WSPÓŁCZESNE PROBLEMY PRAWA

Tom 2

NADUŻYCIA PRAWA

Pod redakcją naukową
Izabeli Nowickiej
Doroty Mocarskiej

Szczytno 2016

Recenzenci
dr hab. Jacek Dworzecki, profesor WSPol w Szczytnie
dr hab. Katarzyna Laskowska, profesor Uniwersytetu w Białymstoku

Redakcja Wydawcy
Wojciech Pączek
Beata Miszczuk
Robert Ocipiński

Projekt okładki
Agnieszka Kamińska

ISBN 978-83-7462-550-0
e-ISBN 978-83-7462-551-7

Druk i oprawa:
Dział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie
12-100 Szczytno, ul. Marszałka Józefa Piłsudskiego 111
tel. 89 621 51 02, fax 89 621 54 48
e-mail: wwip@wspol.edu.pl
Objętość: 17,43 ark. wyd. (1 ark. wyd. = 40 tys. znaków typograficznych)

Spis treści

Wstęp

Oddajemy w ręce Czytelników kolejną publikację z cyklu *Współczesne problemy prawa*. Tom II z uwagi na konieczność ograniczenia „problemów", które w momencie podejmowania decyzji o realizacji przedsięwzięcia przedstawiciele nauki uznali za najbardziej węzłowe, zyskał podtytuł „Nadużycia prawa". W doktrynie wskazuje się, iż problem nadużycia prawa nie jest zjawiskiem nowym. Kodyfikacje cywilne XIX i XX wieku, które koncepcję praworządności oparły na bazie prawa pozytywnego przy aprioryczny założeniu, że prawo to jest wyczerpujące w stopniu stwarzającym warunki do rozstrzygnięcia każdej sprawy, ukazały złożoność zagadnienia, tym bardziej że istniała możliwość wykorzystania przez podmioty stosujące prawo narzędzi wypracowanych przez metodologię prawa, tj. zasad wykładni prawa, sposobów wypełniania luk prawnych itp.

Nie ulega wątpliwości, że w dobie tak częstych zmian regulacji prawnych tematyka zasługuje na baczniejszą uwagę. Dzięki temu publikacja stała się forum dyskusyjnym w tematyce zjawisk, które wymagają, według wspomnianych przedstawicieli doktryny, stałego monitorowania. Swojego głosu w debacie nad problemami udzielili zarówno „cywilni" nauczyciele akademiccy, jak i ci, którzy naukowe doświadczenia zdobywają w mundurach. W publikacji przeplatają się zagadnienia teoretyczne i praktyczne. Zarówno takie, które odnoszą się do interpretacji nowych regulacji prawnych, jak i tych, które pomimo wieloletniego funkcjonowania w teorii i praktyce nastręczają wielu problemów. Pomimo zawężenia tematyki kwestia nadużycia prawa została omówiona wszechstronnie i wieloaspektowo, na co wskazują tytuły poszczególnych wypowiedzi. Punktem odniesienia, jak daje się zauważyć, jest szeroko rozumiane prawo, ale pozostające w sąsiedztwie kryminologii, socjologii, pedagogiki i psychologii.

dr hab. Izabela Nowicka
dr Dorota Mocarska

dr hab. Tomasz R. Aleksandrowicz

Agresja w cyberprzestrzeni. Problematyka art. 51 Karty Narodów Zjednoczonych. Uwagi *de lege lata* i *de lege ferenda*

Streszczenie. Radykalne zmiany środowiska bezpieczeństwa spowodowały powstanie nowych wyzwań i zagrożeń tworzących sytuacje nieprzewidziane przez obowiązujące prawo międzynarodowe. Zmuszone do reakcji państwa działają w swoistej próżni prawnej, *praeter legem*, w wielu przypadkach wedle zasady *necessitas legem non habet*. Stwarza to ryzyko nadużyć prawa międzynarodowego. Przykładem takiej sytuacji są zagrożenia dla bezpieczeństwa państwa w postaci ataków z cyberprzestrzeni. Powstaje pytanie, czy taki atak może być uznany za formę agresji/napaści zbrojnej w rozumieniu prawa międzynarodowego i czy w związku z tym państwa mają prawo do reakcji w formie samoobrony na podstawie art. 51 Karty Narodów Zjednoczonych. Niniejszy artykuł stanowi próbę rozstrzygnięcia tego problemu na płaszczyźnie *de lege lata* i *de lege ferenda*.

Słowa kluczowe: cyberprzestrzeń, agresja, wojna informacyjna, samoobrona

Abstract. Radical changes in the security environment cause new challenges and threats creating situations that have not been regulated by contemporary international law. States have to react in the *black hole*, *praeter legem*, according to the ancient roman saying *necessitas legem non habet*. Good example of such a situation is an cyber attack threats the security of the state. A problem occurs whether such an attack can be interpreted as an aggression/armed attack and consequently whether a victim state can react in the framework of self-defense as provided for the article 51 of the United Nation Chart. In this part of the book the Author analyses this problem *de lege lata* and puts some proposals *de lege ferenda* as well.

Keywords: cyberspace, aggression, information warfare, selfdefence

Wprowadzenie

Rewolucja technologiczna, a przede wszystkim rozwój technologii informacyjnych, spowodowała jakościowe zmiany w środowisku bezpieczeństwa. Jedną z nich jest powstanie nowych zagrożeń dla bezpieczeństwa państwa, związanych z funkcjonowaniem cyberprzestrzeni i pojawienie się możliwości podejmowania w jej ramach wrogich (szkodliwych) działań. Zagrożenia te wiążą się bezpośrednio z coraz bardziej widocznym uzależnieniem współczesnego państwa i społeczeństwa od technologii informatycznych. Dotyczy to zarówno szeroko rozumianej infrastruktury krytycznej — od systemów zaopatrzenia w wodę czy energię elektryczną, aż po systemy bankowe, jak też sił zbrojnych (systemy dowodzenia i łączności)[1].

[1] Zob. T. Aleksandrowicz, *Świat w sieci. Państwa — społeczeństwa — ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 81 i nast.

Powstawanie społeczeństwa informacyjnego na skutek dokonującej się rewolucji informacyjnej powoduje istotną, a w niektórych parametrach rewolucyjną, zmianę środowiska bezpieczeństwa, charakteru i sposobu rozwiązywania kryzysów, charakteru konfliktów zbrojnych i wojen. „W erze informacyjnej innego sensu nabiera stosowanie przemocy drogą tradycyjnie pojmowanej wojny”[2]. Uznanie informacji za kluczowy element stanowi immanentną cechę współczesnych konfliktów, w których informacja jest wykorzystywana zarówno jako broń, jak i traktowana jako cel.

Piotr Sienkiewicz podejmując próbę konceptualizacji problematyki wojny informacyjnej, za punkt wyjścia przyjmuje pojęcie bezpieczeństwa informacyjnego państwa jako integralnej części bezpieczeństwa narodowego, a następnie zagrożeń informacyjnych[3].

Nie bez powodu zatem coraz większą popularnością — nie tylko wśród teoretyków — cieszy się pojęcie „walki informacyjnej”, nie powinno też dziwić, iż wywodzi się ono z nauk wojskowych. Jak podkreślają Piotr Sienkiewicz i Halina Świeboda, nie istnieje jedna, uzgodniona definicja walki informacyjnej, jednakże w większości proponowanych rozwinięć tego terminu występują wspólne treści. Wszystkie one sprowadzają się do postrzegania walki informacyjnej jako konfliktu, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią, a zarazem obejmuje on fizyczne niszczenie infrastruktury, wykorzystywanej przez przeciwnika do działań operacyjnych. „Obecnie słusznie uważa się, że ‘*cyberwar*’, ‘*infowar*’, walka informacyjna, cyberterroryzm, ‘*netwar*’, informacyjni wojownicy, informacyjna dominacja, obrona w cyberprzestrzeni (‘*cyberspace defence*’) czy informacyjny chaos to tylko neologizmy, dotyczące tego samego, ale bardzo szerokiego pojęcia wojny ery informacyjnej (‘*information age warfare*’)”[4].

---

[2] B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 218.

[3] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, s. 373–374, <http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf>, dostęp: 5 kwietnia 2012 r.

[4] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa — zjawisko walki informacyjnej* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 80 i nast. Autorzy zamieścili w cytowanym artykule przegląd definicji walki informacyjnej i działań informacyjnych. Zob. też P. Sienkiewicz, *Wizje i modele wojny informacyjnej…*, wyd. cyt.

Cyberprzestrzeń jako środowisko walki i wojny

Nie ulega wątpliwości, iż cyberprzestrzeń musi być traktowana jako środowisko walki, w którym operuje nowy rodzaj sił zbrojnych — wojska informacyjne (cybernetyczne)[5]. W znaczeniu militarnym cyberprzestrzeń oznacza zatem środowisko, w którym prowadzone są działania wspomagające toczący się konflikt zbrojny, nakierowana na zniszczenie lub modyfikację systemów informacyjnych przeciwnika, jak też ochronę własnych systemów informacyjnych[6]. Można zatem stwierdzić, iż wojna cybernetyczna oznacza prowadzenie walki informacyjnej w cyberprzestrzeni. Oznacza to atakowanie systemów dowodzenia i kierowania przeciwnika, logistyki, transportu, rozpoznania, ostrzegania etc.; w opracowaniach RAND Corp. traktowana jest jako konflikt o wysokiej intensywności[7].

W literaturze przedmiotu pojawia się także kategoria *cyberkonfliktu* definiowanego jako konflikt „angażujący różne systemy ludzi, rzeczy, procesów i postrzegania, które związane są z sieciami komputerowymi, choć niekoniecznie całkowicie skomputeryzowane. Konfliktem cybernetycznym będzie zatem każdy konflikt, w którym sukces lub porażka są dla większości jego uczestników uzależnione od działań prowadzonych w sieciach komputerowych"[8]. Konflikt cybernetyczny może przybrać formę aktywizmu (niedestrukcyjna działalność informacyjno-propagandowa, np. na forach internetowych, czatach, portalach społecznościowych), haktywizmu (stanowiącego kombinację aktywizmu i działań zakłócających funkcjonowanie określonych systemów komputerowych, np. poprzez blokowanie dostępu do serwerów) lub cyberterroryzmu — politycznie motywowanego ataku na komputery, sieci lub systemy informatyczne w celu zniszczenia

[5] W ten sposób traktuje to m.in. *Wizja Sił Zbrojnych RP — 2030*, wg której wojska informacyjne stanowią odpowiedź na przeniesienie części przyszłej walki w sferę informacyjną (elektroniczną, psychologiczną i medialną). *Wizja Sił Zbrojnych RP — 2030*, s. 13, 14, 23–25, <http://www.wp.mil.pl/pliki/File/Wizja_SZRP_2030.pdf>, dostęp: 6 kwietnia 2012 r.

[6] Zob. T. Jemioło, P. Sienkiewicz (red.), *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka),* t. I, *Raport z badań*, Warszawa 2004, s. 74–75; por. K. Liedel, P. Piasecka, *Wojna cybernetyczna — wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1(17), s. 17.

[7] Zob. J. Arquilla, D. Ronfeldt, *Cyberwar is Coming!* [w:] *In the Athena's Camp: Preparing for Conflict in the Information Age*, RAND Corp., Santa Monica 1993, s. 30.

[8] K. Liedel, P. Piasecka, *Wojna cybernetyczna…*, wyd. cyt., s. 17.

infrastruktury i wymuszenia na rządzie lub organizacji określonego działania lub zaniechania)[9].

Kwestia przeprowadzenia granicy pomiędzy *cyberkonfliktem* a *cyberwojną* pozostaje otwarta; granica ta jest rozmyta, płynna i — jak zauważa James A. Lewis[10] — jest decyzją polityczną. Dokonując takiego rozróżnienia trzeba brać pod uwagę podmiot dokonujący ataku (inna będzie ocena działania pojedynczego hakera włamującego się np. na stronę internetową Pentagonu czy Centralnej Agencji Wywiadowczej w celu umieszczenia na witrynie internetowej obraźliwego napisu, np. w proteście przeciwko określonemu zjawisku[11], inna zaś w przypadku fali ataków typu *Distributed Denial of Service* paraliżujących w kwietniu i maju 2007 r. sieć internetową w Estonii, uniemożliwiając korzystanie z usług elektronicznych)[12]. Drugim czynnikiem jest skala zniszczeń i wrażliwość danych, które zostały zniszczone lub wykradzione. Ataki na systemy dowodzenia bez wątpienia uznane zostałyby za akt wojny, natomiast włamania na serwery firm

[9] Zob. tamże, s. 18.

[10] J.A. Lewis, *Treshold for Cyberwar*, Center for Strategic and International Studies, 2010, <http://csis.org/files/publication/101001_ieee_insert.pdf>, dostęp: 6 kwietnia 2012 r.

[11] Taki charakter miały np. ataki DDoS w styczniu 2012 r. przeciwko serwerom rządowym i sejmowym w Polsce — była to forma protestu przeciwko planom ratyfikacji porozumienia ACTA, które — zdaniem protestujących — miało stanowić zagrożenie dla wolności w Internecie. Zob. np. *Walka polityczna czy terroryzm?*, <http://www.computerworld.pl/news/380025_1/Walka.polityczna.czy.terroryzm.html>, dostęp: 6 kwietnia 2012 r.; por. E. Bendyk, *Bunt sieci*, Warszawa 2012.

[12] Atak ten był dokonany prawdopodobnie na zlecenie władz Federacji Rosyjskiej. Zob. M. Terlikowski, *Ataki elektroniczne na Estonię. Implikacje dla bezpieczeństwa międzynarodowego i Polski*, „Polski Przegląd Dyplomatyczny" 2007, t. 7, nr 4(38); tenże, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne…*, wyd. cyt., s. 107–108. O ile w przypadku ataków na Estonię można żywić wątpliwości co do podmiotu atakującego, o tyle w przypadku ataków na serwery amerykańskiej firmy zajmującej się bezpieczeństwem komputerowym RSA (marzec 2011 r.) czy włamań do 71 sieci komputerowych rządowych, biznesowych i organizacji międzynarodowych (sierpień 2011 r.), specjaliści jednoznacznie wskazują na Chiny. Zob. A. Segal, *Chinese Computer Games. Keeping Safe in Cyberspace*, "Foreign Affairs", March/April 2012, s. 14 i nast. Na temat zagrożenia w cyberprzestrzeni ze strony Chin także Ł. Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Kraków 2009, s. 230.

komercyjnych i kradzież danych rozpatrywano by w kategoriach przestępstwa popełnionego z chęci zysku[13].

Oznacza to ekspansję i eskalację konfliktów poza tradycyjnie rozumiane pole walki[14]. Siłą rzeczy — wobec traktowania celów miękkich już nie tyle na równi z celami militarnymi, co wręcz w kategoriach priorytetów — oznacza to radykalne zwiększenie zagrożeń dla ludności cywilnej, katastrof różnego typu (także cywilizacyjnych, jak np. uszkodzenie sieci teleinformatycznych czy energetycznych) i zwiększenie liczby ofiar w ludziach i strat materialnych[15]. Leon Panetta, jako dyrektor Centralnej Agencji Wywiadowczej, przestrzegał przed tego typu zagrożeniami dla bezpieczeństwa USA, mówiąc wręcz o zagrożeniu „elektronicznym Pearl Harbour"[16]. Jest też oczywiste, iż możliwości, jakie stwarza cyberprzestrzeń wykorzystywane są również w celach wywiadowczych[17].

Wydaje się, iż jeśli celem działań jest pozbawienie przeciwnika zdolności do reagowania militarnego (np. poprzez zniszczenie systemów dowodzenia i łączności) to można uznać za zasadne stosowanie pojęcia cyberwojny. Co prawda, rządzi się ona specyficznymi zasadami, lecz przecież działania wojenne prowadzone w pozostałych środowiskach walki także mają swoją specyfikę. Można też dodać, że działania w cyberprzestrzeni plasują się na granicy pomiędzy wojną a kryzysem.

Ranga i znaczenie konfliktów toczonych w cyberprzestrzeni i związanych z nimi zagrożeniami dla bezpieczeństwa państwa — choćby

[13] Na temat tego rodzaju przestępczości zob. np. K. Poulsen, *Haker. Prawdziwa historia szefa cybermafii*, Kraków 2011, passim.

[14] T. Aleksandrowicz, *Świat w sieci…*, wyd. cyt. s. 109 i nast.

[15] Zob. D.E. Hoffman, *The New Virology*, „Foreign Policy" March/April 2011, <http://www.foreignpolicy.com/articles/2011/02/22/the_new_virology?page=full>, dostęp: 29 października 2011 r. Zob. np. hipotetyczny scenariusz cyberataku Chin na USA opracowany przez Christophera Bronka, <http://www.idg.pl/news/368859/jak.moglaby.wygladac.cyberwojna.chin.z.usa.html>, dostęp: 27 października 2011 r.

[16] <http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/t/story?id=12888905>, dostęp: 15 kwietnia 2012 r.

[17] Otwarcie mówią o tym przedstawiciele amerykańskiej administracji, wskazując jednoznacznie na aktywność w tym zakresie Chin i Federacji Rosyjskiej. Zob. Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Select Committee on Intelligence, James R. Clapper, Director of National Intelligence, January 31, 2012, Office of the Director of National Intelligence of the United States of America, <http://intelligence.senate.gov/120131/clapper.pdf>, dostęp: 6 kwietnia 2012 r.

w kontekście rozwoju technologicznego i coraz większego znaczenia informacji w formie cyfrowej — będzie w dającej się przewidzieć przyszłości wzrastać[18]. W tym kontekście należy wskazać na kilka elementów.

Po pierwsze, nie ulega wątpliwości, że walka informacyjna w cyberprzestrzeni prowadzona w ramach toczącego się konfliktu zbrojnego jest immanentną częścią tego konfliktu.

Po drugie, coraz większego znaczenia nabiera walka informacyjna prowadzona w cyberprzestrzeni samoistnie, tj. w warunkach pokoju — bez konfliktu z wykorzystaniem orężnych środków walki. W takiej walce cele nie mają bezpośredniego znaczenia militarnego (jak np. w przypadku konfliktu zbrojnego cybernetyczne ataki na systemy dowodzenia i łączności przeciwnika), lecz należą do kategorii infrastruktury krytycznej państwa[19]. Tego typu ataki mogą wywołać zagrożenia dla bezpieczeństwa międzynarodowego (globalnego bezpieczeństwa informacyjnego), destabilizację infrastruktury krytycznej, zakłócenia w funkcjonowaniu administracji publicznej, straty gospodarcze (zahamowanie rozwoju firm i przedsiębiorstw) czy nawet straty osobiste obywateli[20]. Istotne znaczenie ma kwestia skali ataku i strat.

Taki stan rzeczy znalazł swoje odbicie w oficjalnych dokumentach strategicznych wielu państw, w tym Rzeczypospolitej Polskiej. Strategia Bezpieczeństwa Narodowego RP wyraźnie stanowi, że „wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych oraz cyberwojna, rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa

[18] T. Aleksandrowicz, *Świat w sieci…*, wyd. cyt., s. 171 i nast.

[19] W polskim ustawodawstwie infrastruktura krytyczna definiowana jest jako systemy i 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. Pojęcie infrastruktury krytycznej obejmuje następujące systemy: zaopatrzenie w energię i paliwa, łączności i sieci teleinformatyczne, finansowe; zaopatrzenia w żywność i w wodę, ochrony zdrowia, transportowe i telekomunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych, ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym, DzU nr 89, poz. 590.

[20] Zob. P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne…*, wyd. cyt., s. 90.

domeny cyfrowej na bezpieczeństwo ogólne kraju. Przy rosnącym uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw". Ponieważ „cyberprzestrzeń stała się kolejnym środowiskiem walki zbrojnej", Siły Zbrojne RP „muszą dysponować zdolnościami defensywnymi i ofensywnymi w tej sferze tak, aby realizować funkcję odstraszania potencjalnego przeciwnika. W szczególności muszą one być gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na większą skalę w razie cyberkonfliktu lub cyberwojny"[21]. Pojęciem cyberwojny posługuje się także Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej[22].

Co więcej, reakcje zbrojne na ataki cybernetyczne są już przewidywane w strategiach państw, np. Stany Zjednoczone zastrzegają sobie prawo do reakcji na tego typu zagrożenia wszelkimi koniecznymi i odpowiednimi środkami[23]. W polskim ustawodawstwie ataki z cyberprzestrzeni zostały potraktowane na równi ze zbrojną napaścią na terytorium Rzeczypospolitej Polskiej czy atakami terrorystycznymi, jako zagrożenie zewnętrzne państwa uzasadniające wprowadzenie stanu wojennego[24].

---

[21] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014, pkt 31 i 77.

[22] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, pkt 14, 23.

[23] International Strategy for Cyberspace. Prosperity, Security and Openess in the Networked World. May 2011, <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>, dostęp: 23 kwietnia 2012 r.

[24] Art. 2 ust. 1 ustawy z 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach naczelnego dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, DzU nr 156, poz. 1301 z późn. zm. Ust. 1a przywołanej ustawy precyzuje, iż przez zewnętrzne zagrożenie państwa, o którym mowa w ust. 1, rozumie się celowe działania, godzące w niepodległość, niepodzielność terytorium, ważny interes gospodarczy Rzeczypospolitej Polskiej lub zmierzające do uniemożliwienia albo poważnego zakłócenia normalnego funkcjonowania państwa, podejmowane przez zewnętrzne w stosunku do niej podmioty. Analogiczne rozwiązanie znalazło się także w ustawie o stanie wyjątkowym, DzU z 2002 r., nr 113 poz. 985 — art. 2 ust. 1 stanowi, iż w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu do prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego.

Stare pojęcia — nowe znaczenia

Zarysowane powyżej zmiany skłaniają wielu teoretyków i praktyków do dokonania rewizji szeregu pojęć, które w nauce były od dawna ugruntowane, od niedawna zaś ich konotacje zaczęły budzić wątpliwości. Operowanie nieostrymi pojęciami, jak słusznie zauważa Bolesław Balcerowicz, nie służy dobremu komunikowaniu się[25]. Przegląd literatury dowodzi, że bardzo często pojęciami takimi jak wojna czy konflikt zbrojny posługiwano się w pewnej mierze intuicyjnie, dodając różnego rodzaju przymiotniki (np. zimna wojna) czy tworząc *de facto* nowe pojęcia nie podając ich precyzyjnej definicji (np. *Global War on Terror*)[26]. Wywoływało to (i wywołuje nadal) wiele nieporozumień, terminologiczny i metodologiczny zamęt. Trudno np. zgodzić się z tezą jednego z badaczy głoszącą, iż „współczesna (XXI wiek) wojna legalizuje terroryzm jako równoprawną z innymi dotychczas uznawanymi za dopuszczalne metodę prowadzenia konfliktu zbrojnego" i uznającą terroryzm za „nowy paradygmat wojny"[27].

Stanisław Koziej w nowym wydaniu *Teorii sztuki wojennej* stwierdza wprost, że „zmiany warunków polityczno-militarnych oraz gwałtowny rozwój środków walki zbrojnej wprowadzają wiele nowych elementów do całej sztuki wojennej. Pojawia się potrzeba ponownego przejrzenia i skorygowania niektórych istniejących do tej pory poglądów, koncepcji, ustaleń. Dotyczy to także sfery pojęciowej. Niektóre z pojęć zmieniają swoje znaczenie, mają też miejsce całkiem nowe zjawiska, które muszą znaleźć swoje odzwierciedlenie w terminologii"[28]. Wtóruje mu Bolesław Balcerowicz, postulując dokonanie przeglądu znaczeniowego takich pojęć, jak konflikt między państwami, przemoc zbrojna, organizacja czy siły zbrojne[29].

Przegląd literatury przedmiotu pod kątem rozumienia pojęcia wojny i konfliktu zbrojnego pozwala na postawienie wniosku, iż zasadniczym elementem tych definicji jest obecność w nich „krwawej walki zbrojnej toczonej przez zorganizowane siły", „akt zorganizowanej przemocy zbrojnej", „walka zbrojna rozumiana jako bezpośrednie starcie zgrupowań wojsk; destrukcyjne oddziaływanie za pomocą środków rażenia". To, rzecz jasna, Clausewitzowskie rozumienie wojny, podkreślające związek między

[25] B. Balcerowicz, *O wojnie, o pokoju. Między esejem a traktatem*, Warszawa 2013, s. 81.

[26] Zob. M.L. Dudziak, *War Time. An Idea, It's History, It's Consequences*, Oxford 2012.

[27] K. Karolczak, *Terroryzm. Nowy paradygmat wojny*, Warszawa 2010, s. 17.

[28] S. Koziej, *Teoria sztuki wojennej*, Warszawa 2011, s. 9.

[29] B. Balcerowicz, *O wojnie, o pokoju…*, wyd. cyt., s. 85–86.

polityką, państwem i wojną. Równocześnie podkreśla się element prawny: wojna rozumiana jest jako stan prawny, pozwalający dwóm lub większej liczbie wrogich grup rozwiązywać konflikt poprzez użycie siły zbrojnej. Pomimo wszelkich różnic, pomiędzy podejściem Clausewitza i Sun Tzu, także ten ostatni kojarzy wojnę ze starciem zbrojnym (choć ponad nie stawia sztukę zwodzenia, strategię, konfrontację i walkę umysłów). Co więcej, następuje powrót do postulatów strategicznych Sun Tzu, który wojnę rozumianą jako krwawe starcia zbrojne uważał za ostateczność. Jeśli zatem uznamy, że celem wojny jest narzucenie swojej woli przeciwnikowi poprzez pozbawienie go zdolności do walki, to trzeba wziąć pod uwagę, iż dzisiejsze technologie pozwalają na osiągnięcie tego celu „bez jednego wystrzału". Charakter wojny jest bowiem zmienny, niezmienna pozostaje tylko jej istota.

Problem pogłębia fakt, iż pojęcia wojny, konfliktu zbrojnego czy użycia siły pozostają niezdefiniowane również na gruncie prawa międzynarodowego publicznego (tak normatywnie, jak i doktrynalnie). Jak słusznie zauważa Patrycja Grzebyk, choć Karta Narodów Zjednoczonych używa pojęć agresji, siły, samoobrony, zbrojnej napaści czy interwencji, to jednak żadnego z nich nie zdefiniowano. Był to zabieg celowy, zakładano bowiem, że Rada Bezpieczeństwa będzie podejmowała decyzje *ad casum* i dokona odpowiednich kwalifikacji[30]. Konsekwencją takiego podejścia jest Definicja agresji. 14 grudnia 1974 r. Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych przyjęło rezolucję pod nazwą Definicja agresji[31]. Zgodnie z art. 1 agresja polega na użyciu siły zbrojnej przez państwo przeciwko suwerenności, terytorialnej integralności lub politycznej niepodległości innego państwa, lub w jakikolwiek inny sposób niezgodny z Kartą Narodów Zjednoczonych. Definicja opiera się na zasadzie *first strike* — co oznacza, iż pierwsze użycie siły zbrojnej będzie uznane za popełnienie aktu agresji. Jednakże ocena ta może się zmienić, jeśli Rada Bezpieczeństwa dojdzie do wniosku, że uznanie danego aktu za agresję byłoby nieuzasadnione w świetle innych istotnych okoliczności. W samej definicji wymienia się jako taką okoliczność „wystarczająco doniosłą wagę" samego aktu i jego konsekwencji, co oznacza, że np. incydent graniczny, nawet z użyciem siły zbrojnej, nie będzie uznany za agresję. Jednakże, zakres włączeń również nie nosi charakteru zamkniętego, Rada może bowiem wziąć pod uwagę także inne okoliczności.

[30] P. Grzebyk, *Odpowiedzialność karna za zbrodnię agresji*, Warszawa 2010, s. 45, 46, 86.

[31] UN Doc. A/RES/3314/XXIX.

Definicja potwierdza, iż żadne względy, jakiejkolwiek byłyby natury, czy to polityczne, gospodarcze, wojskowe czy inne, nie mogą stanowić usprawiedliwienia agresji, której dokonanie pociąga za sobą odpowiedzialność na gruncie prawa międzynarodowego. Wojna agresywna została uznana *expressis verbis* za zbrodnię przeciwko ludzkości, czego konsekwencją jest m.in. fakt, iż żadne nabytki terytorialne lub specjalne korzyści wynikające z agresji nie są i nie mogą być uznane jako zgodne z prawem (art. 5 Definicji agresji).

Art. 3 Definicji zawiera katalog czynów uznawanych za akt agresji:

— inwazja lub atak na terytorium innego państwa przy pomocy sił zbrojnych jakiegoś państwa lub każda wojskowa okupacja, chociażby tymczasowa, wynikająca z takiej inwazji lub ataku, lub wszelka aneksja terytorium innego państwa lub jego części przy użyciu siły;
— bombardowanie terytorium jakiegoś państwa przez siły zbrojne innego państwa;
— blokada portów lub wybrzeży jakiegoś państwa przez siły zbrojne innego państwa;
— atak za pomocą sił zbrojnych jakiegoś państwa na siły lądowe, morskie lub powietrzne, lub flotę morską lub powietrzną innego państwa;
— użycie sił zbrojnych jednego państwa znajdującego się na terytorium innego państwa za zgoda państwa przyjmującego, naruszające warunki ustanowione w porozumieniu lub wszelkie przedłużenie ich obecności na takim terytorium poza okres wygaśnięcia porozumienia;
— działalność jakiegoś państwa, które oddało do dyspozycji innego państwa swe terytorium, zezwalająca na użycie go przez to państwo dla popełnienia aktu agresji przeciwko państwu trzeciemu;
— wysyłanie przez lub w imieniu jakiegoś państwa uzbrojonych band, grup, sił nieregularnych lub najemnych, które dopuszczają się aktów zbrojnych o takiej doniosłości przeciwko innemu państwu, że oznaczają akty wyżej wymienione lub oznaczają mieszanie się do nich.

Nie jest to katalog zamknięty, bowiem Rada Bezpieczeństwa może uznać za agresję także inne czyny (art. 4). To bardzo ważne upoważnienie, bowiem analiza czynów zawartych w katalogu prowadzi do wniosku, iż podstawowym i jedynym podmiotem stwarzającym zagrożenie aktem agresji jest państwo, zaś ostatni punkt należy traktować jako opis działań nazywanych w doktrynie *proxy warfare*. Oznacza to, że Definicja agresji nie obejmuje aktów walki popełnianych przez podmioty niepaństwowe, działające w oderwaniu od państwa, a więc nie na jego zlecenie, nie w jego imieniu i nie wspierane przez państwo.

Warto w tym miejscu podkreślić, że w zasadzie do dziś nie rozstrzygnięto, czy pod pojęciem siły należy rozumieć wyłącznie siłę zbrojną, czy też różnego rodzaju naciski pozamilitarne (np. presja ekonomiczna i/lub polityczna). Co więcej, w prawie międzynarodowym niemal nie występuje pojęcie wojny, bowiem konwencje (i sama Karta Narodów Zjednoczonych) posługują się sformułowaniem „użycie siły zbrojnej", które również pozostaje niezdefiniowane[32]. Dotyczy to także Paktu Północnoatlantyckiego i Unii Europejskiej oraz przyjmowanych przez te organizacje dokumentów.

Kluczowy dla NATO jest art. 5 Definicji[33] określający zasady działania Paktu w przypadku napaści zbrojnej. Zbrojna napaść na jedno lub kilka państw członkowskich „będzie uważana za napaść przeciwko nim wszystkim". Jeśli taka napaść zbrojna nastąpi, każde państwo członkowskie, wykonując swoje prawo do indywidualnej lub zbiorowej samoobrony uznane w art. 51 Karty Narodów Zjednoczonych, udzieli pomocy państwu lub państwom napadniętym, podejmując natychmiast indywidualnie i w porozumieniu z innymi państwami członkowskimi taką akcję, jaką uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego. Ponadto, o każdej takiej napaści zbrojnej i o wszystkich środkach zastosowanych w jej wyniku zostanie bezzwłocznie powiadomiona Rada Bezpieczeństwa. Środki takie zostaną zaniechane, gdy tylko Rada Bezpieczeństwa podejmie działania konieczne do przywrócenia i utrzymania międzynarodowego pokoju i bezpieczeństwa.

Podobne rozwiązania zostały przyjęte w ramach Unii Europejskiej w traktacie lizbońskim i stanowią obecnie część Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB), a w tym Wspólnej Polityki Bezpieczeństwa i Obrony (WPZiO)[34]. Art. 42 ust. 7 Traktatu o Unii Europejskiej (TUE) stanowi, iż w przypadku, gdy jakiekolwiek państwo członkowskie stanie się ofiarą zbrojnej napaści na jego terytorium, pozostałe państwa

[32] *Pro domo sua* należy zauważyć, iż w polskim prawodawstwie występuje termin „czas wojny" (w Konstytucji RP, w ok. 40 ustawach i 70 rozporządzeniach), który nie doczekał się definicji normatywnej i budzi wiele wątpliwości interpretacyjnych, zob. M. Surmański, *Pojęcie „czasu wojny" oraz problemy wynikające z jego niedookreśloności w polskim systemie prawnym*, „Bezpieczeństwo Narodowe" 2014, nr II/30, s. 95 i nast.

[33] Tekst polski zob. S. Bieleń (oprac.), *Prawo w stosunkach międzynarodowych. Wybór dokumentów*, Warszawa 2004, s. 340 i nast.

[34] Zob. T. Aleksandrowicz, *Bezpieczeństwo w Unii Europejskiej*, Warszawa 2011, s. 71 i nast.

członkowskie mają w stosunku do niego obowiązek udzielenia pomocy i wsparcia przy zastosowaniu wszelkich dostępnych im środków, zgodnie z art. 51 Karty Narodów Zjednoczonych. Nieco inny charakter nosi klauzula solidarności określona w art. 222 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), która nakazuje zarówno Unii, jak i państwom członkowskim podjęcie wspólnych działań „w duchu solidarności" w przypadku, jeżeli jakiekolwiek państwo członkowskie stanie się przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej, lub katastrofy spowodowanej przez człowieka.

O wojnie nie wspominają także dokumenty określające strategię tych organizacji. W 2003 r. Rada Europejska przyjęła w Brukseli dokument definiujący podstawowe zagrożenia dla bezpieczeństwa europejskiego[35]. W punkcie „Główne zagrożenia" strategia stwierdza, że choć atak na wielką skalę na którekolwiek państwo członkowskie jest mało prawdopodobny, to Europa staje przed nowymi zagrożeniami: bardziej różnorodnymi, mniej widocznymi i mniej przewidywalnymi. Wśród nich dokument wymienia:

— terroryzm, wykazując jednocześnie, że Europa jest zarówno celem, jak i bazą współczesnego terroryzmu, szczególnie motywowanego religijnym fundamentalizmem;
— rozprzestrzenianie broni masowego rażenia, w tym potencjalnie najgorszy scenariusz zakładający, że broń masowego rażenia dostanie się w ręce ugrupowań terrorystycznych;
— konflikty regionalne, zarówno te, które toczą się z dala od Europy (Kaszmir, Półwysep Koreański), jak i te, które mają miejsce blisko jej granic (przede wszystkim Bliski Wschód) oraz tzw. konflikty zamrożone, a więc takie, które znajdują się niejako pod kontrolą, lecz w każdej chwili grożą ponownym wybuchem (np. Kaukaz Północny). Strategia stwierdza w tym punkcie jasno, że wszystkie one wpływają pośrednio i bezpośrednio na interesy Europy, niszcząc życie, infrastrukturę społeczną i fizyczną, zagrażają mniejszościom, podstawowym wolnościom i prawom człowieka prowadząc do ekstremizmu, terroryzmu i niewydolności państwa, otwierając przy tym drogę przestępczości zorganizowanej. Szczególnie niebezpieczne stają się w tym kontekście konflikty rozgrywające się w pobliżu granic UE, bowiem bezpośrednio zagrażają stabilności regionalnej;

[35] *Bezpieczna Europa w lepszym świecie. Europejska Strategia Bezpieczeństwa*, 2003, <http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIPL.pdf>, dostęp: 22 czerwca 2012 r.

— niewydolność państwa, rozumiana jako złe rządy — korupcja, nadużycie władzy, słabe instytucje, brak odpowiedzialności oraz konflikty wewnętrzne. Zapaść państwa — stwierdza Strategia, przytaczając przykłady Somalii, Liberii czy Afganistanu pod rządami talibów, może być związana z takimi zagrożeniami jak: przestępczość zorganizowana, terroryzm, niestabilność regionalna oraz osłabienie ładu globalnego;
— przestępczość zorganizowana. Strategia określa ten czynnik jako wewnętrzne zagrożenie dla bezpieczeństwa państw członkowskich Unii Europejskiej, które nosi istotny wymiar zewnętrzny: transgraniczny nielegalny handel narkotykami, kobietami i bronią oraz przemyt nielegalnych imigrantów, a także — jako nowym wymiarem przestępczości zorganizowanej — piractwem morskim.

Podobne sformułowania znalazły się w Koncepcji Strategicznej NATO z 2010 r.[36] W zawartej w dokumencie ocenie środowiska bezpieczeństwa podkreśla się jego następujące cechy:
— obecnie obszar euroatlantycki jest spokojny i zagrożenie terytorium NATO atakiem konwencjonalnym jest niewielkie. Jest to historyczny sukces polityki silnej obrony, euroatlantyckiej integracji i aktywnego partnerstwa, które wytyczały drogę NATO przez ponad pół wieku;
— konwencjonalne zagrożenie nie może być jednak zignorowane. Wiele regionów i państw na świecie pozyskuje istotne, nowoczesne zdolności wojskowe, a konsekwencje tych działań dla międzynarodowej stabilności i euroatlantyckiego bezpieczeństwa trudno przewidzieć. Dotyczy to między innymi proliferacji pocisków balistycznych, które stwarzają realne i rosnące zagrożenie dla obszaru euroatlantyckiego;
— proliferacja broni nuklearnej i innej broni masowego rażenia oraz środków jej przenoszenia zagraża nieobliczalnymi konsekwencjami dla globalnej stabilności i dobrobytu. W następnej dekadzie proliferacja będzie wyjątkowo ostrym problemem w niektórych najbardziej niestabilnych regionach świata;
— terroryzm stwarza bezpośrednie zagrożenie dla bezpieczeństwa obywateli państw NATO i szerzej dla międzynarodowej stabilności i dobrobytu. Grupy terrorystyczne przenikają i rozprzestrzeniają się na obszarach o strategicznym znaczeniu dla Sojuszu; nowoczesna technologia powoduje wzrost zagrożenia i zwiększa potencjał ataków terrorystycznych, w szczególności gdyby terroryści weszli w posiadanie nuklearnych, chemicznych, biologicznych lub radiologicznych zdolności;

[36] Tekst polski, <http://www.bbn.gov.pl/portal/pl/2/2694/Koncepcja_Strategiczna_NATO__tlumaczenie.html>, dostęp: 10 marca 2011 r.

— brak stabilności lub konflikt poza granicami NATO może bezpośrednio zagrozić bezpieczeństwu Sojuszu, w tym poprzez podsycanie ekstremizmu, terroryzmu i transnarodowych nielegalnych działań, takich jak przemyt broni, narkotyków i ludzi;
— ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej; mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne;
— wszystkie państwa są w coraz większym stopniu zależne od dróg tranzytowych, na których opiera się międzynarodowy handel, bezpieczeństwo energetyczne i dobrobyt. Wymagają one większych międzynarodowych wysiłków, żeby zapewnić ich odporność na atak lub przerwanie. Niektóre państwa NATO staną się bardziej zależne od zagranicznych dostawców energii i w niektórych przypadkach od zagranicznych sieci dostaw i dystrybucji energii. Ponieważ większość światowej konsumpcji jest transportowana na skalę światową, dostawy energii są w coraz większym stopniu narażone na załamania;
— niektóre znaczące trendy związane z technologią — włączając w to rozwój broni laserowej, walkę elektroniczną oraz technologie, hamujące dostęp do przestrzeni kosmicznej, najprawdopodobniej będą w poważny sposób oddziaływać na planowanie wojskowe i operacje NATO;
— kluczowe ograniczenia w dziedzinie środowiska naturalnego i zasobów, włączając w to ryzyka zdrowotne, zmiany klimatu, niedobory wody i wzrastające potrzeby energetyczne, będą dalej kształtowały przyszłe środowisko bezpieczeństwa w dziedzinach zainteresowania NATO oraz będą miały możliwość znacząco wpłynąć na planowanie i operacje NATO.

Prawnomiędzynarodowy wymiar cyberwojny

Uznanie cyberprzestrzeni za środowisko walki/wojny zmusza do postawienia szeregu pytań. Czy możliwa jest wojna samoistna w cyberprzestrzeni, tzn. bez działań stanowiących o klasycznej przemocy zbrojnej?

Innymi słowy — czy wrogie działania podejmowane w cyberprzestrzeni same w sobie stanowią wojnę? Czy programy komputerowe w postaci *malware*, ataki DDoS czy niszczenie danych możemy uznać za środki walki, przemoc zbrojną? A zatem, czy możliwa jest wojna bez krwawej walki zbrojnej, fizycznego starcia dwóch czy więcej przeciwników?[37]

Pierwsze próby rozwiązania tego problemu zostały już podjęte. W 2009 r. *NATO Cooperative Cyber Defence Center of Excellence* (NATO CCD COE) zaprosiło grupę ekspertów prawa międzynarodowego do prac nad określeniem prawnych ram prowadzenia wojny w cyberprzestrzeni. Głównym zadaniem zespołu ekspertów było określenie sposobu zastosowania obowiązujących norm prawa międzynarodowego, zarówno w zakresie *ius ad bellum*, jak i *ius in bello*, do nowego środowiska walki, jakim stała się cyberprzestrzeń[38]. Innymi słowy — dokonanie prawnomiędzynarodowej analizy cyberprzestrzeni i zjawisk w niej zachodzących. Autorzy pomysłu wzorowali się na projektach, których efektami są „Manual on International Law Applicable to Armed Conflicts at Sea"[39] oraz „Manual on International Law Applicable to Air and Missile Warfare"[40].

Zadanie okazało się być bardzo trudne, by nie powiedzieć — karkołomne. Oba opracowania powstały na przełomie stuleci, a więc w sytuacji, której morskie i powietrzne środowiska walki były znane już od dziesiątek lat, istniały normy prawa międzynarodowego — zarówno umownego, jak i zwyczajowego — znajdujące do nich bezpośrednie zastosowanie, istniała też praktyka i orzecznictwo oraz bogata doktryna. W przypadku cyberprzestrzeni mamy diametralnie inną sytuację. Cyberprzestrzeń jest stosunkową nowym środowiskiem, nie tyle opanowywanym (jak w przypadku przestrzeni powietrznej i obszarów morskich), lecz stworzonym przez człowieka, o diametralnie innych cechach, brak jest norm prawa międzynarodowego regulujących jej funkcjonowanie jako środowiska walki, brak również norm odnoszących się do środków i metod walki prowadzonej w jej ramach. Nie istnieje orzecznictwo, a doktryna dopiero zaczyna się tworzyć. Z punktu widzenia przedmiotu badań zespół poruszał się zatem w swoistej próżni prawnej.

---

[37] Zob. T. Aleksandrowicz, *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny* [w:] K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014, s. 45 i nast.

[38] Tamże, s. 49 i nast.

[39] <http://www.icrc.org/ihl/385ec082b509e76c41256739003e636d/7694fe2016f347e1c125641f002d49ce>, dostęp: 8 maja 2013 r.

[40] <http://www.ihlresearch.org/amw/manual/>, dostęp: 8 maja 2013 r.

Zespół ekspercki NATO CCD COE dokonał interpretacji obowiązujących norm prawa międzynarodowego, dążąc do ustalenia czy, które z nich i w jaki sposób można zastosować do sfery cyberprzestrzeni. Efektem tych prac stał się „Tallinn Manual on the International Law Applicable to Cyber Warfare"[41].

Za punkt wyjścia twórcy „Tallinn Manual" przyjęli koncepcję suwerenności terytorialnej państwa. Rzecz jasna, trudno odnieść ją do cyberprzestrzeni jako takiej, znajduje ona wszakże zastosowanie do infrastruktury (tj. serwerów, komputerów etc.) znajdujących się na terytorium danego państwa, które ponosi odpowiedzialność za ich bezpieczeństwo i wykorzystanie zgodne z prawem międzynarodowym. Stąd i jurysdykcja państwa: wobec sprawców przebywających na jego terytorium, wobec czynów dokonanych przeciwko infrastrukturze znajdującej się na jego terytorium i tzw. jurysdykcja eksterytorialna, która jest ustanawiana w związku z narodowością sprawcy, narodowością ofiary, naruszeniem bezpieczeństwa narodowego i naruszeniem powszechnie obowiązujących norm prawa międzynarodowego (np. złamanie zakazu agresji czy dokonanie aktu terroryzmu międzynarodowego).

Drugim założeniem jest uznanie, iż cyberoperacja może stanowić i może być traktowana jako użycie siły w rozumieniu Karty Narodów Zjednoczonych wówczas, gdy jej efekty są porównywalne z konwencjonalnym użyciem siły, a więc ze stratami fizycznymi (utrata życia lub zdrowia przez ludzi, straty materialne). Konsekwencją takiego stanowiska jest uznanie, że tzw. operacje niedestrukcyjne (np. propagandowe czy szpiegowskie) nie mieszczą się w kategoriach użycia siły. Jeśli przynoszą efekty fizyczne — podlegają obowiązującemu prawu międzynarodowemu regulującemu kwestie *ius ad bellum*, mają do nich zatem zastosowanie normy dotyczące agresji, zakazu użycia siły, samoobrony w trybie art. 51 Karty Narodów Zjednoczonych. Równocześnie — jeśli cyberoperacje spełniają kryterium użycia siły i są prowadzone w ramach konfliktu zbrojnego — podlegają one międzynarodowemu prawu konfliktów zbrojnych, czyli *ius in bello*. Twórcy „Tallinn Manual" precyzują, iż *casus* Estonii *ius in bello* nie podlegał (brak było konfliktu zbrojnego), w przeciwieństwie do ataków cybernetycznych towarzyszących konfliktowi rosyjsko-gruzińskiemu w 2008 roku.

[41] *Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts by the Invitation of the NATO Cooperative Cyber Defence Center of Excellence*, M.N. Schnitt (general editor), Cambridge University Press, 2013. Tekst dostępny również na stronach internetowych NATO CCD COE, <http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=window>, dostęp: 8 maja 2013 r.

Uwagi *de lege lata* i *de lege ferenda*

Powyższe rozważania pozwalają na postawienie tezy, iż obowiązujące prawo międzynarodowe nie zawiera postanowień uwzględniających radykalne zmiany, jakie w ostatnich dwudziestu latach nastąpiły w środowisku bezpieczeństwa. Zmusza to poszczególne państwa do dokonywania ryzykownych reinterpretacji istniejących norm prawnych lub też podejmowania działań wedle zasady głoszącej, iż konieczność nie zna prawa. W obu przypadkach państwa mogą narażać się na zarzut naruszenia prawa międzynarodowego, zarówno jeśli chodzi o użycie siły, jak i sposób prowadzenia konfliktu zbrojnego i stosowane w jego ramach środki. Co więcej, prawo międzynarodowe z trudnością pozwala na dokonanie kwalifikacji środków walki powstałych w rezultacie rewolucji w sprawach wojskowych, w tym także, jeśli kwestie te dotyczą działań podejmowanych w cyberprzestrzeni. Można zatem stwierdzić, iż co najmniej część współczesnych konfliktów toczy się w swoistej próżni prawnej. Nie powinno to dziwić, skoro podstawowe normy prawa międzynarodowego odnoszące się do omawianych kwestii powstały, *de facto*, w połowie XX stulecia, a ich rozwój ukierunkowany był przede wszystkim na wzmocnienie ochrony praw człowieka i ofiar konfliktów zbrojnych.

Możliwości podjęcia odwetu o charakterze *stricte* militarnym czy jedynie cybernetycznym wywołują wątpliwości. Nie jest bowiem jasne (przynajmniej nie wynika to *explicite* z obowiązującego prawa międzynarodowego) czy atak cybernetyczny na infrastrukturę krytyczną można uznać za uzasadnienie do podjęcia działań w trybie art. 51 Karty NZ, a zatem działań zbrojnych w samoobronie. Bez wątpienia musiałby to być atak poważny, tj. nie incydent, lecz działanie pociągające za sobą znaczne straty w sferze materialnej i ofiary w ludziach (np. doprowadzenie do wybuchu elektrowni jądrowej[42]). Konsekwencją tego byłoby uznanie takiego ataku za napaść zbrojną, a co najmniej za zagrożenie dla międzynarodowego pokoju i bezpieczeństwa. W dzisiejszym stanie prawnym mogłaby to uczynić jedynie Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych, tak jak stało

[42] Taka próba została podjęta wobec irańskiej elektrowni jądrowej i polegała na przejęciu kontroli nad systemami sterowania za pomocą złośliwego programu (robaka) Stuxnet. Ostatecznie okazała się nieudana, nie wiadomo też czy jej celem było wywołanie niekontrolowanej reakcji łańcuchowej i wybuchu, choć nie można takiej możliwości wykluczyć. Zob. K. Pielesiek, *Światowa cyberwojna — nie zobaczysz jej w telewizji*, „Gazeta pl. Technologie", 19 kwietnia 2012 r., <http://technologie.gazeta.pl/internet/1,104530,11557651,Swiatowa_cyberwojna___nie_zobaczysz_jej_w_telewizji.html>, dostęp: 19 kwietnia 2012 r.

się to po zamachach 11 września 2001 odnośnie do ataków terrorystycznych. Można zatem uznać, że klasyczna reakcja militarna na samoistny atak cybernetyczny podjęta w ramach art. 51 Karty NZ mogłaby zostać uznana za nadużycie prawa do samoobrony. Jednakże gdyby taki atak wymierzony był w systemy dowodzenia i łączności sił zbrojnych, państwo-ofiara mogłoby uznać go za przygotowanie do klasycznego ataku militarnego, co stanowi uzasadnienie do podjęcia antycypacyjnej akcji zbrojnej typu *preemptive*. Operacja zbrojna uprzedzająca polega na podjęciu działań militarnych przeciwko potencjalnemu napastnikowi w sytuacji, w której mamy do czynienia z bezpośrednią groźbą napaści zbrojnej i wysokim prawdopodobieństwem jej dokonania, koniecznością podjęcia natychmiastowych działań, potencjalnie wysokimi stratami, jakie w rezultacie ataku poniosłoby państwo-ofiara oraz brakiem innych, w tym dyplomatycznych, możliwości działania na rzecz uniknięcia zastosowania siły zbrojnej. Działania podejmowane w ramach takiej operacji uprzedzającej nie mogą być „nierozsądne" i „przesadne". Kryteria te wywodzą się jeszcze ze sprawy ostrzelania statku *Caroline* — ostatecznie zbrojna akcja wojsk brytyjskich na terytorium Stanów Zjednoczonych została podjęta w celu zapobieżenia (uprzedzenia) kolejnych dostaw broni dla zbuntowanych przeciw Koronie mieszkańców Kanady[43].

Kryteria zastosowania operacji uprzedzającej nie są jasno sformułowane i wywodzą się z międzynarodowego prawa zwyczajowego. W doktrynie[44] najczęściej wymienia się następujące:

[43] Dotyczyła ona zniszczenia przez dwóch obywateli brytyjskich statku *Caroline* zacumowanego w jednym z portów Stanów Zjednoczonych. Statek ten był wykorzystywany do transportu broni i ochotników do Kanady, w której trwało antybrytyjskie powstanie. Już po zakończeniu incydentu amerykański sekretarz stanu w nocie do swojego brytyjskiego odpowiednika stwierdził, iż każde państwo ma prawo do zastosowania samoobrony, w sytuacji, gdy istnieje „pilna i nagląca" konieczność tego typu działań, niepozostawiająca „żadnego wyboru co do możliwych środków ani czasu na rozważania". Ponadto, działania podejmowane w samoobronie nie mogą być „nierozsądne" i „przesadne", bowiem „samo działanie, usprawiedliwione koniecznością samoobrony, musi być ograniczone do tej konieczności i bez żadnej wątpliwości utrzymane w jej granicach". Zasady te zostały wówczas uznane przez rząd brytyjski i są obecnie uznawane za część międzynarodowego prawa zwyczajowego. Zob. M.N. Shaw, *Prawo międzynarodowe*, Warszawa 2006, s. 647. Potwierdził to w swoim orzecznictwie Międzynarodowy Trybunał Sprawiedliwości w sprawie *Nicaragua v. USA*. Zob. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA),* <http://www.icj-cij.org/docket/index.php?p1=3&p2=3&k=66&case=70&code=nus&p3=0>, dostęp: 13 marca 2001 r.

[44] Przegląd poglądów w doktrynie na temat zbrojnej operacji uprzedzającej zob. J. Kranz, *Między wojną a pokojem: świat współczesny wobec użycia siły zbrojnej* [w:] J. Kranz (red. nauk.), *Świat współczesny wobec użycia siły zbrojnej.*

— poważne znaczenie potencjalnego ataku, którego skutkami byłyby liczne ofiary i zniszczenia, jak np. w przypadku użycia broni masowego rażenia;
— natura ataku, co w tym przypadku oznacza możliwość rozpoznania przygotowań i zamiarów strony atakującej. W praktyce chodzi rzecz jasna o ustalenia dokonane przez służby wywiadowcze potencjalnej ofiary: w doktrynie podkreśla się w tym kontekście, iż należy zawsze brać pod uwagę możliwość błędnej oceny zamiarów i możliwości potencjalnego napastnika;
— moment dokonania ataku musi być *imminent*, a więc nieodległy w czasie, zagrożenie musi być więc bezpośrednie;
— brak jest już możliwości rozwiązania kwestii środkami niemilitarnymi, a więc nie istnieje realna możliwość uniknięcia ataku;
— ocena prawdopodobieństwa ataku uwzględnia politykę prowadzoną przez potencjalnego napastnika, jego dotychczasowe zachowanie na arenie międzynarodowej, przeprowadzone przezeń w przeszłości operacje militarne, wypowiedzi przywódców, podejmowane przygotowania etc.

Należy w tym kontekście zacytować dokument ONZ zatytułowany „Raport Panelu Wysokiego Szczebla ds. Zagrożeń, Wyzwań i Zmian. Bezpieczny świat: nasza wspólna odpowiedzialność", który odnosząc się do omawianej kwestii podkreśla, iż „międzynarodowe prawo zwyczajowe wyraźnie stwierdza, że państwa mogą podjąć akcje zbrojne, w przypadkach, gdy zagrożenie atakiem jest nieuchronne, nie da się ataku odeprzeć przy użyciu innych metod oraz gdy akcja militarna jest proporcjonalna do skali zagrożenia"[45].

Reakcja zaatakowanego w cyberprzestrzeni państwa, polegająca na przeprowadzeniu odwetowego ataku cybernetycznego, należałaby do tzw. kontrśrodków (*countermeasures*) zwanych niegdyś represaliami. Przy ich stosowaniu należy zachować zasadę proporcjonalności środka odwetowego do dokonanego naruszenia i zamierzonego celu, a przed ich uruchomieniem państwo pokrzywdzone powinno wystąpić z roszczeniem reparacji. W doktrynie prawa międzynarodowego podkreśla się, iż represalia jako środki odwetowe polegają na tymczasowym zawieszeniu stosowania

Dylematy prawa i polityki, Warszawa 2009, s. 148 i nast. oraz przywołana przez autora literatura.

[45] A More Secure World: Our Shared Responsibility. Report of the High — level Panel on Threats, Challenges and Change (2004), <www.un.org/secure world>, tekst polski: <http://www.unic.un.org.pl/dokumenty/raport_bezpieczny-swiat.php>, dostęp: 13 marca 2011 r.

określonej normy prawa międzynarodowego przez państwo poszkodowane podejmowane w odpowiedzi na sprzeczne z prawem międzynarodowym innego państwa. W normalnej sytuacji środki użyte jako represalia pozostają w sprzeczności z prawem międzynarodowym, a jedynie uprzednie działanie innego państwa uzasadnia sięgnięcie po nie w odwecie. Jednakże, zastosowane represalia nie mogą naruszać zakazu groźby lub użycia siły, naruszać fundamentalnych praw człowieka, zobowiązań o charakterze humanitarnym i innych zobowiązań wynikających z norm peremptoryjnych (norm typu *iuris cogentis*) powszechnego prawa międzynarodowego[46].

Podsumowując należy sformułować *de lege ferenda* postulat wypracowania projektu regulacji prawnomiędzynarodowych (np. w postaci Konwencji Genewskiej V) czy choćby — jako początek długiego i niełatwego procesu — rezolucji Zgromadzenia Ogólnego ONZ noszącej charakter interpretacji postanowień Karty NZ na wzór Definicji Agresji[47].

Jest to zadanie bez wątpienia trudne z kilku przyczyn, a przede wszystkim:

— sprzecznych w wielu przypadkach interesów państw w kształtującym się porządku politycznym;
— szybkości i głębokości przemian w środowisku bezpieczeństwa;
— dynamicznego postępu technologicznego dokonującego się zarówno w sektorze cywilnym, jak i militarnym (RMA);
— konieczność harmonizacji interesów i wartości związanych z bezpieczeństwem międzynarodowym, narodowym i ludzkim, w tym ochrona praw człowieka i podstawowych wolności. Innymi słowy, przyszłe regulacje muszą rozstrzygnąć dylemat w postaci antynomii pomiędzy bezpieczeństwem i wolnością.

Postulowane regulacje powinny dotyczyć prawnomiędzynarodowego charakteru konfliktów toczonych w cyberprzestrzeni. Szczególnie istotną kwestią jest określenie dopuszczalnego sposobu reakcji państwa na atak cybernetyczny, jej ram, przesłanek uzasadniających etc. przede wszystkim zaś możliwości stosowania art. 51 Karty Narodów Zjednoczonych do samoistnego (tj. bez zastosowania klasycznych, kinetycznych form działań wojennych) ataku cybernetycznego.

[46] Zob. J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2007, s. 10–13; 465–467; por. W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2004.

[47] Szerzej na ten temat zob. T. Aleksandrowicz, *Świat w sieci…*, wyd. cyt., s. 177–180.

Nie ulega wątpliwości, iż jest to zadanie niezwykle trudne, zarówno z politycznego, jak i prawnego punktu widzenia. Jednakże przyjęcie takich regulacji wydaje się być niezbędne, bowiem coraz częstsze stosowanie zasady *konieczność nie zna prawa* powoduje degradację prawa międzynarodowego jako regulatora stosunków międzynarodowych i siłą rzeczy wpływa na ich stan, bezpieczeństwo międzynarodowe i narodowe, także w wymiarze ludzkim. Jedynym rozwiązaniem wydaje się zatem być wzmocnienie zasady rządów prawa na arenie międzynarodowej, a więc wzmocnienie roli prawa międzynarodowego jako regulatora stosunków międzynarodowych, będącego równocześnie ich odzwierciedleniem.

Bibliografia

Literatura

1. Aleksandrowicz T., *Bezpieczeństwo w Unii Europejskiej*, Warszawa 2011.
2. Aleksandrowicz T., *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny* [w:] K. Liedel, Piasecka P., Aleksandrowicz T. (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014.
3. Aleksandrowicz T., *Świat w sieci. Państwa — społeczeństwa — ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014.
4. Arguilla J., Ronfeldt D., *Cyberwar is Coming!* [w:] *In the Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica 1993.
5. Balcerowicz B., *O wojnie, o pokoju. Między esejem a traktatem*, Warszawa 2013.
6. Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010.
7. Barcik J., Srogosz T., *Prawo międzynarodowe publiczne*, Warszawa 2007.
8. Bendyk E., *Bunt sieci*, Warszawa 2012.
9. Bieleń S. (oprac.), *Prawo w stosunkach międzynarodowych. Wybór dokumentów*, Warszawa 2004.
10. Czapliński W., Wyrozumska A., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2004.
11. Dudziak M.L., *War Time. An Idea, It's History, It's Consequences*, Oxford 2012.

12. Grzebyk P., *Odpowiedzialność karna za zbrodnię agresji*, Warszawa 2010.
13. Jemioło T., Sienkiewicz P. (red.), *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka),* t. I, *Raport z badań*, Warszawa 2004.
14. Kamieński Ł., *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Kraków 2009.
15. Karolczak K., *Terroryzm. Nowy paradygmat wojny*, Warszawa 2010.
16. Koziej S., *Teoria sztuki wojennej*, Warszawa 2011.
17. Kranz J., *Między wojną a pokojem: świat współczesny wobec użycia siły zbrojnej* [w:] J. Kranz (red. nauk.), *Świat współczesny wobec użycia siły zbrojnej. Dylematy prawa i polityki*, Warszawa 2009.
18. Liedel K., Piasecka P., *Wojna cybernetyczna — wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1(17).
19. Poulsen K., *Haker. Prawdziwa historia szefa cybermafii*, Kraków 2011.
20. Segal A., *Chinese Computer Games. Keeping Safe in Cyberspace*, "Foreign Affairs", March/April 2012.
21. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa — zjawisko walki informacyjnej* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.
22. Shaw M.N., *Prawo międzynarodowe*, Warszawa 2006.
23. Surmański M., *Pojęcie „czasu wojny" oraz problemy wynikające z jego niedookreśloności w polskim systemie prawnym*, „Bezpieczeństwo Narodowe" 2014, nr II/30.
24. Terlikowski M., *Ataki elektroniczne na Estonię. Implikacje dla bezpieczeństwa międzynarodowego i Polski*, „Polski Przegląd Dyplomatyczny" 2007, t. 7, nr 4(38).
25. Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.

Akty prawne

26. Ustawa z 21 czerwca 2002 r. o stanie wyjątkowym, DzU nr 113, poz. 985.
27. Ustawa z 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach naczelnego dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, DzU nr 156, poz. 1301 z późn. zm.