonomistów, naukowców i prawników, ponieważ stanowi wielkie zagrożenie dla bezpieczeństwa zarówno krajowego, jak i międzynarodowego. Wynika to z kilku powodów⁶:

⁴ M. Karatysz, *Zjawisko cyberprzestępczości, a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski*, Poznań 2013, s. 140.

⁵ M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, „E-Politykon” 6/2013, Warszawa 2013, s. 101.

⁶ J. Świątkowska, I. Bunsch, *Cyberterroryzm, nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku*, Warszawa 2011, s. 2.

1. niskich kosztów przeprowadzenia ataku, aby prowadzić działalność w cyberprzestrzeni nie trzeba dużych nakładów finansowych, a jedynie specjalistycznej wiedzy;
2. bezpieczeństwa, ogranicza on konieczność narażania zdrowia lub życia;
3. względnej anonimowości, trudno jest namierzyć osobę, która przeprowadziła atak, a jeśli już to się uda nie wiadomo czy działała ona samodzielnie, czy jest też częścią większej organizacji;
4. cech środowiska działania, atak w cyberprzestrzeni można przeprowadzić w dowolnym czasie, z dowolnego miejsca na ziemi, tak więc nie ma ograniczenia czasowego czy miejscowego;
5. efekt psychologiczny, ponieważ z Internetu korzystają rządy poszczególnych krajów, przedsiębiorstwa i organizacje międzynarodowe trudno oszacować skutki i skalę takiego ataku.

Z powodu wyżej wymienionych przyczyn cyberprzestrzeń stała się wyjątkowo atrakcyjnym miejscem dla działań prowadzonych przez ugrupowania terrorystyczne, pozwalającą na podejmowanie innowacyjnych i nieszablonowych działań o poważnych konsekwencjach. Powstaje tu swoisty konflikt asymetryczny, z jednej strony organy i siły odpowiedzialne za bezpieczeństwo państwa powinny być przygotowane na wystąpienie szeregu przestępstw, zabezpieczać muszą wszelkie punkty newralgiczne sieci, z drugiej strony – cyberterrorystom wystarczy tylko jeden słaby punkt do przeprowadzenia ataku⁷.

2. POJĘCIA ZWIĄZANE Z CYBERTERRORYZMEM

Cyberprzestrzeń jest to przestrzeń cyfrowa, w której następuje przetwarzanie i wymiana informacji i wiadomości. Tworzą ją sieci i systemy teleinformatyczne, jak również powiązania pomiędzy nimi i użytkownikami⁸.

Cyberprzestrzeń może być również rozumiana jako obszar, domena cyfrowa służąca do wymiany informacji. Ma ona charakter ponadnarodowy i stanowi ją suma działań wykonywanych przez użytkowników. Jest to więc nowy wymiar ludzkich działań⁹.

Cyberprzestępstwo jest to wszelkiego rodzaju czyn zabroniony, który popełniony został w cyberprzestrzeni¹⁰.

Inny typ definicji uwzględnia pojmowanie tego terminu w sposób szeroki i wąski¹¹:

- w szerokim rozumieniu, będą to wszelkiego rodzaju działania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, godzące nie tylko w informację, ale również cały system połączeń komputerowych, jak i w sam komputer;
- w wąskim znaczeniu są to czyny zabronione dokonywane przy pomocy komputera.

⁷ Tamże, s. 4.

⁸ J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne”, 1–2/2014, s. 24.

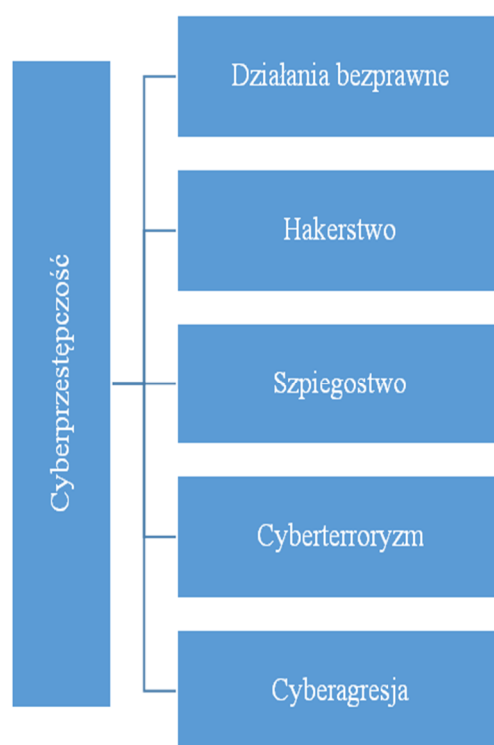
⁹ J. Wasilewski, *Zarys definicji cyberprzestrzeni* [w:] *Przegląd bezpieczeństwa narodowego*, red. B. Hołyst, Warszawa 2013, s. 231.

¹⁰ J. Kowalewski, M. Kowalewski, *Cyberterroryzm...*, s. 24.

¹¹ G. Kuta, *Cyberterroryzm – zagrożenie dla bezpieczeństwa informacji i danych osobowych*, Poznań 2012, s. 8.

Zgodnie ze stanowiskiem Rady Europy pod pojęciem cyberprzestępczości należy rozumieć, fałszerstwa i oszustwa komputerowe, naruszania praw autorskich i pokrewnych, jak również czyny zabronione związane z treściami pedofilskimi. Natomiast według Interpolu, omawiany termin rozpatrywać należy w dwóch kategoriach: wertykalnej (są to przestępstwa popełniane tylko w cyberprzestrzeni) i horyzontalnej (to przestępstwa popełnione przy pomocy techniki elektronicznej)¹².

Wyróżnić można kilka typów działań zaliczanych do cyberprzestępczości, co przedstawia rys. 1.



Rys. 1. Działania zaliczane do cyberprzestępczości

Źródło: T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Gdynia 2005, s. 177.

Hakerstwo, to poszukiwanie i wykorzystywanie dziur w oprogramowaniu komputerowym, pozwalająca na uzyskanie dostępu do zabezpieczonych informacji. Są to działania zmierzające do dokonania zmian na stronach internetowych, jak również kradzieży i zniszczenia danych¹³.

¹² <http://lexblog.pl/definicja-cyberprzestepstwa/> (dostęp: 15.02.2017 r.).

¹³ S. Forlicz, *Informacja w biznesie*, Warszawa 2008, s. 174.

Szpiegostwo komputerowe są to działania dokonywane na szkodę państwa, przedsiębiorstwa, instytucji, które polegają na zbieraniu i przekazywaniu informacji obcemu wywiadowi, przedsiębiorstwu lub instytucji¹⁴.

Cyberagresja to forma prześladowania, w skład której wchodzi: kłamstwa, plotki, zamieszczanie nieprzyjaznych i obraźliwych komentarzy, które realizowane są poprzez czaty, pocztę elektroniczną, strony internetowe; jest to również zamieszczanie niechcianych zdjęć lub filmów¹⁵.

W literaturze można spotkać się z wieloma definicjami cyberterroryzmu. Według D. Denning jest to bezprawny atak (lub jego groźba), który wymierzony jest w dane lub sam system informatyczny. Ma on na celu zastraszenie lub wymuszenie na władzach pewnych zachowań, a jego skutki powodują powszechne poczucie zagrożenia i strachu¹⁶.

Cyberterroryzm jest formą terroryzmu wykorzystującą cyberprzestrzeń jako pole działania, a jej celem jest wywołanie paniki lub zastraszenie, tak aby osiągnąć zamierzenia polityczne lub zmusić władze do pewnych działań¹⁷.

J. Lewis podkreśla, że celem cyberterroryzmu jest nie tylko wymuszenie określonych działań, ale również sparaliżowanie lub osłabienie działania energetyki, transportu i innych struktur narodowych¹⁸.

Cyberterroryzm może być też rozumiany jako działanie blokujące, zniekształcające lub niszczące informacje przechowywane i przekazywane w cyberprzestrzeni oraz obezwładniające systemy teleinformatyczne. Jego celem jest dezinformacja oraz prowadzenie walki psychologicznej¹⁹.

Należy pamiętać, że cyberterroryzm ma dokładnie te same cele co terroryzm klasyczny, wraz z jego zamachami bombowymi, porwaniami czy braniem zakładników, jedyna różnica pomiędzy nimi wynika z rodzaju zastosowanego sprzętu i wykorzystywania oprogramowania komputerowego.

3. CYBERTERRORYŚCI

Cyberterroryści są rodzajem hakerów, którzy działają według pewnej ustalonej ideologii, a ich działanie ma na celu wyrządzenie jak największych szkód swojej ofierze²⁰, zarówno o podłożu społecznym, jak i politycznym. W drugim przypadku można mówić o atakach przede wszystkim na systemy informatyczne strategicznych dla znaczenia państwa placówek takich jak np. banki, transport, telekomunikacja.

Jako jedną z pierwszych osób, które przeprowadziły tego rodzaju atak był czterdziestodwuletni wówczas Vitek Boden, który odpowiadał za wylanie milionów litrów ścieków do rzek oraz gruntów, co spowodowało katastrofę ekologiczną w rejonie Sunshine Coast w Australii. Vitkowi Bodenowi udowodniono dokonanie 46 ataków na oczyszczalnie ścieków, które dokonywał na przełomie marca i kwietnia 2000 r., za co został

¹⁴ <http://stachowiak.home.pl/kreator/data/documents/pk-1.pdf> (dostęp: 16.02.2017 r.).

¹⁵ Tamże.

¹⁶ T. Szubrycht, *Cyberterroryzm...*, s. 175.

¹⁷ J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym...*, s. 25.

¹⁸ M. Karatysz, *Zjawisko cyberprzestępczości...*, s. 141.

¹⁹ E. Lichocki, *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy*, Gdynia 2011, s. 34.

²⁰ A. Bógdał-Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 61.

skazany na dwa lata więzienia. Udowodnienie winy nie byłoby możliwe, gdyby nie odnaleziono laptopa sprawcy z informacjami oraz narzędziami dotyczącymi przeprowadzenia ataku.

Samo zjawisko cyberterroryzmu jest dość nowym rodzajem przestępczości o dość specyficznym charakterze działania z powodu jego nieprzewidywalnego i bezprawnego sposobu działania na poszczególne cele, wykorzystując przy tym nowoczesne technologie. Przyczyniło się do tego na pewno rozwój informatyzacji oraz typ społeczeństwa, w jakim teraz żyjemy²¹. Niepokojący jest również fakt, że wraz z rozwojem zagrożenia cyberprzestępczością powstają coraz to nowsze sposoby zabezpieczania się przed nimi, należy jednak pamiętać, że równolegle do rozwoju systemów zabezpieczających rośnie również wiedza osób chcących się do nich włamać.

W przypadku, kiedy mówimy o atakach cyberterrorystycznych musi występować szereg następujących warunków:

- występują osoby o odpowiedniej wiedzy i umiejętnościach, które te ataki wykonują;
- muszą występować cele, które w swojej strukturze są podatne na tego typu ataki, a przerwanie ich działania bądź zniszczenie wywoła odpowiedni efekt;
- informacja o ataku musi zwrócić uwagę na polityczne żądania terrorystów.

Samo zjawisko cyberterroryzm jest działaniem zmierzającym przeciwko komputerom oraz sieciom, z którymi się łączą a także informacją przechowywanych w nich, mające na celu wywołać określone zachowanie u atakowanego. Działania wykonane w ten sposób najczęściej mają na celu wywołać szkody, wzbudzić panikę bądź strach, a niekiedy także obniżyć obronność państwa w sytuacji, kiedy atak jest wymierzony np. w infrastrukturę krytyczną. Sam termin „cyberterroryzm” powstał już w latach 80. XX wieku w Kalifornii poprzez fuzję dwóch zjawisk, tj. terroryzmu oraz cyberprzestrzeni przez Barry’ego Collina. Z Początku cyberterroryzm przybierał formę jedynie teoretyczną jednak już po kilkunastu latach zauważono, że Stany Zjednoczone za bardzo uzależniły się od komputerów, co teoria B. Collina uznaje już nie tylko za coś bardzo prawdopodobnego, ale traktuje jako realne zagrożenie. Tego typu zjawisko nie musi być jedynie utożsamiane z działaniem przez grupy przestępcze czy terrorystyczne, można je bowiem rozpatrywać jako rodzaj działania, który prowadzi do osiągnięcia określonego celu. Głównymi celami ataków cyberterrorystów jest przede wszystkim infrastruktura krytyczna państw.

Każde wysoko rozwinięte państwo do harmonijnego funkcjonowania potrzebuje mieć ciągły nieprzerwany nadzór nad systemami finansowymi, zaopatrzenia (w wodę, gaz itp.). Gdy dojdzie do nagłego przerwania któregoś z tych systemów może spowodować to wzrost niepokoju i utratę poczucia zaufania do władz państwowych, a także przyczynić się do poważnych strat finansowych dla państwa, związanych z przejęciem kontroli przez terrorystów. Co gorsza, coraz częściej się mówi o unowocześnianiu oraz informatyzacji infrastruktury krytycznej, co w pewien sposób zwiększa korzyści w zarządzaniu nimi, ale tym samym stawia łatwe cele dla samych terrorystów, czyli ułatwia im zadanie.

Przykłady zagrożeń, jakie mogą wystąpić podczas ataków cyberterrorystycznych na poszczególne sektory państwa:

- sieć telekomunikacyjna (szeroko rozumianą infrastrukturę zarówno telefoniczną, satelitarną oraz komputerową. Zakłócenie tej gałęzi infrastruktury doprowadziłoby

²¹ A. Podraza, P. Potakowski, K. Wiak, *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa patologiczna i prawna*, Warszawa 2013, s. 224.

do poważnych strat finansowych poszczególnych instytucji i przedsiębiorstw z powodu opóźnień w przepływie informacji);

- sektor finansowy oraz bankowy (choć chwilowe zachwianie tej instytucji mogłoby spowodować zamrożenie wszystkich środków finansowych na kontach lub poważny problem z ich dostępnością [narzucone limity dotyczące wybrania środków finansowych], ewentualny spadek wiarygodności na arenie międzynarodowej a nawet osłabienie waluty);
- transport (w przypadku przejęcia kontroli nad Centrum Zarządzania Ruchem Kolejowym może doprowadzić do kolizji poszczególnych połączeń kolejowych);
- sektor energetyczny (w wyniku awarii sektora energetycznego może dojść do chwilowych awarii prądu bądź jego całkowitego braku);
- sektor władz publicznych (w przypadku ataku na ten rodzaj instytucji może dojść do dezorganizowania bądź zatrzymania pracy instytucji państwowych w zależności od skali ataku oraz w jakim czasie uda się powrócić do statusu *quo ante*).

Tego typu cele nie są wybierane przypadkowo przez cyberterrorystów, ponieważ zakłócenie działania choćby jednego z wymienionych wyżej sektorów może doprowadzić do ogromnych konsekwencji dla każdego obywatela danego państwa.

4. CYBERTERRORYZM W PRAWODAWSTWIE MIĘDZYNARODOWYM

W prawodawstwie Rady Europejskiej najważniejszymi dokumentami są: Konwencja Rady Europy o cyberprzestępczości oraz Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne.

Konwencja o cyberprzestępczości jest logiczną kontynuacją decyzji dotyczącej powołania Europejskiego Komitetu do spraw Przestępczości z 1996 r. Komitet ten postulował o utworzenie specjalnej komórki, która miała się zajmować przestępczością komputerową i teleinformatyczną, a jej zasięg miał być ponadnarodowy. Do końca 2011 r. większość państw członkowskich oraz kilka państw partnerskich (m.in.: USA, Kanada, Japonia i RPA) podpisało się pod ratyfikacją dokumentu. Konwencja ta jest umową o charakterze międzynarodowym. Składa się z kilku części²²:

- preambuły,
- 3 rozdziałów,
- postanowień końcowych.

Zgodnie z postanowieniami ujętymi w preambule celem Konwencji jest prowadzenie wspólnej polityki, która ma za zadanie ochronę społeczeństwa przed przestępczością cybernetyczną, między innymi poprzez prowadzenie działań mających powstrzymać czynności związane z łamaniem zasad poufności, integralności, czy dostępności do systemów teleinformatycznych, jak też z nieprawidłowym wykorzystywaniem tych systemów. Aby działania takie były skuteczne niezbędne było przyjęcie odpowiednich przepisów prawnych, które miały opierać się na międzynarodowej współpracy. Współpraca taka powinna odbywać się nie tylko pomiędzy poszczególnymi państwami, ale również pomiędzy prywatnymi przedsiębiorstwami i organizacjami. Wszystkie te instytucje powinny współdziałać, ponieważ tylko dzięki temu możliwe jest prowadzenie skoordynowanych

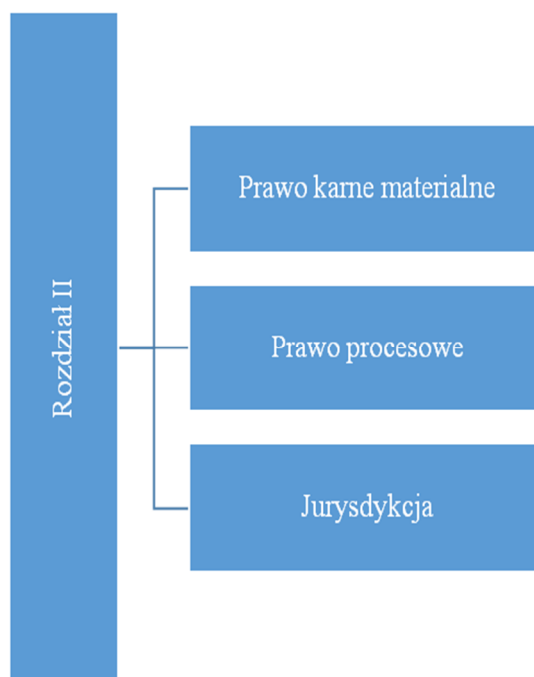
²² J. Skrzypczak, *Bezpieczeństwo teleinformatyczne w świetle europejskiej Konwencji o cyberprzestępczości*, „Przegląd Strategiczny” 1/2011, s. 53–54.

działań, które ułatwią wykrywanie przestępstw, prowadzenie śledztw oraz ściganie winnych, zarówno na szczeblu krajowym, jak i międzynarodowym

Dodatkowo w preambule podkreślone zostało, że wszystkie wymienione wyżej działania powinny być prowadzone z poszanowaniem praw człowieka, a szczególnie tych dotyczących wolności opinii, wypowiedzi oraz poszanowania prywatności²³.

Pierwszy rozdział zawiera przegląd najważniejszych definicji, natomiast drugi to przedstawienie propozycji środków mających zapobiegać cyberprzestępczości, kolejny poświęcony został międzynarodowej współpracy²⁴.

Rozdział II Konwencji składa się z trzech części, które prezentuje rys. 2.



Rys. 2. Rozdział II Konwencji Rady Europy o Cyberprzestępczości

Źródło: J. Skrzypczak, *Bezpieczeństwo teleinformatyczne...*, s. 55.

W części dotyczącej prawa karnego materialnego ustawodawca zaprezentował katalog przestępstw, które sygnatariusze powinni wprowadzić do ustawodawstwa krajowego; są to między innymi²⁵:

- przestępstwa przeciwko poufności, dostępności i integralności systemów i danych informatycznych. Zalicza się tutaj następujące działania: nielegalny dostęp i prze-

²³ Tamże.

²⁴ Tamże, s. 54.

²⁵ Tamże, s. 55–57.

chwytywanie danych, jak również naruszenie ich integralności i integralności systemu;

- przestępstwa komputerowe, do których zalicza się: fałszerstwa i oszustwa komputerowe;
- przestępstwa związane z charakterem informacji, to między innymi działania związane z pornografią dziecięcą;
- przestępstwa związane z naruszeniem praw autorskich i pokrewnych.

Na część drugą tego rozdziału składa się prawo procesowe, czyli propozycje rozwiązań w zakresie procedury. Innymi słowy, każde z państw powinno przyjąć odpowiednie środki prawne, które umożliwią przeprowadzenie dochodzenia i postępowania karnego. Środki takie prezentuje rys. 3.



Rys. 3. Środki prawne dotyczące przepisów procesowych

Źródło: Konwencja Rady Europy o Cyberprzestępczości z 23 listopada 2001 r., art. 16–21.

Zabezpieczenie danych informatycznych oznacza, że każde państwo zobowiązane jest do wprowadzenia odpowiednich procedur, które pozwolą uprawnionym organom na zabezpieczenie danych, jak również identyfikację osób dokonujących przekazu i sposobów dokonania tego przekazu²⁶.

Nakaz dostarczenia, czyli wprowadzenie środków niezbędnych do przejmowania danych oraz informacji dotyczących abonentów (tożsamość, adres, numer telefonu i dostępu).

Przeszukanie i zajęcie danych stosowane jest w przypadku konieczności: uzyskania dostępu do systemów informatycznych, nośników oraz również danych w nich przechowy-

²⁶ Konwencja Rady Europy o Cyberprzestępczości z 23 listopada 2001 r., art. 16–17.

wywanych, wykonania kopii danych, jak również usunięcie danych z systemów informatycznych.

Każdy kraj powinien wprowadzić odpowiednie regulacje prawne, które powinny umożliwić gromadzenie i rejestrowanie danych przez odpowiednie instytucje państwowe oraz umożliwić im zmuszenie dostawcy usług teleinformatycznych do rejestracji i gromadzenia danych. Dodatkowo należy wprowadzić odpowiednie środki prawne, które pozwolą odpowiednim organom na przechwytywanie w czasie rzeczywistym danych, szczególnie tych, których treści uważane są za niebezpieczne lub niezgodne z prawem.

Wszystkie kraje, które podpisały Konwencję zobowiązane zostały do ustanowienia jurysdykcji odnośnie do przestępstw, które popełnione zostały:

- na terytorium danego kraju;
- na statku pływającym pod banderą tego kraju;
- na pokładzie samolotu zarejestrowanego na dany kraj;
- przez obywatela danego kraju poza jego granicami.

Kolejny rozdział Konwencji dotyczy współpracy międzynarodowej, która opisana zostanie w dalszej części pracy.

Dyrektywa Parlamentu Europejskiego z 12 sierpnia 2013 r. dotyczy ataków na systemy informatyczne. Jej głównym celem jest zbliżenie prawa państw członkowskich w zakresie przestępstw związanych z systemami teleinformatycznymi, co jest możliwe dzięki ustanowieniu minimalnych zasad dotyczących kar oraz definicji tychże przestępstw. Kolejnym zadaniem Dyrektywy jest doprowadzenie do ścisłej i poprawnej współpracy pomiędzy organami w poszczególnych państwach, jak również pomiędzy nimi, a instytucjami Europejskimi (Eurojust, Europol, ENISA i Europejskim Centrum do spraw Walki z Cyberprzestępczością)²⁷.

Zgodnie z Dyrektywą do cyberprzestępstw zalicza się:

- nielegalny dostęp do systemu;
- nielegalną integrację w system;
- nielegalną integrację w dane;
- nielegalne przechwytywanie danych;
- nielegalne narzędzia do popełniania cyberprzestępstw.

Dyrektywa wprowadziła również zaostrzenie kar za przestępstwa związane z przestępczą działalnością cybernetyczną. Najniższy wyrok za ciężkie przestępstwa tego typu to dwa lata, natomiast pięć lat grozi za popełnienie przestępstw związanych z ingerencją w system lub dane w ramach organizacji przestępczej, powodujące znaczne szkody lub w przypadku ataku na dane lub systemy należące do infrastruktury krytycznej.

Do odpowiedzialności pociągnięte mogą być nie tylko osoby fizyczne, ale też i prawne. Kary nałożone na nie powinny być odstraszające i proporcjonalne, zalicza się do nich: grzywnę, zakaz prowadzenia działalności gospodarczej (stały lub czasowy), nadzór sądowy, likwidacja, zamknięcie działalności (stałe lub czasowe) oraz pozbawienie praw do korzystania z pomocy i świadczeń publicznych²⁸.

²⁷ A. Adamski, *Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady. 2005/222/WSiSW – próba oceny*, za: http://www.secure.edu.pl/pdf/2013/D2_1630_B_Adamski.pdf (dostęp: 28.03.2017 r.).

²⁸ Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne, art. 11.

Nie tylko UE prowadzi wiele czynności w celu przeciwdziałania zagrożeniom związanym z siecią. Na szczycie NATO w 2006 r. przyjęto *Comprehensive Political Guidance*, czyli strategię pozwalającą na wspólne działania w zakresie zapobiegania cyberterroryzmowi. Dwa lata później w ramach tej organizacji powołano w Talinie *Cooperative Cyber Defence Centre of Excellence*, czyli Centrum Doskonalenia Obrony przed Cyberatakami. Jest to organizacja bezpieczeństwa, która ma za zadanie badanie i wspieranie państw członkowskich w ich działaniach przeciwko przestępstwom internetowym²⁹.

5. PODSUMOWANIE

Cyberterroryzm staje się jednym z newralgicznych niebezpieczeństw, z którym zmierzają się współczesne państwa i społeczeństwa. Dokonują się one w wirtualnej przestrzeni, trudno je kontrolować, ale nie mogą być lekceważone np. poprzez brak odpowiedniej kontroli i unormowań prawnych. Cyberterroryzm jest zjawiskiem wpływającym negatywnie na wiele sfer życia i stanowi zagrożenie dla interesów jednostek, poszczególnych państw oraz wspólnot międzynarodowych. Przynosi wymierne straty. Uderzając w bazy danych, może przyczynić się do destrukcji i dezorganizacji życia każdej społeczności. Ataki na systemy obronności, bankowości, sektora energetyki, a zwłaszcza elektrowni jądrowych czy też sieci monitorujące szpitale oraz na systemy ratownictwa mogą doprowadzić do chaosu w państwie i załamania systemu obronności państwa.

Z analizy literatury i przede wszystkim z dokumentów normatywnych regulujących tę materię wynika, że aktualnie obowiązujące regulacje prawne proponują rozwiązania, aczkolwiek niewystarczające dla właściwej ochrony przetwarzania informacji w systemach. Świadczą o tym statystyki obrazujące skalę ataków, jakie są przeprowadzane na systemy informatyczne państwa. Obecnie podejmowane działania nie zapewniają całkowicie bezpieczeństwa przekazywanych informacji przed atakami cyberterrorystycznymi w Polsce. Trzeba pamiętać, że cyberterroryzm jest zjawiskiem ewaluującym, niosącym z każdym dniem nowe zagrożenia, dlatego też opracowywane projekty powinny zawierać kompleksowe, dobrze zaplanowane działania zmierzające do przeciwdziałania i ochrony cyberprzestrzeni RP. Właściwym kierunkiem w celu budowy systemu ochrony cyberprzestrzeni jest Doktryna cyberbezpieczeństwa RP, która wyznacza kierunki stałego rozwoju ochrony państwa.

Wszystkie systemy informatyczne, zarówno w sektorze publicznym, jak i prywatnym powinny być budowane z wielką rzetelnością. Muszą być określone obowiązki i odpowiedzialność właścicieli, dostawców i użytkowników systemów. Należy wzmacniać świadomość oraz budować etykę korzystania z systemów informacyjnych. Środki, dobre praktyki i procedury zapewniające bezpieczeństwo systemów powinny uwzględniać aspekty techniczne, administracyjne, organizacyjne, handlowe, edukacyjne i prawne. Poziomy zabezpieczeń, koszty, środki, praktyki i procedury powinny być odpowiednio dobrane i proporcjonalne do wartości systemów. Jednocześnie należy brać pod uwagę to, że wymagania dla poszczególnych systemów są różne. Na bieżąco należy szacować ryzyko wystąpienia szkody oraz jak poważne i jak prawdopodobne byłyby szkody i ich zasięg. W przypadku naruszeń bezpieczeństwa systemów bardzo istotne jest zapewnienie „działania w porę”, polegające na współpracy wszystkich użytkowników, w tym na poziomie

²⁹ M. Łapczyński, *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, „Pulaski Policy Service” 7/2009, s. 11.

międzynarodowym. Systemy, szczególnie systemy informatyczne państwa, powinny być skoordynowane i zintegrowane ze sobą. Powinny tworzyć spójny system bezpieczeństwa. Każde państwo musi chronić zasoby, sieci i systemy teleinformatyczne przed zamierzonymi i niezamierzonymi szkodliwymi działaniami w cyberprzestrzeni. W interesie wspólnoty międzynarodowej jest, aby każde państwo zaostrzyło politykę ochrony własnej cyberprzestrzeni.

Niemniej jednak, trzeba zdać sobie sprawę, że nawet najlepsze uregulowania prawne, czy wdrażanie najnowocześniejszych systemów zabezpieczeń nie uchronią informacji przed cyberatakami. To człowiek jest najsłabszym ogniwem, dlatego szczególnie ważne jest budowanie świadomości i odpowiedzialności, poprzez edukację społeczeństwa na temat zagrożeń związanych z cyberprzestrzenią. Świadomość ludzka jest najlepszą ochroną.

Literatura

1. Bógdał-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.
2. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r., dotycząca ataków na systemy informatyczne.
3. Forlicz S., *Informacja w biznesie*, PWE, Warszawa 2008.
4. <http://lexblog.pl/definicja-cyberprzestepstwa/> (dostęp: 15.02.2017 r.).
5. <http://stachowiak.home.pl/kreator/data/documents/pk-1.pdf> (dostęp: 16.02.2017 r.).
6. http://www.secure.edu.pl/pdf/2013/D2_1630_B_Adamski.pdf (dostęp: 28.03.2017 r.).
7. Karatysz M., *Zjawisko cyberprzestępczości, a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski*, Wydawnictwo Naukowe UAM, Poznań 2013.
8. Konwencja Rady Europy o Cyberprzestępczości z 23 listopada 2001 r.
9. Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne”, 1–2/2014.
10. Kuta G., *Cyberterroryzm – zagrożenie dla bezpieczeństwa informacji i danych osobowych*, Wydawnictwo KSOIN, Poznań 2012.
11. Lakomy M., *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, „E-Politykon” 6/2013, Warszawa 2013.
12. Lichocki E., *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy*, Wydawnictwo AMW, Gdynia 2011.
13. Łapczyński M., *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, „Pulaski Policy Service” 7/2009.
14. Podraza A., Potakowski P., Wiak K., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa patologiczna i prawna*, Difin, Warszawa 2013.
15. Skrzypczak J., *Bezpieczeństwo teleinformatyczne w świetle europejskiej Konwencji o cyberprzestępczości*, „Przegląd Strategiczny” 1/2011.
16. Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Wydawnictwo AMW, Gdynia 2005.
17. Świątkowska J., Bunsch I., *Cyberterroryzm, nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku*, Wydawnictwo Instytutu Kościuszki, Warszawa 2011.

18. Wasilewski J., *Zarys definicji cyberprzestrzeni* [w:] *Przegląd bezpieczeństwa narodowego*, red. B. Hołyst, Wydawnictwo ABW, Warszawa 2013.

CYBERTERRORISM AS CONTEMPORARY WEAPONS OF MASS WEIGHT

With the development of computer technology a new term appeared – cyberterrorism as a modern type of weapons of mass destruction, which along with further development will become more and more dangerous. Cyber terrorism as a specific category of threats includes actions in relation to ICT systems, undertaken to achieve specific terrorist goals. Terrorist organizations are usually associated with a state, its special services, religious denominations, criminal groups or they can function in order to gain popularity in the national (local) or international arena. These activities have specific goals that allow them to influence social, political or even military decisions. The article attempts to analyze the essence and conditions of cyberterrorism. It indicates which elements determine the ease of dissemination of cyberaggression and what determines the asymmetry of the conflict caused by the undesirable activities of criminals in the network. Concepts closely related to the topics discussed include: cyberspace, cybercrime, cyberaggression, cyberterrorists and reference to the framework of functioning of entities in the network, which sets international legislation. It was, therefore, indicated the basic regulations approved by the European Union, but also the countries gathered around NATO. Because the activities of cyber-terrorists are oriented towards causing paralysis of the political, social, psychological and economic levels, the attempts to monitor threats concern a very wide field of influence. The study points out that sectors exposed to cybernetic networks (telephone, satellite and computer infrastructure), the financial and banking sector, transport, energy sector and public authorities are particularly vulnerable to cyber terrorists. The authors of the study discuss the thesis that disrupting the operation of one of the sectors mentioned above can lead to enormous negative consequences for every citizen of a given country.

Keywords: cyberspace, cybercrime, cyberaggression, cyberterrorists, international legislation.

DOI: 10.7862/rz.2018.mmr.3

Tekst złożono w redakcji: styczeń 2018 r.

Przyjęto do druku: marzec 2018 r.

