Kamil Leśniewski

CYBERPRZESTRZEŃ JAKO PIĄTE POLE WALKI, CZYLI SŁÓW KILKA O WYBRANYCH WYZWANIACH W STOSOWANIU ZASADY ROZRÓŻNIANIA PODCZAS DZIAŁAŃ CYBERNETYCZNYCH

Wprowadzenie

Bezspornym wydaje się być pogląd, iż prawo, by cechować się wysoką skutecznością, powinno być w dużej mierze odzwierciedleniem swoich czasów. Stwierdzenie powyższe to niestety w dużej mierze tylko postulat *de lege ferenda*. Zasady międzynarodowego prawa humanitarnego nie są w tej kwestii wyjątkiem. Główne dokumenty regulujące tę gałąź prawa uchwalone zostały w początkowych latach „zimnej wojny". Uważny obserwator bez trudu spostrzeże zmiany, jakie zaszły w geopolitycznym układzie świata od tamtej pory. Zauważy również, że równolegle diametralnej przemianie uległy zarówno realia pola walki, jak i wyposażenie sił zbrojnych. Pomimo zachodzących zmian, reguły prawa humanitarnego w głównych zrębach pozostały jednak niezaktualizowane. Sytuacja ta stanowi częstokroć nie lada wyzwanie dla jego interpretatorów starających się połączyć otaczająca nas rzeczywistość z brzmieniem i treścią przedmiotowych norm. W zarysowanym powyżej kontekście lokują się niewątpliwie rozważania obracające się wokół pojęcia cyberprzestrzeni. Termin ten, zgodnie ze „Słownikiem Języka Polskiego PWN" oznacza: „*przestrzeń wirtualną, w której odbywa się komunikacja między komputerami połączonymi siecią internetową*"[1]. Dla międzynarodowego prawa humanitarnego (MPH) cyberprzestrzeń stanowi przede wszystkim piąty (po przestrzeni lądowej, powietrznej, morskiej, wodnej i kosmicznej) wymiar hipotetycznego pola walki[2]. W doktrynie trafnie sygnalizowane jest, iż wyróżnia się ona zasadniczo odmienną od pozostałych wskazanych wymiarów naturą i jest w całości bytem sztucznym, wykreowanym przez człowieka. Również środki walki w cyberprzestrzeni i sam jej przebieg odbiegają diametralnie od tradycyjnie pojmowanej wojny. Niemałe znacznie ma także fakt, iż działania wykonywane przez siły zbrojne danych państw w cyberprzestrzeni mogą być bardzo różnorodne - począwszy od blokowania dostępu do *Facebooka* dla mieszkańców danego regionu, a skończywszy na bezpośrednim ataku hakerskim na systemy teleinformatyczne elektrowni jądrowej znajdującej się na terytorium danego kraju, celem spowodowania jej awarii. W literaturze słusznie podkreśla się tym samym konieczność stosowania odpowiednio dostosowanej, funkcjonalnej wykładni norm MPH, gdy chodzi o analizę działań przebiegających na rozpatrywanej płaszczyźnie[3].

Zagadnienia będące obiektem zainteresowania niniejszego artykułu stają się szczególnie istotne, gdy zważy się na zauważalną co najmniej od dwóch dekad tendencję do znacznego rozrostu w poszczególnych armiach świata jednostek odpowiedzialnych za operacje w cyberprzestrzeni, kosztem tych odpowiedzialnych za działania konwencjonalne[4]. Nie budzi także większych kontrowersji teza, iż przyszłe konflikty będą rozgrywać się jeśli nie wyłącznie w sferze wirtualnej - to z przytłaczającym jej udziałem[5]. Problem ten został zauważony przez doktrynę prawa międzynarodowego, której część przedstawicieli wprost wskazuje nawet na konieczność przyjęcia specjalnej „*Konwencji genewskiej o cyberwojnie*". Wydaje się jednak, iż niestety nie należy liczyć na powstanie tego typu dokumentu w najbliższym czasie, zważywszy na rozbieżne stanowiska w tej kwestii wyrażane przez poszczególnych przedstawicieli społeczności międzynarodowej[6]. Biorąc powyższe pod uwagę, niniejszy artykuł pochyla się nad ramową dla prawa humanitarnego regulacją - zasadą rozróżniania - i poszukuje jej właściwej interpretacji, gdy chodzi o prowadzenie działań w badanej przestrzeni.

Zasada rozróżniania a cyberprzestrzeń

Pojęciem, którego znaczenia w realiach cyberprzestrzeni poszukiwać należy w pierwszej kolejności jest pojęcie „ataku" - bez ustalenia jego zaistnienia, stosowanie zasady rozróżnienia byłoby przedwczesne. Innymi słowy, uprzednie stwierdzenie ataku - w rozumieniu I Protokołu Dodatkowego do Konwencji Genewskich z 1977 roku (I PD)[7] - stanowi warunek *sine qua non* zastosowania analizowanej zasady. Przez literaturę w poszczególnych okresach rozwoju cyberprzestrzeni przewijały się różne propozycje definicyjne w tym zakresie. Współcześnie najbardziej trafną oraz odpowiednio pojemną wydaje się być ta zaproponowana przez Cordule Droege na łamach *International Review of the Red Cross*, tj.: „*cyberoperacja może stanowić atak w myśl MPH, jeśli powoduje lub doprowadza do śmierci, urazu ciała, fizycznego*

---

[1] *Słownik Języka Polskiego PWN – wydanie internetowe* [online], dostęp: 02.12.2018, http://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915.
[2] R. Ciastoń, *Piąty element*, „Polska Zbrojna" 2013, nr 11, s. 18.
[3] B. Mueller, *The laws of war and cyberspace on the need for a treaty concerning cyber conflict*, London 2014, s. 1-17.
[4] P.W. Singer, A. Friedman, *Cyber security and Cyber war: What Everyone Needs to Know*, New York 2014, s. 163.
[5] B. Valeriano, R. C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford 2015, s. 38.
[6] R. Liivoja, *Technological change and the evolution of the law of war*, „International Review of the Red Cross" 2015, t. 97 nr 900, s. 1160.
[7] Dz.U. 1992, nr 41, poz. 175.

zniszczenia danego obiektu, a także gdy zakłóca właściwą pracę danego obiektu"[8]. Definicja ta jest zbieżna z tą przedstawioną przez grono ekspertów skupionych wokół *NATO Cooperative Cyber Defence Centre of Excellence* w tzw. Podręczniku Tallińskim[9]. Tym samym podkreślić należy, iż nie każde działanie sił zbrojnych w cyberprzestrzeni względem przeciwnika będzie mogło zostać zakwalifikowane jako atak i być przedmiotem rozważań z perspektywy reguł ochronnych prawa humanitarnego, tj. m. in. zasad rozróżniania, proporcjonalności, czy też humanitaryzmu. I tak działania niewiążące się z przemocą, takie jak przykładowo masowe rozsyłanie wiadomości e-mail do mieszkańców danego terytorium wzywających ich do poddania się, co ma na celu osłabienie morale przeciwnika - nie będzie mieściło się w zakresie badanego pojęcia[10].

Będąca obiektem uwagi niniejszego artykułu zasada rozróżniania obiektów cywilnych oraz wojskowych słusznie uznawana jest za ścisły rdzeń prawa humanitarnego. Zobowiązuje ona strony konfliktu do rozróżniania osób cywilnych i kombatantów, a także obiektów cywilnych i wojskowych. Zasada ta od wieków stanowi normę prawa zwyczajowego, zaś w prawie pozytywnym skodyfikowana została po raz pierwszy w Deklaracji Petersburskiej z 1868 roku o zakazie używania małokalibrowych pocisków eksplodujących[11]. Współcześnie jej obowiązywanie łączy się głównie z art. 48, 51, 52, 53, a także 57 I PD. Była ona wielokrotnie potwierdzana w orzecznictwie sądów międzynarodowych[12]. Zgodnie z badaną zasadą przedmiotem ataku nie mogą być osoby oraz obiekty cywilne, przy czym obiekty te charakteryzowane są jako coś widocznego i namacalnego (ang. *visible and tangible*)[13]. Zaznaczyć należy również, iż ochrona obiektów cywilnych nie jest bezwarunkowa i bezwzględna. W sytuacji, gdy obiekt cywilny jest wykorzystywany dla celów wojskowych, traci on ochronę wynikającą z uregulowań MPH, przy czym w sytuacji niepewności co do statusu obiektu, powinno uznać się go za obiekt cywilny[14]. Rozpatrując kwestię podziału na obiekty wojskowe oraz cywilne, za pierwsze z wymienionych - zgodnie z art. 52 I PD - należy uważać: *„dobra, które z powodu swej natury, rozmieszczenia, przeznaczenia lub wykorzystania wnoszą istotny wkład do działalności wojskowej i których całkowite lub częściowe zniszczenie, zajęcie bądź zneutralizowanie daje określoną korzyść w danej sytuacji"*. W związku z dychotomicznością wskazanego podziału, wszelkie pozostałe dobra uznać należy - *a contrario* - za obiekty cywilne. Przedstawiona powyżej definicja ze względu na nieostrość zawartych w niej pojęć powoduje szereg niejasności i sporów pomiędzy poszczególnymi przedstawicielami doktryny. Przykładowo kontrowersje budzi sformułowanie „wnoszenia istotnego wkładu do działalności wojskowej". Choć niewątpliwie aspekt ten musi być rozpatrywany *in concreto* to wydaje się, że nie będzie nadużyciem stwierdzenie, iż wkład jest istotny, jeżeli znacznie zwiększa możliwości taktyczne lub operacyjne danej strony lub w inny sposób wpływa na proporcje sił, nawet jeśli efekt ten jest krótkotrwały i dotyczy tylko ograniczonego obszaru. Dodatkowego podkreślenia wymaga sygnalizowana w literaturze konieczność dokonywania powyższej oceny zarówno w perspektywie bieżących działań, jak i odpowiednio uwidocznionego zamiaru użycia danego obiektu w badanym celu w przyszłości[15]. O ile stosowanie analizowanej zasady stwarza już szereg problemów na współczesnym „tradycyjnym" polu walki - związanych z zacieraniem się granicy między kombatantami i niekombatantami (jest szczególnie widoczne w konfliktach asymetrycznych[16]), to w odniesieniu do działań prowadzonych w cyberprzestrzeni spotyka się ono z szeregiem dalszych, wielokrotnie bardziej złożonych, wynikających ze swoistości tego pola walki problemów[17]. Przykładowo już sama kwalifikacja danej rzeczy należącej do szeroko pojętej cyberprzestrzeni jako obiektu we wskazanym powyżej znaczeniu nie jest jednoznacznie przyjmowana w literaturze. O ile komputery, ich sieci i inne fizycznie namacalne elementy infrastruktury sieciowej (np. kable światłowodowe) nie budzą większych kontrowersji przy kwalifikacji w tym zakresie, to już nie można tego samego odnieść do wywołującego spory wśród poszczególnych autorów statusu danych *per se*, z uwagi na ich nienamacalny, tj. niematerialny charakter. Większość komentatorów stoi w tej kwestii na stanowisku odmawiającym przyznania danym *per se* przedmiotowego statusu. Przekonanie to wydaje się o tyle kontrowersyjne - zdaniem jego opo-

---

[8] C. Droege, *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*, „International Review of the Red Cross" 2012, t. 94 nr 886, s. 560.

[9] M. N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge 2013, s. 92.

[10] *Tamże*, s. 92-93.

[11] *Międzynarodowe Prawo Humanitarne Konfliktów Zbrojnych*, red. Z. Falkowski, M. Marcinko, Warszawa 2014, s. 69.

[12] Reprezentatywnym przykładem w tej kwestii może być pkt. 78 opinii doradczej MTS z dnia 7 lipca 1996, wydanej w sprawie w sprawie legalności użycia lub groźby użycia broni jądrowej, *ICJ Rep. 1996*, s. 226 i nn.

[13] *The Law of Armed Conflict and the Use of Force: The Max Planck Encyclopedia of Public International Law* red. F. Lachenmann, R. Wolfrum, Oxford 2017, s. 364.

[14] ICRC, *IHL Data Base, Rule 9. Definition of Civilian Objects* [online], dostęp: 10.12.2018, http://ihl-databases.icrc.org/customary ihl/eng/docs/v1_cha_chapter2_rule9.

[15] R. Geiss, H. Lahmann, *Cyber warfare: applying the principle of distinction in an interconnected space*, Israel Law Review 2012, t. 45 nr 3, s. 383.

[16] K. Leśniewski, *No attacks on mosques policy - ochrona miejsc kultu religijnego a współczesne asymetryczne działania zbrojne*, „Studia Prawnicze i Administracyjne" 2017, nr 21(3), s. 50 i nn.

[17] C. Droege, *Get...*, s. 552.

nentów - iż jego praktyczną implikacją byłoby znaczne osłabienie ochrony wypływającej z zasady rozróżniania, gdy chodzi o tak kluczowe i pierwotne pojęcie dla cyberświata, jakim niewątpliwie są dane[18]. Do poglądu tego należy się przychylić, zważywszy na wskazaną na wstępie konieczność dokonywania odpowiednio elastycznej i funkcjonalnej wykładni prawa humanitarnego w odniesieniu do realiów cyberprzestrzeni, która z samej już definicji łączy się nierozerwalnie ze światem niematerialnym. Problem ten został jednakże tylko zasygnalizowany, gdyż jego rozwiązanie wymaga przeprowadzenia osobno poświęconej mu analizy.

Robin Geiß i Henning Lahmann słusznie zauważają, iż dopóki celem ataku są obiekty militarne w powszechnie przyjętym rozumieniu, np. bazy wojskowe i znajdujące się na nich elementy informatyczne, stosowanie zasady rozróżnia na polu działań cybernetycznych nie różni się znacząco od przypadku wykorzystania konwencjonalnych metod walki. Bez znaczenia dla dokonywanej oceny jest bowiem czy dany obiekt zostanie zniszczony lub unieszkodliwiony w wyniku uderzenia pocisku rakietowego, desantu oddziału sił lądowych, czy też przeprowadzenia analizowanego cyberataku[19]. Nieporównywalnie większych problemów natury prawnej dostarcza uczynienie celem ewentualnego ataku elementu kluczowego dla wirtualnego świata - jego infrastruktury samej w sobie. Problem ten wydaje się niezwykle aktualny, albowiem z uwagi na stale rosnącą rolę szybkiego przepływu informacji w funkcjonowaniu nowoczesnych armii, można zaryzykować stwierdzenie, iż jednym z kluczowych aspektów mogących przechylić szalę zwycięstwa w hipotetycznym konflikcie zbrojnym może być odpowiednie sparaliżowanie sieci przeciwnika do tego celu wykorzystywanej. Kwestia ta wymaga poświęcenia jej osobnej uwagi i słusznie bywa określana największym problemem prawa humanitarnego, gdy chodzi o cyberdziałania[20]. Już na wstępie rozważań dotyczących powyższego aspektu wskazać należy na specyfikę infrastruktury sieciowej, w której to praktycznie każdy z obiektów wchodzących w jej skład posiada dwoistą cywilno-wojskową naturę (ang. *dual-use*)[21]. Innymi słowy, uwypuklenia wymaga fakt, iż wojsko wykorzystuje w przewarzającej ilości przypadków tę samą infrastrukturę, z której korzystają osoby cywilne. Z analogiczną problematyką można się spotkać również, gdy chodzi o tradycyjnie pojmowane teatry działań, to jednak w cyberprzestrzeni - z uwagi na jej zdecentralizowaną strukturę i sposób działania - nabiera ona fundamentalnego znaczenia[22]. Do komunikacji między sobą w sieci komputery wykorzystują - co do zasady- protokół TCP/IP. Dane (w tym te o wojskowym przeznaczeniu, np. zaszyfrowane poufne wiadomości przesyłane między centrami dowodzenia poszczególnych jednostek) są najpierw rozdzielane na wiele małych „pakietów", a następnie wysyłane, przy czym każdy z nich może podróżować do odbiorcy różnymi kanałami infrastruktury sieciowej - tj. dane te mogą przechodzić przez serwery umieszczone w różnych państwach, przez odpowiednie satelity telekomunikacyjne, światłowody[23]. Określenie *ex ante* drogi, jaką pokona konkretny pakiet danych w takiej sytuacji wydaje się być praktycznie niemożliwym. W większości przypadków wszystkie wymienione elementy infrastruktury sieciowej służą do użytku cywilnego, jednakże te same kanały wykorzystywane są często również do przesyłania danych o charakterze wojskowym. Tak ujęte współdzielenie infrastruktury sieciowej czyni ją celem prawnie dopuszczalnego ataku[24]. Powszechnie aprobowanym w doktrynie poglądem jest bowiem przyjęcie, że dany obiekt nie może z perspektywy prawa być równocześnie obiektem cywilnym i wojskowym, zaś staje się on drugim z wymienionych nawet w przypadku, gdy jego militarne wykorzystanie w stosunku do użytku cywilnego jest marginalne. Tym samym obiekty o dwoistej naturze podlegają prawnej klasyfikacji jako obiekty wojskowe[25]. Z podobnych powodów celem ataku może stać się również inny element cyfrowego świata - np. serwer komercyjnej firmy zawierający w przytłaczającej części dane osób prywatnych, jeśli choćby niewielka część przestrzeni dyskowej wykupiona została tamże na składowanie danych o znaczeniu wojskowym. Wskazane zagrożenie dla całej infrastruktury sieciowej danego kraju nie jest problemem czysto akademickim - Eric Talbot Jensen szacuje przykładowo, iż aż 98% komunikacji cyfrowej podmiotów stanowiących emanację rządu Stanów Zjednoczonych, włączając w to dane objęte stosownymi klauzulami tajności, przekazywane jest właśnie za pomocą cywilnej infrastruktury sieciowej[26]. Z dużym prawdopodobieństwem można założyć, że sytuacja w tym zakresie przedstawia się analogicznie w innych krajach świata - w tym także w Polsce. Poczynione spostrzeżenia co do modelu komunikacji w sieci, tj. rozproszonego przesyłania pakietów danych różnymi kanałami na linii adresat-odbiorca i wynikająca z nich konieczność przyjęcia, iż przytłaczająca część infrastruktury sieciowej w wypadku konfliktu może stać się obiektem ataku, prowadzą do konieczności zwrócenia szczególnej uwagi na potencjalnie możliwy paraliż systemów teleinformatycznych danego państwa o niezwykle poważnych dla ludności cywilnej skutkach. Zważywszy bowiem

[18] M. N. Schmitt, *Tallinn*..., s. 108.
[19] R. Geiss, H. Lahmann, *Cyber*..., s. 384.
[20] C. Droege, *Get*..., s. 566.
[21] J. Andress, S. Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham 2014, s. 251.
[22] R. Geiss, H. Lahmann, *Cyber*..., s. 383.
[23] R. Patterson, *Silencing the Call to Arms: A Shift Away From Cyber Attacks as Warfare*, „Loyola of Los Angeles Law Review" 2015, t. 48 nr 3, s. 979.
[24] R. Geiss, H. Lahmann, *Cyber*..., s. 385-386.
[25] M. N. Schmitt, *Tallinn*..., s. 113.
[26] E. T. Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, „Texas Law Review" 2010, t. 88 nr 7, s. 1542.

na to jak wiele sfer życia we współczesnym świecie zostało nierozerwalnie połączonych z siecią - począwszy od bankowości elektronicznej, poprzez coraz częstsze przechowywanie przez placówki medyczne danych pacjentów w tzw. „chmurze", a skończywszy na wykorzystywaniu Internetu do celów komunikacyjnych, wskazane zagrożenie uznania całości lub chociażby znacznej części infrastruktury sieciowej za dopuszczalny cel ataku nie może nie budzić obaw. Kwestia ta uwidacznia sens powstania odrębnej, odpowiednio dostosowanej, szczególnej regulacji prawnej poświęconej wyłącznie zasadom prowadzenia wojny w cyberprzestrzeni. *De lege lata* wobec przedstawionej częściowej bezradności zasady rozróżniania, gdy chodzi o działania w cyberprzestrzeni w związku z obiektami o naturze *dual-use*, doktryna prawa humanitarnego słusznie wskazuje na drugą z fundamentalnych dla niego zasad - zasadę proporcjonalności, jako na główne źródło ochrony ludności i obiektów cywilnych na analizowanym polu[27].

Zasada proporcjonalności w swoich założeniach odnosi się bowiem do zapewnienia równowagi między dwoma różnymi interesami - interesem uwzględniającym potrzeby wojskowe, a interesem wynikającym wprost z zasady humanitaryzmu[28]. Według powyższego, żadna ze stron konfliktu zbrojnego nie może wszczynać ataków, co do których nie ma pewności, że nie spowodują nadmiernych strat po stronie ludności cywilnej, i to zarówno w sferze niematerialnej, jak i materialnej. Podobnie jak przy zasadzie rozróżniania, jej redakcja dokonana w I PD budzi sporo niejasności - zwłaszcza, gdy chodzi o ustalenie znaczenia pojęcia proporcjonalności[29]. Odrzucić jako niewłaściwe należy wszelkie próby poszukiwania z góry ustalonego, uniwersalnego współczynnika w tym zakresie[30]. Opowiedzieć się trzeba za poglądem, iż ocenę zachowania zasady proporcjonalności należy każdorazowo dokonywać *in concreto*. Wszelkie oceny dokonywane *ex ante* w oderwaniu od specyfiki sytuacji, można uznać za co najwyżej narzędzie do wyeliminowania planów ataków *prima facie* rażąco niewspółmiernych, nigdy zaś jako element uzasadniania ataku z perspektywy *ex post*. Aktualność w przedmiotowej kwestii zachowuje orzeczenie Międzynarodowego Trybunału Karnego dla byłej Jugosławii w sprawie *Galića*, który stwierdził, iż: „*Przy ustalaniu, czy atak był proporcjonalny konieczne jest zbadanie czy rozsądna i dobrze poinformowana osoba znajdująca się w sytuacji w jakiej znalazł się dowódca wydający rozkaz ataku i zdolna przy tym do uczynienia rozsądnego użytku z posiadanych informacji mogła była przewidzieć wystąpienie nadmiernych strat cywilnych związanych z badanym atakiem*"[31]. Tym samym Trybunał opowiedział się za koniecznością przeprowadzania swoistego testu modelowego dowódcy, gdy chodzi o ocenę zachowania proporcjonalności danego ataku. Powyższa zasada odgrywa szczególną rolę, gdy chodzi o ocenę skutków działań w środowisku cybernetycznym. Te są bowiem częstokroć - zważywszy na strukturę cyberprzestrzeni i licznych powiązań oraz zależności między systemami komputerowymi wchodzącymi w jej skład - niezwykle trudne do przewidzenia *ex ante*, zwłaszcza, gdy chodzi możliwe następstwa ataku na element infrastruktury sieciowej o wskazywanym powyżej charakterze *dual-use*. Obrazowym i wartym przytoczenia przykładem w tej kwestii posłużyli się eksperci opracowujący przywoływany już Podręcznik Talliński. Przytoczyli oni kazus hipotetycznego ataku cybernetycznego na system GPS (*Global Positioning System*), jako obiektu o dwoistej naturze, a tym samym dopuszczalnego celu wojskowego. Trafnie spostrzegli oni, iż poza bezspornym wykorzystywaniem go przez siły zbrojne dla swoich celów, odgrywa on także kluczową rolę w wielu dziedzinach życia cywilnego - przykładowo w lotnictwie komercyjnym. Atak taki mógłby - w zależności od swojego zasięgu - poprzez zakłócenie działania przedmiotowego systemu nie tylko uniemożliwić lub znacznie utrudnić np. dokonanie przemieszczenia oddziałów wojsk przeciwnika, ale także z dużym prawdopodobieństwem doprowadzić do bliżej nieokreślonej liczby katastrof lotniczych w krótkim okresie czasu, gdyż system ten wykorzystywany jest jako podstawa nawigacji w lotnictwie cywilnym[32]. W kontekście badanej zasady należy mieć także na uwadze omawiane powyżej poważne zagrożenia dla ludności cywilnej związane z atakiem na infrastrukturę sieciową jako taką. Pozbawienie jej sprawności działania (zwłaszcza -średnio i długoterminowe), w związku z coraz to większym przenoszeniem wielu sfer życia do sfery cyfrowej, miałoby niewątpliwie katastrofalne konsekwencje społeczno-gospodarcze. Tym samym w oparciu o zasadę proporcjonalności postulować należy szczególną ostrożność w procesie planowania prowadzącym do podjęcia decyzji o dokonaniu cyberataku. W razie zauważenia przekroczenia - ustalonej każdorazowo *in concreto* - dopuszczalnej proporcji spodziewanej korzyści wojskowej w stosunku do możliwych nadmiernych skutków ubocznych (a te mogą być zarówno bezpośrednie, jak i pośrednie) - atak taki, jako niezgodny z analizowaną zasadą, powinien zostać zaniechany[33].

---

[27] C. Droege, *Get...*, s. 566.

[28] M. Marcinko, P. Łubiński, *Wybrane zagadnienia z zakresu międzynarodowego prawa humanitarnego*, Szkoła Aspirantów Państwowej Straży Pożarnej, Kraków 2009, s. 35-36.

[29] Y. Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, „Journal of Conflict & Security Law" 2012, t. 17 nr 2, s. 267-272.

[30] Wyrazistym przykładem takiej próby może być ustalenie przedmiotowego współczynnika przez izraelskich uczonych w liczbie 3.14, jako dopuszczalnego stosunku zabitych cywilów do wyeliminowanego terrorysty - zob. E. R. Koch, *Licencja na zabijanie*, Warszawa 2015, s. 290.

[31] Wyrok Międzynarodowego Trybunału Karnego dla byłej Jugosławii z dnia 5 grudnia 2003, sygnatura IT-98-29-T, pkt. 58.

[32] M. N. Schmitt, *Tallinn...*, s. 133.

[33] C. Droege, *Get...*, s. 673.

Podsumowanie

Rzeczywistość cyfrowa odgrywa coraz to większe znaczenie dla funkcjonowania współczesnego świata. Jest ona tworem sztucznym, w całości stworzonym przez człowieka, a rządzące nią reguły częstokroć odbiegają od tych, do których ludzkość była od setek lat przyzwyczajona. Jak wskazano w treści niniejszego artykułu świat cyfrowy służyć może nie tylko do celów rozwoju ludzkości, lecz wykorzystywany bywa także jako kolejne, niezwykle specyficzne pole walki między poszczególnymi jej narodami[34]. Powstałe w zupełnie innych realiach środków i metod prowadzenia działań zbrojnych podstawowe dokumenty prawa humanitarnego nie przystają w dużej mierze do realiów rządzących cyberprzestrzenią i coraz częściej wymagają pogłębionych analiz, aby móc je efektywnie stosować do tak zmienionej rzeczywistości - tyczy się to niestety nie tylko analizowanej w niniejszym artykule zasady rozróżniania, ale także innych zasad leżących u podstaw MPH[35]. Biorąc powyższe pod uwagę, wydaje się, że można wręcz uznać cyberprzestrzeń - obok asymetrycznych konfliktów zbrojnych i autonomicznych systemów bojowych - za najbardziej palący problem jaki stoi przed prawem humanitarnym w XXI wieku. Z zadowoleniem przyjąć należy fakt, że specyfika „piątego pola walki" została w porę dostrzeżona zarówno przez doktrynę, jak i licznych członków społeczności międzynarodowej. Żywym wyrazem powyższego było opracowanie w latach 2009-2012 przez grupę ekspertów związanych z *NATO Cooperative Cyber Defence Centre of Excellence* Podręcznika Tallińskiego w całości poświęcone istocie przedmiotowego zagadnienia. Warto podkreślić, iż w 2017 roku wydana została jego zaktualizowana wersja „2.0"[36] - co świadczy o tym, że projekt ten jest ciągle rozwijany. Opracowanie tallińskie słusznie uznaje się za kamień milowy w dziedzinie regulacji walki w cyberprzestrzeni[37]. Jest ono, jednakże wyłącznie obszernym studium akademickim i nie ma mocy wiążącej, choć jego wkład w rozwój *ius in bello* w odniesieniu do cyberprzestrzeni - wydaje się być nie do przecenienia. Opowiedzieć należy się po stronie autorów stojących na stanowisku, że nie jest to rozwiązanie wystarczające i z uwagi na zbyt dużą swoistość cyberprzestrzeni najlepszym rozwiązaniem byłoby przyjęcie stosownej prawnie wiążącej konwencji jej poświęconej. Potrzebne jest bowiem precyzyjne narzędzie, które sprosta w całości specyfice cyberprzestrzeni - np. opisanego problemu związanego z dwoistą naturą wielu jej elementów - i zapewni w obliczu coraz to bardziej realnego zagrożenia cyberwojną odpowiednio klarowne oraz bezsporne zasady jej prowadzenia. Niestety, nic nie wskazuje, iż przyjęcie takiej konwencji nastąpi w najbliższym czasie.

***

CYBERSPACE AS THE FIFTH DOMAIN OF WARFARE. A FEW WORDS ABOUT SELECTED ISSUES IN APPLYING THE PRINCIPLE OF DISTINCTION DURING CYBER ACTIONS

International humanitarian law (IHL) presently faces a number of complicated challenges. The issue of application of IHL to cyberwarfare is one of them. Cyberspace has become an inseparable aspect of modern societies including field of military operations. The main aim of the paper is to evaluate if IHL can provide sufficient framework for the protection of civilians in the realm of cyberspace. The author shows the difficulties of applying basic norms of IHL to means and methods of cyberwarfare, focusing especially on the principle of distinction. The paper emphasises that in spite of the fact that the principle of distinction is a core of IHL, character of cyberspace oft-times calls it into question. The salient point of the issue is that in the cyber realm military and civilian infrastructure are systemically interconnected and because of that infrastructure as a whole can be considered as a legitimate military target, which strongly impacts on the scope of the protection of civilians.

Keywords: international humanitarian law, modern warfare, cyberspace, cyberwarfare, principle of distinction.

[34] D. I. Voitașec, *Means and methods of cyber warfare*, „Lex ET Scientia International Journal" 2015, t. 1 nr 22, s. 130.

[35] H. P. Faga, The *Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century*, „Baltic Journal of Law & Politics" 2017, t. 10 nr 1, s. 25-26.

[36] Zob. M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017.

[37] D. Efrony, Y.Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, „American Journal of International Law", 2018, t. 112 nr 4, s. 583.