Ius Novum
1/2017

CYBERTERRORYZM A CYBERPRZESTĘPSTWA O CHARAKTERZE TERRORYSTYCZNYM

MAREK SMARZEWSKI*

We współczesnym świecie terroryzm i zagrożenie tym zjawiskiem mają globalny charakter. W sytuacji znoszenia barier w przemieszczaniu się, jak i rozwoju technologicznego powstają coraz to nowe pola działania i możliwości funkcjonowania dla terrorystów i ugrupowań terrorystycznych. Można zatem zaobserwować wzrastanie zagrożeń, które mogą przeistoczyć się w realne akty naruszeń dóbr prawnych zarówno poszczególnych państw, jak i jednostek wchodzących w skład wspólnot istniejących w ich obrębie i je kreujących. Państwo staje zatem przed poważnym wyzwaniem, którym jest niewątpliwie zapewnienie bezpieczeństwa, nie tylko z uwagi na konieczność zabezpieczenia własnego bytu, lecz również, a może nawet przede wszystkim, dla zabezpieczenia egzystencji biernych podmiotów, których dobra prawne, takie jak życie, zdrowie, wolność są narażone na szwank w nawiązaniu do zagrożeń o charakterze terrorystycznym[1].

Istotne jest przy tym to, że państwo jest zmuszone zapewnić wielopłaszczyznową ochronę dla dóbr prawnych chronionych przez prawo, w tym dla bezpieczeństwa czy związanego z tym porządku publicznego – kwestie te stanowią bowiem punkt wyjścia dla bezpieczeństwa podmiotów tworzących wspólnotę. Nie jest przy tym oczywiście wystarczające stworzenie abstrakcyjnych instrumentów prawnych, ale konieczne jest również zagwarantowanie ich realizacji w praktyce przez kreowanie środków, mogących stanowić podstawę dla efektywnego przeciwdziałania terroryzmowi[2]. To ostatnie zadanie zyskuje na znaczeniu, szczególnie zważywszy na postępujący rozwój technologiczny i wzrost znaczenia nowych technologii w życiu człowieka, pozostający w związku m.in. z informatyzacją administracji publicznej. Szczególny deficyt bezpieczeństwa można zaobserwować w tzw. cyberprzestrzeni,

* dr, adiunkt na Wydziale Prawa Kanonicznego i Administracji Katolickiego Uniwersytetu Lubelskiego Jana Pawła II w Lublinie

1 Por. K. Wiak, *Prawnokarne środki przeciwdziałania terroryzmowi*, Lublin: Wydawnictwo KUL, 2009, s. 11.

2 Por. D. Caldwell, R.E. Williams Jr., *Seeking Security in an Insecure World*, Lanham: Rowman & Littlefield Publishers, 2012, s. 191.

co rzutuje na ogólne odczucia w przedmiocie bezpieczeństwa, w tym zaś kontekście cyberbezpieczeństwa. Za uzasadnione można zatem uznać odwołanie się do treści „Ram dla polepszania cyberbezpieczeństwa krytycznych infrastruktur" wydanych w Stanach Zjednoczonych przez Narodowy Instytut Standardów i Technologii w dniu 12 lutego 2014 r., w których to postawiono tezę, iż zagrożenia dla cyberbezpieczeństwa powstają ze względu na coraz większą złożoność i łączność w ramach infrastruktury krytycznej, podczas gdy narodowe i ekonomiczne bezpieczeństwo państwa uzależnione jest od jej niezawodnego funkcjonowania[3].

Powyżej przytoczone okoliczności, połączone z faktem nieokreśloności i poważnych problemów z definiowaniem rzeczywistości informatycznej w aktach prawnych, stanowi grunt dla powstania i istnienia stanu abstrakcyjnego strachu przed nieraz bliżej nieokreślonymi niebezpieczeństwami czyhającymi w cyberprzestrzeni. Jeżeli zatem terroryzm nie jest czymś spekulatywnym, a pozostaje zjawiskiem, które znalazło i znajduje swoje potwierdzenie w rzeczywistości przez grupę działań nań się składających, to biorąc wzgląd na znaczenie nowych technologii w życiu prywatnym i publicznym i gwałtownie rozwijającą się cyberprzestępczość, a także związany z tym wzrost liczby przestępstw popełnianych w cyberprzestrzeni, za zagadnienie istotne nie tylko z teoretycznego punktu widzenia zaczęto postrzegać cyberterroryzm. Dla poczynienia dalszych ustaleń w zasygnalizowanym zakresie niezbędne jest wyjaśnienie pojęć terroryzmu i cyberterroryzmu.

Definiując terroryzm, uzasadnione jest odniesienie się do regulacji § 2331 (tytuł 18, część 1, rozdział 113B) Kodeksu Stanów Zjednoczonych[4], gdzie wyjaśniono znaczenie pojęć terroryzmu międzynarodowego i wewnętrznego. Terroryzm międzynarodowy rozumie się jako działalność, która przejawia się w aktach przemocy lub działaniach niebezpiecznych dla ludzkiego życia, które stanowią naruszenia prawa federalnego lub stanowego lub które podlegałyby jurysdykcji terytorialnej Stanów Zjednoczonych, zgodnie z takim prawem, występujące zasadniczo poza jurysdykcją terytorialną Stanów Zjednoczonych lub wykraczające poza granice państwa m.in. ze względu na środki, za pomocą których zostały wykonane. Dla dopełnienia definicji należy wskazać, iż wskazane aktywności muszą być przedsiębrane w celu: zastraszenia lub wymuszenia określonego zachowania na ludności cywilnej; wywarcia wpływu na politykę rządu przez zastraszenie lub przymus; wpływanie na zachowanie rządu przez masowe rażenie, zabójstwa czy porwania. Terroryzm międzynarodowy oznacza terroryzm z udziałem obywateli lub na terytorium więcej niż jednego państwa[5]. Terroryzm wewnętrzny wyróżnia natomiast to, iż dotyczy on działalności prowadzonej na obszarze jednego państwa. Terroryzm można zatem definiować jako znamionującą się premedytacją, politycznie umotywowaną przemoc popełnioną przeciwko nieuzbrojonym celom przez grupy subnarodowe lub tajnych agentów, często obliczony na przyciągnięcie uwagi publicznej i wywołanie

---

[3] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* [online], s. 1, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [dostęp: 6.02.2016].

[4] Zob. *United States Code*, https://www.law.cornell.edu/uscode/text/18/2331 [dostęp: 6.02.2016].

[5] Zob. L.J. Siegel, *Criminology*, Belmont: Cengage Learning, 2012, s. 385.

określonego wpływu, np. przez osiągnięcie efektu zastraszenia[6]. Dokonując zaś analizy pojmowania terroryzmu w doktrynie, uzasadnione jest zwrócenie szczególnej uwagi na interpretację tego pojęcia, którą zaproponował T. Hanausek. Autor ten postrzegał terroryzm jako pewne zjawisko, a to planowaną, zorganizowaną i zazwyczaj uzasadnioną ideologicznie, a w każdym razie posiadającą polityczne podłoże motywacyjne, działalność osób lub grup, mającą na celu wymuszenie od władz państwowych, społeczeństwa lub poszczególnych osób określonych świadczeń, zachowań czy postaw, a realizowaną w przestępczych formach obliczonych na wywołanie szerokiego i maksymalnie zastraszającego rozgłosu w opinii publicznej oraz z reguły polegającą na zastosowaniu środków fizycznych, które naruszają dobra osób postronnych[7].

Rozważając natomiast znaczenie pojęcia cyberterroryzm należy zauważyć, iż w doktrynie słusznie podkreśla się – jakkolwiek jednak jest to istotne głównie z teoretycznego punktu widzenia – że cyberterroryzm to coś więcej aniżeli przedrostek rodzajowy zestawiony ze standardową aktywnością o charakterze terrorystycznym[8]. W myśl definicji sformułowanej przez K. Liedela, cyberterroryzm to politycznie umotywowany atak lub groźba ataku na komputery, sieci lub systemy informatyczne w celu zniszczenia infrastruktury oraz zastraszenia bądź też wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów[9]. Autor ten akcentuje cel stanowiący istotny element, który sprawca chce osiągnąć dopuszczając się tego typu działań i ataków, co może wskazywać – w związku z wykładnią zaprezentowanego rozumienia cyberterroryzmu – jego bliskość z definicją przestępstwa o charakterze terrorystycznym. Inną jeszcze definicję cyberterroryzmu przyjmuje D. Jagiełło, podnosząc, że jest to politycznie lub militarnie motywowany atak albo groźba ataku na systemy i sieci teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia infrastruktury krytycznej państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno-militarnych działań, a także świadome wykorzystanie sieci teleinformatycznych oraz sieci Internet m.in. przez organizacje terrorystyczne, ruchy narodowo-wyzwoleńcze oraz ruchy powstańcze do sparaliżowania narodowej infrastruktury krytycznej albo do zastraszenia lub wymuszenia na rządzie lub ludności określonego zachowania się[10]. Odmienne w stosunku do wskazanych wyżej definicji rozumienie zaproponował J.A. Lewis. Zgodnie z tym ujęciem, cyberterroryzm stanowi użycie sieci komputerowej jako narzędzia do sparaliżowania narodowej infrastruktury krytycznej (np. w sektorze energetyki lub transportu) albo do zastraszenia lub

---

[6] Por. L.J. Siegel, J.L. Worrall, *Introduction to Criminal Justice*, Belmont: Cengage Learning, 2014, s. 638.

[7] T. Hanausek, *W sprawie pojęcia współczesnego terroryzmu*, „Problemy Kryminalistyki" 1980, nr 143, s. 30 i n.

[8] P.A. Yannakogeorgos, *Rethinking the Threat of Cyberterrorism*, [w:] T.M. Chen, L. Jarvis, S. Macdonald (red.), *Cyberterrorism: Understanding, Assessment, and Response*, New York: Springer, 2014, s. 44.

[9] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń: Wydawnictwo Adam Marszałek, 2006, s. 36.

[10] Zob. D. Jagiełło, *Cyberterroryzm*, „Edukacja Prawnicza" 2013, nr 5, s. 12.

wymuszenia na rządzie lub ludności cywilnej określonych zachowań[11]. Dostrzegając bowiem niewątpliwie bardziej ogólny charakter definicji J.A. Lewisa można domniemywać, iż stanowi ona o pojmowaniu cyberterroryzmu jako pewnej abstrakcyjnej kategorii pojęciowej, mieszczącej w sobie ogół zachowań, stanowiącej zjawisko, nie zaś poszczególny akt terrorystyczny[12].

O ile zatem określono cyberterroryzm jako zjawisko, znamionujące się wysokim stopniem abstrakcyjności, o tyle postępujący rozwój technologii informacyjnych pozwala na stwierdzenie, iż ryzyko cyberataku terrorystycznego rzeczywiście wzrasta. Realność zrealizowania takiego cyberataku wynika z faktu, iż terroryści używają Internetu do planowania i przeprowadzania fizycznych ataków, szerzenia ideologii, manipulowania opinią publiczną i mediami, rekrutowania i trenowania nowych terrorystów, zdobywania i pomnażania funduszy, pozyskiwania informacji o potencjalnych celach działania, kontrolowania prowadzonych operacji, czy uzyskiwania poufnych informacji, stanowiących różnego rodzaju tajemnice[13]. Świadczy to dobitnie o niewątpliwie dużym znaczeniu nowych technologii w kontekście prawnokarnym, w tym w perspektywie zagrożenia zmasowanym atakiem, w szczególności w wariancie zestawienia cyberataku z atakiem fizycznym. Należy się jednak zastanowić czy takie postrzeganie analizowanych zagadnień nie doprowadzi do rozmycia oczywistych – jakby się mogło zdawać – różnic pomiędzy cyberterroryzmem, jako zjawiskiem i kategorią abstrakcyjną, a cyberprzestępstwem o charakterze terrorystycznym. Rzecz jasna można podnosić, iż dyferencjacja wskazanych pojęć posiada walor teoretyczny, niemniej jednak przy takim założeniu można by w ogóle rozważać sens operowania pojęciami cyberterroryzmu czy cyberprzestępstwa o charakterze terrorystycznym.

W nawiązaniu do treści art. 115 § 20 k.k. w doktrynie przyjmuje się niekiedy, iż cyberterroryzm stanowi jedną z form terroryzmu związaną z cyberprzestrzenią. W tym zaś świetle podnosi się – w oparciu o definicję przestępstwa o charakterze terrorystycznym – że cyberterroryzm polega na przestępnym działaniu związanym z informatyką i mającym na względzie jeden z poniższych celów:

- poważne zastraszenie wielu osób;
- zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności;

---

[11] Zob. N. Lee, *Counterterrorism. And Cybersecurity. Total Information Awareness*, New York: Springer, 2013, s. 112.

[12] Por. N. Veerasamy, M. Grobler, B. Von Solms, *Building an Ontology for Cyberterrorism*, [w:] E. Filiol, R. Erra (red.), *Proceedings of the 11th European Conference on Information Warfare and Security. The Institute Ecole Supérieure en Informatique Electronique et Automatique, Laval, France 5–6 July 2012*, Reading: Academic Publishing International Limited, 2012, s. 286. Zob. również K. Indecki, *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź: Wydawnictwo Uniwersytetu Łódzkiego, 1998, s. 18–24.

[13] Zob. M. Smarzewski, *Bezpieczeństwo państwa jako przedmiot ochrony niektórych przestępstw popełnianych za pośrednictwem sieci teleinformatycznej*, [w:] Z. Dziemianko, A. Kijas (red.), *Bezpieczeństwo współczesnego świata. Edukacja i komunikowanie*, Poznań: Wydawnictwo Wyższej Szkoły Handlu i Usług, 2013, s. 184 i literatura tamże cytowana.

- wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu.

Takie definiowanie cyberterroryzmu nie wydaje się być jednak prawidłowe i logicznie zasadne, o ile świadczy o identyfikacji tego pojęcia z cyberprzestępstwem o charakterze terrorystycznym. Jeżeli dodatkowo zważyć przy tym, iż idąc za art. 115 § 20 k.k. przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat i popełniony w realizacji jednego spośród określonych wyżej celów, powoduje to konieczność poczynienia założenia, zgodnie z którym ustawodawca odnosi wskazaną konstrukcję do konkretnych czynów zabronionych. Taka zaś teza przekreśla możliwość utożsamiania cyberterroryzmu z pojęciem cyberprzestępstwa o charakterze terorrystycznym, wyrażonego przez zestawienie istoty cyberprzestępstwa z elementami przestępstwa o charakterze terrorystycznym.

Pod pojęciem cyberprzestępczości rozumie się zachowania odnoszące się do wykorzystywania technologii informacyjnych (komputerów i sieci komputerowych) do popełniania przestępstw[14]. Nawiązując zatem do definicji wyrażonej w art. 115 § 20 k.k. w części szczególnej Kodeksu karnego można zlokalizować następujące typy czynów, wpisujące się potencjalnie w schemat cyberprzestępstwa o charakterze terrorystycznym – z uwagi na opcjonalność popełnienia takich czynów jako cyberprzestępstw i dodatkowego wypełnienia znamion przestępstwa terrorystycznego z przywołanego przepisu, tj. w szczególności:

– szpiegostwo komputerowe (art. 130 § 2 i § 3 k.k.);
– sprowadzenie niebezpieczeństwa przez zakłócenie, uniemożliwienie lub wpłynięcie w inny sposób na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych (art. 165 § 1 pkt 4 k.k.);
– zorganizowana grupa i związek przestępczy (art. 258 § 1 k.k.);
– ujawnienie lub wykorzystanie, wbrew przepisom ustawy, informacji niejawnej o klauzuli „tajne" lub „ściśle tajne" (art. 265 k.k.);
– sabotaż informatyczny (art. 269 k.k.);
– zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej (art. 269a k.k.).

Należy przy tym podkreślić, iż zaproponowane typy nie muszą być rzecz jasna uznane za wyłącznie wpisujące się w definicję cyberprzestępstwa o charakterze terrorystycznym. Kryterium zakwalifikowania czynu zabronionego do określonej grupy stanowiła bowiem możliwość jego zaistnienia w określonej konwencji, zarówno ze względu na możliwy cel zachowania sprawcy, jak i górną wysokość sankcji przewidzianej w przypadku realizacji znamion danego typu ustawowego. Wydaje się więc, iż w ramach grupy cyberprzestępstw – ze względu na punkt odniesienia lub środek, który stanowią systemy i/lub sieci teleinformatyczne – uprawnione byłoby wyodrębnienie kategorii przestępstw o charakterze cyberterrorystycznym. Taka

[14] E. Kraemer-Mbula, P. Tang, H. Rush, *The cybercrime ecosystem: Online innovation in the shadows?*, „Technological Forecasting & Social Change" 2013, vol. 80, iss. 3, s. 543; N. Kshetri, *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives*, Heidelberg–London: Springer, 2010, s. 3.

terminologia znajdowałaby wprawdzie uzasadnienie, dopiero zakładając przyjmowanie cyberterroryzmu jako rzeczywistego zjawiska, które uzyskało już potwierdzenie w jego realizacji. Niemniej jednak, zważywszy na fakt, iż zjawisko to wciąż pozostaje realnym, lecz jednak nadal tylko zagrożeniem, właściwszym mieni się przyjęcie bezpieczniejszej w swej treści (i prawdopodobnie także terminologicznie) konstrukcji cyberprzestępstwa o charakterze terrorystycznym.

Ponadto z zaprezentowanym pojęciem trzeba by zestawić także kategorię tzw. cyberprzestępstw związanych z działalnością terrorystyczną, które co prawda nie stanowią cyberprzestępstw terrorystycznych z art. 115 § 20 k.k., aczkolwiek uzupełniają klasę zachowań wpisujących się ogólnie rzecz biorąc w definicję cyberterroryzmu, z uwagi na możliwość ich dokonania w sposób znamienny dla przestępstw terrorystycznych, dodatkowo zaś popełnionych w postaci cyberprzestępstwa. We wskazanych przypadkach może zaistnieć sytuacja, w której brak jest albo nie da się ustalić w ogóle lub wystarczająco wyraźnie terrorystycznych celów określonych w ustawie. W innym przypadku sankcję lub tryb ścigania albo np. okoliczność przygotowania można odczytywać jako elementy decydujące o kwalifikacji czynu jako cyberprzestępstwa związanego z działalnością terrorystyczną. Do grupy takich zachowań zdecydowano się zaliczyć m.in.:

– publiczne nawoływanie do wszczęcia wojny napastniczej lub publiczne pochwalanie wszczęcia lub prowadzenia takiej wojny (art. 117 § 3 k.k.);
– publiczne pochwalanie przestępstw lub nawoływanie do ich popełnienia (art. 126a k.k.);
– przygotowanie do popełnienia przestępstwa zamachu stanu (art. 127 § 2 k.k.);
– przygotowanie do zamachu terrorystycznego (art. 140 § 3 k.k.);
– sfinansowanie przestępstwa o charakterze terrorystycznym (art. 165a k.k.);
– nawoływanie do popełnienia takiego przestępstwa i pochwalanie popełnienia przestępstwa o charakterze terrorystycznym (art. 255 k.k.);
– rozpowszechnianie treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym (art. 255a k.k.);
– utrudnianie dostępu i niszczenie informacji (art. 268 k.k.);
– niszczenie, uszkadzanie, usuwanie lub zmienianie oraz utrudnianie dostępu do danych (art. 268a k.k.);

Na stwierdzenie, czy dane cyberprzestępstwo posiada charakter terrorystyczny – bądź też nie – pozwala zatem spełnienie znamion określonych w ustawie w powiązaniu z możliwością jego potencjalnej kwalifikacji jako cyberprzestępstwa. Ustalenie katalogu czynów, które można klasyfikować w kontekście tego typu zachowań jest więc zadaniem trudnym. Kolejny problem stanowi dopełnienie definicji cyberterroryzmu przez wskazanie przestępstw, popełnionych w realizacji celów terrorystycznych lub w zamiarze ich realizacji, stanowiących – obok cyberprzestępstw o charakterze terrorystycznym – o istocie cyberterroryzmu. W niniejszym artykule przyjęto dla określenia tej kategorii czynów miana cyberprzestępstw związanych z działalnością terrorystyczną, z uwagi na odpadnięcie elementu w postaci zagrożenia karą pozbawienia wolności w górnej granicy ustawowej co najmniej 5 lat lub celu wymaganego dla przestępstwa o charakterze terrorystycznym, idąc za treścią art. 115 § 20 k.k. Należy przy tym zaznaczyć możliwe wątpliwości, czy dla opi-

sania analizowanej kategorii czynów powinno się używać przywołanego pojęcia cyberprzestępstw związanych z działalności terrorystyczną czy też może sygnalizowanego w doktrynie terminu przestępstw okołoterrorystycznych[15], formułowanego m.in. w nawiązaniu do regulacji Konwencji Rady Europy o zapobieganiu terroryzmowi, sporządzonej w Warszawie dnia 16 maja 2005 r.[16]. W niniejszym opracowaniu, ze względu na wolę przyjęcia uproszczonej, aczkolwiek *in genere*, możliwie komplementarnej konwencji dla ujmowania cyberterroryzmu, przyjmuje się pojęcie cyberprzestępstw związanych z działalności terrorystyczną, jako dopełniających istotę cyberterroryzmu, obok cyberprzestępstw o charakterze terrorystycznym.

Uzasadnienia dla posługiwania się powyżej przytaczanym określeniem można się doszukiwać ze względu na tytuł art. 3 Decyzji Ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu[17]. W zakresie wymienionej regulacji zarówno dokonano wyjaśnienia kilku pojęć odnośnie do typów przestępstw związanych z działalnością terrorystyczną, jak i zawarto dyrektywę co do wprowadzenia na listę czynów zabronionych przez państwa członkowskie Unii Europejskiej niektórych czynów umyślnych.

Zdefiniowano w tym kontekście pojęcia „publicznego nawoływania do popełniania przestępstw terrorystycznych", „rekrutacji na potrzeby terroryzmu" oraz „szkolenia terrorystycznego". Zgodnie z treścią decyzji ramowej „publiczne nawoływanie do popełniania przestępstw terrorystycznych" oznacza rozpowszechnianie lub inną formę udostępniania publicznego przekazu w celu podżegania do popełnienia jednego z przestępstw terrorystycznych, o których mowa art. 1 ust. 1 lit a–h decyzji, jeżeli takie postępowanie, niezależnie od tego, czy stanowi ono bezpośrednie nakłanianie do popełnienia przestępstw terrorystycznych, powoduje zagrożenie popełnienia co najmniej jednego spośród tych przestępstw. „Rekrutację na potrzeby terroryzmu" zinterpretowano w decyzji jako nakłanianie innej osoby do popełnienia jednego z przestępstw terrorystycznych wymienionych w art. 1 ust 1 lit. a-h lub przestępstwo dotyczącego grupy terrorystycznej z art. 2 ust. 2. Z kolei „szkolenie terrorystyczne" oznacza prowadzenie instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub szkodliwych bądź niebezpiecznych substancji lub instruktażu w zakresie innych konkretnych metod lub technik do celów popełnienia jednego z przestępstw wymienionych w art. 1 ust. 1 lit. a-h decyzji, ze świadomością, że przekazywane umiejętności mają posłużyć do tych celów.

W decyzji ramowej z 2002 r. nałożono także na państwa członkowskie Unii Europejskiej obowiązek wciągnięcia na listę przestępstw następujących typów czynów umyślnych:

---

15 Por. T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa: Wydawnictwa Akademickie i Profesjonalne, 2008, s. 77–78.

16 Dz.U. 2008 nr 161, poz. 998.

17 Dz.U. UE. L. 2002.164.3 ze zm. Podobne spostrzeżenie poczynił Z. Galicki. Zob. Z. Galicki, *Ekspertyza prawna w sprawie zgodności z zasadą subsydiarności projektu Decyzji Ramowej Rady z dnia 6 listopada 2007 r. KOM(2007) wersja ostateczna, zmieniającej decyzję ramową 2002/475/WSiSW w sprawie zwalczania terroryzmu* [online], s. 1, http://ww2.senat.pl/k7/dok/opinia/2008/080108.pdf [dostęp: 6.02.2016].

– publiczne nawoływanie do popełniania przestępstw terrorystycznych;
– rekrutacja na potrzeby terroryzmu;
– szkolenie terrorystyczne;
– kwalifikowany typ kradzieży dokonanej z zamiarem popełnienia jednego z przestępstw wymienionych w art. 1 ust. 1 decyzji;
– wymuszenie dokonane z zamiarem popełnienia jednego z przestępstw wymienionych w art. 1 ust. 1 decyzji;
– sporządzanie fałszywych dokumentów urzędowych dokonane z zamiarem popełnienia jednego z przestępstw wymienionych w art. 1 ust. 1 lit. a–h oraz w art. 2 ust 2 lit. b decyzji.

Odnosząc się do ogółu przytoczonych przepisów decyzji, analizując problem z perspektywy terroryzmu, należy zauważyć, iż chociaż tenże akt prawny nie zawiera *expressis verbis* definicji cyberterroryzmu, określa jednak poszczególne elementy składowe ważnego pojęcia przydatnego do jej rekonstrukcji. Wydaje się bowiem, iż wskazane w art. 3 decyzji typy przestępstw związanych z działalnością terrorystyczną mogą być zasadniczo zakwalifikowane jako potencjalne cyberprzestępstwa[18].

Podsumowując te rozważania, uprawnione zdaje się być założenie, zgodnie z którym kategorie cyberprzestępstw o charakterze terrorystycznym i cyberprzestępstw związanych z działalnością terrorystyczną składają się na zjawisko cyberterroryzmu. Jest to o tyle ciekawe rozwiązanie, że prowadziłoby do przyjęcia rozumienia cyberterroryzmu jako kategorii znajdującej oparcie w prawie krajowym (art. 115 § 20 k.k.) i m.in. również w prawie europejskim (art. 1–3 decyzji ramowej w sprawie zwalczania terroryzmu), opierającej się na typologii zachowań, przejawiających się szerzej w działalności zmierzającej do sparaliżowania narodowej infrastruktury krytycznej albo do zastraszenia lub wymuszenia na rządzie lub ludności cywilnej określonych zachowań[19]. Jeżeli więc zakładać, że cyberterroryzm najlepiej pojąć przez pryzmat poszczególnych typów cyberprzestępstw o charakterze terrorystycznym lub tych związanych z działalnością terrorystyczną, oznaczałoby to, że zjawisko to stanowi sumę pewnych kategorii zachowań, co powodowałoby błędność tezy o możliwości utożsamiania poszczególnych z nich z cyberterroryzmem. Czym innym jest jednak konieczność stwierdzenia, że każde z nich stanowiłoby wyraz realizacji działalności terrorystycznej w cyberprzestrzeni.

Cyberataki o charakterze terrorystycznym, a także czyny zabronione związane z działalnością terrorystyczną wydają się stanowić realne zagrożenie, ponieważ, m.in. zważywszy na fakt rozwoju grup i związków terrorystycznych, cyberprzestępcy zdają sobie doskonale sprawę z tego, że w dzisiejszych czasach zmieniły się punkty warte do wzięcia pod uwagę w kontekście ustalania celów tych akcji. Jeżeli zatem szczególnie cenny, o ile nie kluczowy element życia społecznego stanowi

---

[18] Por. S. Summers, Ch. Schwarzenegger, G. Ege, F. Young, *The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society*, Oxford–Portland: Hart Publishing, 2014, s. 251–252.

[19] Por. M. Conway, *What is Cyberterrorism and How Real is the Threat. A Review of the Academic Literature, 1996–2009*, [w:] P.C. Reich, E. Gelbstein (red.), *Law, Policy, and Technology. Cyberterrorism, Information Warfare, and Internet Immobilization*, Hershey: IGI Global, 2012, s. 288.

informacja, to wobec jej olbrzymiego znaczenia coraz bardziej realnych kształtów nabiera bliżej nieokreślony cyberterroryzm, zaś jeszcze częściej praktykowane stają się ataki wpisujące się w definicję cyberprzestępstw o charakterze terrorystycznym czy też cyberprzestępstw powiązanych z działalnością terrorystyczną. Terroryści dla osiągnięcia swoich celów praktykują różnorodne środki, tj. naciski psychologiczne, przemoc i groźby przemocy fizycznej, użycie broni i ładunków wybuchowych, użycie najnowszych technologii informatycznych i satelitarnych w warunkach nadania im odpowiedniego rozgłosu i w atmosferze wytworzonego w społeczeństwie lęku. Zagrożenia atakami cybernetycznymi ze strony terrorystów stają się tym bardziej realne, gdy zważy się, że grupy terrorystyczne posiadają często olbrzymie środki finansowe, a w związku z tym najlepszy i najdroższy sprzęt elektroniczny na świecie, wyposażony w najnowocześniejsze oprogramowanie. Kolejną kwestią jest szeroka propaganda terrorystyczna, szkolenia prowadzone dla terrorystów – w sieci Internet. Postęp technologiczny, w tym w obszarze informatyzacji sfery publicznej i prywatnej wiąże się z narażeniem państwa, instytucji czy wreszcie jednostki na niebezpieczeństwo w cyberprzestrzeni. W przypadku państwa, w mniej poważnych przypadkach, może to przejawiać się np. w atakach na domeny państwowe. Na ataki z cyberprzestrzeni są jednak potencjalnie narażone także inne punkty kryzysowe, jak np.:

– fabryki chemiczne i laboratoria;
– rafinerie naftowe;
– elektrownie termojądrowe;
– zapory wodne;
– wieże kontroli lotów;
– linie kolejowe;
– sieci przekazywania poleceń i sterowania systemami militarnymi oraz wywiadowczymi;
– urządzenia nawigacyjne;
– szpitale;
– giełdy papierów wartościowych[20].

Cyberterroryzm jest więc niewątpliwie zjawiskiem, którego istotą jest działalność prowadzona w określony sposób, a obliczona na sparaliżowanie infrastruktury krytycznej. Pytaniem, które należy postawić jest jednak to, czy jedynie drogą serii ataków, realizujących znamiona przestępstw o charakterze terrorystycznym, czy też przestępstw związanych z działalnością terrorystyczną możliwe jest przeprowadzenie ataku porównywalnego swymi efektami z fizycznym atakiem terrorystycznym. Otóż wydaje się, że tego typu działania będą raczej stanowić swego rodzaju uzupełnienie dla konwencjonalnego ataku. Niemniej, nie można lekceważyć zagrożeń płynących z cyberprzestępczości terrorystycznej i z nią związanej. Faktycznie jednak to właśnie przeprowadzenie tzw. *swarming attack*, polegającego na jednoczesnym wykonywaniu wielu ataków fizycznych i cyberataków wymierzonych w liczne

[20] Zob. K. Dzięgielewski, *Cyberterrorystyczna internetyzacja*, [w:] J. Bednarek, A. Andrzejewska (red.), *Cyberświat: możliwości i zagrożenia*, Warszawa: Wydawnictwo Akademickie „Żak", 2009, s. 339–347.

infrastruktury, stanowi najgroźniejszą metodę, jaką mogą posłużyć się terroryści. Polega ona na spiętrzeniu i nałożeniu na siebie ataków przeciwko infrastrukturze krytycznej państwa prowadzonych w cyberprzestrzeni oraz fizycznie, przeciwko jej materialnym nośnikom. W trakcie takiego ataku dochodzi zazwyczaj do uszkodzenia lub degradacji linii i usług telekomunikacyjnych, co może doprowadzić do zakłócenia działania materialnych elementów infrastruktury krytycznej[21].

Wraz z rozwojem technologii komputerowych, ewolucją i pozostającym w związku z tym wzrostem wątpliwości i niepewności terroryści i ugrupowania terrorystyczne uzyskują szeroki zakres możliwości do wykorzystania w ich działaniach. W tym kontekście pojawiają się także sposobności rozwoju działalności grupy, m.in. przez nawiązywanie kontaktu z innymi ugrupowaniami terrorystycznymi, dzielenie się „wiedzą" z innymi sprawcami cyberprzestępstw, wpisujących się w zakres pojęcia cyberterroryzmu. Należy przy tym zauważyć, iż o ile uprawnione jest wyodrębnianie klas cybeprzestępstw o charakterze terrorystycznym oraz cyberprzestępstw związanych z działalnością terrorystyczną, o tyle nie jest potrzebne, ani uzasadnione z praktycznego punktu widzenia posługiwanie się pojęciem cyberterroryzmu. Ten ostatni stanowi bowiem zjawisko o tyle abstrakcyjne, że niezaistniałe w praktyce. Wiele zachodzi bowiem cyberprzestępstw, a cyberprzestrzeń staje się *spectrum* coraz liczniejszych zachowań zagrożonych przez ustawę pod groźbą kary. Kontrowersje musi zatem budzić zakładanie realności istnienia zjawiska faktycznie niestwierdzonego. Nie można jednak zakładać, iż dotychczasowy brak potwierdzenia dla zjawiska cyberterroryzmu w rzeczywistości zezwala na odgórne przyjęcie twierdzenia o niemożliwości jego zaktualizowania się w przyszłości. W tej kwestii należy więc pozostać z odpowiednią dozą sceptycyzmu, wynikającą z wątpliwości występujących w przedmiotowym zakresie.

BIBLIOGRAFIA

Aleksandrowicz T., *Terroryzm międzynarodowy*, Warszawa: Wydawnictwa Akademickie i Profesjonalne, 2008.

Caldwell D., Williams Jr. R.E., *Seeking Security in an Insecure World*, Lanham: Rowman & Littlefield Publishers, 2012.

Conway M., *What is Cyberterrorism and How Real is the Threat. A Review of the Academic Literature, 1996–2009*, [w:] P.C. Reich, E. Gelbstein (red.), *Law, Policy, and Technology. Cyberterrorism, Information Warfare, and Internet Immobilization*, Hershey: IGI Global, 2012, s. 279–307.

Dzięgielewski K., *Cyberterrorystyczna internetyzacja*, [w:] J. Bednarek, A. Andrzejewska (red.), *Cyberświat: możliwości i zagrożenia*, Warszawa: Wydawnictwo Akademickie „Żak", 2009, s. 338–354.

Galicki Z., *Ekspertyza prawna w sprawie zgodności z zasadą subsydiarności projektu Decyzji Ramowej Rady z dnia 6 listopada 2007 r. KOM(2007) wersja ostateczna, zmieniającej decyzję ramową*

[21] Zob. N. Noga, *Cyberterroryzm – nowe oblicze terroryzmu, cz. V. Internet jako cel ataków terrorystów – Klasyfikacja ataków w cyberprzestrzeni* [online], „e-Terroryzm.pl" 2013, nr 8, s. 18, http://www.academia.edu/5409045/Zjawisko_terroryzmu_w_Inguszetii_E-Terroryzm_nr_8_2013 [dostęp: 6.02.2016].

2002/475/WSiSW w sprawie zwalczania terroryzmu [online], s. 1, http://ww2.senat.pl/k7/dok/opinia/2008/080108.pdf [dostęp: 6.02.2016].

Hanausek T., *W sprawie pojęcia współczesnego terroryzmu*, „Problemy Kryminalistyki" 1980, nr 143, s. 30–48.

Indecki K., *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź: Wydawnictwo Uniwersytetu Łódzkiego, 1998.

Jagiełło D., *Cyberterroryzm*, „Edukacja Prawnicza" 2013, nr 5, s. 10–14.

Kraemer-Mbula E., Tang P., Rush H., *The cybercrime ecosystem: Online innovation in the shadows?*, „Technological Forecasting & Social Change" 2013, vol. 80, iss. 3, s. 541–555.

Kshetri N., *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives*, Heidelberg–London: Springer, 2010.

Lee N., *Counterterrorism. And Cybersecurity. Total Information Awareness*, New York: Springer, 2013.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń: Wydawnictwo Adam Marszałek, 2006.

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* [online], s. 1, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [dostęp: 6.02.2016].

Noga N., *Cyberterroryzm – nowe oblicze terroryzmu, cz. V. Internet jako cel ataków terrorystów – Klasyfikacja ataków w cyberprzestrzeni* [online], „e-Terroryzm.pl" 2013, nr 8, s. 18, http://www.academia.edu/5409045/Zjawisko_terroryzmu_w_Inguszetii_E-Terroryzm_nr_8_2013 [dostęp: 6.02.2016].

Siegel L.J., *Criminology*, Belmont: Cengage Learning, 2012.

Siegel L.J., Worrall J.L., *Introduction to Criminal Justice*, Belmont: Cengage Learning, 2014.

Smarzewski M., *Bezpieczeństwo państwa jako przedmiot ochrony niektórych przestępstw popełnianych za pośrednictwem sieci teleinformatycznej*, [w:] Z. Dziemianko, A. Kijas (red.), *Bezpieczeństwo współczesnego świata. Edukacja i komunikowanie*, Poznań: Wydawnictwo Wyższej Szkoły Handlu i Usług, 2013, s. 173–192.

Summers S., Schwarzenegger Ch., Ege G., Young F., *The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society*, Oxford-Portland: Hart Publishing, 2014.

United States Code, https://www.law.cornell.edu/uscode/text/18/2331 [dostęp: 6.02.2016].

Veerasamy N., Grobler M., Von Solms B., *Building an Ontology for Cyberterrorism*, [w:] E. Filiol, R. Erra (red.), *Proceedings of the 11th European Conference on Information Warfare and Security. The Institute Ecole Supérieure en Informatique Electronique et Automatique, Laval, France 5–6 July 2012*, Reading: Academic Publishing International Limited, 2012, s. 286–295.

Wiak K., *Prawnokarne środki przeciwdziałania terroryzmowi*, Lublin: Wydawnictwo KUL, 2009.

Yannakogeorgos P.A., *Rethinking the Threat of Cyberterrorism*, [w:] T.M. Chen, L. Jarvis, S. Macdonald (red.), *Cyberterrorism: Understanding, Assessment, and Response*, New York: Springer, 2014, s. 43–62.

CYBERTERRORYZM A CYBERPRZESTĘPSTWA O CHARAKTERZE TERRORYSTYCZNYM

Streszczenie

Cyberprzestępczość stanowi problem, który wymaga szerokich rozważań również na gruncie teoretycznoprawnym. Jaskrawy przykład stanowi cyberterroryzm, postrzegany często nie jako zagadnienie teoretyczne, ale realny byt. W doktrynie można zaobserwować błędne utożsamianie cyberterroryzmu z cyberprzestępstwem o charakterze terrorystycznym, w nawiązaniu do definicji przestępstwa o charakterze terrorystycznym z art. 115 § 20 k.k. W Kodeksie karnym ujęte są typy czynów zabronionych, wpisujące się z założenia w zaproponowany przez ustawodawcę schemat. Wydaje się, iż w tym kontekście można byłoby rozważać wyodrębnienie grupy przestępstw o charakterze cyberterrorystycznym. Niemniej jednak, zważywszy na fakt, iż cyberterroryzm pozostaje realnym, aczkolwiek nadal tylko zagrożeniem, właściwszym mieni się przyjęcie bezpieczniejszej w swej treści (i prawdopodobnie także terminologicznie) konstrukcji cyberprzestępstwa o charakterze terrorystycznym. Obydwu wskazanych kategorii pojęciowych nie można jednak uznawać za jednostkowo odpowiadające w swej treści cyberterroryzmowi.

Słowa kluczowe: cyberprzestępstwo, terroryzm, cyberterroryzm, przestępstwo o charakterze terrorystycznym, przestępstwo o charakterze cyberterrorystycznym, cyberprzestępstwo o charakterze terrorystycznym, prawo karne

CYBER-TERRORISM AND TERRORIST CYBER-CRIME

Summary

Cyber-crime constitutes a problem, which requires broad theoretical-legal solutions. Cyber-terrorism is a flagrant example often not perceived as a theoretical issue, but a real being. In the doctrine, cyber-terrorism is often wrongly identified with terrorist cyber-crime with reference to the definition of the features of terrorist crime laid down in Article 115 § 20 CC. The Criminal Code encloses types of illegal acts that fit in a system proposed by the legislator. It seems that in this context, a separate group of cyber-terrorist crimes might be considered. However, taking into account the fact that cyber-terrorism remains a real threat (although still only a threat), it seems that it would be more appropriate to adopt a safer in its content (and probably also from the point of view of terminology) term of terrorist cyber-crime. The two above-mentioned conceptual categories cannot be recognised as adequate to cyber-terrorism.

Key words: cyber-crime, terrorism, cyber-terrorism, terrorist crime, terrorist cyber-terrorist crime, terrorist cyber-crime, criminal law