DYLEMATY STRATEGICZNE XXI WIEKU

Księga Jubileuszowa
dedykowana Profesorowi
Michałowi Chorośnickiemu
z okazji czterdziestolecia
pracy naukowej

Pod redakcją naukową
Roberta Kłosowicza
Bogdana Szlachty
Janusza Józefa Węca

Dylematy strategiczne XXI wieku

Dylematy strategiczne XXI wieku

Księga Jubileuszowa dedykowana Profesorowi Michałowi Chorośnickiemu z okazji czterdziestolecia pracy naukowej

Pod redakcją naukową
Roberta Kłosowicza
Bogdana Szlachty
Janusza Józefa Węca

Kraków 2013

Recenzent: prof. dr hab. Andrzej Zięba

Opracowanie redakcyjne: Dagmara Małysza, Justyna Wójcik

Korekta: Mateusz Kijewski

Projekt okładki: Igor Stanisławski

Skład i łamanie: Małgorzata Manterys-Rachwał

Publikacja dofinansowana
przez
Wydział Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego

ISBN 978-83-7638-375-0

KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel./faks: 012 431-27-43, 012 421-13-87
e-mail: akademicka@akademicka.pl

Księgarnia internetowa:
www.akademicka.pl

Spis treści

Część pierwsza. Historia – państwo – prawo

Część druga. Polityka międzynarodowa

TABULA GRATULATORIA

Piotr Bajor
Piotr Borowiec
Krystyna Chojnicka
Anna Citkowska-Kimla
Zbigniew Czubiński
Krystyna Daniel
Agnieszka Dębska
Andrzej Dudek
Magdalena Geodecka
Irena Głuszyńska
Marcin Grabowski
Łukasz Jakubiak
Małgorzata Jasińska
Agnieszka Kastory
Piotr Kimla
Małgorzata Kiwior-Filo
Beata Kosowska-Gąstoł
Grzegorz Kowalski
Wiesław Kozub-Ciembroniewicz
Renata Król-Mazur
Małgorzata Kułakowska
Roman Kuźniar
Michał Matyasik
Maciej Miżejewski
Tomasz Młynarski
Ewa Myślak
Agnieszka Nowakowska-Swół
Dorota Pietrzyk-Reeves
Agnieszka Podoba
Marta Polaczek-Bigaj
Błażej Sajduk
Dominik Sieklucki
Agnieszka Sikora
Jacek Sokołowski
Irena Stawowy-Kawka
Krzysztof Szczerski
Paweł Ścigaj
Monika Ślufińska
Damien Thiriet
Adrian Tyszkiewicz
Magdalena Ullman-Kulik
Tomasz Wieciech
Rafał Wordliczek
Rafał Woźnica
Andrzej Zięba
Agnieszka Zyza

Dominika Dziwisz
Uniwersytet Jagielloński

„Tallinn Manual" – próba interpretacji prawa międzynarodowego dla cyberprzestrzeni

Ponad pół wieku temu odbył się pierwszy lot człowieka w kosmos. To epokowe wydarzenie po raz kolejny w historii przesunęło granicę ludzkich możliwości. Od tego momentu w doktrynie wojennej zaczął funkcjonować czwarty i ostatni, jak wtedy zakładano – obok lądu, powietrza i morza – wymiar prowadzenia wojny: przestrzeń kosmiczna. Jednak utworzenie Dwudziestej Czwartej Armii Powietrznej USA (Twenty-Fourth Air Force, 24 AF – Air Forces Cyber, AFCYBER), a następnie Dowództwa Cybernetycznego USA (United States Cyber Command, USCYBERCOM) są dowodem na to, że wojny XXI w. mogą zostać przeniesione w nowy, jedyny wymiar strategiczny stworzony w całości przez człowieka – cyberprzestrzeń.

W 2002 r. Donald Rumsfeld razem z kilkoma innymi wysoko postawionymi urzędnikami administracji George'a W. Busha zadecydowali, że nie warto „wysadzać w powietrze" Afganistanu, bo nie jest to teren posiadający rozwiniętą infrastrukturę wojskową. Myśląc w kategoriach wojny cybernetycznej, można przyjąć, że Korea Północna jest cyberodpowiednikiem Afganistanu[1] i dlatego nie jest atrakcyjnym celem ataku cybernetycznego. Jest na to proste wytłumaczenie. Oglądając zdjęcia kuli ziemskiej zrobione w nocy, dobrze widać, że najjaśniejsze miejsca na mapie to wschodnie wybrzeża USA i Kanady, Europa, Japonia oraz południowa część Półwyspu Koreańskiego. Część północna półwyspu z powodu słabo rozwiniętej sieci elektrycznej jest niemal całkowicie zacieniona. Ograniczony dostęp do Internetu mają tam tylko nieliczni mieszkańcy[2]. To oznacza, że kraje takie jak Korea Północna mogą zadać dużo więcej obrażeń, niż przyjąć. Natomiast kraje jak Korea Południowa, których ekonomia, handel i każdy aspekt życia codziennego są uzależnione od działania Internetu, są atrakcyjnym celem ataku hakerskiego. Potwierdzeniem tego były wydarzenia z marca 2013 r., kiedy południowokoreańskie sektory finansowy, energetyczny oraz medialny doświadczyły

[1] R.A. Clarke, R.K. Knake, *Cyber War. The Next Threat to National Security and What to Do About It*, HarperCollins e-books, 2011, s. 36.

[2] Zob. *ibidem*, s. 36-37.

zaawansowanego ataku cybernetycznego DDoS[3]. Jeśli, jak się powszechnie podejrzewa, za tymi atakami stoją hakerzy z Północy, dowodzi to tego, że reżim północnokoreański jest liczącym się zawodnikiem w rozgrywce cybernetycznej. Niektórzy eksperci uważają nawet, że możliwości ofensywy cybernetycznej Korei Północnej są porównywalne albo nawet większe niż Chińczyków. James Thruman, dowódca amerykańskich sił w Korei Południowej (United States Forces Korea, USFK) powiedział, że „Najnowszym dodatkiem do północnokoreańskiego arsenału asymetrycznego jest rosnąca zdolność prowadzenia wojny w cyberprzestrzeni. Korea Północna zatrudnia wykwalifikowanych hakerów wytrenowanych do prowadzenia infiltracji cybernetycznej i ataków cybernetycznych przeciwko Korei Południowej i USA"[4]. Niektórzy twierdzą nawet, że Korea Północna nie ma nic do stracenia, bo nawet jeśli udowodni się, że jest stroną atakującą, to nie musi martwić się odwetem[5]. Wymaga to jednak założenia, że odwet będzie symetryczny.

Ataki na infrastrukturę południowokoreańską, a także inne poważne ataki cybernetyczne w Estonii, Gruzji albo atak robakiem Stuxnet na irańskie instalacje nuklearne „są często wynoszone przez autorów do poziomu wojny, czyli stanu tradycyjnie rozumianego jako prawnie, moralnie i strategicznie wyjątkowego"[6]. Jednak zdaniem większości ekspertów jak do tej pory żadne ataki nie nosiły znamion wojny. Dlatego zasadniczym problemem w analizie cyberataków jest brak uniwersalnej definicji cyberwojny i odróżnienie jej od innych form wrogiej aktywności cybernetycznej. Z tego powodu nie wiadomo, kiedy taka wojna się zaczyna, jak wygląda i kiedy się kończy. Zdefiniowanie cyberwojny, cyberterroryzmu i różnych form przestępczości internetowej pozwoliłoby właściwie ocenić ryzyko z nimi związane oraz wybrać najbardziej skuteczne sposoby odpowiedzi na atak. Dlatego autorka podziela zdanie Jasona Healeya z Atlantic Council, że wojna w cyberprzestrzeni jest możliwa, ale mało prawdopodobna. „Piętnaście lat temu byliśmy przekonani, że za pięć lat doświadczymy wojny cybernetycznej. Również dziesięć lat temu myśleliśmy, że cyberwojna czeka nas za pięć lat. Dzisiaj nic się nie zmieniło i zobaczymy, co się wydarzy w ciągu najbliższych pięciu lat". Nato-

[3] Celem ataku typu DoS (Denial of Service) jest uniemożliwienie dostępu do pewnych treści (np. strony WWW) lub usług (np. poczty elektronicznej). Odbywa się to poprzez przeciążenie aplikacji uruchomionych na atakowanym serwerze, tak aby w celu obsłużenia ruchu generowanego przez atakującego zajmowane były wszystkie dostępne zasoby. W wyniku tego obsługiwanie ruchu pochodzącego od rzeczywistych użytkowników zostaje całkowicie zablokowane lub też spowolnione poniżej progu tolerancji (np. wyświetlenie strony głównej zajmuje kilka minut). Distributed Denial of Service (DDoS) jest jedną z wersji ataku DoS. Atak DDoS, jak sugeruje nazwa, jest rozproszony, tzn. przeprowadzany z wielu komputerów jednocześnie.

[4] Y. Lee, *North Korea Cyber Warfare. Hacking 'Warriors' Being Trained in Teams, Experts Say*, [on-line] http://www.huffingtonpost.com/2013/03/24/north-korea-cyber-warfare-warriors--trained-teams_n_2943907.html, dostęp: 20 IV 2013.

[5] *Ibidem*.

[6] D.J. Betz, T. Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-power*, London 2011, s. 81.

miast „nic nie usprawiedliwia nieprzygotowania na wypadek wojny cybernetycznej. To, co powiedział Leon Panetta o cyber Pearl Harbour może się wydarzyć"[7].

Choć nigdy dotąd nie doświadczono wojny cybernetycznej i nie wiadomo, czy do takiej dojdzie, to jednak oddziaływanie cyberprzestrzeni na wojny w klasycznym znaczeniu jest ogromne. Ochrona cyberprzestrzeni i kształtowanie możliwości ataku są nowym i niezwykle istotnym zadaniem państwa. Powołanie USCYBERCOM, przyjęcie ważnych dokumentów międzynarodowoprawnych, jak Międzynarodowej strategii USA dla cyberprzestrzeni, a przede wszystkim nowej koncepcji strategicznej NATO, która wyniosła zagrożenie cybernetyczne do rangi zagrożenia strategicznego, dowodzą, że cyberbezpieczeństwo jest traktowane przez rządy państw poważnie, a niekiedy nawet priorytetowo.

Faktem jest, że państwa przygotowują grunt pod nowe cybernetyczne pole bitwy, jednak jak do tej pory próby odpowiedzi na najważniejsze wątpliwości prawne – kiedy cyberatak jest aktem wojny oraz w jakim stopniu, jeśli w ogóle, normy prawa międzynarodowego określające zachowanie państw w czasie konfliktu i w czasie pokoju mają zastosowanie również w cyberprzestrzeni – nie dawały wystarczających rozwiązań. Często znawcy tematu odpowiadali wymijająco na pytanie o stosowalność międzynarodowego prawa w cyberprzestrzeni. „Zaczynając od roku 1999, każdy cyberekspert, który powiedział, że zastosowanie prawa międzynarodowego w cyberprzestrzeni jest «interesującym pytaniem», dowodził, że prawdopodobnie nie ma on pojęcia o masowo tworzonych interpretacjach tego zagadnienia przez prawników akademickich oraz wojskowych Kiedy zatem następnym razem usłyszy się coś takiego, najlepiej grzecznie przycisnąć takiego «cybereksperta» do muru pytaniem – […] jakie jego zdaniem powinno być to prawo. Postęp w dziedzinie cyberbezpieczeństwa zbyt długo był spowalniany przez tych, którzy lubią zadawać pytania, a nie odpowiadać"[8].

NATO a bezpieczeństwo cybernetyczne

Ataki na systemy komputerowe NATO i państw członkowskich nie są zjawiskiem nowym, jednak coraz częstszym i w coraz większym stopniu zakłócającym ich działanie. Zazwyczaj ataki takie przeprowadzane są „poniżej progu intensywności wywołującego niepokój na poziomie politycznym"[9]. Jak do tej pory nie

[7] Z wywiadu D. Dziwisz z J. Healeyem, Atlantic Council, Waszyngton 2012 (wywiad złożony do druku, planowana publikacja: czerwiec 2013).

[8] J. Healey, *Reason Finally Gets Voice the Tallinn Manual on Cyberwar and Internetional Law*, Atlantic Council, [on-line] http://www.acus.org/new_atlanticist/reason-finally-gets-voice-tallinn-manual-cyber-war-and-international-law, dostęp: 14 IV 2013.

[9] *NATO 2020. Zapewnione bezpieczeństwo, dynamiczne zaangażowanie (Raport Albright)*, red. A.D. Rotfeld, Polski Instytut Spraw Międzynarodowych, Warszawa 2010, s. 87, [on-line] http://www.pism.pl/zalaczniki/NATO_2020.pdf, dostęp: 19 II 2013.

udało się przeprowadzić ataku cybernetycznego na większą skalę: nigdy nie spowodował większych strat ekonomicznych, niebezpiecznego zaburzenia działania infrastruktury krytycznej państwa, a tym bardziej śmierci ludzi. Zdaniem ekspertów jest to jednak prawdopodobne. Na przykład atak wymierzony przeciw systemom dowodzenia i kontroli NATO lub jego sieciom energetycznym może być wystarczającym powodem przeprowadzenia konsultacji zgodnie z art. 4 traktatu waszyngtońskiego i w konsekwencji może uzasadniać zastosowanie art. 5 i uruchomienie środków obrony zbiorowej[10]. Chociaż NATO podjęło już kroki zmierzające do wzmocnienia zdolności obrony cybernetycznej, to nadal ma w tym zakresie spore braki. Dlatego na etapie opracowywania nowej koncepcji strategicznej NATO eksperci „grupy mędrców"[11] zalecili nadanie wysokiego priorytetu „likwidacji tych słabości jako nie tylko nieakceptowanych, ale też coraz bardziej niebezpiecznych"[12].

Na szczycie w Pradze w 2002 r. obrona cybernetyczna została wpisana do agendy politycznej NATO, ale rzeczywistym przełomem dla bezpieczeństwa cybernetycznego państw NATO było przyjęcie w Lizbonie w 2010 r. nowej koncepcji strategicznej. Wtedy, po raz pierwszy w historii Sojuszu Północnoatlantyckiego, państwa członkowskie wymieniły zagrożenia cybernetyczne – obok ataku za pomocą rakiety balistycznej i uderzenia międzynarodowych grup terrorystycznych – jako jedne z najniebezpieczniejszych w nadchodzącej dekadzie. Oznacza to, że centralna misja funkcjonowania NATO, jaką jest obrona zbiorowa i zapewnianie bezpieczeństwa, została rozciągnięta na cyberprzestrzeń. Z tego powodu NATO musi być przygotowane na skuteczne zapobieganie zagrożeniom, a w razie ataku na szybką reakcję, właściwą ochronę swoich systemów komunikacji i dowodzenia oraz udzielenie państwom członkowskim pomocy w zapobieganiu atakom i usuwaniu ich skutków.

W czerwcu 2011 r. ministrowie obrony NATO zatwierdzili zrewidowaną Politykę NATO w dziedzinie cyberobrony zgodną z nową koncepcją strategiczną[13]. Ponieważ zbiorowe bezpieczeństwo cybernetyczne zależy od bezpieczeństwa najsłabszego ogniwa w systemie, to nowa polityka wskazuje, że w pierwszej kolejności to państwa członkowskie ponoszą odpowiedzialność za bezpieczeństwo swoich własnych systemów teleinformatycznych. Natomiast NATO przygotowało strukturę współpracy z i pomiędzy państwami członkowskimi w celu optymalizacji wymiany informacji i podejścia sytuacyjnego oraz współpracy na bazie uzgodnionych standardów NATO. Ponieważ do właściwego funkcjonowania cyberobrony niezbędna jest sprawna współpraca między państwami członkowski-

[10] *Ibidem*, s. 87.

[11] „Grupa mędrców" to stosowane w mediach określenie na dwunastu autorów Raportu Albright.

[12] *NATO 2020. Zapewnione bezpieczeństwo…*, s. 88.

[13] North Atlantic Treaty Organization, http://www.nato.int/cps/en/natolive/topics_78170.htm, dostęp: 10 IV 2013.

mi i dzielenie się informacjami na temat cyberzagrożeń, nowa polityka wyznacza także zasady współpracy z państwami partnerskimi, organizacjami międzynarodowymi, sektorem prywatnym i środowiskiem akademickim oraz precyzyjnie przypisuje zakres działania poszczególnym organom NATO[14]. Przykładowo, Komitet Planowania Obronnego (Defence Policy and Planning Committee) nadzoruje i doradza państwom sojuszniczym w zakresie cyberobrony, Rada ds. Konsultacji, Dowodzenia i Kierowania (Consultation, Control and Command Board, NC3) jest głównym organem konsultacyjnym w zakresie rozwiązań technicznych cyberobrony oraz wdrażania cyberobrony, a NATO Computer Incident Response Capability (NCIRC) jest inicjatywą NATO w zakresie reagowania na incydenty komputerowe, w której skład wchodzą Centrum Wsparcia Technicznego (NCIRC Technical Center) oraz Centrum Koordynacyjne (NCIRC Coordination Centre).

Obok wymienionych wyżej organów NATO ważną funkcję w usprawnianiu kooperacji i dzielenia się informacjami na temat cyberzagrożeń między państwami pełni powołane po szczycie w Bukareszcie w 2008 r. Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi (Cooperative Cyber Defence Centre of Excellence, CCD COE) w Tallinie (dalej nazywane Centrum). Jest ono jednym z osiemnastu centrów doskonalenia NATO. Jego działalność uzupełnia pracę Urzędu NATO ds. Zarządzania Cyberobroną (Cyber Defense Management Authority, CDMA) oraz NATO Computer Incident Response Capability (NCIRC)[15]. Przede wszystkim Centrum jest jednym z najbardziej zaawansowanych na świecie ośrodków analityczno-badawczych ds. cyberbezpieczeństwa[16]. Zajmuje się bieżącą analizą zagrożeń z cyberprzestrzeni, podejmuje kwestie prawne, organizuje ćwiczenia oraz prowadzi prace koncepcyjne, konferencje i szkolenia specjalistyczne z zakresu cyberobrony. Rada Północnoatlantycka przyznała Centrum pełną akredytację jako The NATO Centre of Excellence oraz status międzynarodowej organizacji bezpieczeństwa (The International Military Organization**,** IMO). Centrum nie jest natomiast jednostką operacyjną NATO. Nie podlega także strukturom dowodzenia NATO[17].

Najważniejszym jak do tej pory osiągnięciem Centrum jest opublikowanie w marcu 2013 r. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (dalej nazywanego Podręcznikiem). Podręcznik jest efektem trwającego trzy lata projektu badawczego, w którym zespół dwudziestu ekspertów złożony z prawników, przedstawicieli nauki i praktyków technicznych zaproszonych do współpracy przez Centrum podjął próbę interpretacji norm prawa międzynaro-

[14] *Ibidem*.

[15] Agencja Informacji i Komunikacji NATO (Communications and Information Agency, NCI) przez swoją inicjatywę NATO Computer Incident Response Capability (NCIRC) dostarcza technicznych i operacyjnych usług w NATO.

[16] Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, [on-line] http://www.ccdcoe.org/11.html, dostęp: 20 I 2013.

[17] *Ibidem.*

dowego pod kątem ich zastosowania do cyberkonfliktów. Choć Podręcznik nie stanowi zbioru obowiązującego prawa międzynarodowego ani też nie jest oficjalnym stanowiskiem Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi, państw zaangażowanych w jego działanie ani samego NATO, to stanowi cenny wkład w wiedzę o konfliktach cybernetycznych. Przede wszystkim jest solidną podstawą do dalszej dyskusji na ten temat.

Obszerny, bo ponadtrzystustronicowy Podręcznik, zawiera dziewięćdziesiąt pięć najważniejszych zasad prawa regulujących konflikt w cyberprzestrzeni. W większości pozostają one w zgodzie z perspektywą rządu USA. Potwierdził to w swoim przemówieniu doradca prawny Departamentu Stanu USA (Legal Adviser of the Department of State) Harold Koh na konferencji pod patronatem USCYBERCOM we wrześniu 2012 r.[18] Ponieważ referat Koha został zautoryzowany w procesie międzyagencyjnym, można uznać, że wyraża nie tylko myśli samego autora i Departamentu Stanu, ale także odzwierciedla poglądy rządu USA w podjętym temacie[19].

Obiektem badań ekspertów były wyłącznie *ius ad bellum*, czyli prawo stanowiące o możliwości użycia siły, oraz *ius in bello*, czyli prawo międzynarodowe regulujące zasady i sposób prowadzenia wojny. Szczególny nacisk położono na operacje cybernetyczne *sensu stricto*, czyli takie, kiedy na przykład cyberoperacje przeprowadzane są przeciwko infrastrukturze krytycznej państwa albo przeciw wojskowym systemom dowodzenia. Z analizy wyłączono ataki fizyczne w odpowiedzi na ataki cybernetyczne, jak na przykład bombardowanie centrów kontroli cybernetycznej. Z zakresu badań wyłączono też inne niż wojna formy aktywności w cyberprzestrzeni, jak wywiad elektroniczny i przestępczość cybernetyczna, tłumacząc, że są one poniżej progu uzasadniającego użycie siły militarnej, w związku z czym prawo międzynarodowe regulujące konflikty zbrojne nie ma do nich zastosowania.

Stosowalność prawa międzynarodowego w cyberprzestrzeni

W maju 2011 r. administracja Stanów Zjednoczonych Ameryki opublikowała Międzynarodową strategię USA dla cyberprzestrzeni. Chociaż istniejące dokumenty prawa międzynarodowego nie przewidują możliwości prowadzenia wojny w cyberprzestrzeni, to zgodnie z Międzynarodową strategią USA traktują cyberprzestrzeń jako kolejne, obok lądu, morza, powietrza i przestrzeni kosmicznej, pole walki. W związku z tym istniejące normy prawa międzynarodowego określające zachowanie państw w czasie konfliktu i w czasie pokoju mają, zgodnie ze sta-

[18] M.N. Schmitt, *Internetional Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, „Harvard International Law Journal" vol. 54, 2012, s. 14.

[19] *Ibidem*.

nowiskiem rządu amerykańskiego, zastosowanie również w cyberprzestrzeni[20]. Natomiast szczególny charakter cyberprzestrzeni, który zdecydowanie wyróżnia ten nowy obszar prowadzenia działań wojennych na tle innych, tradycyjnych, wymusza odpowiedź na pytanie, w jaki sposób normy prawa międzynarodowego mają do niej zastosowanie.

Eksperci zaproszeni przez Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi w Tallinie podjęli się niełatwego zadania określenia stosowalności prawa międzynarodowego do konfliktów w cyberprzestrzeni. Na wstępie eksperci jednogłośnie zakwestionowali poglądy wyróżniające cyberprzestrzeń jako odrębną domenę prowadzenia wojny w kontekście stosowania prawa. Opinia doradcza Międzynarodowego Trybunału Sprawiedliwości (MTS) w sprawie legalności groźby lub użycia broni nuklearnej z 1996 r., którą eksperci wzięli za podstawę, rozstrzyga, czy użycie tego typu broni jest prawnie dopuszczalne w świetle obowiązującego prawa międzynarodowego. Trybunał zaopiniował, że zakaz użycia siły wprowadzony art. 2 pkt 4 Karty Narodów Zjednoczonych[21] i wynikający z innych przepisów Karty regulujących *ius ad bellum* ma także zastosowanie do użycia broni nuklearnej. Zakaz ten stosuje się do „jakiegokolwiek użycia siły, niezależnie od rodzaju stosowanej broni"[22]. Posługując się normatywną analogią, eksperci uzasadnili: „fakt, że komputer […] używany jest w czasie operacji, nie ma związku z tym, czy ta operacja jest równoznaczna z «użyciem siły». Podobnie, nie ma to związku z tym, czy dane państwo może użyć siły w celu samoobrony"[23]. Założono także, że w celu prowadzenia jakiejkolwiek aktywności w cyberprzestrzeni dana osoba musi działać w konkretnym miejscu i używać rzeczywistej, materialnej infrastruktury. Innymi słowy, rozstrzygnięcie, jakie reguły prawa międzynarodowego powinny mieć zastosowanie do konkretnego przypadku wrogiej aktywności w cyberprzestrzeni, jest wyłącznie problemem identyfikacji osoby, miejsca, obiektu albo rodzaju przeprowadzanego ataku[24].

---

[20] *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, The White House, Washington, V 2011, [on-line] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, dostęp: 20 XII 2012.

[21] Art. 2 ust. 4 Karty NZ stanowi: „Wszyscy członkowie powinni w swych stosunkach międzynarodowych powstrzymywać się od stosowania groźby lub użycia siły przeciwko nietykalności terytorium albo niepodległości politycznej któregokolwiek państwa, lub wszelkiego innego sposobu, niezgodnego z zasadami Narodów Zjednoczonych".

[22] Opinia doradcza Międzynarodowego Trybunału Sprawiedliwości w sprawie legalności groźby lub użycia broni nuklearnej, 1996, [on-line] http://www.icj-cij.org/docket/files/95/7495.pdf, dostęp: 11 IV 2013.

[23] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, red. M.N. Schmitt, International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, New York 2013, s. 42.

[24] W przypadku cyberprzestrzeni nie jest to zadanie łatwe. Ryzyko wykrycia sprawcy jest znikome, a złapanie go na gorącym uczynku prawie niemożliwe. Równie trudne jest późniejsze wykrycie miejsca przeprowadzenia operacji. Znając adres IP komputera oraz inne jego dane charakterystyczne, można ustalić jego położenie. Dlatego połączenie do atakowanego kompu-

Brak uniwersalnych definicji i kryteriów oceny stopnia zagrożenia cybernetycznego sprawia jednak, że zastosowanie *ius ad bellum* w szybko zmieniającym się środowisku cybernetycznym jest niepewne. Rząd USA stoi na stanowisku, że fizyczny efekt cyberoperacji rozstrzyga, kiedy atak cybernetyczny pogwałca zakaz użycia siły wynikający z Karty NZ[25]. Innymi słowy, kiedy konsekwencje ataku cybernetycznego są porównywalne ze zniszczeniami spowodowanymi zrzuceniem bomby albo wystrzeleniem pocisku rakietowego, wtedy taki atak powinien być tak samo jak atak fizyczny rozpatrywany w kategorii użycia siły[26]. Eksperci zgadzają się ze stanowiskiem rządu USA: „Cyberoperacje stanowią użycie siły, kiedy ich skala i konsekwencje są porównywalne do operacji niecybernetycznych osiągających poziom użycia siły"[27].

Cyberoperacje porównywalne do operacji militarnych w klasycznym znaczeniu, które powodują obrażenia lub śmierć osób albo zniszczenie lub uszkodzenie obiektów, są bezsporne. Inaczej jest w przypadku ataków cybernetycznych, które nie mają analogicznego odpowiednika kinetycznego. Aby wyjaśnić takie sytuacje, eksperci posługują się wyrokiem MTS z 1986 r. w sprawie działalności militarnej i paramilitarnej USA przeciwko Nikaragui[28]. MTS w wyroku uzasadnił, że uzbrajanie i szkolenie antyrządowych partyzantów Contras może zostać zakwalifikowane jako groźba użycia siły lub jej użycie. Innymi słowy, konkretne działanie nie musi wiązać się z bezpośrednimi konsekwencjami fizycznymi, aby mogło być uznane za użycie siły. Można zatem wnioskować, że zaopatrywanie zorganizowanej grupy w złośliwe oprogramowanie i szkolenie w zakresie jego wykorzystania w celu przeprowadzenia cyberataku przeciwko danemu państwu także będzie kwalifikowane jako użycie siły[29].

W związku z tym, że nie wypracowano jednoznacznej odpowiedzi na pytanie: kiedy atak, który nie powoduje obrażeń lub śmierci ludzi albo zniszczenia lub uszkodzenia obiektów, zostanie uznany przez stronę atakowaną za użycie siły, eksperci opracowali zespół czynników rozstrzygających w tej kwestii. Pierwszym jest dotkliwość ataku (*severity*) szacowana na podstawie wpływu na bezpieczeństwo

tera zwykle przechodzi przez wiele komputerów pośrednich oraz „pralnie" adresów IP. Chętnie stosowane przez hakerów anonimowe serwery pośredniczące ukrywają wszystkie dane mogące umożliwić identyfikację użytkownika. Chociaż ich wydobycie jest możliwe od administratorów serwera, to jednak zajmuje dużo czasu.

[25] M.N. Schmitt, *op. cit.*, s. 19.

[26] *Ibidem*, s. 19.

[27] *Tallinn Manual…*, reguła 11, s. 45.

[28] Nikaragua zarzucała USA naruszenie zasady Karty NZ zakazującej interwencji w sprawy wewnętrzne drugiego państwa oraz zakazu groźby użycia siły lub jej użycia przeciwko całości terytorialnej lub niepodległości któregokolwiek państwa. *Military and Paramilitarny Activities in and against Nikaragua* (Nicaragua *vs.* United States of America), Międzynarodowy Trybunał Sprawiedliwości, 1986, [on-line] http://www.icj-cij.org/docket/index.php?p1=3&p2=3&k=66&case=70&code=nus&p3=4, dostęp: 1 II 2013.

[29] *Tallinn Manual…*, reguła 11, pkt 4, s. 46.

infrastruktury krytycznej państwa, zakresu i czasu trwania ataku, jego nasilenia i konsekwencji. Użyciem siły nie jest zatem atak powodujący pewne niedogodności lub irytację, ale atak, który ma rzeczywisty wpływ na bezpieczeństwo narodowe. Drugim czynnikiem jest natychmiastowość (*immediacy*) – im szybciej konsekwencje ataku są dostrzegalne, tym mniejsze szanse na pokojowe rozstrzygnięcie sporu. Wynika to z tego, że państwa zauważają większe niebezpieczeństwo w działaniach wywołujących szybkie efekty niż w zmianach powolnych. Zatem łatwiej jest zakwalifikować cyberoperacje, które wywołują natychmiastowe rezultaty jako użycie siły cyberoperacje, które wywołują natychmiastowe rezultaty, niż te, które osiągają ten sam efekt w dłuższym, na przykład kilkutygodniowym okresie. Trzecia zasada to bezpośredniość (*directness*) – im wyraźniejszy jest związek między cyberoperacją a jej konsekwencjami, tym bardziej prawdopodobne, że atak stanowi naruszenie zakazu użycia siły. Czwarta zasada – inwazyjności (*invasiveness*) – odnosi się do stopnia, w jakim operacja cybernetyczna narusza funkcjonowanie atakowanego państwa albo jego systemów operacyjnych. Logiczne jest, że systemy ważne dla funkcjonowania i bezpieczeństwa państwa są lepiej zabezpieczane. Dlatego operacje przeciwko domenom *dot-mil* albo *dot-gov* będą rozumiane jako bardziej inwazyjne niż ataki przeciwko domenom komercyjnym. Kolejnym czynnikiem jest wymierność efektów ataku (*measurability of effects*). W świecie wirtualnym konsekwencje ataku mogą być mniej oczywiste niż te w świecie realnym. Im konsekwencje dają się łatwiej wyliczyć i są łatwiejsze do zidentyfikowania, tym decyzja, czy atak jest użyciem siły, będzie prostsza. Czynnikiem rozstrzygającym o tym jest także jego wojskowy charakter (*military character*). Związek cyberoperacji z trwającymi działaniami militarnymi zwiększa prawdopodobieństwo uznania go za użycie siły. Ostatnie dwa czynniki to stopień zaangażowania państwa (*state involvement*) w cyberoperację oraz domniemanie legalności (*presumptive lagality*). Ostatni z wymienionych sprowadza się do tego, że akty niezakazane prawem międzynarodowym są dozwolone. Na przykład prawo międzynarodowe nie zakazuje propagandy, operacji psychologicznych, akcji wywiadowczych czy presji ekonomicznej. Jakiekolwiek działania podchodzące pod te kategorie są w domniemaniu legalne, a w związku z tym istnieje mniejsze prawdopodobieństwo, że zostaną uznane za użycie siły.

Podsumowanie

Podręcznik talliński jest pierwszym i jedynym jak do tej pory tak obszernym i szczegółowym opracowaniem, które podejmuje temat stosowalności prawa międzynarodowego na wirtualnym polu bitwy. W mniejszym stopniu eksperci analizują także inne – powiązane z prawem konfliktów zbrojnych – tematy, jak m.in. koncepcje suwerenności państw, jurysdykcji i kontroli (reguły 1-5) czy odpowiedzialności państw (reguły 6-9). Najważniejszy cel ekspertów, jakim była

odpowiedź na pytanie, czy prawo konfliktów zbrojnych ma zastosowanie do cyberprzestrzeni, został osiągnięty. Teraz uwaga została przeniesiona na pytanie o sposoby zastosowania prawa międzynarodowego do cyberprzestrzeni. Jak skomentował dyrektor projektu profesor Michael N. Schmitt: „Ta długo opóźniana podróż przynajmniej w końcu się rozpoczęła"[30].

Na koniec warto zwrócić uwagę na niepokojące artykuły prasowe, które ukazały się po opublikowaniu Podręcznika tallińskiego. Wielokrotnie autorzy sugerują, że eksperci uzasadniają legalność użycia śmiercionośnej broni przeciwko grupom hakerów, takim jak Anonymous. W odpowiedzi na te zarzuty można przytoczyć komentarz Kevina Jona Hellera z Melbourne Law School: „Reguły Podręcznika wyraźnie dotyczą osób zaangażowanych w cyberwojnę w imieniu państw i podmiotów niepaństwowych, jak rebeliantów i terrorystów. Podręcznik ma zastosowanie tylko do międzynarodowych i niemiędzynarodowych konfliktów zbrojnych; hakowanie w czasie pokoju zostało wykluczone z analizy. Podręcznik odnosi się wyłącznie do hakowania w czasie konfliktu, które w jakiś sposób jest z tym konfliktem powiązane. Nic w Podręczniku nie usprawiedliwia ataku wojsk lądowych USA na Anonymous […] w odwecie za ich ataki cybernetyczne na Departament Sprawiedliwości USA w proteście przeciw śmierci Aarona Swartza. Nawet jeśli były one w jakiś sposób częścią «globalnego niemiędzynarodowego konfliktu zbrojnego» z Al-Kaidą"[31]. Zabicie hakera jest możliwe tylko w bardzo wyjątkowych okolicznościach i użycie śmiercionośnej broni przeciwko hakerom zaangażowanym w wojnę cybernetyczną obwarowane jest wieloma ograniczeniami prawa międzynarodowego. Dlatego użycie siły przeciwko członkom grupy Anonymous jest prawie nie do pomyślenia, nawet jeśli skutki ich ataków byłyby bardzo dotkliwe[32].

[30] M.N. Schmitt, *op. cit.*, s. 37.

[31] K.J. Keller, *Does the Tallinn Manual Allow States to Kill Hackers? Not Really*, [on-line] http://opiniojuris.org/2013/03/25/does-the-tallin-manual-allow-states-to-kill-hackers-not-really, dostęp: 22 IV 2013.

[32] *Ibidem*.

www.akademicka.pl

ISBN 978-83-7638-375-0