

Izabela OLEKSIEWICZ<sup>1</sup>

## **OCHRONA PRAW JEDNOSTKI A PROBLEM CYBERTERRORYZMU**

Globalna sieć zyskuje coraz większy zasięg, świat wirtualny rozrasta się coraz szybciej i staje się podobny do realnego świata. W związku z tym wiele zjawisk przenosi się ze świata rzeczywistego do sieci. Ta sytuacja odnosi się także do przestępczości czy terroryzmu. Współcześnie zmieniają one swoje oblicza, wykorzystując zdobycze społeczeństwa informacyjnego. Podstawowym towarem w sieci jest informacja. Rozpowszechnianie informacji za jej pomocą następuje błyskawicznie. Sieć stanowi zatem idealne miejsce współczesnej wymiany informacji między różnorodnymi grupami i środowiskami<sup>2</sup>.

Niniejszy artykuł ma na celu ukazanie, jak istotny obszar aktywności państwa stanowi we współczesnym świecie cyberbezpieczeństwo, które odnosi się do nowej sfery aktywności człowieka, jaką jest cyberprzestrzeń, i nie daje się ujmować w tradycyjne ramy. O ile zapewnienie i ochrona bezpieczeństwa stanowi niezwykle istotny obszar aktywności państwa i jego organów, to działania w zakresie ochrony bezpieczeństwa są zróżnicowane i zależą od specyfiki zagrożeń bezpieczeństwa. Pojawienie się problemu cyberbezpieczeństwa i jego ochrony jest więc wynikiem coraz szerszego pojmowania klasycznego bezpieczeństwa człowieka. Autorka stara się w swoim artykule zwrócić uwagę na fakt, że we współczesnym świecie bezpieczeństwo odnoszone jest nie tylko do sfery militarnej i politycznej. Bezpieczeństwo rozpatruje się zarówno w kontekście zjawisk o charakterze globalnym, europejskim, państwowym, jak i w kontekście problemów poszczególnych obywateli<sup>3</sup>.

**Słowa kluczowe:** cyberterroryzm, polityka antyterrorystyczna, prawa człowieka, ochrona praw jednostki.

### **1. POJĘCIA CYBERTERRORYZM I CYBERPRZSTĘPCZOŚĆ**

Cyberprzestrzeń powstała w wyniku upowszechniania się technologii informatycznych. Specyfika cyberprzestrzeni dotyczy odmienności podejmowanych w jej ramach działań. Najbardziej typową cechą cyberprzestrzeni jest jej aterytorialność i niematerialność. Ważną cechą cyberprzestrzeni jest możliwość zachowania anonimowości przez podmiot dokonujący działań. Wynika to z obecnej konstrukcji cyberprzestrzeni, a nie z samej jej istoty<sup>4</sup>.

Według jednej z pierwszych definicji przestępczości komputerowej zaproponowanej w 1973 roku przez Rainer von Zur-Mühlena przestępczość komputerowa to: „każde

---

<sup>1</sup> Dr hab. Izabela Oleksiewicz, Katedra Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska, ul. Poznańska 1, 35-084 Rzeszów, e-mail: oleiza@prz.edu.pl

<sup>2</sup> Zob. A. Janowska, *Cyberterroryzm – rzeczywistość czy fikcja?*, [w:] *Spółczesność informacyjnowizja czy rzeczywistość?*, Kraków 2003, s. 446.

<sup>3</sup> M. Brzeziński, *Rodzaje bezpieczeństwa państwa*, [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. S. Sulowski, M. Brzeziński, Warszawa 2009, s. 33.

<sup>4</sup> M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007, s. 328–331.

przestępcze działanie, w którym komputer stanowi albo narzędzie, albo przedmiot zamachu”<sup>5</sup>. Natomiast Hans J. Schneider termin ten definiuje jako „przestępstwa, przy których urządzenia służące do elektronicznego przetwarzania danych zostają wykorzystane jako narzędzie przestępstwa lub przy których takie urządzenia są przedmiotem zamachu”<sup>6</sup>.

Definicję cyberterroryzmu podał również Mark Pollitt, określając go jako celowe, politycznie motywowane ataki dokonywane przez pozapaństwowe grupy lub tajnych agentów przeciwko informacji, systemom komputerowym, oprogramowaniu oraz danym, na skutek czego osoby nieuczestniczące w walkach doznają przemocy<sup>7</sup>.

Termin „cyberterrorizm” pojawił się po raz pierwszy w 1979 roku w Szwecji w raporcie przedstawiającym zagrożenia komputerowe. Obejmował on wszelką działalność z użyciem komputerów, mającą na celu niszczenie systemów teleinformatycznych, systemów nadzoru i kontroli, programów, danych itp., a w konsekwencji zastraszanie rządów i społeczeństw, wywieranie presji psychologicznej, doprowadzenie do zagrożenia życia lub powstania znacznych strat materialnych. W latach osiemdziesiątych XX wieku terminem tym posługiwano się w amerykańskich służbach specjalnych, wskazując na możliwości przeprowadzenia ataków elektronicznych przez wrogów Stanów Zjednoczonych. W 1998 roku w Centrali FBI utworzono Centrum Ochrony Infrastruktury Narodowej (NIPC, *National Infrastructure Protection Center*), którego zadaniem jest koordynowanie działań w zakresie gromadzenia informacji o zagrożeniach, reagowanie na zagrożenia informacyjne lub zamachy na elementy krytycznej infrastruktury państwa.

Zdefiniowanie cyberterroryzmu jako połączenia cyberprzestrzeni i terroryzmu oznacza, że taka aktywność wiąże się nie tylko z wrogim użyciem IT i działaniem w sferze wirtualnej, ale także cechuje się wszystkimi elementami konstytuującymi aktywność terrorystyczną<sup>8</sup>. Pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji w nich przechowywanych, których celem jest zastraszanie lub zmuszenie rządu albo jego ludzi, aby osiągnąć pewne korzyści polityczne lub społeczne. Ponadto aby móc zakwalifikować atak jako cyberterrorizm, powinien on być dokonany w wyniku przemocy wobec osób lub mienia albo przynajmniej powodować znaczne szkody w celu wywołania strachu. Przykładami takich ataków mogłyby być te, które prowadzą do śmierci lub obrażeń ciała, powodują eksplozje lub straty gospodarcze. Jak twierdzi Dorothy Denning, poważne ataki na infrastrukturę krytyczną mogą być również uznane za akty cyberterroryzmu w zależności od ich wpływu. Natomiast ataki, które zakłócają nieistotne usługi lub są przede wszystkim kosztowne, do nich nie należą<sup>9</sup>.

Tak więc należy stwierdzić, że pojęcie cyberterroryzmu używane jest w kontekście politycznie umotywowanego ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszania lub wymuszenia na rządzie i ludziach daleko

<sup>5</sup> M. Siwicki, *Materiały szkoleniowe*, „Prokuratura i Prawo” 2012/7–8, s. 242.

<sup>6</sup> *Ibidem*, s. 243.

<sup>7</sup> M. Pollitt, *Cyberterrorism – Fact or Fancy?*, [www.cs.georgetown.edu/~denning/infosec/pollitt.html](http://www.cs.georgetown.edu/~denning/infosec/pollitt.html) (dostęp: 14.05.2009).

<sup>8</sup> D. Denning, *Is Cyber Terror Next?*, [www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc](http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc) (dostęp: 14.05.2009).

<sup>9</sup> D. Denning, *Cyberterrorism*, „Global Dialogue” 2000, s. 57.

idących politycznych i społecznych celów w szerokim rozumieniu tego słowa<sup>10</sup>. Pojęcie to jest obiektem szerszego zainteresowania przynajmniej od lat osiemdziesiątych XX wieku, a spekulacje na ten temat nasiliły się po zamachach 11 września 2001 roku w Stanach Zjednoczonych. Jako typowe zagrożenia wskazywane są systemy kontroli lotów, infrastruktura bankowa, systemy dostarczania energii czy wody oraz bazy danych osobowych, a także systemy instytucji rządowych<sup>11</sup>.

Cyberprzestępczość jest zjawiskiem stosunkowo nowym, rozprzestrzeniającym się w zawrotnym tempie w społeczeństwach dobrze z informatyzowanych i mocno usieciowionych. Stanowi bardzo poważne, trudne do zwalczania zagrożenie. Decydują o tym szczególnie właściwości, jakimi cechuje się to zjawisko. Pierwsza z cech – transgraniczność – powoduje, że działania cyberprzestępców z łatwością przenikają bariery, na przykład granice państw. Bardzo często cyberprzestępcy prowadzą swoje działania w jednym miejscu, ich skutki zaś ujawniają się zupełnie gdzie indziej w miejscu oddalonym o setki kilometrów, nierzadko w innym kraju, na innym kontynencie. Uniemożliwia to określenie systemu prawnego, według którego miałyby następować ściganie takich przestępstw, a jednocześnie znacznie utrudnia wyznaczenie podmiotów odpowiedzialnych za podejmowanie działań ochronnych i zapobiegawczych. Kolejna cecha – anonimowość – na pewno nie ułatwia szybkiego ustalenia sprawców przestępstw oraz wykrycia sposobów ich działania. Nie jest to jednak całkowicie niemożliwe, ale wymaga podjęcia żmudnych poszukiwań i wdrożenia dobrze przemyślanych zaplanowanych działań. Wygoda i szybkość zaś, jaką zapewnia korzystanie z nowoczesnych technik komputerowych i sieciowych, sprzyjają ogromnemu narastaniu tej formy przestępczości w państwach najbardziej rozwiniętych<sup>12</sup>.

Reasumując, można stwierdzić, że grupa czynów, określana jako cyberprzestępstwa, polega na posługiwaniu się systemami lub sieciami informatycznymi wykorzystywanymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne. Należy jednak zastrzec, że pojęcia cyberprzestępstwa nie należy utożsamiać i stosować zamiennie z określeniem przestępstwo internetowe. To drugie pojęcie obejmuje bowiem jedynie grupę czynów, które mogą być popełnione tylko w Internecie<sup>13</sup>.

## 2. POJĘCIE PRAW CZŁOWIEKA

Podjętując rozważania w zakresie problematyki praw i wolności jednostki, należy ustalić treść tych pojęć. Chcąc zrozumieć, czym są prawa człowieka, trzeba wyjść poza prawo stanowione, jego teorię, poza politologię czy etologię<sup>14</sup>. Prawa człowieka są

<sup>10</sup> K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006, s. 36.

<sup>11</sup> M. Pomykała, *Cyberterroryzm*, [w:] *Bezpieczeństwo i zagrożenia współczesnego świata*, red. A. Olak, I. Oleksiewicz, Rzeszów 2008, s. 112–113. Patrz też: A. Janowska, *op. cit.*, s. 445–450.

<sup>12</sup> Szerzej zob. M. Polinceusz, M. Pomykała, *Ochrona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat*, [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, Warszawa 2013, s. 660–661.

<sup>13</sup> Patrz szerzej: M. Siwicki, *op. cit.*, s. 250.

<sup>14</sup> M. Piechowiak, *Powszechność praw człowieka. Zagadnienia filozoficzno-prawne*, [w:] *O prawach człowieka w podwójną rocznicę paktów*, Księga pamiątkowa w hołdzie profesor Annie Michalskiej, red. T. Jasudowicz, C. Mik, Toruń 1996, s. 50.

pojmowane jako realne relacje, które w różnych dziedzinach działalności ludzkiej, w tym w prawie stanowionym, rozumiane są w rozmaity sposób.

Najczęściej pod pojęciem wolności jednostki rozumie się kategorię uprawnień jednostki, która ma na celu zapewnienie jej sfery prywatności. W sferze określonej jako wolność jednostka jest uprawniona do podejmowania decyzji, zachowań i działań motywowanych własną wolą, a co najważniejsze jest to sfera wolna od ingerencji państwa, tym samym jest to dobro chronione prawem. Co więcej, nie bez podstaw uznaje się, że wolności stanowią gwarancję pozostałych uprawnień, gdyż tylko człowiek wolny może korzystać z pełni przysługujących mu praw.

Należy podzielić stanowisko Wiśniewskiego<sup>15</sup> i przyjąć, że aktualnie koncepcję jednostki tworzą trzy przesłanki:

1. wolność wyboru;
2. nieszkodzenie innym podczas realizacji własnych decyzji;
3. ograniczenie władzy państwowej nad jednostką.

Bogusław Banaszak i Artur Preisner uważają z kolei, że prawa człowieka to prawa pierwotne w stosunku do państwa przysługujące każdemu człowiekowi bez względu na jego przynależność państwową czy pozycję w społeczeństwie.<sup>16</sup>

Z kolei według Louisa Henkina prawa człowieka to prawa jednostek żyjących w społeczeństwie, mające charakter uniwersalny i podstawowy. Prawa człowieka nie mają jednak charakteru absolutnego, co oznacza, że mogą one podlegać pewnym ograniczeniom, ale tylko w wyjątkowych, z góry przewidzianych wypadkach oraz zgodnie z uznanymi procedurami<sup>17</sup>.

W sensie formalnym – jak uważa Roman Kuźniar – prawa człowieka stanowią dziedzinę prawa konstytucyjnego i międzynarodowego, której zadaniem jest obrona w sposób zindywidualizowany praw osoby<sup>18</sup>.

Niekiedy w terminologii konstytucyjnej te same uprawnienia jednostki raz są określane jako prawa, innym razem jako wolności, co nie jest bez znaczenia i bez konsekwencji prawnej dla osób z nich korzystających. Wolność jednostki nie wynika bowiem z aktów prawnych, czyli prawa podmiotowego<sup>19</sup>. Prawo ich nie nadaje, a jedynie określa granice ich stosowania. Zadaniem państwa jest ochrona i gwarancja wolności człowieka. Cechą charakterystyczną wolności jest to, że państwo i jego organy mają obowiązek powstrzymywania się od działania w sferach życia objętych konkretną wolnością.

Wolności mogą dotyczyć różnych dziedzin życia, stąd wyróżnia się wolności osobiste, a także wolności polityczne, społeczne i ekonomiczne. Współcześnie przyjmuje się, że wszystkie wolności zagwarantowane w konstytucji przysługują jednostkom bez względu na ich przynależność państwową. Najbardziej typowe wolności osobiste to: nietykalność osobista, wolność sumienia i wyznania.

<sup>15</sup> L. Wiśniewski, *Prawo a wolność człowieka – pojęcie i konstrukcja prawna*, [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, red. L. Wiśniewski, Warszawa 1997, s. 53.

<sup>16</sup> B. Banaszak, Preisner A., *Prawo konstytucyjne. Wprowadzenie*, Wrocław 1993, s. 17.

<sup>17</sup> *Prawa człowieka i systemy ich ochrony*, red. B. Banaszak, Wrocław 1995, s. 36.

<sup>18</sup> R. Kuźniar, *Prawa człowieka. Prawo, instytucje, stosunki międzynarodowe*, Warszawa 2000, s.

12; I. Oleksiewicz, *Cyberterrorizm jako przykład łamania prawa godności człowieka*, [w:]

*Cyberterrorizm – wyzwania XXI wieku*, red. T. Jemiolo, J. Kisielnicki, K. Rajchel, Warszawa 2009.

<sup>19</sup> Patrz szerzej: W. Skrzydło, *Ustrój polityczny RP*, Kraków 2002, s. 85.

Prawa natomiast służą ochronie interesów jednostki. Poza stosunkowo wąską sferą ograniczeń, prawa jednostki przyznawane są każdej osobie niezależnie od posiadanego przez nią obywatelstwa. Prawa jednostki, ich zakres i dziedziny, których dotyczą, ulegały ewolucji. Prawa jednostki muszą mieć oparcie w konstytucji lub w ustawach, czyli nie ma prawa podmiotowego bez normy prawnej. Zadanie państwa w tym wypadku polega na zapewnieniu jednostce realizacji jej praw lub ich ochronie.

Co przesądza o tym, że ustrojodawca zalicza dane prawo do grupy praw podstawowych czy też nie otrzymujemy, stosując kryterium materialne. Można spotkać stanowisko głoszące, że prawo podstawowe charakteryzuje się tym, że dotyczy „najbardziej istotnych stosunków społecznych w danym etapie rozwoju”<sup>20</sup>. Inni uważają, że prawa podstawowe to takie, które „rozstrzygają o pozycji jednostki w danym państwie, są bowiem niezbędne do realizacji i zagwarantowania innych”<sup>21</sup>. Spotkać można też pogląd, że podstawowe prawa i wolności to te, „które gwarantują akty prawa międzynarodowego”<sup>22</sup>, czy te, „które mają najistotniejsze znaczenie z punktu widzenia interesów obywatela i państwa”<sup>23</sup>. Definicje te, chociaż nie są jednoznaczne, to jednak dają podstawę do stwierdzenia, że kryterium podmiotowe odgrywa bardzo ważną rolę w kształtowaniu konstytucyjnego katalogu praw podstawowych.

Zbyt wielkie są na świecie różnice w rozwoju cywilizacyjnym, kulturowe i geopolityczne, by możliwe było wyraźniejsze określenie tego, co wspólne wszystkim ludziom w sferze ich praw, co dałoby się generalizować, określić, sprawnie zapewnić i strzec przed naruszeniami. Na gruncie tych założeń są rozwijane regionalne systemy praw człowieka. Nie budzi wątpliwości, że konieczne są współpraca i harmonizacja obu tych tendencji oraz formowanie na ich podstawie konkretnych systemów ochrony praw człowieka.

Również w powszechnym systemie ochrony prawa człowieka już od dłuższego czasu widoczna jest tendencja do poszukiwania sposobu zwiększenia stopnia ochrony poszczególnych grup ludzi, na przykład uchodźców, więźniów czy dzieci. Pojawia się tu także kategoria praw zbiorowych, a w ich perspektywie i przez ich pryzmat ochrona praw człowieka z uwzględnieniem całej złożoności współwystępowania praw zbiorowych *sensu stricto* i praw jednostki realizowanych zbiorowo<sup>24</sup>.

W systemie uniwersalnym ochrony praw człowieka, oprócz wskazanych już traktatów, współwystępuje wiele innych istotnych umów międzynarodowych, takich jak Konwencja w sprawie Zapobiegania i Karania Zbrodni Ludobójstwa, Konwencja w sprawie Zwalczenia i Karania Zbrodni Apartheidu, Konwencja w sprawie Zakazu Stosowania Tortur oraz Innego Okrutnego, Nieludzkiego lub Poniżającego Traktowania albo Karania, Konwencja o Ochronie Uchodźców. Wyróżnienie systemów uniwersalnego i regionalnych w ochronie praw człowieka nie może jednak prowadzić do zatracenia kompleksowości tej ochrony. Kompleksowość zezwala uchwycić rzeczywistą sytuację

<sup>20</sup> A. Burda, *Polskie prawo państwowe*, Warszawa 1978, s. 370.

<sup>21</sup> W. Sokolewicz, *O socjalistycznej koncepcji podstawowych praw i obowiązków obywateli*, „Studia prawnicze” 1978/2, s. 4.

<sup>22</sup> W. Zakrzewski, *Zakres przedmiotowy i formy działalności prawotwórczej*, Warszawa 1979, s. 173.

<sup>23</sup> Z. Jarosz, S. Zawadzki, *Prawo konstytucyjne*, Warszawa 1987, s. 213.

<sup>24</sup> A. Redelbach, *Prawa naturalne – prawa człowieka – wymiar sprawiedliwości. Polacy wobec Europejskiej Konwencji Praw Człowieka*, Toruń 2000, s. 111.

konkretnej osoby w danym czasie i na określonym terytorium. Zawsze też będą powracać pytania o priorytet poszczególnych praw, ich znaczenia dla pokoju. Nie mniej złożona jest relacja między prawami jednostki a prawami zbiorowości oraz prawami i obowiązkami danej osoby. Wysoki poziom ochrony praw jednostki nie może przecież paraliżować społeczeństwa w zwalczaniu takich zagrożeń jak: klęski żywiołowe czy przestępczość zorganizowana.

Prawa człowieka ponadto, będąc prawami fundamentalnymi, stanowią uprzywilejowaną kategorię powszechnych praw moralnych. Ich przyrodzony charakter polega na tym, że nie wymagają one jakichkolwiek uzasadnień, a konieczne jest uzasadnienie odstępstwa od tych praw. W razie naruszenia praw człowieka można się odwoływać, jak w przypadku naruszenia innych praw moralnych, do sumienia, poczucia sprawiedliwości, opinii publicznej czy powszechnie panujących zwyczajów społecznych<sup>25</sup>.

Wszelkie podejmowane wysiłki, zmierzające do zagwarantowania mechanizmów ochrony praw człowieka, zarówno w aktach prawa międzynarodowego, jak i przepisach prawa krajowego, prowadzą do przeniesienia praw człowieka ze sfery powinności do sfery rzeczywistości prawnej, tak aby były one jednocześnie prawem moralnym i prawem pozytywnym<sup>26</sup>.

Najważniejszym aspektem praw człowieka jest zdolność dochodzenia tych praw. Prawa człowieka bowiem to przede wszystkim usprawienia stanowiące podstawę roszczeń w przypadku ich naruszenia. Roszczenie opiera się na wcześniejszym założeniu wolności jednostki i jest istotnym składnikiem godności ludzkiej. Z kolei ochrona godności to jedna z głównych funkcji praw człowieka. Prawa człowieka regulują ponadto stosunki między jednostką i państwem, jego organami i funkcjonariuszami sprawującymi władzę na różnych szczeblach. W odróżnieniu od wielu innych praw moralnych czy nadanych przepisami, praw człowieka dochodzi się właśnie od państwa<sup>27</sup>.

Odwoływanie się do praw człowieka jako elementu ładu międzynarodowego tak oczywiście u końca XX wieku wyrosło na negatywnych doświadczeniach minionego stulecia. Filarem obecnego systemu współpracy stało się demokratyczne państwo prawne respektujące swobody obywatelskie i prawa człowieka. Doświadczenia II wojny światowej i późniejszego okresu zimnej wojny uświadomiły państwom europejskim, że ustroje demokratyczne są mniej podatne na destabilizację wewnętrzną i mniej skłonne do wszczynania agresji zewnętrznej niż ustroje autorytarne.

### **3. ZNACZENIE CYBERTERRORYZMU JAKO WSPÓŁCZESNEGO ZAGROŻENIA**

Człowiek jest otwartym systemem komunikującym się z otoczeniem poprzez przepływy materialne, informacyjne i energetyczne. Szczególnym celem ataków może być ludzka psychika, ponieważ świadomość i podświadomość mogą być niewłaściwie

<sup>25</sup> M. Piechowiak, *Filozofia praw człowieka*, Lublin 2000, s. 29.

<sup>26</sup> *Podstawowe prawa jednostki i ich sądowa ochrona*, red. L. Wiśniewski, Warszawa 1997, s. 49.

<sup>27</sup> W. Osiatyński, *Wprowadzenie do pojęcia praw człowieka*, [www.hfhrpol.waw.pl](http://www.hfhrpol.waw.pl), s. 2; I. Oleksiewicz, *Ochrona praw człowieka jako naczelną zasadą demokratycznego państwa*, [w:] *Człowiek między prawem a ekonomią w procesie integracji europejskiej*, red. G. Dammacco, B.Sitek, O.Cabaj, Olsztyn–Bari 2008, s. 359–369.

chronione przed przemyślanym atakiem<sup>28</sup>. Państwo ma natomiast obowiązek przedsięwziąć wszelkie środki, aby uniemożliwić jakiegokolwiek działania przestępcze. Wydaje się, że jedyną skuteczną metodą przeciwdziałania tym zagrożeniom jest systematyczne doskonalenie technik przy jednoczesnym wytwarzaniu, gromadzeniu i przesyłaniu technik wrażliwych<sup>29</sup>. Ochrona informacji w systemie teleinformatycznym to przedsięwzięcia techniczne i informacyjne mające na celu zabezpieczenie poszczególnych elementów systemu. Bezpieczeństwo teleinformatyczne musi zapewnić informacjom w nich przetwarzanym: poufność, integralność, dostępność, rozliczalność, autentyczność i niezawodność<sup>30</sup>.

Duże możliwości zaatakowania systemów informacyjnych stwarza poczta elektroniczna. Jedną z form ataku pocztowego polega na takim przesyłaniu informacji, aby uniemożliwić korzystanie z tego typu usługi. Drugą formą jest wykorzystanie poczty elektronicznej do zaatakowania systemów informacyjnych. Głównym narzędziem stosowanym do tego rodzaju celów są strony internetowe utrzymywane i obsługiwane bądź bezpośrednio przez dany podmiot pozapaństwowy bądź przez jego sympatyków<sup>31</sup>. Terrorysty wykorzystują cyberprzestrzeń w celach wywiadowczych. Przeważnie polega to na posługiwaniu się Internetem w celu uzyskania pewnej fachowej wiedzy. Czasami jednak działania operacyjne terrorystów polegają na przykład na dokładnym poznaniu potencjalnych celów ataku czy rozmaitych działaniach wywiadowczych lub kontrwywiadowczych.

W odniesieniu do zorganizowanych grup przestępczych użycie Internetu jako broni ma większe znaczenie w kontekście podejmowanych prób wymuszeń i szantażu mogących mieć pewien wpływ na gospodarkę państw, w których podmioty gospodarcze doświadczałyby tego rodzaju ataków. Uformowanie się sfery wirtualnej znacznie poszerzyło ten zakres, powodując zresztą, podobnie jak w wypadku legalnie prowadzonej działalności *e-commerce*, pojawienie się nowych obszarów aktywności przestępczej<sup>32</sup>.

Cyberterrorystami mogą się stać raczej osoby fizyczne<sup>33</sup> lub zorganizowane grupy, które kierują swoją aktywnością przeciwko sieciom komputerowym i zawartym w nich danym. Ich motywacja ma najczęściej charakter typowy dla klasycznych terrorystów i wynika z zaangażowania ideologicznego. Oznacza to, że podstawowym motywem podejmowanych działań jest chęć uzyskania wpływu na decyzje polityczne i upowszechnianie określonej ideologii<sup>34</sup>. W działaniach tych podmiotów sieć jest środkiem do przeprowadzenia ataku, a zamierzonym celem może być sparaliżowanie sieci

<sup>28</sup> M. Kinasiewicz, *Identyfikacja zjawiska infoterroryzmu*, „Zeszyty Naukowe WSIZiA” 2008/1, s. 216.

<sup>29</sup> Patrz szerzej: M. Kinasiewicz, *Zagrożenia dla systemów informacyjnych*, „Zeszyty Naukowe WSIZiA” 2008/1, s.234–235.

<sup>30</sup> J. Janczar, G. Świdzikowski, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Warszawa 2004, s. 11.

<sup>31</sup> M. Madej, *op. cit.*, s. 336.

<sup>32</sup> I. Oleksiewicz, *Polityka antyterrorystyczna Unii Europejskiej*, Lublin 2013, s. 276.

<sup>33</sup> W tym wypadku podmiotami dokonującymi ataków sieciowych są najczęściej hobbyści lub nastoletni hakerzy, sprawdzający swoje możliwości i umiejętności, a także niełojalni pracownicy, wykorzystujący legalny dostęp przynajmniej do części zasobów swojej firmy. W tym ostatnim wypadku o wykorzystaniu dostępu do sieci decyduje najczęściej czynnik ekonomiczny.

<sup>34</sup> P. Maj, *Cyberterrorizm w stosunkach międzynarodowych*, „Studenckie Zeszyty Naukowe, Wydział Politologii UMCS” 2001/1, s. 79.

rządowych służących do zarządzania, komunikowania, wywiadu oraz systemów użyteczności publicznej opartych na technologii informatycznej. Wykorzystując techniki informatyczne czy tradycyjne, grupy te dążą do spowodowania powszechnego niebezpieczeństwa.

Wielu specjalistów zwraca jednak uwagę, że sieci i systemy teleinformatyczne nie stanowią szczególnie atrakcyjnego celu dla terrorystów, występują jedynie jako cel pośredni lub wspomagający. Ataki tradycyjne cały czas są postrzegane jako skuteczniejsze, ponieważ pozwalają na wywołanie efektu destrukcyjnego tańszymi i prostszymi metodami konwencjonalnymi<sup>35</sup>.

Przedmiotem ataku mogą być obiekty infrastruktury o dużym znaczeniu dla gospodarki, dla obronności państwa, obiekty użyteczności publicznej, systemy informatyczne instytucji publicznych. Wielu autorów analizujących bliżej problematykę cyberterrorystów zwraca uwagę, że jest to działanie polegające na stosowaniu przemocy lub groźby jej użycia, dokonywane w celu realizacji postulatów ideologicznych, politycznych bądź religijnych, wykorzystujące cyberprzestrzeń jako środek ataku<sup>36</sup>.

Zamierzone straty muszą dotyczyć nie przestrzeni wirtualnej, ale świata realnego. Jednakże podejmowane działania powinny się charakteryzować wykorzystaniem cyberprzestrzeni do przeprowadzenia ataku przestępczego. Należy to traktować jako pewne uproszczenie i metaforę, chodzi bowiem o wykorzystanie możliwości, jakie daje połączenie serwerów za pomocą odpowiedniego oprogramowania i przepływ danych pomiędzy poszczególnymi jednostkami.

Potencjalnie jednak sieć może się stać polem walki politycznej czy ideologicznej o charakterze bardziej agresywnym, a nawet destrukcyjnym<sup>37</sup>. Ataki dokonywane za pośrednictwem sieci mogą zostać skierowane na zniszczenie informacji, wykradzenie, sprzedanie, wykorzystanie ich dla własnych celów w celu uzyskania korzyści materialnych albo z powodów ideologicznych. Pokusa jest bardzo duża. Dlatego ochrona informacji dostępnych w sieci staje się tak ważnym priorytetem.

Ataki wykorzystujące techniki hakerskie i spammerskie są codziennością dla wszystkich korzystających z internetu. Cyklicznie pojawiają się informacje o modyfikacji stron www lub ich podmianie, o przeciążeniach i zablokowaniu serwerów różnych instytucji poprzez sztuczne generowanie dużej liczby wejść. Jednakże – jak słusznie zwraca uwagę Andrzej Adamski – działania te wprawdzie mają na celu osiągnięcie efektu psychologicznego, ale ich skutki ujawniają się przede wszystkim w rzeczywistości wirtualnej. Choć powodują zakłócenia w funkcjonowaniu urządzeń sieci globalnej, nie wyrządzają one poważnych szkód majątkowych ani nie wywołują zagrożenia dla życia i zdrowia ludzi<sup>38</sup>.

Najbardziej interesującym przykładem cyberterrorystycznej wojny była działalność Usamy Ibn Ladina (twórcy Al-Kaidy)<sup>39</sup>, mającego wpływ na sieć względnie

<sup>35</sup> A. Adamski, *Cyberterrorystyczny*, [w:] *Terrorystyczny*, red. V. Kwiatkowska-Darul, Toruń 2002, s. 119.

<sup>36</sup> *Ibidem*; P. Maj, *Cyberterrorystyczny w stosunkach...*, s. 69; A. Janowska, *op. cit.*, s. 449; D. Skowera, *Akademia cyber-policyjna policja i organizacje międzynarodowe wobec wyzwań przestępczości internetów*, „Zeszyty Naukowe ISP UJ” 2006/2, s.139.

<sup>37</sup> A. Adamski, *op. cit.*, s. 117; D. Littlejohn Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004, s. 37.

<sup>38</sup> A. Adamski, *op. cit.*, s. 119.

<sup>39</sup> Działającej od 1988 roku do maja 2011 placówki znajdowały się na terenie około 55 państw i z nich atakowane były wybrane cele.



autonomicznych, finansowanych przez niego grup. Jego tak zwana „święta wojna” wypowiedziana Stanom Zjednoczonym i całemu Zachodowi jest świetnym przykładem postępu technik informacyjnych. Jak podkreśla Brunon Hołyst, to nowe techniki komunikacji i informatyzacji nadają sieci trojaki cechy. Po pierwsze, zredukowanie czasu transmisji. Po drugie, znaczenie zmieszenie kosztów, co z kolei sprzyja rozproszeniu organizacji przez decentralizację. Po trzecie, zwiększenie zakresu i kompleksowości informacji. Po jego śmierci 2 maja 2011 roku Al-Kaida sprzymierza się z innymi ruchami politycznymi, by je „przejąć”, prowadzić walki partyzanckie na spornych terytoriach i stworzyć nowy kalifat, który rozciągałby się daleko poza Bliski Wschód<sup>40</sup>. Jednak coraz większa rzesza ekspertów twierdzi, że przyszłością terroryzmu jest tak zwany terroryzm indywidualny. Na naszych oczach zbrojny dżihad przestaje być zajęciem na pełen „etat”, wykonywanym gdzieś w dalekich górach Afganistanu, a przeradza się w działalność, w której prócz wiary w świętą wojnę, kluczową rolę odgrywają nowoczesne formy komunikacji i odpowiednie obywatelstwo. Najlepiej jednego z zachodnich, „zepsutych” państw<sup>41</sup>.

#### 4. WPLYW CYBERTERRORYZMU NA OGRANICZENIE PRAW I WOLNOŚCI CZŁOWIEKA

Należy w tym miejscu przedstawić koncepcję godności człowieka. Prawa człowieka są ze swej natury uniwersalne, ponieważ ich źródłem jest równa godność wszystkich ludzi. Nie negując bynajmniej różnorodności kultur istniejących na świecie oraz różnic w rozwoju ekonomicznym, trzeba stanowczo przypomnieć, że ludzkie prawa przysługują każdemu człowiekowi. Godność jest wewnętrznym, wrodzonym i naturalnym znamieniem człowieka, niezależnym od kontekstu społecznego i historycznego. Społeczeństwo i historia nie nadają jej człowiekowi, ale mają obowiązek jej poszanowania i chronienia<sup>42</sup>. Dotyczy ona w ten sam sposób kobiet i mężczyzn, dzieci, ludzi starszych i młodych, zdrowych i niepełnosprawnych, biednych i bogatych. Wszyscy ludzie, mając tę samą naturę i to samo pochodzenie, cieszą się równą godnością. Skoro wszyscy ludzie są równi pod względem godności, upada podstawa wszelkiej teorii lub praktyki, która wprowadza różnice między ludźmi ze względu na ich godność<sup>43</sup>.

Akty prawa międzynarodowego podkreślają, że godność ludzka jest godnością przyrodzoną. Jest ona zatem wpisana niezależnie od prawa pozytywnego w istotę ludzką. Prawo może ją jedynie uznać, deklorować, potwierdzić, bo bynajmniej nie zależy ona od woli państwa. Powszechna Deklaracja Praw Człowieka, uznając przyrodzoną godność człowieka, wiąże ją równocześnie ze sferą powinności. Ścisły związek pomiędzy tą wartością a prawami człowieka, jedynie zasygnalizowany w Deklaracji, jest doprecyzowany przez Międzynarodowe Pakty Praw Człowieka. W ich wstępach

<sup>40</sup> I. Sanchez-Cuenca, *The dynamics of nationlists terrorism: ETA and IRA*, „Terrorism and Political Violence” 19/3 (2007), s. 289–306.

<sup>41</sup> <http://wiadomosci.wp.pl/kat,1020229,title,Zamachowiec-na-zlecenie-Czy-przyszlosc-terroryzmu-to-male-grupy-zwerbowane-na-Zachodzie,wid,15365996,wiadomosc.html> (dostęp: 26.02.2013).

<sup>42</sup> J. W. Gałkowski, *Jan Paweł II o godności człowieka*, [w:] *Zagadnienie godności człowieka*, red. J. Czerkawski, Lublin 1994, s. 108.

<sup>43</sup> Por. wyrok SN z 16 kwietnia 2004 roku, I CK 495/03 oraz wyrok WSA w Warszawie z 15 kwietnia 2004 r., I SA 2731/03.

wyrażona jest zasada, że wszystkie prawa wynikają z godności przyrodzonej osobie ludzkiej<sup>44</sup>.

Za Robertem Alexym można wysunąć następującą hipotezę, że norma godności człowieka w systemie prawa zachowuje się równocześnie jako reguła i jako zasada prawa<sup>45</sup>. Formuła godności człowieka rekonstruowana z poszczególnych jednostek redakcyjnych umów międzynarodowych pełni funkcję, w której akcentowana jest albo nienaruszalność wartości chronionej przez normę, albo jej charakter deklaratoryjny, wskazujący ideał wyznaczony do osiągnięcia. Klauzula godności człowieka, zachowując się jak reguła, pozwala jednocześnie ocenić daną sytuację jako odstępstwo od normy.

Z godnością człowieka ściśle związana jest prywatność. Istotą i celem prawa do prywatności jest ochrona godności człowieka. Mówi się, że godność jest źródłem wszystkich praw. Godność po prostu mamy i nikt nie może jej odebrać<sup>46</sup>. Każdy człowiek ma wrodzone poczucie dumy i honoru osobistego<sup>47</sup>. Nikt nie powinien być źle traktowany, poniżany, wyśmiewany czy w jakikolwiek sposób obrażany. Każdy człowiek ma prawo do ochrony przed poniżającym traktowaniem, takim, które narusza jego poczucie godności. Dlatego nie mówimy o prawie do godności, tylko o zasadzie poszanowania godności<sup>48</sup>.

Prawa fundamentalne nie mają jednak charakteru absolutnego, możliwość ich czasowego uchylecia bądź zmiany w każdym przypadku musi być rozważana na podstawie ich funkcji społecznej. Wszelkie ograniczenia w ich wykonaniu nakładane zarówno przez organy Unii Europejskiej, jak i państw członkowskich mogą zaistnieć jedynie w celu zapewnienia ogólnego interesu Unii z uwzględnieniem zasady konieczności i proporcjonalności. W żadnym razie ograniczenia te nie mogą stanowić naruszenia substancji tych praw.

Postępująca globalizacja, nowe technologie sprawiły, że badacze wskazują dziś na nową postać terroryzmu, tak zwany terroryzm ponowoczesny. Za Jenkinsem można zauważyć, że definicja terroryzmu jest uzależniona od moralności, prawa, podczas gdy sam terroryzm kształtowany jest przez kulturę, ideologię i politykę<sup>49</sup>. Zakorzenienie terroryzmu w rzeczywistości zmusza do przyjrzenia się kilku teoriom, próbującym wyjaśnić naturę omawianego zjawiska.

Pierwszą z nich jest teza Francisca Fukuyamy, ogłaszająca zwycięstwo liberalnej demokracji. Poglądy te znalazły oparcie w platońskiej nauce o duszy, a także filozofii Hegla i Kojève'a. Historia według Fukuyamy to walka o uznanie. To nie zasoby naturalne czy bogactwa, ale właśnie tymotejska część duszy prowadzi niewolników do opanowania sił przyrody i rozwoju, a jedynie „liberalne demokracje zastąpiły irracjonalne pragnienie bycia uznanym za potężnego, potrzebą bycia uznanym za równego”<sup>50</sup>. Ewolucja ustrojów

<sup>44</sup> Międzynarodowy Pakt Praw Gospodarczych, Socjalnych i Kulturalnych z 1966 roku oraz Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966 roku.

<sup>45</sup> R. Alexy, *Teorie der Grundrechte*, Baden–Baden 1985, s. 94–97.

<sup>46</sup> Por. wyrok TK z 4.05.2004 r., sygn. K 8/03, OTK-A 2004 nr 5 poz. 37.

<sup>47</sup> Por. wyrok SA w Białymstoku z 5 listopada 2004 roku, I ACa 550/04, OSAB 2005 nr 1 poz. 3; wyrok SN z 25 stycznia 2005 roku, II PK 152/04, OSNP 2005 nr 17 poz. 266.

<sup>48</sup> Por. postanowienie TK z 9 czerwca 2004 r., sygn. Tw 33/03, OTK-B 2004 nr 4/227.

<sup>49</sup> B. M. Jenkins, *The new age of terrorism*, [w:] *The McGraw-Hill Homeland Security Handbook*, red. D. G. Kamien, New York 2006, s. 117.

<sup>50</sup> F. Fukuyama, *Koniec historii*, przekł. M. Bieroń [i in.], Poznań 1996, s. 45.

społecznych doprowadzi do odrzucenia państwa o tradycyjnym charakterze na poczet uniwersalnego państwa homogenicznego, zapewniającego wszystkim uznanie<sup>51</sup>. Rywalizacja na polu bitwy zastąpiona będzie rywalizacją w ramach polityki, biznesu, nauki czy sztuki<sup>52</sup>.

Fukuyama, głosząc swe prognozy na podstawie analizy rozwoju biotechnologii, postuluje ponowne odnalezienie wspólnego fundamentu dla praw stanowionych, jakim jest według niego natura ludzka. Jest ona jednak zagrożona ze względu na rozwój biotechnologii. Fukuyama, nie występując jako przeciwnik nauki, próbuje ustalić granice jej interwencji w istotę człowieczeństwa<sup>53</sup>. Tak więc przewidywania rozwoju stosunków społecznych, dotyczące płaszczyzn uzależnionych od wiedzy, są niemożliwe, jeśli nie uwzględni się nauki, po jej uwzględnieniu zaś również takie pozostają<sup>54</sup>.

Albert Bergesen i Omar Lizardo wskazują na trzy okresy, w każdym z nich występuje hegemon chylący się ku upadkowi, który swą polityką doprowadza do konfliktu: w pierwszym okresie były to Hiszpania i wojna trzydziestoletnia, w drugim Brytania i II wojna światowa, w trzecim Stany Zjednoczone i konflikt, którego autorzy nie określają. W każdej z tych „epok” polityczna hegemonia jednego z państw prowadzi do niestabilności w polityce międzynarodowej i konfliktów<sup>55</sup>; teoria ta wydaje się modyfikacją starego stanowiska Fukuyamy.

Drugą z tez, które wywołały znaczne spory, jest teza o zderzeniu cywilizacji. Według Huntingtona „historia ludzkości to dzieje cywilizacji”<sup>56</sup>, a upadek świata dwubiegunowego doprowadził do rywalizacji pomiędzy cywilizacjami reprezentującymi wiele odmiennych wartości<sup>57</sup>. Konflikty współczesnego świata rozgrywać się więc będą wzdłuż linii dzielących obszary odmienne kulturowo; Huntington wymienia następujące przyczyny tego zjawiska<sup>58</sup>: różnice pomiędzy cywilizacjami dotyczące historii, języka, kultury, tradycji i, co najważniejsze, jak zauważa Huntington, religii – są one nie tylko realne, ale mają charakter decydujący. O ile różnice pomiędzy państwami nie muszą być zarzewiem konfliktu, o tyle w przypadku cywilizacji je generują.

Świat staje się coraz mniejszy, prowadzi to do coraz częstszych kontaktów między ludźmi, podnosząc świadomość ich odrębności, proces rozwoju ekonomicznego odrywa ludzi od korzeni, państwa narodowe nie stanowią już źródła identyfikacji, a lukę tę zapelnia religia i fundamentalizm, powrót do korzeni na terenach nienależących do

<sup>51</sup> Szerzej: B. Bolechów, *Terroryzm w świecie podwubiegunowym*, Toruń 2003, s. 76 i n.

<sup>52</sup> F. Fukuyama, *Ostatni człowiek*, Poznań 1997, s. 170.

<sup>53</sup> F. Fukuyama, *Koniec człowieka*, Kraków 2004, s. 10

<sup>54</sup> K.R. Popper, *Nęcza historyczmu*, Warszawa 1999, s. 10. Podobnie Michio Kaku: „Ów prymitywizm futurologii wynika stąd, że nasze umysły myślą liniowo, podczas gdy wiedza rośnie wykładniczo”, „nauka rozwija się w nieprzewidywalny sposób. [...] Kiedy próbujemy przewidzieć, co się będzie działo za kilkadziesiąt lat, odkrywamy, że dominującym czynnikiem stają się jakościowe przełomy w nowych dziedzinach, a nowe możliwości otwierają się w nieoczekiwanych miejscach” (*Hiperprzestrzeń. Wszechświaty równoległe, pętla czasowe i dziesiąty wymiar*, Warszawa, s. 241 i n.).

<sup>55</sup> A. J. Bergesen, O. A. Lizardo, *Terrorism and World-System Theory*, [w:] *Transnational Terrorism in the World System Perspective*, red. R. Stemplowski, Warszawa 2002, s. 17.

<sup>56</sup> S. P. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, tłum. A. Jankowska, Warszawa 2006, s. 46.

<sup>57</sup> Szerzej: B. Bolechów, *op. cit.*, s. 82.

<sup>58</sup> S. P. Huntington, *op. cit.*, s. 46.

cywilizacji zachodniej, będący reakcją na jej supremację, która „stara się potwierdzać swoją wartość i bronić swych interesów, co stawia inne społeczeństwa przed wyborem”<sup>59</sup>: albo dołączenie do Zachodu, albo sprzeciwienie się mu poprzez budowę potęgi gospodarczej i militarnej, jak czynią to społeczeństwa muzułmańskie i konfucjańskie<sup>60</sup>.

Różnice o charakterze kulturalnym i ekonomicznym są mniej podatne na niwelowanie niż polityczne i ekonomiczne. Według Huntingtona cywilizacja Zachodu traci swoją siłę, i choć jej dominacja potrwa jednak jeszcze jakiś czas, utraci go na poczet innych cywilizacji, w szczególności muzułmańskiej i konfucjańskiej. Powodem tego są nie tylko potencjał demograficzny, ale i zdolność do mobilizacji<sup>61</sup>.

Teza Huntingtona spotkała się z ostrą krytyką; Laquer<sup>62</sup> twierdzi, że: ucisk muzułmanów istnieje także w krajach cywilizacji muzułmańskiej, a jego źródło tkwi nie w instytucjach zachodnich, lecz właśnie w muzułmańskich. Marc Cogen z kolei uważa, że dla Huntingtona największy spór rozgrywa się między cywilizacją zachodu a ruchami fundamentalistycznymi islamu. Nie można jednak generalizować i zapominać, iż wiele podobnych tendencji istnieje wewnątrz krajów islamskich, takich jak Turcja czy Filipiny<sup>63</sup>. Stwierdza również, że Huntington minął się z prawdą, dowodząc, że charakter konfliktu związany jest ze zderzeniem cywilizacji. Według Cohena jego źródłem jest ideologia, będąca mieszaniną idei i wartości kształtujących społeczeństwo<sup>64</sup>. Jenkins zaś wymienia inne powody i przejawy rozwoju terroryzmu: staje się on bardziej krwawy, a terroryści zyskują nowe źródła finansowania, rozwijają nowe modele organizacji, prowadzą kampanie o charakterze globalnym, wprowadzając do swoich działań nowe technologie komunikacyjne.

Wskazanie na te względnie nowe kwestie nie pozwala jednak na przewidywania, a tym bardziej na proroctwa, jak zostało to już wyjaśnione. Wiele rzeczy bowiem, które były źródłem lęku 30 lat temu, nie zaistniało, przyszłość zaś może nas całkowicie zaskoczyć i obalić wszystkie z naszych prognoz<sup>65</sup>.

W dyskusji na temat terroryzmu jednym z najistotniejszych elementów wydaje się stosunek działalności o charakterze terrorystycznym i antyterrorystycznym do praw człowieka. Według Biura Wysokiego Komisarza ds. Praw Człowieka: „jednoznacznie i oficjalnie potępiając działania o charakterze terrorystycznym, kładzie się nacisk na ochronę podstawowych praw człowieka, a w szczególności prawa do życia, a normy prawa człowieka muszą być rygorystycznie respektowane w każdym przypadku”. Szacunek dla praw człowieka, podstawowych wolności i zasad prawa to „niezbędne narzędzie na drodze do zwalczania terroryzmu – nie zaś przywilej, który może być poświęcony w trudnych czasach”<sup>66</sup>.

<sup>59</sup> *Ibidem*, s. 23.

<sup>60</sup> Huntington wymienia następujące cywilizacje: Zachodnia, Latynoamerykańska, Prawosławna, Afrykańska, Islamska, Buddyjska, Chińska, Japońska (*ibidem*, s. 21).

<sup>61</sup> Szerzej: B. Bolechów, *op. cit.*, s. 83.

<sup>62</sup> *Ibidem*, s. 57.

<sup>63</sup> M. Cogen, *The West Europe and the Islam. The Centre for the Study of European Politics and Society*, <http://hsf.bgu.ac.il/europe>. (dostęp: 24.07. 2009 r.)

<sup>64</sup> *Ibidem*, s. 4.

<sup>65</sup> B.M. Jenkins, *op. cit.*, s. 118.

<sup>66</sup> *Terrorism and Human Rights* <http://www.unhcr.ch/terrorism/index.html> (odczyt z dnia 17.08.2010 r.)

## 5. WNIOSKI

Najnowszym problem obecnego stulecia pozostaje jednak bezpieczeństwo informacyjne, które często rozumiane jest jako ochrona informacji przed nieporadnym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. Środki bezpieczeństwa są podejmowane w celu zapewnienia poufności, integralności i dostępności informacji<sup>67</sup>. Ochrona informacji niejawnych pozostaje w dobie zagrożeń cyberterrorystycznych i cyber-wojny jednym z najważniejszych zadań ochrony bezpieczeństwa informacyjnego państwa. Skuteczność aktywności państwa w wielu dziedzinach zależy właśnie od sprawności ochrony informacji<sup>68</sup>. Cyberterroryzm jest tym groźniejszy dla współczesnych społeczeństw, im bardziej uzależnione są one od technologii informatycznych. Hakerska penetracja systemów informatycznych stanowi dzisiaj podstawowy problem w walce z cyberterroryzmem, zwłaszcza gdy ma to duże znaczenie dla państwa.

Cyberterroryzm jest poważnym wyzwaniem dla światowego bezpieczeństwa, a jego znaczenie wzrasta. Fakt ten oraz proces globalizacji współczesnego terroryzmu powodują, że odpowiedź na to wyzwanie również musi być globalna, a współpraca w zwalczaniu omawianego zjawiska powinna być efektywna, ścisła i skoordynowana, obejmująca jak największą liczbę państw i organizacji międzynarodowych<sup>69</sup>. Co prawda, zjawisko cyberterroryzmu ze względu na swoją specyfikę wymaga badań i przedsięwzięć interdyscyplinarnych, jednak to przede wszystkim prawo, zarówno wewnętrzne, jak i międzynarodowe, powinno się zająć tworzeniem odpowiednich środków i metod w celu zwalczania aktów terrorystycznych, a także wszelkich źródeł i sposobów służących wspieraniu i finansowaniu omawianego zjawiska. Prawo międzynarodowe zdołało już wypracować odpowiednie instrumenty prawne pomocne przy przeciwdziałaniu i zwalczaniu procederu finansowania terroryzmu, uznawanego za poważne przestępstwo. Jednak skuteczna walka możliwa jest tylko wówczas, gdy państwa wyrażą polityczną wolę jej prowadzenia i będą czynnie w niej uczestniczyć, nie tylko w granicach własnego terytorium, ale również współpracując z innymi, chętnymi do tej współpracy państwami i organizacjami międzynarodowymi, a stworzenie stosownych przepisów prawnych byłoby tego najlepszym dowodem.

Godność człowieka jest najogólniejszą normą ładu społeczno-gospodarczego każdego państwa. Pozwala ona analizować i oceniać zastaną rzeczywistość, podczas gdy zasady społeczne opisują poszczególne płaszczyzny życia społeczno-ekonomicznego, wskazując, jak je kształtować, aby zabezpieczyć i afirmować jednostkę. Godność człowieka stanowi zatem aksjologiczną i normatywną bazę zarówno dla międzynarodowego, jak i dla państwowego systemu praw człowieka<sup>70</sup>. Natomiast ochrona bezpieczeństwa i porządku publicznego jest jednym z najważniejszych i najstarszych zadań publicznych, związanym ściśle z samym powstawaniem władzy publicznej. Newralgiczne dla każdego państwa obszary bezpieczeństwa mogą podlegać różnego rodzaju zagrożeniom, w związku z czym

<sup>67</sup> K. Liedel, *op. cit.*, s. 19.

<sup>68</sup> K. Liedel, *op. cit.*, s. 45.

<sup>69</sup> Sprawa Irlandia v. Wielka Brytania, 18 stycznia 1978; sprawa Soering v. Wielka Brytania, 7 lipca 1989; sprawa Clauhal v. Wielka Brytania, 15 listopada 1966; sprawa Aksoy v. Turcja 18 grudnia 1966; sprawa Tomasi v. Francja, 27 sierpnia 1992.

<sup>70</sup> Wyrok TK z 21 kwietnia 2004 roku, sygn. akt K 45/02, OTK-A 2004/4/30.

w celu zapewnienia normalnego funkcjonowania obywateli oraz kraju każdy z tych obszarów musi być z wyprzedzeniem poddany odpowiedniej ochronie, gwarantowanej szczególnymi kompetencjami stosownych podmiotów. Kompatybilność działań ochronnych zarówno w wymiarze wewnętrznym (wewnątrzpaństwowym), jak i zewnętrznym, zazwyczaj związanym z instytucjonalizowaną współpracą poszczególnych państw, najczęściej wymaga ograniczenia lub nawet wyłączenie praw i wolności jednostki. Istotne jest jednak to, aby ograniczenia praw, wolności i swobód przynależnych jednostkom, po pierwsze, miały na celu wyłącznie zastosowanie stosownych instrumentów umożliwiających państwu wykorzystanie niezbędnej ochrony własnych interesów, a po drugie, aby oznaczały wyłącznie działania niezbędne i jednocześnie proporcjonalne do osiągnięcia ochrony danego interesu.

#### LITERATURA

- [1] Adamski A., *Cyberterroryzm*, [w:] *Terroryzm*, red. V. Kwiatkowska-Darul, Toruń 2002
- [2] Alexy R., *Teorie der Grundrechre*, Baden–Baden 1985.
- [3] Banaszak B., Preisner A., *Prawo konstytucyjne. Wprowadzenie*, Wrocław 1993.
- [4] Bergsen A. J., Lizardo O.A., *Terrorism and World-System Theory*, [w:] *Transnational Terrorism in the World System Perspective*, red. Stemplowski R., Warszawa 2002.
- [5] Bolechów B., *Terroryzm w świecie podwubiegunowym*, Toruń 2003.
- [6] Brzeziński M., *Rodzaje bezpieczeństwa państwa*, [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, red. Sulowski S., Brzeziński M., Warszawa 2009.
- [7] Burda A., *Polskie prawo państwowe*, Warszawa 1978.
- [8] Cogen M., *The West Europe and the Islam. The Centre for the Study of European Politics and Society*, <http://hsf.bgu.ac.il/europe>. (dostęp: 24.07. 2009 r.)
- [9] Denning D., *Cyberterrorism*, „Global Dialogue” 2000, s. 57.
- [10] Denning D., *Is Cyber Terror Next?*, [www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc](http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc) (dostęp: 14.05.2009).
- [11] Fukuyama F., *Koniec człowieka*, Kraków 2004.
- [12] Fukuyama F., *Koniec historii*, przekł. M. Bieroń [i in.], Poznań 1996.
- [13] Fukuyama F., *Ostatni człowiek*, Poznań 1997.
- [14] Gałkowski J.W., *Jan Paweł II o godności człowieka*, [w:] *Zagadnienie godności człowieka*, red. Czerkawski J., Lublin 1994.
- [15] Huntington S.P., *Zderzenie cywilizacji i nowy kształt ładu światowego*, tłum. Jankowska A., Warszawa 2006,
- [16] Janczar J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Warszawa 2004
- [17] Janowska A., *Cyberterroryzm – rzeczywistość czy fikcja?*, [w:] *Spółczesność informacyjnowizja czy rzeczywistość?*, Kraków 2003.
- [18] Jarosz Z., Zawadzki S., *Prawo konstytucyjne*, Warszawa 1987.
- [19] Jenkins B.M., *The new age of terrorism*, [w:] *The McGraw- Hill Homeland Security Handbook*, red. D. G. Kamien, New York 2006.

- [20] Kaku M., *Hiperprzestrzeń. Wszechświaty równoległe, pętle czasowe i dziesiąty wymiar*, Warszawa 2003..
- [21] Kinasiewicz M., *Identyfikacja zjawiska infoterroryzmu*, „Zeszyty Naukowe WSIZiA” 2008/1.
- [22] Kinasiewicz M., *Zagrożenia dla systemów informacyjnych*, „Zeszyty Naukowe WSIZiA” 2008/1.
- [23] Kuźniar R., *Prawa człowieka. Prawo, instytucje, stosunki międzynarodowe*, Warszawa 2000.
- [24] Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006.
- [25] Littlejohn Shinder D., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004.
- [26] Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.
- [27] Maj P., *Cyberterroryzm w stosunkach międzynarodowych*, „Studenckie Zeszyty Naukowe, Wydział Politologii UMCS” 2001/1.
- [28] Międzynarodowy Pakt Praw Gospodarczych, Socjalnych i Kulturalnych z 1966 roku oraz Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966 roku.
- [29] Oleksiewicz I., *Polityka antyterrorystyczna Unii Europejskiej*, Lublin 2013.
- [30] Oleksiewicz I., *Cyberterroryzm jako przykład łamania prawa godności człowieka*, [w:] *Cyberterroryzm – wyzwania XXI wieku*, red. Jemioło T., Kisielnicki J., Rajchel K., Warszawa 2009.
- [31] Oleksiewicz I., *Ochrona praw człowieka jako naczelną zasadą demokratycznego państwa*, [w:] *Człowiek między prawem a ekonomią w procesie integracji europejskiej*, red. G. Dammacco, B.Sitek, O.Cabaj, Olsztyn–Bari 2008, s. 359–369.
- [32] Osiatyński W., *Wprowadzenie do pojęcia praw człowieka*, [www.hfhrpol.waw.pl](http://www.hfhrpol.waw.pl).
- [33] Piechowiak M., *Filozofia praw człowieka*, Lublin 2000.
- [34] Piechowiak M., *Powszechność praw człowieka. Zagadnienia filozoficzno-prawne*, [w:] *O prawach człowieka w podwójną rocznicę paktów*, Księga pamiątkowa w hołdzie profesor Annie Michalskiej, red. Jasudowicz T., C. Mik, Toruń 1996.
- [35] *Podstawowe prawa jednostki i ich sądowa ochrona*, red. Wiśniewski L., Warszawa 1997.
- [36] Polinceusz M., Pomykała M., *Ochrona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat*, [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. Bogdalski P., Nowakowski Z., Plusa T., Rajchel J., Rajchel K., Warszawa 2013.
- [37] Pollitt M., *Cyberterrorism – Fact or Fancy?*, [www.cs.georgetown.edu/~denning/infosec/pollitt.html](http://www.cs.georgetown.edu/~denning/infosec/pollitt.html) (dostęp: 14.05.2009).
- [38] Pomykała M., *Cyberterroryzm*, [w:] *Bezpieczeństwo i zagrożenia współczesnego świata*, red. Olak A., Oleksiewicz I., S. Wieczorek, Rzeszów 2008.
- [39] Popper K.R., *Nędza historycyzmu*, Warszawa 1999.

- [40] *Prawa człowieka i systemy ich ochrony*, red. Banaszak B., Wrocław 1995.
- [41] Redelbach A., *Prawa naturalne – prawa człowieka – wymiar sprawiedliwości. Polacy wobec Europejskiej Konwencji Praw Człowieka*, Toruń 2000.
- [42] Sanchez-Cuenca I., *The dynamics of nationlists terrorism: ETA and IRA*, „Terrorism and Political Violence” 19/3 (2007).
- [43] Siwicki M., *Materiały szkoleniowe*, „Prokuratura i Prawo” 2012/7–8.
- [44] Skowera D., *Akademia cyber-policyjna policja i organizacje międzynarodowe wobec wyzwań przestępczości internetów*, „Zeszyty Naukowe ISP UJ” 2006/2.
- [45] Skrzydło W., *Ustrój polityczny RP*, Kraków 2002.
- [46] Sokolewicz W., *O socjalistycznej koncepcji podstawowych praw i obowiązków obywateli*, „Studia prawnicze” 1978/2.
- [47] *Terrorism and Human Rights* <http://www.unhchr.ch/terrorism/index.html> (odczyt z dnia 17.08.2010 r.)
- [48] Wiśniewski L., *Prawo a wolność człowieka – pojęcie i konstrukcja prawna*, [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, red. Wiśniewski L., Warszawa 1997.
- [49] Zakrzewski W., *Zakres przedmiotowy i formy działalności prawotwórczej*, Warszawa 1979.
- [50] Sprawa Clauhal v. Wielka Brytania, 15 listopada 1966.
- [51] Sprawa Aksoy v. Turcja 18 grudnia 1966.
- [52] Sprawa Irlandia v. Wielka Brytania, 18 stycznia 1978.
- [53] Sprawa Soering v. Wielka Brytania, 7 lipca 1989.
- [54] Sprawa Tomasi v. Francja, 27 sierpnia 1992.
- [55] Wyrok SA w Białymstoku z 5 listopada 2004 roku, I ACa 550/04, OSAB 2005 nr 1 poz. 3.
- [56] Wyrok SN z 16 kwietnia 2004 roku, I CK 495/03 oraz wyrok WSA w Warszawie z 15 kwietnia 2004 r., I SA 2731/03.
- [57] Postanowienie TK z 9 czerwca 2004 r., sygn. Tw 33/03, OTK-B 2004 nr 4/227.
- [58] Wyrok SN z 25 stycznia 2005 roku, II PK 152/04, OSNP 2005 nr 17 poz. 266.
- [59] Wyrok TK z 4.05.2004 r., sygn. K 8/03, OTK-A 2004 nr 5 poz. 37.
- [60] <http://wiadomosci.wp.pl/kat,1020229,title,Zamachowiec-na-zleczenie-Czy-przyszlosc-terroryzmu-to-male-grupy-zwerbowane-na-Zachodzie,wid,15365996,wiadomosc.html> (dostęp: 26.02.2013).

#### **PROTECTING THE RIGHTS OF THE UNIT VS. A PROBLEM OF CYBERTERRORISM**

The global network is gaining the greater extent, the virtual world is growing faster and faster and becomes similar to the real world. Therefore, many phenomena are transferred from the real world to the network. This situation also applies to crime or terrorism. Today, they change their faces, using the gains of the information society. The main article in the network is information. The dissemination of information by network follows immediately. The network is, therefore, an ideal place of modern information exchange between diverse groups and communities. The aim of this article is to present how significant area of the modern state activity is cyber security, which refers to new sphere of human activity, which is cyberspace, and cannot be accounted in the traditional framework. While ensuring the safety and protection is an extremely important area of activity of the state and its bodies, the protection measures of security are varied and depend on the specific security risks. The appearance of the cybersecurity problem and its protection is thus the result of more and



wider understanding of the classical human security. The author tries in his article to draw attention to the fact that in the modern world, security is recognized not only in the military and political spheres. The security is considered both in the context of the phenomena of global, European, national, as well as in the context of the problems of individual citizens.

**Keywords:** cyberterrorism, counter-terrorism policy, human rights, protection of individual rights.

DOI:10.7862/rz.2014.hss.8

Przesłano do redakcji: czerwiec 2014

Przyjęto do druku: czerwiec 2014