DOI: 10.2478/v10226-012-0041-7

A N N A L E S
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA
VOL. XX, 2 SECTIO K 2013

Uniwersytet Warszawski, Instytut Nauk Politycznych
Instytut Badań nad Człowiekiem i Społeczeństwem im. Elżbiety Mider z d. Korzun

DANIEL MIDER

Analiza pojęcia cyberterroryzmu. Próba uporządkowania chaosu

Analyzing the concept of cyberterrorism. An attempt at organizing chaos

ABSTRAKT

Artykuł skupia się na zagadnieniach terminologicznych związanych z pojęciem cyberterroryzmu. W rozważaniach wykorzystano autorską metodę analizy obejmującą analizę etymologiczną (wydobycie słownikowego sensu pojęcia), indukcyjną (identyfikującą ogół cech charakteryzujących dany termin na podstawie reprezentatywnej grupy jego definicji) i kontekstową (służącą ustaleniu stosunku rozpatrywanego pojęcia do współwystępujących pojęć). Podsumowanie rozważań stanowi regulująca definicja pojęcia cyberterroryzmu eliminująca zastane nieostrości.

Słowa kluczowe: terroryzm, cyberterroryzm, bezpieczeństwo teleinformatyczne, bezpieczeństwo państwa

WSTĘP

Pojęcie cyberterroryzmu funkcjonuje w języku potocznym, w tym w języku subkultur Internetu, języku prawnym, publicystyce, a także w nauce. Jest ono pojęciem nieostrym i kontrowersyjnym, co stanowi istotną barierę poznawczą stosowania go na użytek analiz naukowych. Popularyzacja pojęcia cyberterroryzmu, w tym na gruncie nauki, a w szczególności nauk społecznych, stała się pierwotnym impulsem podjęcia w niniejszym artykule próby jego konceptualizacji – analizy jego znaczeń i próby uregulowania. Jednak nie jest to jedyny i najważniejszy motyw wysiłku analitycznego, choć jasny, ostry, precyzyjny język stanowi warunek *sine qua non* uprawiania nauki, a ponadto „nie tylko niektóre, ale wszystkie sądy, które przyjmujemy i które tworzą cały nasz obraz świata […] zależą od wyboru aparatury pojęciowej, przy pomocy

której odwzorowujemy dane doświadczenia" [Silver 1985: 175–195]. Kwestię tę podnosili liczni badacze[1]. Analizą pojęć podstawowych zajmuje się filozofia analityczna[2] i wydaje się, że reguły i sposoby procedowania przez nią wskazywane mogą również posłużyć do analizy pojęć innych niż podstawowe w danej dyscyplinie, jednak sens ich badania należy drobiazgowo uzasadnić.

Nader często badacze sami stosują pewne procedury badania i definiowania pojęć wynikające z predyspozycji i preferencji indywidualnych oraz zwyczajów środowiskowych lub ustaleń w danej dyscyplinie. Taki stan chaosu i niejednoznaczności jest niekorzystny, a w przypadku interdyscyplinarnych problemów badawczych (w niniejszym przypadku problemów na przecięciu informatyki i nauk społecznych) może wręcz uniemożliwiać pracę, dlatego zaproponowano autorskie narzędzie opracowane na podstawie studium literatury przedmiotu: schemat definiowania pojęć w naukach społecznych. Niniejszy tekst składa się z dwóch następujących części: w pierwszej – krótszej – przedstawiono propozycję dotyczącą standaryzowanej analizy i konceptualizacji pojęć, zaś w drugiej zastosowano ją w praktyce do analizy pojęcia cyberterroryzmu.

Konieczne jest – jak wskazano wcześniej – wyjaśnienie przesłanek podjęcia rozważań nad cyberterroryzmem. Wysiłek badawczy wynika z chęci i konieczności oczyszczenia „przedpola badawczego" w celu prowadzenia dalszych studiów – *stricte* empirycznych – nad tym zagadnieniem: próbą zrozumienia, czym to zjawisko jest w praktyce, systematyzacją jego przejawów, zagrożeniem cyberterroryzmem i jego potencjalnymi skutkami. Jednakże samego faktu zainteresowania badacza nie należy uznawać za wystarczający, bowiem podejmowanie określonego wysiłku analitycznego powinno mieć ważkie poznawcze i społeczne przesłanki.

W pierwszej kolejności należy rozważyć, dlaczego pojęcie, które – w uproszczeniu – powstało na gruncie publicystyki, ma stać się przedmiotem akademickich rozważań i – potencjalnie – być rozpatrywane jako mogące zostać w przyszłości włączone do słownika nauki o polityce. Wątpliwości budzi przede wszystkim publicystyczna proweniencja pojęcia cyberterroryzmu – zaczęło ono funkcjonować w dyskursie eksperckim oraz opinii publicznej. Wciąż pojawiają się liczne nowe terminy, które

[1] Na przykład Rudolf Carnap sprowadzał wszystkie problemy filozofii do zagadnienia składni, Alfred Tarski zaś redukował filozofię do logiki formalnej, z kolei Stanisław Ossowski wskazywał, że język nauki to język treści pojęciowych, *ergo* musi mieć jednoznaczną aparaturę pojęciową, która jest ostra i z której można korzystać w sposób operatywny, czyli dający niezawodną możliwość rozstrzygnięcia o przynależności lub nie danego przedmiotu do określonego zbioru. Niektórzy filozofowie, w szczególności ci związani z kołem wiedeńskim, postulowali stworzenie języka idealnego, składającego się z terminów pozbawionych nieostrości czy wieloznaczności.

[2] Filozofia analityczna (lub – za chemikiem Antoine'em Lavoisierem – logika nauki) stanowi konglomerat kilku szkół filozoficznych. Może być ujmowana szeroko – jako każdy typ refleksji ogniskujący się na analizie i definiowaniu pojęć. Ten typ rozważań podejmowali już starożytni myśliciele. W węższym rozumieniu filozofię analityczną rozumie się jako pewien nurt filozofii współczesnej, na który składa się głównie dorobek szkoły lwowsko-warszawskiej, koła wiedeńskiego oraz oksfordzkiej filozofii lingwistycznej.

mogą wejść do słownika nauk społecznych. W historii nauk społecznych wielokrotnie zdarzało się już, że liczne szeroko używane obecnie pojęcia trafiły do języka nauki z języka potocznego lub zostały zapożyczone z innych dyscyplin. Warto przy tym zauważyć, że często zakres i treść tych terminów zmieniała się istotnie, gdy zostały zaszczepione na nowym gruncie. Stało się tak między innymi – to bardzo często przytaczany przykład – z pojęciem „kultura", co pokazują Alfred L. Kroeber i Clyde Kluckhohn w *Culture: A critical review of concepts and definitions* [1952]. Można długo wymieniać pojęcia wprowadzone w analogiczny sposób do języka nauki: „biurokracja", „rewolucja", „dyskryminacja rasowa", „sztuka", „proletariat", „państwo", „klasa społeczna", „kasta" czy „religia". Wciąż, obok swojej definicji naukowej, mają one również znaczenie potoczne. Tak stało się też z innymi, mniej znaczącymi terminami – na przykład na gruncie badań nad partycypacją polityczną między innymi z pojęciami „bojkot", „nieposłuszeństwo obywatelskie" czy „pucz". Wiele terminów zapożyczono też z innych dyscyplin – należy przywołać popularną na gruncie nauk społecznych „konsumpcję", zaczerpniętą ze słownika XIX-wiecznej medycyny, kluczowe dla socjologii pojęcie „struktura", przyswojone wprost z architektury, czy równie istotną dla tej dyscypliny „warstwę", przejętą z geologii. Tę samą drogę wydaje się przechodzić „cyberterroryzm", lecz – naturalnie – podobne losy terminów nie są warunkiem wystarczającym dla podjęcia analiz nad nimi i nie uprawniają do twierdzenia, że jest ono choćby w ułamku tak znaczące jak wyżej wymienione. Warto także zwrócić uwagę, że używający pojęcia cyberterroryzmu popełnia grzech „amerykanizacji" języka nauki, lecz w sferach stykających się z zagadnieniami informatycznymi wydaje się to (niestety) nieuniknione – cały socjolekt związany z nowymi technologiami, cała siatka pojęciowa została wytworzona w języku angielskim. Przesłanką w pewnym stopniu uprawniającą do podjęcia rozważań nad terminem „cyberterroryzm" jest fakt, że wszedł on do dyskursu akademickiego – spośród 46 zgromadzonych na potrzeby analiz w niniejszym tekście definicji tego pojęcia aż 14 z nich, a więc blisko trzecia część, ma proweniencję *stricte* akademicką. Choćby dlatego warto przyjrzeć się temu terminowi uważniej, by rozstrzygnąć, czy i dlaczego wart jest włączenia do słownika nauk społecznych. Ważne wydaje się – niezależnie od wagi i statusu pojęcia – by uczeni, którzy zechcą zeń korzystać, jednakowo je rozumieli. Skoncentrowanie wysiłków analitycznych na pojęciu cyberterroryzmu wynika przede wszystkim z innych przesłanek. Zjawisko cyberterroryzmu wydaje się – potencjalnie – stanowić istotny problem polityczny i społeczny. Szczególnej wagi nabiera on w kontekście umieszczenia go w obszarze dynamicznie rozwijającej się w ostatnich latach, w tym i w Polsce, nauki o bezpieczeństwie, a w szczególności badaniach nad terroryzmem. Pewnych analogii można doszukiwać się w wydarzeniach lat osiemdziesiątych XX wieku, kiedy uwaga środowiska naukowego została przyciągnięta i zogniskowana na problemie związanym z nowymi technologiami wedle schematu analogicznego do tego, jaki funkcjonuje obecnie w odniesieniu do zagrożeń związanych z sieciami teleinformatycznymi. Wówczas to, co pierwotnie było tylko eksperckim sporem (mającym silny oddźwięk

publicystyczny i w dyskursie opinii publicznej) dotyczącym ryzyka związanego z energią atomową, w latach osiemdziesiątych Ulrich Beck zdiagnozował jako „społeczeństwo ryzyka". Stało się w efekcie ważną kategorią poznawczą i jednym z kluczowych elementów akademickich dyskusji na temat kondycji współczesnych społeczeństw [Beck 1988, 2002, 2007; Stankiewicz 2008; Strydom 2002]. Dynamiczny rozwój technologiczny w informatyce sprawił, że kluczowe dla funkcjonowania państwa, społeczeństwa i jednostki systemy zostały skrajnie uzależnione od sieci teleinformatycznych. Narażone na nieautoryzowaną ingerencję i poważne skutki są takie elementy (nazywane infrastrukturą krytyczną) jak systemy zaopatrzenia w energię, surowce energetyczne i paliwa, systemy łączności, sieci teleinformatyczne, systemy finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony życia i zdrowia, system transportowy, ratowniczy, system zapewniający ciągłość działania administracji publicznej, a także systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

1. SCHEMAT DEFINIOWANIA POJĘCIA CYBERTERRORYZMU

Budowanie słownika nauki, konstrukcja siatki pojęciowej powinny mieć charakter możliwie najbardziej precyzyjny, jednoznaczny, wielowymiarowy i przejrzysty, dlatego zasady definiowania pojęć powinny być wyłożone w sposób standaryzowany i sekwencyjny. Takie podejście, w przeciwieństwie do tak zwanego problemowego definiowania pojęć, stanowi urzeczywistnienie zasady poprawności warsztatu badawczego.

Pierwszy etap refleksji badacza nad danym terminem powinien polegać na sięgnięciu do źródłosłowu, słownikowego rozumienia danego wyrazu lub wyrazów składających się na dane pojęcie. Procedura analizy w tej fazie powinna obejmować następujące kroki analityczne: rozłożenie definiowanego wyrazu na części, z jakich powstał, odnalezienie sensu każdej z cząstek, z jakich go utworzono, a następnie wydobycie etymologicznego sensu całości słowa po połączeniu przeanalizowanych cząstek znaczących. W ramach analizy należy poddawać refleksji również takie części wyrazu jak przyrostki, a także zastanawiać się, jakie znaczenie ma zastosowanie poszczególnych spójek. Tadeusz Pawłowski zabieg taki jak wyżej opisany nazywa definiowaniem metodą etymologiczną [Pawłowski 1986: 29–30]. Etap ten nie jest konieczny we wszystkich rozpatrywanych przypadkach; badacz decyduje arbitralnie o jego pominięciu lub podjęciu. Integralnym elementem rozważań w tej fazie – obok kwestii *stricte* językowych, powinien być historyczny kontekst analizy terminu, w tym również zmieniające się niuanse jego znaczenia.

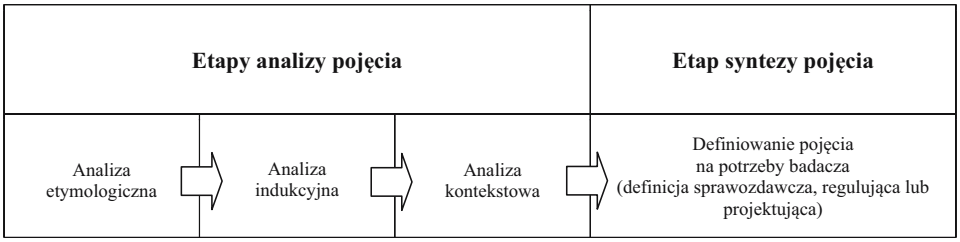
Drugi etap rozpatrywania przez badacza pojęcia polega na zidentyfikowaniu ogółu cech je charakteryzujących [Chandler 2001]. Innymi słowy, jest to zabieg polegający na określeniu treści pojęcia (nazwy), to jest jego konotacji lub – jeśli

wolimy – intensji. Pierwszym nieodzowny krok polega na rozpatrzeniu możliwie licznych i reprezentatywnych przypadków użycia danego terminu. Stanowi to nieodzowny warunek przeprowadzenia kolejnej procedury: dokonania zestawienia cech dla analizowanego pojęcia wspólnych, a także wskazania sprzeczności, niejasności i problemów tkwiących w analizowanym pojęciu. Na tym etapie analizy pomocne może okazać się wydobycie głównych kontrowersji i problemów dotyczących analizowanego terminu. Taki sposób analizy nazywany jest w literaturze przedmiotu metodą sokratyczną lub indukcyjną [Pawłowski 1986: 31–32], możemy także mówić o empirycznej analizie pojęcia. Etap ten może być przeprowadzony – jeśli znajduje to w opinii badacza uzasadnienie – również jako definiowanie intuicyjne, które można stosować wówczas, gdy w jakimś zakresie poddawane analizie pojęcie badacze rozumieją. Definiowanie intuicyjne polega na wielokrotnym doświadczaniu danego pojęcia w pewnych określonych kontekstach i w efekcie ukształtowania się rozumienia lub wielu rozumień danego pojęcia [Pawłowski 1986: 33–34].

Ostatni etap stanowiący dopełnienie refleksji badacza nad analizą pojęcia polega na ustaleniu stosunku rozpatrywanego pojęcia do innych, współwystępujących terminów. Badaniu należy poddać pojęcia nadrzędne i podrzędne, zamienniki oraz pojęcia krzyżujące się (w tym pozostające w stosunku podprzeciwieństwa i niezależności), a także wykluczające się z pojęciem analizowanym. Badacz na tym etapie postępowania analitycznego staje się – posłużmy się taką metaforą – kartografem, który umieszcza dany termin na siatce pojęciowej, wśród innych pojęć, usiłując zrekonstruować mapę. Warto podkreślić, że na tym etapie analizy badacz podejmuje refleksję nie tylko na płaszczyźnie logicznej – jak może sugerować użyta w opisie nomenklatura z zakresu logiki formalnej – ale także na płaszczyźnie semantycznej i merytorycznej. Efektem rozważań powinien być nie tylko monograficzny opis, „słownikowy" indeks pojęć, lecz również odnalezienie ewentualnych zamienników danego terminu oraz rozstrzygnięcie o zasadności używania go. Jeśli odwołamy się do klasycznego sposobu definiowania pojęć zaproponowanego przez Arystotelesa w *Organonie* (konkretnie w *Topikach*), wyrażanego formułą *definitio fit per genus proximum et differentiam specificam*, to na tym etapie badacz odnajduje wyraźnie „rodzaj najbliższy" – *genus proximum*.

Przeprowadzenie analizy pojęcia pozwala badaczowi na skonstruowanie narzędzia analitycznego na własne potrzeby. Może tego dokonać na co najmniej trzy sposoby: przyjmując istniejące już znaczenie danego pojęcia (definicja sprawozdawcza), modyfikując je, co polega na przykład na wykluczeniu nieostrości lub wieloznaczności (definicja regulująca), lub nadając mu nowe znaczenie (definicja projektująca). Ten etap stanowi ukoronowanie poprzedniego – jego syntezę.

Rozpatrywany wyżej uniwersalny schemat analizy i definiowania pojęć przedstawiono na rysunku 1.



Rysunek 1. Ogólny schemat definiowania pojęć

Źródło: opracowanie własne.

Jednakże mechaniczne, izolowane definiowanie pojęć pozostaje zajęciem jałowym, dopóki badacz nie podejmie się refleksji na temat wartości takiego pojęcia, sensu włączenia go do słownika nauki. Czynność ta wykracza poza sam akt definiowania terminu: dokonujemy tu swoistego wartościowania pojęcia, oceny jego przydatności i rozstrzygamy, czy i w jakim miejscu siatki terminologicznej danej dyscypliny proponujemy je umieścić.

2. ANALIZA ETYMOLOGICZNA POJĘCIA CYBERTERRORYZMU

Do analizy etymologicznej badacz powinien podchodzić krytycznie i ostrożnie. Znaczenie potoczne nadane terminowi może być mylące. Z kolei w innych przypadkach dzięki analizie etymologicznej badacz uzyskuje wartościowe wskazówki do pogłębionej analizy pojęcia na gruncie nauki. W przypadku cyberterroryzmu przesłankami podjęcia analizy etymologicznej był fakt zróżnicowanego pochodzenia składników tego terminu: rozwijały się one zarówno w literaturze pięknej, publicystyce, nauce, jak i socjolekcie subkultur Internetu. Odnalezienie znaczenia lub znaczeń pojęcia na wymienionych obszarach wydaje się warunkiem uporządkowania go na gruncie naukowym.

Analizę etymologiczną cyberterroryzmu rozpocznijmy od refleksji nad poszczególnymi częściami, z jakich pojęcie to powstało, i odnalezienia sensu dla każdej z cząstek, z jakich je utworzono. Słowo cyberterroryzm jest derywatem (jednostką złożoną, o dwudzielnej budowie formalnej) składającym się z przedrostka słowotwórczego „cyber" oraz podstawy słowotwórczej „terroryzm".

Rozważmy etymologiczne znaczenie pierwszego z elementów. Przedrostek słowotwórczy „cyber" wywodzi się od nazwy nauki o systemach sterowania oraz o związanym z tym przetwarzaniu i przekazywaniu informacji – cybernetyki. Po raz pierwszy pojęcia „cybernetyka" użył amerykański matematyk Norbert Wiener w 1948 roku [Wiener 1948/1971]. Zostało ono przezeń zapożyczone ze starożytnej greki, gdzie *kybernētikos* (κυβερνητικός) oznacza biegłość w sztuce sterowaniem, zaś *kybernaō* (κυβερνάω) – „sterować", „prowadzić", „przewodzić" lub „zarządzać". Z kolei *kybernán* (κυβερηάη) należy rozumieć jako „sterować" lub „kontrolować". Przedstawione gniazdo semantyczne było w antycznej Grecji używane we współ-

czesnym znaczeniu słowa „rządzić". Pochodzenie przedrostka „cyber" od słowa „cybernetyka" narzuca jednoznaczne asocjacje znaczeniowe z informacją i jej przepływem oraz – co ważne – zarządzaniem tym procesem. Termin „cybernetyka" okazał się nad wyraz atrakcyjny słowotwórczo. W latach sześćdziesiątych pojawiło się pojęcie cyborga – na określenie integracji sztucznych, najczęściej elektronicznych elementów z ciałem ludzkim w celu jego wspomagania, zaś amerykańska Control Data Corporation w latach siedemdziesiątych XX wieku rozpropagowała przedrostek „cyber" jako synonim komputeryzacji [Trappl 1998]. Jednakże od pojęcia cybernetyki do obecnego znaczenia przedrostka „cyber", stosowanego między innymi w takich terminach jak „cyberterroryzm", wiodła długa droga. Przedrostek „cyber" nabrał obecnie metaforycznego i pogłębionego wobec pierwotnego znaczenia dzięki jednemu z gatunków literatury pięknej – fantastyce naukowej (*science-fiction*, a konkretnie jednej z odmian tego gatunku, tzw. cyberpunkowi). Przyjął się on na tym gruncie w zestawieniu z podstawą słowotwórczą „przestrzeń" (cyberprzestrzeń, *cyberspace*). Przedrostek „cyber" został po raz pierwszy w znaczeniu bliskim obecnemu użyty w 1982 roku przez amerykańskiego pisarza Williama Gibsona w opowiadaniu *Wypalić chrom* (*Burning Chrome*). Pisarz wykorzystał go wówczas jako nazwę własną urządzenia Ono-Sendai VII „Cyberprzestrzeń Siedem", służącego do łączenia umysłu użytkownika z informacyjną przestrzenią niefizyczną, wirtualną, utworzoną przez nowe technologie, nazywaną przez autora także matrycą (*matrix*). Koncepcja cyberprzestrzeni została rozwinięta przez W. Gibsona w kultowej dla wielbicieli literatury fantastycznonaukowej powieści *Neuromancer*, opublikowanej w 1984 roku. Znaczenie pojęcia cyberprzestrzeni impresywnie i trafnie charakteryzuje następujący fragment dzieła:

> To jest cyberprzestrzeń. Konsensualna halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych… Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność… [Gibson 1992: 43].

Zwróćmy uwagę na profetyczne walory przytoczonego tekstu, bowiem został on utworzony, zanim powstała sieć WWW. Jednakże sam pisarz, samokrytycznie, po latach wskazuje, że użył słowa „cyberprzestrzeń" z błahych i nieprzemyślanych merytorycznie powodów – przedrostek „cyber" uznał za modny, wydał mu się on ciekawy i sugestywny. Podkreśla również, iż decydując się na jego wykorzystanie, nie rozpatrywał realnego, słownikowego znaczenia tego pojęcia [Thil 1948; Gibson 2009, 2000]. Do dyskursu akademickiego pojęcie cyberprzestrzeni wprowadzili między innymi dwaj Amerykanie – badacz z Vanderbilt University Jay Clayton oraz pisarz związany z literackim nurtem cyberpunk Bruce Michael Sterling [1994]. Przedrostek „cyber" nad wyraz dobrze zadomowił się w naukach społecznych – badacze postulują wprowadzenie interdyscyplinarnych subdyscyplin badawczych takich jak na przykład cybersocjologia i cyberpsychologia [Kubczak 2002: 183–190; Batorski 2007: 5–14; Suler 2006].

Nakreślone tło pozwala stwierdzić, że przedrostek „cyber" nabył swoje obecne znaczenie głównie na płaszczyźnie literatury fantastycznonaukowej i języka potocznego, a w szczególności socjolektu subkultur Internetu i subkultur technicznych (informatyków). Używany jest on wszędzie tam, gdzie chcemy poinformować o umiejscowieniu jakiegoś zjawiska w przestrzeni parafizycznej, wytworzonej przez nowe technologie. Cyberprzestrzeń – pisze B.M. Sterling – stanowi miejsce w sensie przestrzeni komunikacyjnej, jest to zdalna interakcja wraz z jej kontekstem zachodząca pomiędzy dwoma lub więcej podmiotami znajdującymi się w różnych lokalizacjach [Sterling 1994]. Pomimo faktu, że przestrzeń oznaczona jako „cyber" nie istnieje w sensie fizycznym, to jednak jej funkcjonowanie ma realne konsekwencje, jest ona – używając języka socjologii – faktem społecznym. W tym sensie przedrostek „cyber" powinien być utożsamiany z Internetem – w szczególności jego aspektem informacyjnym, komunikacyjnym, jego warstwą społeczną i programistyczną. W mniejszym stopniu będziemy go identyfikować z warstwą fizyczną Internetu – serwerami i łączami pomiędzy nimi, bowiem wpływają one zaledwie pośrednio na percepcję zjawiska Internetu przez jego użytkowników. Warto w tym kontekście zwrócić uwagę na następującą właściwość analizowanego przedrostka – jego elastyczność. Może być on użyty na określenie wciąż powstających i zmieniających się form komunikacji zapośredniczonej przez nowe technologie. Na przykład dzięki jego elastyczności automatycznie znalazła się w jego obrębie przestrzeń komunikacyjna oraz informacyjna utworzona przez technologię telefonii komórkowej. Przedrostek ten może być tak rozumiany dzięki swojemu metaforycznemu znaczeniu – uzyskał je przez długi czas używania na gruncie literatury fantastycznonaukowej i publicystyki.

Podstawa słowotwórcza pojęcia „cyberterroryzm" – „terroryzm" – jest z kolei lepiej rozpoznana w literaturze przedmiotu, ale nie ma ona tak skomplikowanej jak przedrostek „cyber" historii implikującej nieostrość lub nawet wieloznaczność. Słowo „terroryzm" pochodzi z sanskrytu – od słowa *tras*, które oznaczało „drżeć", ale wywodzone jest też z antycznej greki, gdzie *treo* (τρέω) oznaczało „drżeć" i „bać się", lecz również „stchórzyć" lub „uciec". Bywa również wywodzone z łacińskiego *terror* lub *terroris*, oznaczającego „strach", „trwogę" lub „przerażenie", używanego także na oznaczenie „strasznego słowa" bądź „przerażającej wieści". Nasze rozumienie pogłębia pochodny czasownik łaciński *terreo*, tłumaczony jako „wywoływać przerażenie" albo po prostu „straszyć". Pojęcie to było w starożytności odległe od tego, jak rozumiemy je obecnie. W historii starożytnego Rzymu ten związek frazeologiczny zapisał się podczas najazdu germańskich plemion Cymbrów i Teutonów w 105 roku p.n.e., gdy armia rzymska została pokonana, co umożliwiło najeźdźcom rabunek Galii. Pojawiła się wówczas fraza *terror cimbricus*, oznaczająca panikę spowodowaną wkroczeniem Cymbrów wraz z sojusznikami w granice Imperium i w efekcie konieczność wprowadzenia stanu wyjątkowego. Pojęcie terroru zyskało nowe konotacje w XVIII-wiecznej Francji. Amerykańska uczona Carla Hesse przeprowadziła wartościową i ilościową analizę tekstów *Wielkiej encyklopedii francuskiej* (*Encyclopédie, ou dictionnaire raisonné des sciences, des arts et des métiers*) z końca

XVIII wieku i wykazała, że słowo „terror" było już wówczas w języku francuskim nader popularne i powszechnie używane w rozmaitych kontekstach. W *Encyklopedii* odnajdujemy niemal trzystukrotne wykorzystanie tego słowa. Odnosi się ono do pięciu następujących sfer życia społecznego: prawa i polityki (34 przypadki użycia), mitu i religii (45 przypadków), wojny (54 przypadki), estetyki (57 przypadków) oraz nauki, w szczególności fizjologii (77 przypadków) [Hesse 2008: 6]. Rewolucja francuska wykrystalizowała znaczenie tego pojęcia – konkretnie „terror" w znaczeniu pewnej formy wpływania na politykę – lub ściślej – sprawowania rządów należy wiązać z jakobińskimi rządami terroru w latach 1793–1794 (*Le Gouvernement de la Terreur*), podczas których zginęło od kilkunastu do kilkudziesięciu tysięcy Francuzów, a w szczególności z wielkim terrorem, jak nazywano czas nasilenia przemocy w czerwcu i lipcu 1794 roku. Po przewrocie 9 thermidora jako nazwy kolejnego okresu używano frazy „biały terror". Za wprowadzenie tego pojęcia na grunt praktyki polityki i słownika polityki odpowiedzialni są „ojcowie terroru" – Maksymilian Robespierre i Louis Saint-Just (sami siebie i rząd swój nazywający terrorystami). Terror podczas rewolucji nie służył jedynie do represji i wywierania zemsty – miał charakter planowy i stanowił również, a może nawet przede wszystkim, narzędzie politycznego wpływu, instrument transformacji systemu politycznego oraz społeczeństwa. Stał się on jednym ze sposobów wpływania przez klasę rządzącą na politykę, czy – stosując współczesną nomenklaturę – jedną z form partycypacji politycznej. Dla przybliżenia tego ostatniego znaczenia, w jakim używano omawianego pojęcia, warto przytoczyć fragment dekretu *O wprowadzeniu terroru* Konwentu Narodowego z 7 września 1793 roku (opublikowanego później w „Monitorze", numer 250):

> Czas już najwyższy, aby równość przeszła jak kosa po wszystkich głowach. Czas już, aby przerażenie ogarnęło wszystkich konspiratorów. A więc, prawodawcy! Postawcie terror na porządku dziennym.

Terror miał być procesem ciągłym, sformalizowanym i zinstytucjonalizowanym, legitymizowanym na gruncie prawa i stosowanym przez władzę polityczną, bowiem w dalszych częściach dokumentu Konwent postulował utworzenie rewolucyjnej armii oraz trybunałów jako narzędzi terroru przeciwko jednostkom i grupom uznanym za spiskowców i kontrrewolucjonistów. Dał temu jasno wyraz sam M. Robespierre w przemówieniu do Konwentu Narodowego z 5 lutego 1794 roku:

> Terror jest niczym innym jak sprawiedliwością, niezwłoczną, srogą, nieugiętą; dlatego jest emancypacją cnoty; nie tyle jest specjalną zasadą, ale konsekwencją ogólnej zasady demokracji dostosowaną do najpilniejszych potrzeb naszego państwa[3].

[3] W oryginale: „La terreur n'est autre chose que la justice prompte, sévère, inflexible; elle est donc une émanation de la vertu; elle est moins un principe particulier, qu'une conséquence du principe général de la démocratie, appliqué aux plus pressants besoins de la patrie" [Robespierre 1794].

Terror stał się narzędziem tym potężniejszym, że zaopatrzonym – w oczach go wykorzystujących – w uzasadnienie moralne i ideologiczne. Podobnie rozpatrywał go L. Saint-Just, podkreślając, że terror to jedna z form wpływu politycznego, a rząd republikański może stosować go jako alternatywę dla innych form oddziaływania[4].

Co ważne – podczas rewolucji francuskiej „terror" uzyskał sufiks „-yzm" (pol. „-yzm", ang. „-ism", fr. „-isme"). Przyrostek ten pochodzi z greki (od starogreckiego *-ismos* (ισμός), gdzie wykorzystywano go do tworzenia rzeczowników odczasownikowych służących do wyrażania stanu działania, praktyki, ale także zasady lub doktryny. Takie derywaty słowotwórcze nabrały też dodatkowego znaczenia – „doktryna", „teoria", „kierunek", „szkoła" lub „zespół poglądów tworzących pewną całość". Użycie zatem słowa „terroryzm" zamiast „terror" miało znaczenie zasadnicze – oznaczało pewien zintegrowany i zracjonalizowany zespół praktyk politycznych. Pierwsza słownikowa definicja terroryzmu znalazła się w wydanym przez Akademię Francuską w 1798 roku suplemencie do słownika, definiując jego znaczenie jako *système, régime de la terreur*, to jest system lub reżim rządów opierający się na strachu [Shane 2010: 1; Tuman 2003]. Z kolei na gruncie języka angielskiego słowo „terroryzm" pojawiło się po raz pierwszy pod koniec XVIII wieku. Jako jeden z pierwszych użył go brytyjski polityk i prekursor konserwatyzmu Edmund Burke, który w swoich listach z 1795 roku pisał o „tysiącach ogarów piekieł zwanych terrorystami", wskazując na rewolucjonistów we Francji[5]. Z kolei w Burke'owskich *Rozważaniach o rewolucji we Francji* (1790) słowo „terror" i „terrors" odnajdujemy ośmiokrotnie, choć głównie w kategoriach opisu stanów psychicznych jednostek – przynajmniej raz jednak w znaczeniu zbliżonym do formy sprawowania rządów. W języku angielskim w znaczeniu taktyki francuskich rewolucjonistów słowo „terroryzm" pojawiło się (a nie ich nazwy własnej) u brytyjskiego satyryka, nauczyciela i urzędnika Thomasa Jamesa Mathiasa w 1798 roku. Autor wymienił terroryzm obok innych środków osiągania celów politycznych, takich jak morderstwa, masakry czy powstania i bunty [Hesse 2008]. Rewolucji francuskiej zawdzięczamy etymologiczny mariaż pojęć terroru i terroryzmu z polityką, jednakże tego drugiego terminu nie używano wówczas w formie takiej, jaka funkcjonuje dzisiaj. Obecnie słowo „terroryzm" odnosi się do nielegitymizowanych działań podejmowanych przez aktorów pozapaństwowych, a „terror" służy określeniu działań aktorów państwowych [Mider 2008]. Etymologiczne znaczenie pojęcia „terroryzm" ukształtowało się pod koniec XIX wieku i na początku XX wieku. Nie przyjęło się ono od razu, równolegle funkcjonowały inne jego nazwy. Początkowo wykorzystywano pojęcie terroru indywidualnego – na określenie użycia przemocy przez opozycjonistów wobec przedstawicieli władzy i klas uprzywilejowanych. Anarchiści posługiwali się określeniem „propaganda przez czyn", rewolucyjni syndy-

[4] W oryginale: „Un gouvernement républicain a la vertu pour principe; sinon, la terreur. Que veulent ceux qui ne veulent ni vertu ni terreur?" [Saint-Just 1793–4/2005: 1139].

[5] W oryginale: „Thousands of those hell-hounds called Terrorists, whom they had shut up in prison, on their last Revolution, as the satellites of tyranny, are let loose on the people" [Burke 1795/1999: 371].

kaliści stosowali termin „indywidualna ekspropriacja" (*individuelle reprise*) i „akcja bezpośrednia" (*direct action*), zaś ideologowie Narodnej Woli proponowali nazwę „neopartyzanckie działania wojenne". Z kolei Józef Piłsudski, działając w Polskiej Partii Socjalistycznej, zwykł był używać eufemistycznego określenia „czyn zbrojny", natomiast w Indiach terroryzmowi nazywano rosyjską metodą [Iviansky 1977: 44].

Termin „terroryzm" w obecnym znaczeniu ukształtował się na skutek działań XIX-wiecznych ruchów separatystycznych, nacjonalistycznych, a później skrajnie lewicowych: irlandzkich fenian, włoskich karbonariuszy, rosyjskich narodników czy polskich sztyletników. Szczególną rolę w kształtowaniu się współczesnego rozumienia pojęcia terroryzmu odegrał – jak podkreślają niektórzy badacze – Siergiej Nieczajew, rosyjski rewolucjonista, założyciel organizacji Zemsta Ludu, sam określający się jako terrorysta [Pomper 2007]. Przypisuje mu się autorstwo *Katechizmu rewolucjonisty*[6], dokumentu, w którym właściwie przedstawiono archetyp terrorysty [Nieczajew, Bakunin, Ogariow 1869]. Apoteozę terroryzmu wyraża następujący fragment *Katechizmu* (choć to określenie tam nie pada):

> Bezlitosny dla państwa i w ogóle dla całego układu klasowo oświeconego społeczeństwa, nie powinien też od niego oczekiwać dla siebie litości. Między nimi i nim trwa skryta czy otwarta, ale nieustanna i nieprzejednana, na śmierć lub życie, wojna. Każdego dnia powinien być gotowy na śmierć. Powinien nauczyć się znosić tortury [Nieczajew, Bakunin, Ogariow 1869].

Takie właśnie rozumienie terroryzmu jako sprzeciwu wobec tyranii lub nawet wszelkiej władzy państwowej wyrażającej się przemocą stało się istotą terroryzmu. Była to tak zwana pierwsza fala terroryzmu w Europie, której efektem było między innymi zabójstwo cara Aleksandra II przez Ignacego Hryniewieckiego w 1881 roku, prezydenta Francji Marie-François Sadi Carnota (1884), premiera Hiszpanii Antonio Cánovas Del Castillo (1897), cesarzowej austriackiej Elżbiety von Wittelsbach (1898), króla włoskiego Humberta I (1900), prezydenta Stanów Zjednoczonych Williama McKinleya (1901), premiera Hiszpanii José Canalejasa (1912), a także zamach na życie następcy tronu Austro-Węgier arcyksięcia Franciszka Ferdynanda (1914), dokonany przez Gawriło Principa, członka organizacji Młoda Bośnia, co stało się bezpośrednim powodem wybuchu I wojny światowej [Borkowski 2001: 115 i n].

Analiza przedrostka słowotwórczego „cyber" i podstawy słowotwórczej „terroryzm" prowadzi do zrozumienia derywatu po zestawieniu tych dwóch części. W etymologicznym, dosłownym znaczeniu „cyberterroryzm" to działanie, które: 1) ma na celu wywołanie stanu przerażenia, 2) wykorzystuje jakąś formę przemocy, 3) jest skierowane bezpośrednio przeciwko władzy politycznej lub ludności cywilnej, 4) jest podejmowane przez obywateli, 5) ma na celu wywarcie wpływu na politykę, 6) rozgrywa się w przestrzeni niefizycznej, wirtualnej, utworzonej przez

[6] Autorstwo tego dokumentu przypisywane jest również Michałowi A. Bakuninowi oraz Mikołajowi P. Ogariowowi, w owym czasie współpracującym z Nieczajewem.

nowe technologie, a konkretnie przez Internet. Takie etymologiczne rozumienie jest niezadowalające ze względu na liczne jego nieostrości. Po pierwsze, przytoczone rozumienie odwołuje się do pojęć wymagających zdefiniowania – przede wszystkim są to „przemoc" i „przerażenie", które mimo że bardzo dobrze rozumiane potocznie, jednak od lat stanowią przedmiot rozważań i kontrowersji na gruncie nauki. Po drugie, koniecznie należy doprecyzować kwestię liczebności grup podejmujących działania terrorystyczne – rozumienie potoczne pozostawia to zagadnienie nierozstrzygnięte. Po trzecie, refleksji wymaga kwestia działań symbolicznych, ekspresyjnych jako motywu podejmowania cyberterroryzmu – czy takie działania, niemotywowane konkretnym politycznym celem, lecz podejmowane wyłącznie w celu przekazania jakiegoś komunikatu również mogą zostać określone tym mianem? Po czwarte, etymologiczne rozumienie nieprecyzyjnie określa granice cyberprzestrzeni. Po piąte, według powyższego rozumienia nie jest jasne, czy cyberterroryzm to działanie podejmowane za pośrednictwem cyberprzestrzeni, czy też na nią oddziałujące. W drugim przypadku do cyberterroryzmu zaliczylibyśmy również takie zjawiska jak fizyczne zniszczenie infrastruktury Internetu (serwerów i łącz komunikacyjnych). Te wszystkie niejasności zostają wyjaśnione w kolejnych etapach postępowania analitycznego.

3. ANALIZA INDUKCYJNA POJĘCIA CYBERTERRORYZMU

Drugi etap rozpatrywania pojęcia cyberterroryzmu polega na zidentyfikowaniu ogółu cząstkowych cech charakteryzujących ten termin. Zabieg ten sprowadza się do określenia treści pojęcia (intensji). Pierwszy krok postępowania stanowi rozpatrzenie możliwie licznych i reprezentatywnych przypadków użycia terminu „cyberterroryzm". W tym celu zebrano 46 definicji tego pojęcia (a także pojęć uznawanych przez niektórych badaczy za synonimy omawianego terminu: elektroniczny terroryzm i terroryzm informacyjny), by przeprowadzić ilościową, frekwencyjną analizę według przygotowanego modelu badawczego. Definicje zostały wybrane na zasadzie wyczerpującej – odnaleziono i opracowano te dostępne w anglojęzycznej (26 definicji), polskojęzycznej (17) i rosyjskojęzycznej (3) literaturze przedmiotu. Największa liczba definicji miała źródło instytucjonalne – aż 30 z nich zostało opracowanych na potrzeby instytucji sektora pierwszego (głównie resortów siłowych), trzeciego (instytutów badawczych o profilu informatycznym), a także drugiego (firm informatycznych i prawniczych). Dwie spośród tych definicji zaczerpnięto ze słowników – oksfordzkiego i Merriama-Webstera. Analiza zgromadzonych definicji wykazała, że w ramach pojęcia cyberterroryzmu istotne dla badaczy w jego definiowaniu są następujące aspekty: podmiot działania, rodzaj działania, sposób działania, środowisko (miejsce) działania, bezpośredni efekt oddziaływania, pośredni, czyli końcowy efekt oddziaływania, adresat działania, adresat roszczeń oraz cel działania. Celem takiego zabiegu było ilościowe, standaryzowane wykazanie, w jakim stopniu poszczególne elementy definicyjne są u różnych badaczy tożsame, a w jakim odmienne. Identyfi-

kacja cząstkowych znaczeń składających się na pojęcie cyberterroryzmu w ramach wymienionych aspektów odbywała się według następujących pytań analitycznych:

1) *Kto podejmuje działanie nazywane cyberterroryzmem?* – a więc kto jest podmiotem działania. W analizowanych definicjach nie rozstrzygano tego lub sporadycznie jako podmiot dokonujący aktów cyberterrorystycznych wskazywano „grupę lub jednostkę". To pytanie analityczne ma w związku z tym niewielką moc heurystyczną, jednakże z formalnego, logicznego punktu widzenia jego postawienie wydaje się zasadne i konieczne.

2) *Co nazwiemy cyberterroryzmem? Jaki rodzaj działania?* W analizowanych definicjach dały się zidentyfikować trzy następujące wartości: (i) cyberterroryzm to informowanie, komunikowanie się i mobilizowanie zasobów, a więc działania typowo komunikacyjne, (ii) cyberterroryzm oznacza groźbę użycia przemocy oraz (iii) cyberterroryzm to działanie polegające na użyciu przemocy.

3) *Jaki sposób działania nazwiemy cyberterroryzmem?* W tej kategorii jako jedyny przydatny analitycznie przymiotnik pojawiał się wyraz „bezprawne". Niektórzy badacze w stosunku do cyberterroryzmu w swoich definicjach używali takich określeń jak „skryty", „rozmyślny" czy „z premedytacją". Ze względu na niską wartość heurystyczną tych określeń oraz śladową liczbę wystąpień pominięto je w dalszych analizach.

4) *Gdzie odbywa się działanie nazywane cyberterroryzmem?* W odpowiedzi na to pytanie analityczne badacze udzielali w swoich definicjach sprzecznych odpowiedzi: wskazywali, że cyberterroryzmem można nazwać tylko działania mające miejsce w cyberprzestrzeni lub przeciwnie – również takie, które odbywają się poza nią (a więc ataki fizyczne), lecz na nią bezpośrednio oddziałują, to jest zakłócają jej funkcjonowanie lub niszczą jej infrastrukturę. Część badaczy uznawała za właściwe rozróżnienie pomiędzy atakami dokonywanymi bezpośrednio (za pomocą włamania) a przeprowadzanymi za pośrednictwem samodzielnie działających programów – wirusów lub robaków komputerowych. Niektórzy badacze nie precyzowali tego aspektu, z kontekstu jednak można było wnioskować o chęci objęcia definicją pojęcia jak największej liczby zjawisk, a więc nazywania cyberterroryzmem zarówno działań prowadzonych w cyberprzestrzeni, jak i poza nią.

5) *Na co bezpośrednio ma oddziaływać cyberterroryzm?* Bezpośrednim obiektem działań cyberterrorystów są programy i usługi, dane (informacje) zgromadzone w komputerach, komputery i sieci (w tym urządzenia łączące komputery, takie jak na przykład routery). Wskazywano również – jako bezpośredni obiekt ataku cyberterrorystów – tak zwaną infrastrukturę krytyczną[7]. Część badaczy pozostawiała ten

[7] Roboczo, na potrzeby wyjaśnień niniejszego fragmentu rozważań, przyjęto definicję infrastruktury krytycznej za Ustawą z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590). W myśl tego aktu prawnego przez infrastrukturę krytyczną rozumiemy systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym 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. Takie

element nieokreślony, pozwalając się domyślać wszystkich wymienionych oddziaływań łącznie.

6) *Jaki jest bezpośredni efekt działania nazywanego cyberterroryzmem?* Badacze wskazywali, że cyberterroryzm to: manipulowanie informacją, szczególnie w kontekście jej zniekształcania, blokowanie pracy sieci i komputerów, zakłócanie jej pracy, powodowanie zawieszania się urządzeń znajdujących się w sieci, przejmowanie kontroli nad komputerami i sieciami, a także niszczenie komputerów lub informacji. Część badaczy pozostawiała to pytanie bez odpowiedzi, jednak inne elementy definicji pozwalały domyślać się, że bezpośrednim efektem cyberterroryzmu jest zniszczenie lub wyeliminowanie komputerów lub znajdujących się w nich danych.

7) *Jaki jest pośredni efekt działania nazywanego cyberterroryzmem?* Badacze wymieniają w definicjach rozmaite ewentualności: poczucie stanu zagrożenia (obywateli i rządzących), wywołanie strat materialnych, które mogą ograniczać się do infrastruktury sieci (fizycznego nośnika cyberprzestrzeni) lub mogą obejmować szersze kategorie przedmiotów materialnych. Niektórzy badacze uważają również, że efektem działań cyberterrorystycznych mogą być straty w ludziach – zabici i ranni.

8) *Do kogo skierowany jest cyberterroryzm? Kto jest adresatem tego działania w sensie komunikacyjnym?* Innymi słowy – *na powiadomieniu jakich podmiotów społecznych zależy cyberterroryście?* To pytanie analityczne było opatrywane w definicjach badaczy następującymi odpowiedziami: osoby cywilne, media, opinia publiczna, państwo i jego funkcjonariusze, organizacje międzynarodowe. Warto zwrócić uwagę, że niektóre z wymienionych kategorii (osoby cywilne i opinia publiczna) pokrywają się. Niektórzy badacze nie udzielali odpowiedzi na to pytanie analityczne, jednak treść definicji każe się domyślać wszystkich powyższych podmiotów.

9) *Kto jest adresatem roszczeń i żądań cyberterrorystów?* Mogą nimi być: państwo i jego funkcjonariusze, społeczeństwo, organizacje międzynarodowe lub adresat może być nieokreślony (co również i w tym przypadku sugeruje jak najszerszy zakres podmiotów).

10) *W jakim celu podejmowany jest cyberterroryzm?* To pytanie analityczne odnosi się do rodzaju korzyści, jakie dla siebie lub swojej grupy przewiduje osiągnąć podmiot podejmujący działania terrorystyczne w cyberprzestrzeni. Zidentyfikowano następujące kategorie celów: ideologiczne, społeczne, polityczne, religijne oraz kategorię pustą, do której zakwalifikowano badaczy, którzy nie ujmowali celów w swoich definicjach.

---

rozumienie infrastruktury krytycznej jest typowe. Zwykle definiuje się ją przez wskazanie desygnatów, a więc pewnych funkcjonalnych obszarów państwa.

Tabela 1. Analiza frekwencyjna definicji pojęcia „cyberterroryzm”

Lp.	Aspekt analizy definicji	Pytanie analityczne	Elementy definicji	N	%
1.	Podmiot działania	*Kto?*	**ktokolwiek/nie podano**	**38**	**82,6**
			grupa lub jednostka	8	17,4
2.	Rodzaj działania	*Co?*	informowanie, komunikowanie się i mobilizowanie zasobów	3	6,5
			groźba użycia przemocy	22	47,8
			przemoc	**46**	**100,0**
3.	Sposób działania	*Jak?*	bezprawnie (nielegalnie)	8	17,4
4.	Środowisko/ miejsce działania	*Gdzie?*	oddziaływanie w cyberprzestrzeni (atak bezpośredni – poprzez włamanie i ingerencję)	2	4,3
			oddziaływanie w cyberprzestrzeni (atak pośredni – z użyciem wirusa/robaka/bakterii jako pośrednika)	2	4,3
			oddziaływanie w cyberprzestrzeni – nie określono, czy jest to atak pośredni, czy bezpośredni	20	43,5
			oddziaływanie na cyberprzestrzeń spoza cyberprzestrzeni	3	6,5
			nieokreślony w ogóle, należy domyślać się najszerszej definicji	**25**	**54,3**
5.	Bezpośredni obiekt oddziaływania	*Na co?*	programy i usługi	11	23,9
			dane	16	34,8
			komputery i sieci	**22**	**47,8**
			infrastruktura krytyczna	5	10,9
			nieokreślony (definicja każe się domyślać wszystkich powyższych elementów)	18	39,1
6.	Bezpośredni efekt oddziaływania	*Z jakim efektem?*	manipulowanie (zniekształcanie)	6	13,0
			zablokowanie/zawieszenie/zakłócanie/zaszyfrowanie	17	37,0
			przejęcie kontroli	5	10,9
			zniszczenie/wyeliminowanie	17	37,0
			nieokreślony, należy się raczej spodziewać niszczenia	**24**	**52,2**

Lp.	Aspekt analizy definicji	Pytanie analityczne	Elementy definicji	N	%
7.	Pośredni (końcowy) efekt oddziaływania	*Z jakim efektem?*	**poczucie stanu zagrożenia przez obywateli i/lub rządzących**	**23**	**50,0**
			straty materialne dotyczące infrastruktury/niedotyczące infrastruktury	14	30,4
			straty w ludziach (ranni, zabici)	10	21,7
			straty nieokreślone – materialne lub ludzkie	15	32,6
			straty nieokreślone	6	13,0
8.	Adresat działania	*Do kogo?*	osoby cywilne	6	13,0
			media	0	0,0
			opinia publiczna	10	21,7
			państwo i jego funkcjonariusze	20	43,5
			organizacja międzynarodowa	1	2,2
			nieokreślony (domyślnie wszystkie powyższe)	**23**	**50,0**
9.	Adresat roszczeń		organizacja międzynarodowa	1	2,2
			państwo i jego funkcjonariusze	14	30,4
			społeczeństwo	12	26,1
			nieokreślony	**28**	**60,9**
10.	Cel działania (pośredni, odległy efekt oddziaływania)	*W jakim celu?*	ideologiczny	5	10,9
			społeczny	11	23,9
			polityczny	21	45,7
			religijny	2	4,3
			nieokreślony	**27**	**58,7**

Źródło: opracowanie własne.

W tabeli 1 zamieszczono opisanych dziesięć aspektów wraz z odpowiadającymi im pytaniami analitycznymi oraz poszczególnymi elementami definicji. Dla każdego z poszczególnych elementów obliczono liczbę oraz odsetek wystąpień poszczególnych elementów definicyjnych we wszystkich 46 analizowanych definicjach. Obliczono również liczbę oraz odsetek współwystępowania poszczególnych elementów.

1) W definicjach cyberterroryzmu najczęściej podmiot działania nie jest wyszczególniany (82,6 proc. analizowanych definicji). Nieliczni badacze wskazują, że cyberterrorystą może być jednostka lub grupa (17,4 proc.). Podanie podmiotu działania nie ma większego znaczenia analitycznego, z punktu widzenia funkcjonalności

definicji cyberterroryzmu powinna być ona jak najszersza. Zatem brak wskazywania tego elementu przez badaczy w definicjach stanowi działanie prawidłowe.

2) Cyberterroryzm jest, zdaniem wszystkich badaczy (100 proc. wskazań), działaniem polegającym na stosowaniu przemocy. Blisko połowa badaczy uważa, że cyberterroryzm to także działanie mogące polegać na samej groźbie jej użycia (47,8 proc.). Nieliczni badacze definiują cyberterroryzm szerzej: jest to każde działanie, które wspomaga działalność terrorystyczną, a więc także wykorzystywanie przez terrorystów cyberprzestrzeni do komunikowania się i mobilizowania zasobów (6,5 proc. definicji).

3) Część badaczy (17,4 proc.) wskazuje w definicji cyberterroryzmu wymiar formalny – podkreślając, że cyberterroryzm to działanie zakazane prawem.

4) Cyberterroryzm najczęściej definiuje się jako działanie prowadzone w cyberprzestrzeni (52,1 proc. analizowanych definicji). Niewielu jednak badaczy precyzuje typ ataku – czy ma on charakter bezpośredni i odbywa się poprzez włamanie i ingerencję (zaledwie dwie definicje spośród analizowanych), czy też ma charakter pośredni i jest przeprowadzany z użyciem jako pośrednika programu nazywanego wirusem, robakiem lub bakterią (również dwie definicje). Nieliczni badacze (6,5 proc.) definiują cyberterroryzm, wskazując, że może być to również oddziaływanie spoza cyberprzestrzeni, a więc ataki na fizyczne nośniki cyberprzestrzeni – komputery i sieci. W blisko połowie definicji (43,5 proc.) ten parametr pozostaje nieokreślony; należy się jednak domyślać definicji jak najszerszej, obejmującej zarówno ataki dokonywane w cyberprzestrzeni, jak i ataki fizyczne na komputery i sieci zakłócające bądź uniemożliwiające ich działanie.

5) Jako bezpośredni obiekt ataku w definicjach pojęcia cyberterroryzmu najczęściej wskazuje się: komputery i sieci (47,8 proc.), dane zawarte w sieci (34,8 proc.), programy i usługi (23,9 proc.) lub – najrzadziej – infrastrukturę krytyczną (10,9 proc.). Najliczniejsza kategoria w analizowanych definicjach najczęściej występuje obok ataków na dane (11 definicji) oraz ataków na programy i usługi (10 definicji). Wszystkie trzy elementy, to jest komputery i sieci, dane zawarte w sieci oraz programy i usługi, wymieniono w czterech definicjach.

6) W badanych definicjach cyberterroryzmu najczęściej nie określano, co jest bezpośrednim efektem działalności cyberterrorystycznej, jednak nieodmiennie sugeruje się jakiś rodzaj zniszczenia (52,2 proc.). Wskazywane są dwie grupy działań: niszczenie lub eliminowanie (37 proc.) oraz blokowanie, zawieszanie, zakłócanie lub szyfrowanie informacji (również 37 proc.). Jako bezpośredni efekt oddziaływania wymieniano również manipulowanie (zniekształcanie) informacji (13,0 proc.) lub przejmowanie kontroli nad informacją (10,9 proc.).

7) Pośrednim, końcowym efektem oddziaływania cyberterroryzmu jest, według badaczy, przede wszystkim wywołanie poczucia stanu zagrożenia u obywateli i rządzących (50,0 proc.), spowodowanie strat materialnych (30,4 proc.) lub nawet w ludziach (21,7 proc.). Co trzecia z definicji (32,6 proc.) mówi o stratach, jednak nie precyzuje, czy dotyczy to ludzi, czy mienia. W sześciu definicjach (13 proc.) kwestia

spowodowania strat lub poczucia zagrożenia w ogóle nie została poruszona. Wywołanie poczucia stanu zagrożenia najczęściej współwystępuje w definicjach ze stratami ludzkimi (12 przypadków – 26 proc.) lub materialnymi (9 przypadków – 20 proc.).

8) Cyberterroryzm, podobnie jak inne rodzaje terroryzmu, stanowi działanie komunikacyjne, którego adresatem mogą być, według badaczy, państwo i jego funkcjonariusze (43,5 proc.), opinia publiczna (21,7 proc.) lub osoby cywilne (13,0 proc.), organizacje międzynarodowe (2,2 proc.). W połowie definicji (50,0 proc.) adresat działania nie został określony, zaś żaden z badaczy nie wskazał jako adresata mediów. Państwo (jego funkcjonariusze) najczęściej w definicjach jest wskazywane wraz z opinią publiczną, miało to miejsce w ośmiu analizowanych definicjach.

9) Adresatem roszczeń cyberterrorystów, od których chcą oni uzyskać pewne korzyści, do których kierują swoje żądania, są w analizowanych definicjach: państwo i jego funkcjonariusze (30,4 proc. definicji), społeczeństwo (26,1 proc.) lub – znacznie rzadziej – organizacje międzynarodowe (2,2 proc.). Jednakże w większości definicji (60,9 proc.) adresat roszczeń pozostaje nieokreślony. Najczęściej wspólnie wskazywane są w tym charakterze dwa podmioty: państwo i jego funkcjonariusze oraz społeczeństwo (10 przypadków).

10) Celem działania cyberterrorystów są, zdaniem badaczy, przede wszystkim cele polityczne (45,7 proc. definicji), społeczne (23,9 proc.), ideologiczne (10,9 proc.) lub religijne (4,9 proc.). Jednak większość definicji (58,7 proc.) nie określa celu działania. Najliczniejsza kategoria – polityczny cel roszczeń – jest najczęściej wymieniana wspólnie z celami o charakterze społecznym (11 definicji).

Powyższa analiza pozwala na wyróżnienie dwóch typów ilościowych definicji sprawozdawczych. Po pierwsze, umożliwia zidentyfikowanie maksymalnych granic pojęcia cyberterroryzmu. Zabieg taki w logice nazywa się tworzeniem sumy zbiorów. Zbiór taki powstaje ze wszystkich elementów 46 analizowanych definicji poprzez wybranie najszerszych zakresów każdego z aspektów. Dzięki temu pojęciu cyberterroryzmu nadawany jest najszerszy możliwy zakres [Ajdukiewicz 1965: 46–47]. Zabieg ten nazwijmy tworzeniem **sprawozdawczej definicji maksymalistycznej**. Po drugie, dzięki powyższemu procesowi analizy w dziesięciu aspektach możliwe jest utworzenie definicji ilościowej w tym sensie, że uwzględnia ona najczęściej występujące elementy podawane w definicjach. Taki zabieg przypomina w pewnym sensie tworzenie iloczynu zbiorów [Ajdukiewicz 1965: 47] z tą jednak różnicą, że zamiast spełniania wymogu występowania we wszystkich (stanowiącego cechę definicyjną przecięcia zbioru) używa się zasady mniej rygorystycznej, uznając, że wystarczy wskazać dominantę dla danego aspektu. Nazwijmy tę definicję **sprawozdawczą definicją ilościową** lub **sprawozdawczą definicją ilościową opartą na dominancie**. Definicja ta pokazuje nam, na jakie elementy definicyjne pojęcia cyberterroryzmu badacze zgadzają się najczęściej, wyznacza swoiste badawcze „obszary zgody" uczonych odnośnie do tego zjawiska.

W przypadku **sprawozdawczej definicji maksymalistycznej** cyberterroryzmem nazwiemy działanie, które może być podjęte przez jakikolwiek podmiot społeczny

(jednostkę lub grupę). Polega ono na użyciu przemocy lub grożeniu przemocą, a także na wykorzystywaniu cyberprzestrzeni do działań komunikacyjnych, informowania i mobilizowania zasobów. Może być ono podejmowane w cyberprzestrzeni (i wówczas odbywać się bezpośrednio – poprzez włamanie i ingerencję, lub pośrednio – to jest z użyciem programu do tego celu opracowanego), a także poza nią i wtedy polega na fizycznym ataku na cyberprzestrzeń. Obiektem ataku mogą stać się programy i usługi, dane, komputery i sieci, a w szczególności te, które stanowią tak zwaną infrastrukturę krytyczną. Bezpośrednim efektem tych działań może być manipulowanie lub zniekształcanie informacji, blokowanie, „zawieszenie", zakłócanie, zaszyfrowanie, przejęcie kontroli oraz zniszczenie wyżej wymienionych obiektów. Cyberterroryzm ma za zadanie wywoływać poczucie stanu zagrożenia u obywateli i/lub rządzących, straty materialne oraz w ludziach (ranni, zabici). Jako działanie komunikacyjne jest on kierowany do osób cywilnych, opinii publicznej, państwa i jego funkcjonariuszy oraz organizacji międzynarodowych. Roszczenia cyberterrorystów są wysuwane wobec państwa i jego funkcjonariuszy i/lub organizacji międzynarodowych i/lub społeczeństwa. Mogą mieć one dowolny charakter: ideologiczny, społeczny, polityczny lub religijny.

Z kolei jeśli zastosujemy **sprawozdawczą definicję ilościową opartą na dominancie,** cyberterroryzm będzie oznaczał działanie podejmowane przez kogokolwiek (grupę lub jednostkę – niezależnie od ich pochodzenia) wykorzystujące przemoc lub jej groźbę. Może być ono prowadzone w cyberprzestrzeni lub poza nią, ale na cyberprzestrzeń oddziałujące. Obiektem ataku są komputery i sieci, dane w nich zawarte oraz programy i usługi tam działające, a polega on na niszczeniu lub co najmniej destabilizowaniu wyżej wymienionych elementów. Bezpośredni cel cyberterroryzmu to wywołanie stanu poczucia zagrożenia, spowodowanie strat ludzkich lub materialnych. Adresatem tych działań w sensie komunikacyjnym są państwo i jego funkcjonariusze. Może nim być także opinia publiczna. Adresatem roszczeń cyberterrorystów jest państwo, lecz może nim być także społeczeństwo. Działanie to służy najczęściej osiągnięciu korzyści politycznych i społecznych.

Ilościową, indukcyjną analizę definicji warto uzupełnić o wskazanie elementów definicji, na które zgadza się większość (kwalifikowana lub zwykła) badaczy. **Kwalifikowana większość** definicji wskazuje, że cyberterroryzm to działanie:

- z użyciem przemocy (100 proc.),
- którego celem jest dokonanie zniszczeń (89,2 proc.),
- nieograniczone pod względem podmiotowym – czyli podejmowanym przez kogokolwiek (82,6 proc.),
- nieograniczone w kwestii adresata roszczeń – może nim być ktokolwiek (60,9 proc.),
- o dowolnym celu działania, jednak zawierające się w obszarze wyznaczanym przez cele polityczne, ideologiczne, społeczne lub religijne (58,7 proc.),
- prowadzone zarówno w cyberprzestrzeni, jak też poza nią (54,3 proc.),

– którego efektem jest wywołanie poczucia stanu zagrożenia u obywateli i/lub rządzących (50,0 proc.),
– nieograniczone pod względem adresata działania (50,0 proc.).

Z kolei **zwykła większość** definicji wskazuje, iż cyberterroryzm to działanie:

– skierowane na komputery i sieci (47,8 proc.).

Powyższa analiza nie tylko przedstawia w sposób ilościowy i syntetyczny rozumienie pojęcia cyberterroryzmu w literaturze przedmiotu, lecz również pozwala na opracowanie własnej definicji regulującej lub projektującej tego pojęcia. W pierwszym przypadku badacz weźmie pod uwagę wyniki przeprowadzonych powyżej analiz ilościowych, a w drugim zaproponowany powyżej model analizy indukcyjnej.

4. ANALIZA KONTEKSTOWA POJĘCIA CYBERTERRORYZMU

Ostatni etap analizy polega na ustaleniu stosunku rozpatrywanego terminu do innych, współwystępujących z nim pojęć. Badacz na tym etapie postępowania analitycznego staje się – jak już wskazywano – kartografem, który umiejscawia dany termin na siatce pojęciowej, wśród innych pojęć usiłując zrekonstruować swoistą, percepcyjną mapę. Refleksja ta jest podejmowana nie tylko na płaszczyźnie logicznej, ale także semantycznej i merytorycznej. Efekt rozważań stanowi – oprócz „słownikowego" indeksu pojęć – odnalezienie ewentualnych zamienników badanego pojęcia, a także rozstrzygnięcie o zasadności i kontekście jego używania. Rozważmy, w jakim stosunku może pozostawać dany termin wobec innych. Refleksja ta wyznacza porządek dalszej analizy kontekstowej.

Po pierwsze, pojęcia możemy rozważać w układzie hierarchicznym, wyróżniając nadrzędne i podrzędne. Pojęcia **nadrzędne** to te, które obejmują pojęcie analizowane, zaś **podrzędne** to te, które zawierają się w pojęciu analizowanym. Pierwszy przypadek nazywamy na gruncie językoznawstwa hiperonimią, a drugi – hiponimią. Innym typem stosunku zakresowego pojęć jest ich częściowe pokrywanie się lub – jak określa się na gruncie logiki – **krzyżowanie się pojęć**. Oznacza to, że analizowane pojęcie nie zawiera się w nazwie drugiego i odwrotnie, lecz jednocześnie nie wykluczają się one nawzajem. Stanowi to szczególny przypadek stosunku analizowanych nazw do siebie. Z merytorycznego i logicznego punktu widzenia często mamy do czynienia z sytuacją wymagającą poważnych rozstrzygnięć związanych z uregulowaniem nazwy, bowiem są to pojęcia sprawiające problem, ich niejasność wprowadza zamęt do słownika nauki. Kolejny typ stosunku zakresowego to **pokrywanie się pojęć**. W tym przypadku analizowane terminy są równoważne i można je stosować zamiennie. Stanowią więc synonimy. Jeszcze inna sytuacja występuje, gdy pojęcia są wobec siebie neutralne znaczeniowo, nie pokrywają się, jednak należą do tej samej ogólniejszej grupy pojęć. Mówimy wówczas, że stanowią one pojęcia **graniczące** lub **równoległe**.

4.1. POJĘCIA NADRZĘDNE WOBEC TERMINU „CYBERTERRORYZM"

Do pojęć nadrzędnych wobec cyberterroryzmu należą „**terroryzm"** i „**cyberkonflikt"** (*cyberconflict*), które zawiera w sobie pojęcie cyberterroryzmu. Cyberterroryzm jest jednym z typów dokonywania ataków terrorystycznych, analogicznie do terroryzmu biologicznego, chemicznego czy nuklearnego [Liedel 2008] z tą jednak różnicą, że trzy terminy wymienione jako ostatnie są określane wspólnym mianem superterroryzmu, ze względu na konsekwencje, jakie powoduje ich użycie [Alexander, Hoening 2001].

Cyberkonflikt lub **konflikt w cyberprzestrzeni** to pojęcia, które są rozumiane zgodnie ze swoim źródłosłowem: jako uświadomiona sprzeczność interesów wyzwalająca określone działania rozgrywające się w cyberprzestrzeni i mające na celu osiągnięcie korzyści. Terminu tego w literaturze przedmiotu używa się marginalnie, stanowi on na ogół pojęcie pomocnicze [Lin 2013: 476–478]. W Stanach Zjednoczonych istnieje nawet organizacja pozarządowa Cyber Conflict Studies Association, która zajmuje się badaniami konfliktów, do których dochodzi w cyberprzestrzeni w takim właśnie wyżej zdefiniowanym rozumieniu. Każdy akt cyberterroryzmu może być nazwany cyberkonfliktem, lecz nie potencjalnym, a ziszczonym.

Poszukiwanie pojęć nadrzędnych wobec analizowanego pojęcia cyberterroryzmu umożliwia odnalezienie *genus proximum*, czyli rodzaju bliższego pojęcia – pozwala odkryć, w jakich nadrzędnych pojęciach zawiera się badany termin. Powyższa analiza prowadzi do następującej konstatacji: cyberterroryzm jest subtypem terroryzmu wyodrębnionego ze względu na formę dokonywania ataków. Analiza kontekstowa pokrywa się w tym zakresie z potocznym rozumieniem pojęcia cyberterroryzmu, a także z rozumieniem wywiedzionym z analizy indukcyjnej.

4.2. POJĘCIA PODRZĘDNE WOBEC TERMINU „CYBERTERRORYZM"

Do pojęć **podrzędnych** wobec cyberterroryzmu zaliczamy terroryzm internetowy, terroryzm elektroniczny (*e-terrorism*), a także mocno metaforyczne: elektroniczny Czarnobyl (*electronic Chernobyl*), cyfrowe Pearl Harbor (*digital Pearl Harbor*), elektroniczne Waterloo (*electronic Waterloo*).

Terroryzm internetowy lub **terroryzm w Internecie** (*Internet terrorism*) to związki frazeologiczne rzadko stosowane. Dosłowne rozumienie tego pojęcia kieruje nas ku terroryzmowi „mającemu miejsce w Internecie" lub „dokonywanemu przez Internet". Jest to pojęcie węższe niż „cyberterroryzm" w ustalonym wyżej znaczeniu wynikającym z analizy indukcyjnej [Gordon 2005]. Jeszcze inaczej terroryzm internetowy rozumie Michael L. Hummel, definiując go jako działalność komunikacyjną terrorystów z użyciem Internetu [Hummel 2008: 117].

Pojęcia **terroryzmu elektronicznego** (**e-terroryzm,** *e-terrorism*) używa się w literaturze przedmiotu bardzo rzadko i niekonsekwentnie. Jako pierwszy wykorzystał

je Ira Winkler, traktując je jako synonim cyberterroryzmu ograniczonego wyłącznie do cyberprzestrzeni [Winkler 2001]. Analogicznie rozumie je Vivienne Fisher, ekspertka ZDNet (portal informacyjny o tematyce technologii biznesowych istniejący od 1991 roku [Fisher 2002]). Pojęcie to jest problematyczne, ponieważ jego etymologiczne, dosłowne znaczenie ma szeroki zakres i oznacza terroryzm dokonywany za pomocą wszelkiego rodzaju środków elektronicznych, a więc na przykład poprzez użycie zdalnie sterowanych ładunków wybuchowych.

Pojęcia takie jak **elektroniczny Czarnobyl** (*electronic Chernobyl*), **cyfrowe Pearl Harbor** (*digital Pearl Harbor*) lub **elektroniczne Waterloo** (*electronic Waterloo*) mają znaczenie metaforyczne, zasadniczo publicystyczne. Charakteryzują się one zakresem węższym niż cyberterroryzm i w publicystyce oznaczają skrajnie negatywne skutki ataku cyberterrorystycznego [Burnst 2010: 51]. Pojęcia podrzędne pozwalają określić wewnętrzny układ danego terminu. Przesłanką ich powstawania jest często fakt, że jakiś wymiar lub aspekt ma zasadnicze znaczenie i wymaga wyodrębnienia. Przeanalizowane pojęcia nie mają ugruntowanego naukowego statusu, są nieostre lub wieloznaczne, pozostają na marginesie rozważań naukowych, ciążąc raczej ku publicystyce i wydawnictwom popularnonaukowym. Niewiele wnoszą one do wewnętrznej systematyki pojęcia cyberterroryzmu, nie przyczyniają się też do jego pogłębionego rozumienia, dlatego najlepszym wyjściem byłaby rezygnacja z ich używania.

4.3. POJĘCIA KRZYŻUJĄCE SIĘ Z TERMINEM „CYBERTERRORYZM"

Pojęcia krzyżujące się z terminem „cyberterroryzm" są nader liczne. Należą do nich: cyberprzestępstwo (*cybercrime*), cyberatak (*cyberattack*), cyberwojna (*cyberwarfare, cyberwar*) lub cybernetyczne działania wojenne (*cyberhostilities*) oraz wojna internetowa (*Internet war*, *iWar*, *netwar*), haktywizm (*hacktivism*), cybersabotaż (*cybersabotage*), miękki terroryzm (*soft terrorism*), a także dżihad online (*online jihad*), dżihad wirtualny (*virtual jihad*) i elektroniczny (*electronic jihad*). Część tych terminów sprawia badaczom znaczne problemy, ze względu na swój nieuregulowany status.

Szeroko w literaturze przedmiotu funkcjonuje pojęcie **cyberprzestępstwa**. Może być ono rozpatrywane jako pojęcie nadrzędne lub krzyżujące się z terminem „cyberterroryzm". Jest nadrzędne wobec wąskiego rozumienia pojęcia cyberterroryzmu (jeśli uznajemy, że stanowi on działanie, które może rozgrywać się wyłącznie w cyberprzestrzeni). Może też krzyżować się z pojęciem cyberterroryzmu w przypadku zastosowania szerokiej jego definicji. Sarah Gordon i Richard Ford przeanalizowali funkcjonujące definicje cyberprzestępstwa, tworząc ich syntezę. W myśl zaproponowanego przez nich, szeroko rozumianego pojęcia cyberprzestępstwo to czyn zdefiniowany i zagrożony karą na mocy prawa karnego, popełniony z użyciem komputera. Najczęstszymi rodzajami cyberprzestępstw są oszustwa, nieautoryzowany dostęp do komputerów, sieci i danych, pornografia dziecięca oraz nękanie za pomocą internetowych kanałów komunikacyjnych (*cyberstalking*) [Gordon 2006: 13–20]. Takie

rozumienie cyberprzestępstwa oznacza, że każdy akt cyberterroryzmu dokonywany z użyciem cyberprzestrzeni jest cyberprzestępstwem, zaś każdy atak fizyczny na komputery i sieci komputerowe – przestępstwem.

Z kolei **cyberatak** to w najprostszym rozumieniu każdy rodzaj ataku dokonany w Internecie: od przemocy werbalnej, poprzez naruszenie integralności danych, ich kradzież, skończywszy na zakłócaniu funkcjonowania lub niszczenia infrastruktury sieci. Jest to pojęcie najszersze: cyberatakiem można nazwać zarówno cyberprzestępstwo, cyberterroryzm, cybersabotaż, jak i cyberwojnę. Warunek definicyjny, a zarazem element wspólny wymienionych terminów stanowi ich niezgodność z prawem i stosowanie co najmniej symbolicznej przemocy [Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, Spiegel 2012]. Pojęcie cyberataku nie ma charakteru analitycznego, jest to raczej zabieg słowny mający na celu zastąpienie przewodniego pojęcia – na przykład cyberterroryzmu – innym.

W literaturze przedmiotu funkcjonuje pojęcie **cyberwojny** (*cyberwar*) lub **cybernetycznych działań wojennych** (*cyberhostilities*). Cyberwojnę definiuje się jako politycznie motywowany atak w cyberprzestrzeni. Jest ona postrzegana analogicznie do wojny konwencjonalnej, z tą różnicą że prowadzi się ją z użyciem innych środków. Niezależny politycznie tygodnik brytyjski „The Economist" ogłosił cyberprzestrzeń piątą domeną wojny (obok lądu, morza, powietrza i przestrzeni kosmicznej). Cyberwojna oznacza wykorzystanie komputerów i sieci w celu przeprowadzenia ataku na systemy informacyjne wroga. Jeśli uznamy, że aktorami wojny mogą być również podmioty niepaństwowe (jak wskazuje wiele klasycznych definicji pojęcia wojny), to rozgraniczenie cyberwojny i cyberterroryzmu będzie trudne lub niemożliwe. Niektórzy jednak badacze, jak na przykład Richard A. Clarke i Robert K. Knake, zdając sobie sprawę z tego problemu, zawężają pojęcie cyberwojny poprzez wskazanie instytucji państwa jako jedynego jej aktora [Clarke, Knake 2010: 6].

Na obrzeżach literatury przedmiotu pojawia się czasami pojęcie **cyberdywersji** (*cybersubversion*). Należy je rozumieć jako rozgrywające się w cyberprzestrzeni, niszczące działanie wojenne odbywające się na zapleczu wroga, mające najczęściej na celu odwrócenie uwagi przeciwnika i osłabienie go. Cyberdywersja polega na niszczeniu lub uszkadzaniu zasobów zbrojnych wroga. Cyberterroryzm i cybersabotaż korzystają z tego samego repertuaru środków i taktyk, jednak powinien różnić je aktor działań. Nie nakładają się one na siebie, jeśli uznamy, że tym aktorem jest państwo, analogicznie jak w przypadku cyberwojny.

Powszechnie wykorzystuje się pojęcie **wojny sieciowej** (*netwar*) lub **informacyjnej** (*information warfare*, *infowar*), która po raz pierwszy miała miejsce podczas wojny w Zatoce Perskiej w 1991 roku. Wojna informacyjna jest definiowana jako wykorzystanie technologii informacyjnych do zarządzania informacją w celu uzyskania przewagi nad przeciwnikiem. Polega na propagandzie i manipulacji informacją w celu dezinformacji i demoralizacji przeciwnika. Jest to pojęcie bardzo szerokie, obejmujące każdy typ oddziaływania psychologicznego na przeciwnika za pomocą środków masowego przekazu [Hutchinson 2006: 213; Schwartau 1996]. Termin ten

do analiz naukowych wprowadzili John Arquilla i David Ronfeldt, definiując go jako taktykę rozgrywania konfliktów politycznych, lecz również działań przestępczych. W wojnie sieciowej wykorzystuje się sieciowe formy organizacji, doktryny, strategie i technologie charakterystyczne dla społeczeństw informacyjnych [Arquilla, Ronfeldt 2001: 6; Ronfeldt, Arquilla, Fuller, Fuller 1998: 9]. Ważny element tego pojęcia stanowi założenie, że mamy w tym przypadku do czynienia z konfliktem o niskiej intensywności między państwami i aktorami niepaństwowymi, takimi jak międzynarodowe organizacje terrorystyczne, partyzanci i handlarze narkotyków, polegającym przede wszystkim na komunikowaniu się [Bógdał-Brzezińska, Gawrycki 2003: 165]. Najbardziej efektywnym i znanym przykładem wojny sieciowej było zastosowanie Internetu w konflikcie między meksykańskim rządem a indiańskimi powstańcami w stanie Chiapas. Wykorzystanie Internetu jako środka propagandy zapewniło powstańcom poparcie międzynarodowej opinii publicznej i skłoniło meksykański rząd do rozmów i ustępstw pod wpływem silnych nacisków międzynarodowej opinii publicznej [Ronfeldt, Arquilla, Fuller, Fuller 1998]. Jeśli – jak w niektórych definicjach cyberterroryzmu – rozszerzymy ten termin również na działalność propagandową, to pojęcia wojny sieciowej i cyberterroryzmu zaczną się krzyżować. Stąd wydaje się konieczne, by z definicji cyberterroryzmu wyłączać działania o charakterze propagandowym, które co prawda stanowią aktywności wspomagające terroryzm, ale nie są z nim tożsame.

W niektórych analizach „cyberterroryzm" pokrywa się z „**haktywizmem"** (*hacktivism*). Pojęcie haktywizmu w 1996 roku stworzył członek subkulturowej grupy hakerskiej Cult of the Dead Cow znany jako Omega [Mills 2012]. Haktywizm to *portmanteau* pojęć *hack* – oznaczającego nieautoryzowany, oparty na wiedzy i pogłębionym rozumieniu techniki komputerowej dostęp do komputerów i sieci, oraz *activism* – wskazującego na aktywność w sensie politycznym i obywatelskim. Najczęściej wymieniane formy haktywizmu to podmiana stron internetowych (w literaturze anglojęzycznej: *web defacements*), przekierowywanie stron internetowych, ataki polegające na rozproszonej odmowie dostępu do usługi (*Distributed Denial of Service*, *DDoS*), kradzież informacji, parodie stron internetowych, wirtualne *sit-in*, wirtualny sabotaż, tworzenie oprogramowania umożliwiającego aktywność polityczną w Internecie lub zapewniającego wolność słowa [Samuel 2004: 6–7]. Termin „haktywizm" bardzo często krzyżuje się z pojęciem cyberterroryzmu, gdy odnosi się do działań z użyciem przemocy [Krapp 2011]. Proponuję następujące uregulowanie pojęcia haktywizmu (za Alexandre Samuel) – jest to odpowiednik nieposłuszeństwa obywatelskiego, a więc działania bez użycia przemocy. Wówczas cyberterroryzm i haktywizm nie pokrywają się [Samuel 2004: 6–7].

Badacze jedynie w niewielkim stopniu wykorzystują pojęcie **miękkiego terroryzmu** (*soft terrorism*). Jest ono rozumiane jako działania blokujące, niszczące lub zniekształcające informację przetwarzaną, przechowywaną i przekazywaną w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy. W terminie tym

mieści się także wykorzystywanie systemów teleinformatycznych do dezinformacji i walki psychologicznej. Celem ataku jest najczęściej informacja przetwarzana, a nie system jako taki [Elliot 2002: 3; Will 2001]. Pojęciem tym oznaczane są działania odbywające się wyłącznie w cyberprzestrzeni.

Terminy **dżihad online**, **dżihad wirtualny** i **elektroniczny** mają charakter metaforyczny, odnoszą się do kultury islamu [Brickey 2012: 4]. Dżihad w języku arabskim to dosłownie „zmaganie" lub „walka", wyraz ten bywa też nieprecyzyjnie tłumaczony jako „święta wojna". W tym rozumieniu mógłby oznaczać zarówno cyberterroryzm, wojnę internetową, cyberwojnę, jak i działania bez użycia przemocy – wojnę informacyjną – z tym że ograniczone do podejmujących je wyznawców islamu. Pierwsze dwa pojęcia – dżihad online i – dżihad wirtualny – należy traktować jako synonimy odnoszące się do cyberprzestrzeni, Internetu, z kolei dżihad elektroniczny ma zakres szerszy – obejmuje również elementy spoza Internetu, a więc to, co szeroko związane z technologiami informacyjnymi. Pojęcie to ma niewielką moc heurystyczną, ze względu na wąski zakres użycia może być stosowane w publicystyce czy tekstach popularnonaukowych, lecz nie w nauce.

Wojna internetowa (*Internet-based warfare* lub *iWar*) to termin wprowadzony na potrzeby Paktu Północnoatlantyckiego. Wskazuje się, że jest to pojęcie różne od cyberwojny oraz cyberterroryzmu i wojny informacyjnej. Odnosi się ono do ataków na „konsumencką infrastrukturę Internetu" – a więc na strony www i usługi świadczone tą drogą. Oznacza pewien specyficzny typ ataku zaburzający funkcjonowanie w Internecie jednostek, korporacji i społeczności [Ryan 2007]. Niektórzy badacze traktują to pojęcie nieco zbyt szeroko, przenośnie i bezkrytycznie. Na przykład wskazują, że wydarzenia z 2007 roku w Estonii miały charakter wojny internetowej [Guadagno, Cialdini, Evron, 2010: 447–453]. W takiej sytuacji niejasne staje się rozróżnienie pomiędzy wojną internetową a cyberterroryzmem. Wojna stanowi działanie, które ze względu na stosowanie przemocy może być mylone z innymi zjawiskami tego typu, w tym z terroryzmem. Od innych zjawisk można ją jednak odróżnić dzięki trzem następującym kryteriom: kryterium organizacji i masowości (a więc liczby zaangażowanych oraz istnienia ścisłej organizacji i hierarchii), kryterium nasilenia i ciągłości przemocy (wojna jako pewien typ idealny oznacza stan wysokiego i ciągłego natężenia przemocy w dłuższym okresie) oraz kryterium aktorów – są nimi państwa lub duże grupy społeczne (w szczególności etniczne i narodowe). Ponadto tak opracowana definicja wojny internetowej spełnia kryterium przemocy zaledwie częściowo – jej istotą jest zaburzanie, lecz nie niszczenie. Pojęcie to ze względu na obecność w jego nazwie słowa „wojna" wywołuje niejasności; w dużej mierze pokrywa się też z pojęciem cybersabotażu.

Na termin „cyberterroryzm" nakłada się również pojęcie **cybersabotażu** (*cybersabotage*), oznaczające umyślne niewypełnienie albo wypełnianie wadliwe swoich obowiązków w zamiarze wywołania dezorganizacji, strat i szkód w cyberprzestrzeni. Pojęcie to używane jest nader rzadko. Formy cybersabotażu i cyberterroryzmu nie różnią się od siebie. Element różnicujący te dwa pojęcia stanowi fakt,

że cyberterroryzm to działanie, które może być podejmowane zarówno z zewnątrz, jak i od wewnątrz atakowanej instytucji (przez jednostkę lub grupę stanowiącą jej pracowników lub członków), zaś cybersabotaż ma charakter wyłącznie endogenny. Ponadto terminy te odróżnia motyw działania (cybersabotaż może również obejmować motywy niepolityczne – na przykład osobiste lub ekonomiczne). Pojęcia te należą do odmiennych porządków analitycznych, dlatego nie powinny być używane równocześnie.

Przeglądowa analiza wymienionych pojęć krzyżujących się z terminem „cyberterroryzm" pozwoliła na ich wstępne uregulowanie. Wnioski płynące z przeprowadzonych rozważań są następujące. Po pierwsze, pojęcie cyberataku może być stosowane wymiennie na określenie niektórych form cyberterroryzmu. Po drugie, terminy „cyberprzestępstwo", „cybersabotaż", „cyberwojna" i „wojna internetowa" nie powinny być wykorzystywane, ponieważ należą do odrębnych porządków analitycznych. Po trzecie, pojęcie haktywizmu po uregulowaniu staje się pojęciem równoległym, dopełniającym dla terminu „cyberterroryzm". Po czwarte, pojęcia „dżihad online", „dżihad wirtualny" i „dżihad elektroniczny" mają zbyt literackie konotacje, w związku z tym sugeruje się zrezygnowanie z ich używania w dyskursie naukowym.

4.4. POJĘCIA POKRYWAJĄCE SIĘ Z TERMINEM „CYBERTERRORYZM"

W toku analiz zidentyfikowano jedno pojęcie całkowicie pokrywające się z „cyberterroryzmem" – to **terroryzm cybernetyczny**. Z etymologicznego punktu widzenia termin ten właściwie stanowi rozwinięcie derywatu „cyberterroryzm". Funkcjonuje w polskich analizach – takim właśnie pojęciem posługuje się Biuro Bezpieczeństwa Narodowego w dokumencie analitycznym zatytułowanym *Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*.

4.5. POJĘCIA RÓWNOLEGŁE Z TERMINEM „CYBERTERRORYZM"

Pojęciami graniczącymi lub równoległymi wobec terminu „cyberterroryzm" są cyberszpiegostwo (*cyberespionage*, *cyberspying*) oraz – po uregulowaniu w poprzednich partiach tekstu – haktywizm. Cyberszpiegostwo należy rozumieć jako nieautoryzowany dostęp do komputerów w celu kradzieży informacji.

5. SYNTEZA POJĘCIA CYBERTERRORYZMU – DEFINICJA REGULUJĄCA (PODSUMOWANIE)

Synteza stanowi zakończenie trzyetapowej, przeprowadzonej powyżej analizy pojęcia. Badacz uzyskuje definicję odpowiadającą jego potrzebom, biorąc pod uwagę wnioski wynikające z analizy etymologicznej, indukcyjnej i kontekstowej. W zależności od konstatacji i potrzeb decyduje się na jeden z trzech typów definicji: sprawozdawczą, projektującą lub regulującą. Przypomnijmy, że definicje sprawozdawcze to te, które neutralnie referują sens nadany wyrażeniu. Sytuacja taka zdarza się w naukach społecznych nader rzadko, bowiem istniejące pojęcia mają charakter nieostry lub nawet wieloznaczny. W przypadku cyberterroryzmu przyjęcie definicji sprawozdawczej oznaczałoby wykorzystanie jednej z istniejących. Definicje regulujące są częściowo oparte na znaczeniu zastanym, a częściowo – na tym nadanym przez badacza. Z kolei definicję projektującą tworzy arbitralnie sam badacz. Pojęcie cyberterroryzmu definiowane w literaturze przedmiotu wymaga w wielu punktach uregulowania w celu wyeliminowania niejasności, a także elementów definicji kolidujących z definicjami innych pojęć. Oznacza to automatyczne odrzucenie definicji sprawozdawczej oraz projektującej.

W toku regulującego definiowania cyberterroryzmu badacz wybiera spośród typów postępowania badawczego:

I. Przyjęcie cząstkowej definicji sprawozdawczej pojęcia:

a. przyjęcie znaczenia wynikającego z analizy etymologicznej pojęcia,

b. przyjęcie znaczenia wynikającego z analizy indukcyjnej pojęcia, przy czym wybór następuje spośród sprawozdawczej definicji maksymalistycznej, sprawozdawczej definicji ilościowej opartej na dominancie (w tym opartej na kwalifikowanej lub zwykłej większości),

c. przyjęcie znaczenia wynikającego z analizy kontekstowej pojęcia.

II. Przyjęcie cząstkowej definicji regulującej pojęcia:

a. uregulowanie znaczenia wynikającego z analizy etymologicznej pojęcia,

b. uregulowanie znaczenia wynikającego z analizy indukcyjnej pojęcia, przy czym wybór następuje spośród sprawozdawczej definicji maksymalistycznej, sprawozdawczej definicji ilościowej opartej na dominancie (w tym opartej na kwalifikowanej lub zwykłej większości),

c. uregulowanie znaczenia wynikającego z analizy kontekstowej pojęcia.

Tabela 2 zawiera definicję regulującą pojęcia cyberterroryzmu z wyszczególnieniem typu postępowania badawczego oraz wyjaśnieniem zasadności regulowania cząstkowej definicji.

Tabela 2. Definicja regulująca pojęcia cyberterroryzmu

Lp.	Aspekt analizy definicji	Pytanie analityczne	Elementy definicji	Typ postępowania badawczego/uzasadnienie
1.	Podmiot działania	*Kto?*	jakikolwiek podmiot: jednostka lub grupa	Ib, Ic
2.	Rodzaj działania	*Co?*	groźba przemocy (przemoc psychiczna) lub przemoc fizyczna	Ib (definicja ilościowa oparta na dominancie)
3.	Sposób działania	*Jak?*	niezgodne z prawem lub przez prawo nieregulowane	IIb (uregulowano znaczenie indukcyjne pojęcia; uzasadnienie: może zdarzyć się tak, że pozostałe elementy definicji będą zachowane, jednak nieregulowane przez prawo – badacz powinien uniknąć takiej sytuacji).
4.	Środowisko/ miejsce działania	*Gdzie?*	działanie w cyberprzestrzeni (pośrednie i bezpośrednie) oraz poza nią, ale na cyberprzestrzeń oddziałujące	Ib (definicja ilościowa oparta na dominancie)
5.	Bezpośredni obiekt oddziaływania	*Na co?*	– komputery i sieci – zarówno ich warstwa fizyczna, jak i cyfrowa – w szczególności komputery i sieci składające się na infrastrukturę krytyczną	IIb (wprowadzenie wyraźnego rozróżnienia między warstwą fizyczną i cyfrową tworzącą cyberprzestrzeń)
6.	Bezpośredni efekt oddziaływania	*Z jakim efektem?*	– zniszczenie (całkowite/częściowe) lub zakłócenie działania fizycznej warstwy sieci – zniszczenie (całkowite/częściowe) lub zakłócenie działania cyfrowej warstwy sieci	IIb (jw. oraz doprecyzowanie uniwersalnych nazw, wyeliminowanie pojęć kolokwialnych, takich jak np. „zawieszenie")
7.	Pośredni (końcowy) efekt oddziaływania		– poczucie zagrożenia – straty materialne – straty ludzkie	Ib
8.	Adresat działania	*Do kogo?*	dowolne instytucje (w sensie socjologicznym), które mogą przyjąć „komunikat" cyberterrorystów lub też przekazać go innym instytucjom (społeczeństwo i składające się nań grupy, opinia publiczna, instytucje państwa, organizacje, w tym międzynarodowe, media)	IIb (precyzyjne, wyczerpujące wskazanie kategorii adresatów działania oraz włączenie podmiotu niewskazywanego w definicjach – mediów)

9.	Adresat roszczeń		decydenci, to jest osoby lub instytucje mogące bezpośrednio (na przykład rządy państw) lub pośrednio (np. społeczeństwa, poszczególne grupy społeczne) zrealizować postulaty podejmujących atak cyberterrorystyczny	IIb (precyzyjne wskazanie adresatów roszczeń)
10.	Cel działania (pośredni, odległy efekt oddziaływania)	*W jakim celu?*	– dowolny wskazany przez cyberterrorystów cel mający charakter polityczny – cel może mieć zarówno charakter instrumentalny (osiągnięcie określonych, wskazanych korzyści), jak i ekspresywny (gdy działanie ma charakter symboliczny)	IIb (precyzyjne wskazanie celu działań), włącza również te działania, które nie mają na celu osiągnięcia bezpośrednich korzyści

Źródło: opracowanie własne.

W powyższej definicji regulacji poddano sześć z dziesięciu elementów: sposób działania, bezpośredni efekt oddziaływania, bezpośredni obiekt oddziaływania, adresata działania, adresata roszczeń oraz cel działania. Bez zmian pozostawiono podmiot działania, rodzaj działania, środowisko działania oraz pośredni efekt oddziaływania.

W toku syntezy uzyskano zatem następującą definicję regulującą pojęcia cyberterroryzmu: *jest to jedna z odmian terroryzmu wyróżniona ze względu na podejmowane w celu jej wykonania środki. Stanowi działanie niezgodne z prawem lub przez prawo nieregulowane, a podejmowane przez jakikolwiek podmiot: jednostkę lub grupę. Działanie to polega na stosowaniu groźby przemocy (przemocy psychicznej) lub przemocy fizycznej. Jest podejmowane w cyberprzestrzeni (pośrednie i bezpośrednie) oraz poza nią, ale na cyberprzestrzeń oddziałujące. Cyberterroryzm to działanie skierowane przeciwko komputerom i sieciom komputerowym, zarówno ich warstwie fizycznej, jak i cyfrowej, a w szczególności komputerom i sieciom składającym się na infrastrukturę krytyczną. Bezpośrednim celem tych działań jest całkowite lub częściowe zniszczenie lub zakłócenie działania fizycznej lub cyfrowej warstwy sieci. Działania te mają spowodować poczucie zagrożenia, straty materialne lub ludzkie. Widownią tych działań są dowolne instytucje, które mogą przyjąć „komunikat" cyberterrorystów lub też przekazać go innym instytucjom (np. społeczeństwu i składającym się nań grupom, opinii publicznej, instytucjom państwa, organizacjom, w tym międzynarodowym, mediom). Efekt to wywarcie wpływu na ośrodki decyzyjne, czyli osoby lub instytucje mogące bezpośrednio (na przykład rządy państw) lub pośrednio (np. społeczeństwa, poszczególne grupy społeczne) zrealizować postulaty podejmujących atak cyberterrorystyczny. Żądania cyberterrorystów mogą odnosić się do dowolnie wskazanego celu mającego charakter polityczny. Może mieć on zarówno charakter instrumentalny (osiągnięcie określonych, wskazanych korzyści), jak i ekspresywny (gdy działanie ma charakter symboliczny).*

Przedsięwzięty zabieg wieloetapowej analizy i uregulowania pojęcia cyberterroryzmu ma posłużyć autorowi niniejszego artykułu w dalszych etapach badań nad tym zjawiskiem, a konkretnie nad przejawami oraz skutkami cyberterroryzmu.

W tym kontekście warto ocenić, w jakim stopniu pojęcie to czyni zadość standardom terminologii naukowej [Mazur, 1961], a tym samym w jakim stopniu jest przydatne. Po pierwsze, z punktu widzenia tworzenia terminologii naukowej pojęcie cyberterroryzmu spełnia warunek powszechności – do określenia zjawiska jest używane częściej niż inne pojęcia i dlatego też na nim skoncentrowano wysiłek analityczny. Po wtóre, stanowi ono pojęcie systematyczne, bowiem jednoznacznie klasyfikuje cyberterroryzm jako jedną z form terroryzmu. Pojęcie należy także uznać za operatywne – nazwa jest krótka i łatwa do komunikowania oraz nie nastręcza trudności w zestawieniu z innymi wyrazami. Tworzy się również zalążek międzynarodowości tego terminu – rozpowszechniło się ono w nauce anglosaskiej, a następnie na zasadzie kalki językowej także w innych językach. Jest to również pojęcie niekolidujące – nie ma konieczności modyfikacji istniejących już nazw. Właściwości te sprawiają, że z „warsztatowego", empirycznego punktu widzenia termin ten uznać można za przydatny, gdyż jest operatywny i pozwala badać rzeczywistość.

Na zakończenie konieczna wydaje się refleksja nad sensem włączania pojęcia cyberterroryzmu do słownika nauki o polityce. Przede wszystkim należy zaznaczyć, że ów termin nie aspiruje do grupy tak zwanych pojęć podstawowych, które (lub inaczej: podstawowa siatka pojęciowa albo kategorie danej dyscypliny) stanowią zestaw łączących się ze sobą najogólniejszych terminów z danej dyscypliny nauki odzwierciedlających najistotniejsze właściwości i związki zjawisk. Znajomość i umiejętność posługiwania się pojęciami podstawowymi stanowią warunek *sine qua non* rozumienia, interpretacji, komunikowania i dyskutowania wyników badań naukowych. Bez tych pojęć nie jest możliwe poznawanie właściwości zjawisk i ich związku z innymi zjawiskami [Bryła 1984; Lutrzykowski 1982]. „Cyberterroryzm" w hierarchii pojęć naukowych należy do pojęć niższego rzędu, służy do nazwania i analizowania pewnego wąskiego wycinka rzeczywistości. Jego włączenie do słownika nauki wynika jedynie z faktu, że może posłużyć empirycznym badaniom nad bezpieczeństwem, konkretnie nad przejawami oraz skutkami zjawiska cyberterroryzmu. W tym zakresie – i tylko w tym – termin ten spełnia swoją funkcję i może być tymczasowo i warunkowo włączony do słownika nauki o polityce.

BIBLIOGRAFIA

Ajdukiewicz, K. 1965. *Logika pragmatyczna*, Państwowe Wydawnictwo Naukowe, Warszawa.

Alexander, Y., Hoening, M. 2001. *Superterroryzm biologiczny, chemiczny i nuklearny*, Wydawnictwo „Bellona", Warszawa.

Arquilla, J., Ronfeldt, D. 2001. *Networks and Netwars. The Future of Terror, Crime and Militancy*, National Defense Research Institute RAND, Santa Monica.

Batorski, D., Olechnicki, K. 2007. *Wprowadzenie do socjologii Internetu*, „Studia Socjologiczne", nr 3 (186).

Beck, U. 1988. *Gegengifte. Die organisierte Unverantwortlichkeit*, Suhrkamp, Frankfurt am Main.

Beck, U. 2002, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Wydawnictwo Naukowe „Scholar", Warszawa.

Beck, U. 2007, *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit*, Suhrkamp, Frankfurt am Main.

Biuro Bezpieczeństwa Narodowego, *Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*, Biuro Bezpieczeństwa Narodowego, www.bbn.gov.pl/download.php?s=1&id=2359 (dostęp: 23.04.2013).

Borkowski, R. 2001. *Terroryzm* [w:] *Konflikty współczesnego świata*, R. Borkowski (red.), Uczelniane Wydawnictwa Naukowo-Dydaktyczne, Kraków.

Bógdał-Brzezińska, A., Gawrycki, M.F. 2003. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa.

Brickey, J. 2012. *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, Combating Terrorism Centre at West Point, nr 5 (8).

Burke, E. 1999. *Letter No. IV. To the Earl Futzwilliam 1795* [w:] *Select Works of Edmund Burke*, t. 3: *Letters on a Regicide Peace*, Liberty Fund, Indianapolis.

Burnst, P.W. 2010. *Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet* [w:] *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications*, M. Wade, A. Maljevic (red.), Springer Science+Business Media, Nowy Jork.

Clarke, R.A., Knake, R.K. 2010. *Cyber War*, HarperCollins, Nowy Jork.

Cyber Conflict Studies Association, http://www.cyberconflict.org/ (dostęp: 21.04.2013).

Cyberwar. War in the Fifth Domain. 2010. „The Economist", 1.07.

Elliot, J.E. 2002. *Cyber Terrorism: A Threat to National Security*, United States Air Force Reserve, http://www.dtic.mil/dtic/tr/fulltext/u2/a404381.pdf (dostęp: 21.04.2013).

Fisher, V. 2002. *E-Terrorism: An online war?*, http://www.crime-research.org/library/Vivienne.htm (dostęp: 13.04.2013).

Gibson, W. 1992. *Neuromancer*, P.W. Cholewa (tłum.), Wydawnictwo „Alkazar", Warszawa.

Gibson, W. 2000. *No Maps for These Territories*, M. Neale (reż.), Docurama, Stany Zjednoczone.

Gordon, R. 2005. *Cyber Crime and Internet Terrorism: Issues, Regulatory Problems, and Legislation*, „Journal of Comprehensive Research", nr 3, http://jupapadoc.startlogic.com/compresearch/papers/JCR05-3.pdf (dostęp: 26.04.2013).

Gordon, S. Ford, R. 2006. *On the definition and classification of cybercrime*, „Journal of Computer Virology", nr 2.

Guadagno, R.E., Cialdini, R.B., Evron, G. 2010, *Storming the Servers: A Social Psychological Analysis of the First Internet War*, „Cyberpsychology, Behavior, and Social Networking", nr 13 (4).

Handler, D. 2001. *Semiotics: The Basics*, Routledge, Londyn.

Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. 2012. *The Law of Cyber-Attack*, „California Law Review", nr 100, http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf (dostęp: 20.04.2013).

Hesse, C. 2008. *The First Total Terror*, University of California, Berkeley, http://francestanford.stanford.edu/sites/francestanford.stanford.edu/files/Hesse.pdf (dostęp: 22.04.2013).

Hummel, M.L. 2008. *Internet terrorism*, „Homeland Security Review", nr 2 (2).

Hutchinson, W. 2006. *Information Warfare and Deception*, „Informing Science", 9, http://www.inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf (dostęp: 26.04.2013).

Iviansky, Z. 1977. *Individual Terror: Concept and Typology*, „Journal of Contemporary History", nr 12 (1).

Krapp, P. 2011. *Noise Channels: Glitch and Error in Digital Culture*, University of Minnesota Press, Minneapolis.

Kroeber, A.L., Kluckhohn, C. 1952, *Culture: A critical review of concepts and definitions*, Harvard University Peabody Museum of American Archeology and Ethnology Papers 47.

Kubczak, A. 2002. *Cybersocjologia? Internet jako przedmiot zainteresowania socjologów* [w:] *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego: dylematy cywilizacyjno-kulturowe*, WNSS AGH, Kraków.

Liedel, K. *Terroryzm XXI w.*, prywatna strona internetowa, 1 grudnia 2008, www.liedel.pl/?p=54 (dostęp: 26.04.2013).

Lin, H. 2013, *Cyber Conflict and National Security* [w:] *International Politics. Enduring Concepts and Contemporary Issues*, R.J. Art, R. Jervis (red.), Pearson, Boston.

Mazur, M. 1961, *Terminologia techniczna*, PWT, Warszawa.

Mider, D. 2008. *Partycypacja polityczna w Internecie. Studium politologiczne*, Dom Wydawniczy „Elipsa", Warszawa.

Mills, E. *Old-time hacktivists: Anonymous, you've crossed the line*, CNet News, 30 marca 2012 (dostęp: 26.04.2013).

Morningstar, Ch., Farmer, F.R. 2003. *The Lessons of Lucasfilm's Habitat* [w:] *The New Media Reader*, N. Wardrip-Fruin, N. Montfort (red.), The MIT Press, Cambridge.

Nieczajew, S.G., Bakunin, M.A., Ogariow, M.P., *Katiechizm riewoljucjoniera*, http://www.hist.msu.ru/ER/Etext/nechaev.htm (dostęp: 26.04.2013).

Pawłowski, T. 1986. *Tworzenie pojęć w naukach humanistycznych*, Państwowe Wydawnictwo Naukowe, Warszawa.

Pomper, P. 2007. *Russian Revolutionary Terrorism* [w:] *Terrorism in Context*, M. Crenshaw (red.), The Pennsylvania State University, University Park.

Robiespierre, M. 1794. *Sur les principes de morale politique*, przemówienie, do Konwentu Narodowego.

Robiespierre, M. 2005. *Institutions républicaines, 1793–94*, Gallimard, Paryż.

Ronfeldt, D., Arquilla, J., Fuller, G.E., Fuller, M. 1998. *The Zapatista Social Netwar in Mexico*, RAND ArroyoCenter, Santa Monica.

Ryan, J. 2007. *„iWar": A new threat, its convenience – and our increasing vulnerability*, „Nato Review", zima, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html (dostęp: 24.04.2013).

Samuel, A.W. 2004. *Hacktivism and the Future of Political Participation*, niepublikowana rozprawa doktorska napisana pod kierunkiem S. Verby, Uniwersytet Harvarda, Cambridge.

Schoeff, M. 1998. *Cybercrime, Cyberterrorism, Cyberwarfare CSIS Task Force Outlines Strategies to Avert an Electronic Waterloo*, CSIS, Waszyngton.

Schwartau, W. 1996. *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, Thunder's Mouth Press, Nowy Jork.

Shane, S. 2010. *Words as Weapons: Dropping the "Terrorism" Bomb*, „The New York Times", 3.04.

Silver, B. 1985. *Obraz świata i aparatura pojęciowa* [w:] *Język i poznanie*, K. Ajdukiewicz (red.), Państwowe Wydawnictwo Naukowe, Warszawa.

Stankiewicz, P. 2008. *W świecie ryzyka. Niekończąca się opowieść Ulricha Becka*, „Studia Socjologiczne" 3 (190).

Sterling, B.M. 1994. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, www.gutenberg.org/files/101/101-h/101-h.htm (dostęp: 29.04.2013).

Strydom, P. 2002. *Risk, Environment and Society: Ongoing Debates, Current Issues and Future Proscpects*, Buckingham/Philadelphia: Open University Press.

Thil, S. 2009. *1948: William Gibson, Father of Cyberspace*, „Wired", 17.03.

Trappl, R. 2008. *Preface. 14th European Meeting on Cybernetics and Systems Research (EMCSR '98)*, 14–17 kwietnia 1998, University of Vienna, Austrian Society for Cybernetic Studies.

Tuman, J.S. 2003. *Communicating Terror: The Rhetorical Dimensions of Terrorism*, Sage Publications, Thousand Oaks.

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590).

Wiener, N. 1971 (wyd. oryg. 1948). *Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie*, Państwowe Wydawnictwo Naukowe, Warszawa.

Will, G.F. 2001, *Now, Weapons of Mass Disruption?*, „Newsweek", 29.10.

Winkler, I. 2001. *Are companies really ready for e-terrorism?*, http://news.cnet.com/2010-1071-281591.html (dostęp: 16.04.2013).
Znaniecki, F. 2001. *Ludzie teraźniejsi a cywilizacja przyszłości*, Wydawnictwo Naukowe PWN, Warszawa.

BIOGRAFIA

Daniel Mider – ur. 1976, absolwent Instytutu Nauk Politycznych UW (2003, studia ukończone z wyróżnieniem), doktor nauk humanistycznych w zakresie nauk o polityce (2008, *summa cum laude*). Adiunkt w Zakładzie Socjologii i Psychologii INP UW, kierownik Pracowni Metodologii Badań Politologicznych. Jego zainteresowania badawcze obejmują informatykę społeczną, metodologię badań społecznych oraz analizę danych ilościowych i jakościowych. Prowadzi zajęcia z takich przedmiotów jak socjologia, statystyka i demografia, metodologia badań politologicznych, technologie informacyjne, infobrokering polityczny. Egzaminator Europejskiego Certyfikatu Umiejętności Komputerowych, certyfikowany informatyk śledczy. Członek Polskiego Towarzystwa Informatycznego i Polskiego Towarzystwa Socjologicznego. Autor nagrodzonej przez Rektora UW monografii *Partycypacja polityczna w Internecie. Studium politologiczne* oraz współautor (wraz z J. Błuszkowskim) również nagrodzonej *Demokracji późnej nowoczesności* (2012). Autor licznych publikacji z zakresu socjologii Internetu, metodologii badań oraz teorii demokracji. Założyciel Instytutu Badań nad Człowiekiem i Społeczeństwem im. Elżbiety Mider z d. Korzun (2013). E-mail: daniel@mider.biz.

ABSTRACT

The article focuses on the terminological issues bound with the concept of cyberterrorism. The discussion uses own author's method of analysis comprising: etymological analysis (extraction of the dictionary meaning of the concept), inductive analysis (identifying the general characteristics of the concept on the basis of a representative group of its definitions), and contextual analysis (comparing co-occurring terms). Summary contains the regulatory definition of cyberterrorism that eliminates ambiguities existing in the literature.

Key words: terrorism, cyberterrorism, information security, national security

BIOGRAPHY

Daniel Mider, born in 1976, graduated from the Political Science Institute of Warsaw University (2003), PhD in political science (2008). Associate professor in the Department of Sociology and Psychology of the Political Science Institute of WU, secretary of a Methodological Workshop of Political Science Research. Examiner

of the European Computer Driving Licence, certified expert of computer forensics. Author and co-author of several books and dozens of articles on sociology of Internet, political participation, democracy theory and methodology of research. Member of Polish Information Processing Society and Polish Sociology Society. E-mail: daniel@mider.biz.