Tomasz R. Aleksandrowicz

Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego

Normatywne określenie bezpieczeństwa w cyberprzestrzeni jest bez wątpienia zadaniem niezwykle trudnym. Wynika to przede wszystkim z tego, że cyberprzestrzeń jest zjawiskiem stosunkowo nowym, trudnym do jednoznacznego zdefiniowania z uwagi na jej cechy charakterystyczne, stanowiące w wielu przypadkach swoiste novum.

Cyberprzestrzeń: próba definicji i cechy charakterystyczne

Termin cyberprzestrzeń (ang. *cyberspace*) stworzył i upowszechnił już w 1984 r. William Gibson, autor kultowej powieści cyberpunkowej *Neuromancer*. W swojej literackiej wizji określił on cyberprzestrzeń jako (…) *konsensualną halucynację, doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych* (…). *Graficzne odwzorowanie danych z banków wszystkich komputerów świata. Niewyobrażalna złożoność* (…)[1].

W literaturze przedmiotu cyberprzestrzeń określa się jako ogół powiązań o charakterze wirtualnym („nieprzestrzennym" w sensie fizycznym, niematerialnym) powstałych i istniejących dzięki ich fizycznym manifestacjom (komputery, infrastruktura telekomunikacyjna)[2]. Najogólniej można powiedzieć, że cyberprzestrzeń to (…) *całość powiązań ludzkiej działalności z udziałem ICT* (*Information and Communication Technology* – przyp. aut.)[3]. Innymi słowy (…) *mianem cyberprzestrzeni (cyberspace) określa się sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane, sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej i gazowej czy ochrony zdrowia*[4].

Cyberprzestrzeń została w Rzeczpospolitej Polskiej zdefiniowana ustawowo jako przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania) zapewniające przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne[5].

---

[1] W. Gibson, *Neuromancer*, Poznań 1999, s. 53.

[2] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, s. 28.

[3] A. Bógdoł-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 37.

[4] P. Tekielska, Ł. Czekaj, *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (red.), Warszawa 2014, s. 163.

[5] Art. 2 ust. 1b *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. z 2014 poz. 1815, ze zm.). Podobnie jest definiowana cyberprzestrzeń w *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy* [online],

Cyberprzestrzeń jako sfera ludzkiej działalności w zasadniczy sposób różni się od przestrzeni fizycznej. Po pierwsze należy wskazać na uniezależnienie się od miejsca zajmowanego w przestrzeni fizycznej (w sensie geograficznym). Jedynym wymaganiem jest techniczna możliwość włączenia się do sieci. Co więcej – poszczególne urządzenia podłączone w danej chwili do sieci mają szybki i równoprawny dostęp do pozostałych elementów układu, podobnie jak inni uczestnicy o tym samym statusie[6]. Po drugie należy wskazać na obniżający się koszt wejścia do sieci i podejmowania w niej różnych działań. Zmniejsza się także zasób wiedzy i umiejętności niezbędnych do podejmowania takich działań z uwagi na widoczną tendencję do maksymalnego upraszczania interfejsu. Po trzecie wreszcie sieć pozwala w znacznej mierze na zachowanie anonimowości uczestnika. Ślady, które użytkownik pozostawia za sobą w sieci, są tak naprawdę śladami komputera, z którego korzysta. Odrębnym problemem jest powiązanie tego komputera z konkretnym człowiekiem. Istnieje też możliwość pełnej anonimizacji[7].

Cyberprzestrzeń stała się – jak to określono w amerykańskiej *National Strategy to Secure Cyberspace* – „systemem nerwowym państwa": (…) *nasza gospodarka i bezpieczeństwo narodowe stały się w pełni zależne od technologii i infrastruktury informatycznej*[8]. Od sprawności i bezpieczeństwa cyberprzestrzeni zależy funkcjonowanie infrastruktury krytycznej[9].

W podsumowaniu tego wątku można stwierdzić, że cyberprzestrzeń charakteryzuje się następującymi cechami:

- niezależnością od miejsca,
- niezależnością od odległości,
- niezależnością od czasu,
- niezależnością od granic,
- względną anonimowością,
- możliwością ustalenia sprzętu, nie osoby.

Bezpieczeństwo w cyberprzestrzeni

Znaczenie cyberprzestrzeni dla współczesnego państwa i społeczeństwa powoduje, że coraz ważniejszy staje się problem jej bezpieczeństwa. Jak stwierdzają Bogusław Pacek i Romuald Hoffman, (…) *bezpieczeństwo cyberprzestrzeni* (…) *można określić jako brak ryzyka utraty danych informacyjnych w cyberprzestrzeni* (…) *Widać jasno, że zasobem, który chronimy, jest informacja*[10]. Przywołani autorzy wyraźnie sytuują kwestię bezpieczeństwa cyberprzestrzeni w kategoriach walki i wojny informacyjnej, co nakazuje przyjęcie za punkt wyjścia do dalszych rozważań bezpieczeństwa informacyjnego państwa jako integralnej części bezpieczeństwa narodowego, a następnie zagrożeń

April 2011: *Cyberspace is the interdependent network of information technology components that underpins many of our communications; the Internet is one component of cyberspace*, http://www.hsdl.org/?view&did=7010 [dostęp: 15 III 2012].

[6] Zob. T. Aleksandrowicz, *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 75 i nast.

[7] Na temat cech cyberprzestrzeni zob. M. Madej, *Rewolucja informatyczna*…, s. 29–31.

[8] *The National Strategy to Secure Cyberspace* [online], February 2003, http://www.hsdl.org/?view&did=1040 [dostęp: 15 III 2012].

[9] *International Strategy for Cyberspace. Prosperity, Secirity, and Openess in a Networked World* [online], May 2011, http://www.hsdl.org/?view&did=5665 [dostęp: 15 III 2012].

[10] B. Pacek, R. Hoffman, *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, s. 85.

informacyjnych[11]. W ramach takiego podejścia należy uwzględnić wiele uwarunkowań bezpieczeństwa informacyjnego, a przede wszystkim to, że:

- informacja stanowi zasób strategiczny państwa,
- informacja i wynikające z niej wiedza oraz technologie informatyczne stają się podstawowym czynnikiem wytwórczym,
- szeroko rozumiany sektor informacyjny wytwarza znaczną część dochodu narodowego[12],
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego są w znacznej mierze uzależnione od systemów przetwarzania i przesyłania informacji,
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych,
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej[13],
- technologie informatyczne stały się istotnym elementem funkcjonowania bezpieczeństwa państwa, w tym sił zbrojnych[14],
- media masowe mogą być wykorzystywane jako narzędzia skutecznego zakłócania informacyjnego, np. przez prowadzenie dezinformacji[15].

Eugeniusz Nowak i Maciej Nowak proponują bardzo szeroką definicję bezpieczeństwa informacyjnego, zgodnie z którą jest to stan warunków wewnętrznych i zewnętrznych pozwalający państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego. Zdaniem przywołanych autorów ten stan jest osiągnięty, gdy są spełnione następujące warunki:

- nie są zagrożone strategiczne zasoby państwa,
- organy władzy podejmują decyzje na podstawie wiarygodnych, istotnych, dokładnych i aktualnych informacji,
- przepływ informacji pomiędzy organami państwa jest niezakłócony,
- funkcjonowanie sieci teleinformatycznych tworzących teleinformatyczną infrastrukturę krytyczną państwa jest niezakłócone,
- państwo gwarantuje ochronę informacji niejawnych i danych osobowych obywateli,
- instytucje publiczne nie naruszają prawa obywateli do prywatności,
- obywatele, organizacje pozarządowe i przedstawiciele środków masowego przekazu mają dostęp do informacji publicznej[16].

Nie bez powodu zatem coraz większą popularnością – nie tylko wśród teoretyków – cieszy się pojęcie walki informacyjnej. Nie powinno też dziwić, że wywodzi się ono z nauk wojskowych. Jak podkreślają Piotr Sienkiewicz i Halina Świebo-

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

[12] Technologie informatyczne i komunikacyjne stanowią silny czynnik wzrostu gospodarczego. W Unii Europejskiej ten sektor generuje 25% wzrostu PKB i 40% wzrostu produktywności. Takie dane podaje Komisja Europejska w dokumencie *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia* [online], Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Bruksela 1 VI 2005 COM(2005) 229 końcowy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PL:PDF [dostęp: 5 IV 2012].

[13] Zob. K. Liedel, *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, s. 57.

[14] B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 219.

[15] K. Liedel, *Bezpieczeństwo informacyjne*…, s. 57–58.

[16] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103.

da, nie istnieje jedna, uzgodniona definicja walki informacyjnej, jednak 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 konflikt ten obejmuje 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*)[17].

Powyższe wyjaśnienie wymaga doprecyzowania. Proponuje je zresztą sam P. Sienkiewicz, stosując do procesów informacyjnych na współczesnym polu walki zasady analizy systemowej. Jego zdaniem czynnikiem decydującym o rezultatach walki jest stosunek wiedzy stron walczących. Definiuje on w a l k ę i n f o r m a c y j n ą jako (…) *całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki informacyjnej jest 1. zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych, 2. zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych*[18]. Potencjał informacyjny jako czynnik potencjału militarnego tworzą zasoby informacyjne systemu obronnego państwa (dane, informacje, wiedza) oraz systemy informacyjne kształtujące infrastrukturę informacyjną państwa[19].

W świetle powyższego można zatem stwierdzić, że walka informacyjna to całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi nad przeciwnikiem i osiągnięcia zamierzonych celów. Istotą tej walki jest z jednej strony zniszczenie lub degradacja wartości zasobów informacyjnych przeciwnika (w tym także zasobów przestępcy) oraz stosowanych przez niego systemów informacyjnych, a z drugiej – zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych[20]. Elementami walki informacyjnej są destrukcja fizyczna, operacje bezpieczeństwa, operacje psychologiczne, sabotaż i walka elektroniczna[21]. Jako narzędzia wykorzystywane w tej walce można wskazać m.in.:

- dyplomację,
- propagandę,
- kampanie psychologiczne,
- działania wpływające na procesy polityczne lub kulturowe,
- dezinformację, manipulowanie lokalnymi mediami,
- infiltrację sieci komputerowych i baz danych[22].

---

[17] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, w: *Bezpieczeństwo teleinformatyczne państwa*…, s. 80 i nast. Autorzy zamieścili w cytowanym artykule przegląd definicji walki informacyjnej i działań informacyjnych. Zob. też: P. Sienkiewicz, *Wizje i modele wojny*…

[18] P. Sienkiewicz, *Wizje i modele wojny*…, s. 375.

[19] Tamże, s. 376.

[20] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako*…, s. 79–85.

[21] Tamże, s. 87.

[22] Zob. J. Arguilla, D. Ronfeldt, *Cyberwar is Coming!*, w: *In Athena's Camp: Preparing for Conflict in the Information Age,* Santa Monica 1993, s. 28; http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [dostęp: 6 IV 2012]. Por. też K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17, s. 22–23.

Informacja jest zatem w walce informacyjnej zarówno celem ataku, jak i bronią, tarczą i mieczem, zasobem, ale obejmuje także fizyczne niszczenie infrastruktury wykorzystywanej przez przeciwnika do działań operacyjnych, niszczenie (lub degradację wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych, zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych.

W cyberprzestrzeni walka informacyjna przybiera postać „konfliktu cybernetycznego", w którym sukces lub porażka są uzależnione od działań prowadzonych w sieciach komputerowych. Taki konflikt może przybrać postać **aktywizmu** (niedestrukcyjnej działalności informacyjno-propagandowej, np. na forach internetowych, czatach, portalach społecznościowych), **haktywizmu** (aktywizmu i działań zakłócających funkcjonowanie określonych systemów komputerowych, np. przez blokowanie dostępu do serwerów) lub **cyberterroryzmu** (politycznie motywowanych ataków na komputery, sieci lub systemy informatyczne w celu zniszczenia infrastruktury i wymuszenia na rządzie lub organizacji określonego działania lub zaniechania).

Cyberprzestrzeń należy zatem traktować jako nowe środowisko działania, w którym za pomocą zdigitalizowanej informacji jest prowadzona walka informacyjna w jej pełnym zakresie. Można tu mieć do czynienia ze szpiegostwem, przestępczością (ataki na konta bankowe, wyłudzenia, oszustwa itp.), terroryzmem (na szczęście – ciągle jeszcze teoretycznie) i działaniami nakazującymi traktować cyberprzestrzeń jako piąte – po lądzie, morzu, przestrzeni powietrznej i kosmicznej – środowisko walki.

Tak prowadzona walka informacyjna w cyberprzestrzeni wymaga specyficznych narzędzi (zwanych niekiedy potocznie „narzędziami hakerskimi"). W praktyce można wyróżnić 20 podstawowych narzędzi wykorzystywanych do przeprowadzania różnego rodzaju ataków na systemy informatyczne:

1) wirusy, robaki i bakterie (oprogramowanie złośliwe – *malware*) – programy rozprzestrzeniające się w systemie informatycznym i zmieniające sposób jego działania lub reprodukujące się i zajmujące pamięć procesora, przestrzeń dyskową i inne zasoby, a w rezultacie – blokujące dostęp do danych,
2) bomby logiczne – aktywizujące nowe funkcje elementów logicznych komputera i prowadzące do zniszczenia sprzętu i oprogramowania,
3) konie trojańskie – programy umożliwiające podejmowanie w systemie komputerowym działań bez wiedzy i zgody jego prawowitego użytkownika, np. usuwanie plików, formatowanie dysków, kopiowanie danych itp.,
4) próbkowanie – dostęp do komputera przez analizę jego charakterystyki,
5) uwierzytelnianie – podszywanie się pod osobę uprawnioną do dostępu do systemu,
6) ominięcie – ominięcie procesu zabezpieczającego system,
7) czytanie – nieuprawniony dostęp do informacji,
8) kopiowanie – nieuprawnione kopiowanie plików,
9) kradzież – przejęcie zasobów systemu przez osobę nieuprawnioną bez pozostawiania kopii,
10) modyfikacja – zmiana zawartości danych lub charakterystyki obiektu ataku,
11) usunięcie – zniszczenie obiektu ataku,
12) złośliwe podzespoły – umieszczanie w komputerach chipów zawierających programy umożliwiające nieuprawniony dostęp do systemu lub tworzące wady konstrukcyjne,

13) tylne drzwi – pozostawienie przez twórców oprogramowania „furtki" nieznanej użytkownikowi; za pomocą tylnych drzwi można uzyskać nieuprawniony dostęp do systemu,
14) maskarada – udawanie przez atakującego jednego z użytkowników systemu przez np. modyfikację pakietów w trakcie połączenia,
15) przechwycenie transmisji – uzyskanie dostępu do treści przesyłanych między komputerami,
16) podsłuchiwanie – śledzenie ruchu w sieci,
17) receptor van Ecka – oglądanie przez napastnika na oddzielnym monitorze repliki obrazów pojawiających się na monitorze użytkownika atakowanego komputera,
18) *DDoS* – zablokowanie dostępu do strony internetowej przez przesyłanie pod jej adresem olbrzymiego pakietu danych z różnych źródeł, co powoduje zawieszenie się serwera,
19) *e-mail bombing* – przesyłanie na skrzynkę pocztową atakowanego użytkownika wielkiej ilości danych, co powoduje jej przepełnienie,
20) *electromagnetic pulse* – emisja promieniowania elektromagnetycznego należącego do widma radiowego, które niszczy urządzenia elektroniczne i dane[23].

Normatywne ujęcie zagrożeń bezpieczeństwa w cyberprzestrzeni

Powyższe rozważania wskazują na trudności, jakie niosą za sobą próby stworzenia normatywnych definicji czynów wywołujących zagrożenia cyberprzestrzeni. W dziedzinie prawa międzynarodowego taką próbę podjęła po raz pierwszy Rada Europy, która w 2001 r. przyjęła w Budapeszcie konwencję o cyberprzestępczości (dalej: konwencja budapesztańska[24]). Definiując poszczególne pojęcia, konwencja budapesztańska stanowi w art. 1, że:

> a) „system informatyczny" oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych;
>
> b) „dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny;
>
> c) „dostawca usług" oznacza (i) dowolny podmiot prywatny lub publiczny, który umożliwia użytkownikom jego usług komunikowanie się za pomocą systemu informatycznego, oraz (ii) dowolny inny podmiot, który przetwarza lub przechowuje dane informatyczne w imieniu takich usług komunikacyjnych lub użytkowników takich usług,
>
> d) „dane dotyczące ruchu" oznaczają dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez sys-

[23] Wykaz na podstawie: E. Lichocki, *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP*, Wydział Bezpieczeństwa Narodowego Akademii Obrony Narodowej, Warszawa 2009, s. 62–63 (rozprawa doktorska).

[24] *Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.* (Dz.U. poz. 1514). Zob. na ten temat: D. Głowacka, *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji* [online], http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf [dostęp: 3 VII 2014]. Tekst konwencji: *Convention of Cybercrime* [online], Budapest, 23 XI 2001 r., European Treaty Series nr 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [dostęp: 3 VII 2014].

tem informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazujące swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę, rozmiar, czas trwania lub rodzaj danej usługi[25].

Konwencja budapesztańska zobowiązuje państwa członkowskie do uznania za przestępstwa wiele czynów popełnianych w cyberprzestrzeni. Dzieli je na cztery kategorie: przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów; przestępstwa komputerowe; przestępstwa ze względu na charakter zawartych informacji oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Do pierwszej kategorii wyżej wymieniona konwencja zalicza:

- nielegalny dostęp, rozumiany jako umyślny, bezprawny dostęp do całości lub części systemu informatycznego. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione przez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub z innym nieuczciwym zamiarem albo w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym (art. 2),
- nielegalne przechwytywanie danych, a więc umyślne, bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym (art. 3),
- naruszenie integralności danych rozumiane jako umyślne, bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych. Strona może zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie l musi skutkować poważną szkodą (art. 4),
- naruszenie integralności systemu, a więc umyślne, bezprawne, poważne zakłócanie funkcjonowania systemu informatycznego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych (art. 5),
- niewłaściwe wykorzystywanie urządzeń rozumiane jako umyślne i bezprawne działania polegające na produkcji, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:
  - urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim do popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2–5,
  - hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna (art. 6).

Drugą kategorię stanowią przestępstwa komputerowe, a więc fałszerstwo komputerowe (art. 7) i oszustwo komputerowe (art. 8). Fałszerstwem komputerowym jest umyślne, bezprawne wprowadzanie i dokonywanie zmian, wykasowywanie lub usuwanie danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem

[25] http://prawo.vagla.pl/node/1493 (przyp. red.).

jako autentyczne, bez względu na to, czy są one zrozumiałe i czy można je bezpośrednio odczytać. Strona może wprowadzić wymóg, że odpowiedzialność karna dotyczy działania w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze. Natomiast za oszustwo komputerowe konwencja budapeszteńska uznaje umyślne, bezprawne spowodowanie utraty majątku przez inną osobę przez: wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych bądź każdą ingerencję w funkcjonowanie systemu komputerowego z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.

Przestępstwa ze względu na charakter zawartych informacji (trzecia kategoria) dotyczą czynów związanych z bezprawnym i umyślnym produkowaniem, oferowaniem, udostępnianiem, pozyskiwaniem i posiadaniem pornografii dziecięcej za pomocą systemu informatycznego (art. 9). Czwarta kategoria dotyczy naruszania praw autorskich i pokrewnych z wykorzystaniem systemu informatycznego.

W podobny sposób czyny wymierzone w bezpieczeństwo cyberprzestrzeni definiuje prawo Unii Europejskiej, tzw. dyrektywa o atakach na systemy informatyczne[26]. Jej treść jest z punktu widzenia Rzeczpospolitej Polskiej szczególnie istotna, stanowi ona bowiem obowiązujący akt prawotwórczy. Dyrektywa 2013/40/UE obliguje państwa członkowskie Unii Europejskiej do podjęcia kroków umożliwiających karanie jako przestępstw następujących czynów:

- niezgodnego z prawem dostępu do systemów informatycznych, a zatem umyślnego i bezprawnego uzyskiwania dostępu do całości lub jakiejkolwiek części systemu informatycznego, gdy zostało ono popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 3),
- niezgodnej z prawem ingerencji w systemy, czyli umyślnego i bezprawnego uzyskiwania dostępu do całości lub jakiejkolwiek części systemu informatycznego, gdy to przestępstwo zostało popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 4),
- niezgodnej z prawem ingerencji w dane, rozumianej jako umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 5),
- niezgodnego z prawem przechwytywania, a więc umyślnego i bezprawnego przechwytywania za pomocą środków technicznych niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 6).

W art. 7 zatytułowanym *Narzędzia do popełniania przestępstw* stypizowano czyny polegające na umyślnym wytwarzaniu, sprzedaży, dostarczaniu w celu użycia oraz przywozu, rozpowszechnianiu lub udostępnianiu w inny sposób jednego z następujących narzędzi: programu komputerowego, zaprojektowanego lub przystosowanego głównie do popełnienia jednego z wymienionych przestępstw, hasła komputerowego, kodu dostępu lub podobnych danych umożliwiających dostęp do całości lub części systemu informa-

[26] *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiS* (Dz.Urz. UE L 218 z 14 VIII 2013 r. poz. 8).

tycznego. Podobnie jak w przypadku pozostałych czynów, warunkiem jest bezprawność i umyślność działania sprawcy oraz to, że czyn nie stanowi przypadku mniejszej wagi.

Należy zauważyć, że problematyka dotycząca czynów przeciwko bezpieczeństwu cyberprzestrzeni znalazła regulacje w polskim kodeksie karnym[27]. Ustawodawca słusznie potraktował te zagrożenia w kategoriach walki informacyjnej i pogrupował stosowne przepisy w rozdziale XXXIII – *Przestępstwa przeciwko ochronie informacji*. W grę wchodzą przepisy art. 267, 268, 268a, 269, 269a i 269b, które typizują przestępstwa przeciwko ochronie informacji w cyberprzestrzeni.

Za przestępstwa polski ustawodawca uznaje zatem następujące czyny:

Art. 267

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego.

Art. 268

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

[27] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137).

Art. 269

§ 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b

§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Wojna w cyberprzestrzeni

Cyberprzestrzeń stała się także środowiskiem walki i wojny. W tym kontekście trzeba podkreślić problem prawnomiędzynarodowej oceny środków walki informacyjnej prowadzonej w tej przestrzeni. Jej ranga i znaczenie – choćby w przypadku rozwoju technologicznego i coraz większego znaczenia informacji w formie cyfrowej – będzie w dającej się przewidzieć przyszłości wzrastać. Należy tu 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 prowadzenia działań zbrojnych. 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[28]. Tego typu ataki mogą wywołać zagrożenia

[28] W polskim ustawodawstwie infrastruktura krytyczna jest definiowana jako systemy i powiązane ze sobą funkcjonalnie obiekty wchodzące w ich skład, w tym obiekty budowlane, urządzenia, instalacje, usługi ważne dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Pojęcie infrastruktura krytycz-

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[29]. Istotne znaczenie ma kwestia skali ataku i strat.

Po trzecie cyberprzestrzeń jest wykorzystywana przez przestępców działających jedynie z chęci zysku. Ten aspekt został omówiony powyżej.

Faktem pozostaje, że problem walki informacyjnej w cyberprzestrzeni prowadzonej samoistnie w ogóle nie znajduje odniesienia w obowiązującym prawie międzynarodowym. Podczas analizy hipotetycznych ataków cybernetycznych na infrastrukturę krytyczną państwa można wskazać na następujące sytuacje:

- napastnik jest znany, a państwo (ofiara) podejmuje przeciwko niemu działania zbrojne,
- w analogicznej sytuacji państwo (ofiara) odpowiada atakiem cybernetycznym na infrastrukturę agresora,
- napastnik nie jest znany, możliwe jest zidentyfikowanie tylko adresu IP, a zaatakowane państwo, posługując się narzędziami hakerskimi, dokonuje przejęcia kontroli nad twardym dyskiem i np. niszczy zapisane tam dane,
- napastnik w ogóle nie jest identyfikowany, co oznacza, że państwo (ofiara) nie wie, przez kogo zostało zaatakowane, i nie wie, przeciw komu wymierzyć działania odwetowe.

Reakcje zbrojne na ataki cybernetyczne są już przewidywane w strategiach państw. Na przykład Stany Zjednoczone zastrzegają sobie prawo do reakcji na tego typu zagrożenia wszelkimi koniecznymi i odpowiednimi środkami[30]. W polskim ustawodawstwie ataki z cyberprzestrzeni zostały potraktowane na równi ze zbrojną napaścią na terytorium Rzeczpospolitej Polskiej czy atakami terrorystycznymi jako zagrożenie zewnętrzne państwa uzasadniające wprowadzenie stanu wojennego[31].

Czy tego typu działania pozostają w zgodzie z prawem międzynarodowym? O ile kazus Polski jest poza sporem (wprowadzenie stanu wojennego nie oznacza podjęcia działań zbrojnych), o tyle możliwości podjęcia odwetu o charakterze stricte militarnym

---

na obejmuje następujące systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe; zaopatrzenia w żywność i 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. Zob. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (tekst jednolity: Dz.U. z 2013 r. poz. 1166).

[29] Zob. P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako…*, s. 90.

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

[31] Art. 2 ust. 1 *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. z 2014 r. poz. 1815 dla ustawy: Dz.U. z 2002 r. Nr 156 poz. 1301). Ust. 1a przywołanej ustawy precyzuje, że przez zewnętrzne zagrożenie państwa, o którym mowa w ust. 1, rozumie się celowe działania godzące w niepodległość, niepodzielność terytorium, ważny interes gospodarczy Rzeczpospolitej Polskiej lub zmierzające do uniemożliwienia albo poważnego zakłócenia normalnego funkcjonowania państwa, podejmowane przez podmioty zewnętrzne w stosunku do niej. Analogiczne rozwiązanie znalazło się także w *Ustawie z dnia 21 czerwca 2001 r. o stanie wyjątkowym* (tekst jednolity: Dz.U. z 2014 r. poz. 1191); art. 2 ust. 1 tej ustawy stanowi, że 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 przez zastosowanie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu wniosku dotyczącego wprowadzenia stanu wyjątkowego do Prezydenta Rzeczpospolitej Polskiej.

czy jedynie cybernetycznym wywołują wątpliwości. Nie jest bowiem jasne (przynajmniej nie wynika to dobitnie z obowiązującego prawa międzynarodowego), czy atak cybernetyczny na infrastrukturę krytyczną można uznać za uzasadnienie do podjęcia działań w trybie art. 51 Karty Narodów Zjednoczonych (samoobrona), 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[32]). Konsekwencją tego byłoby uznanie takiego ataku za napaść zbrojną, a co najmniej za zagrożenie międzynarodowego pokoju i bezpieczeństwa. W dzisiejszym stanie prawnym mogłaby to uczynić jedynie Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych, tak jak się to stało po zamachach z 11 września 2001 r. odnośnie do ataków terrorystycznych.

Reakcja zaatakowanego 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, że represalia jako środki odwetowe polegają na tymczasowym zawieszeniu stosowania określonej normy prawa międzynarodowego przez państwo poszkodowane, podejmowanym w odpowiedzi na działania 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. Zastosowane represalia nie mogą jednak naruszać zakazu groźby lub użycia siły, fundamentalnych praw człowieka, zobowiązań o charakterze humanitarnym i innych zobowiązań wynikających z norm peremptoryjnych (tj. norm typu *iuris cogentis*, bezwzględnie obowiązujących) powszechnego prawa międzynarodowego[33].

Trzeci przypadek hipotetycznego ataku niezwykle trudno klasyfikować na gruncie prawa międzynarodowego. Tego typu atak nosiłby raczej charakter przestępstwa konwencyjnego, a opisana reakcja państwa jest bardzo trudna do klasyfikacji prawnomiędzynarodowej.

Poruszone problemy wymagają pilnego rozwiązania. Trudno bowiem zgodzić się na dyktat ze strony sił nieuznających żadnych reguł prowadzenia konfliktu, w tym zbrojnego. Trudno też dopuszczać do sytuacji, w której państwa są zmuszone łamać obowiązujące prawo międzynarodowe. Stosowanie wspomnianej kilkakrotnie zasady „konieczność nie zna prawa" to prosta droga do degradacji roli prawa międzynarodowego i tym samym – anarchizacji stosunków międzynarodowych. Ta zasada może zostać uznana jedynie za wyjątek w sytuacjach nadzwyczajnych, wymagających szybkiego i zdecydowanego rozwiązania. Nigdy natomiast nie powinna znaleźć się w zbiorze podstawowych zasad prawa międzynarodowego.

---

[32] 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 [online], 19 IV 2012, http://technologie.gazeta.pl/internet/1,104530,11557651,Swiatowa_cyberwojna_nie_zobaczysz_jej_w_telewizji.html [dostęp: 19 IV 2012].

[33] 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, s. 661–664.

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. Innymi słowy – dokonanie prawnomiędzynarodowej analizy cyberprzestrzeni i zjawisk w niej zachodzących. Autorzy pomysłu wzorowali się na projektach, których wynikami są *Manual on International Law Applicable to Armed Conflicts at Sea*[34] oraz *Manual on International Law Applicable to Air and Missile Warfare*[35].

Zadanie okazało się bardzo trudne, by nie powiedzieć – karkołomne. Oba opracowania powstały na przełomie stuleci, a więc w sytuacji, w której morskie i powietrzne środowiska walki były znane już od dziesiątków lat, gdy istniały już normy prawa międzynarodowego – zarówno umownego, jak i zwyczajowego – znajdujące do nich bezpośrednie zastosowanie oraz praktyka, orzecznictwo i bogata doktryna. W przypadku cyberprzestrzeni zachodzi diametralnie inna sytuacja. Ta przestrzeń jest stosunkowo nowym środowiskiem, nie tyle przez człowieka opanowywanym (jak w przypadku przestrzeni powietrznej i obszarów morskich), ile stworzonym, o zupełnie innych cechach – brakuje tu zarówno norm prawa międzynarodowego regulujących jej funkcjonowanie jako środowiska walki, jak i 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[36].

Z rozwojem prawa międzynarodowego ma się do czynienia wówczas, gdy społeczność międzynarodowa zaczyna funkcjonować w nowych środowiskach lub też gdy napotyka na nowe wyzwania i zagrożenia. Konieczne stają się wtedy również nowe regulacje. Jako klasyczne przykłady takich sytuacji można uznać choćby powstanie i rozwój międzynarodowego prawa morza, międzynarodowego prawa lotniczego i kosmicznego oraz np. powstanie w ramach systemu ONZ wielu konwencji dotyczących zwalczania terroryzmu międzynarodowego. Można w tym zakresie wskazać dwa generalne sposoby: kodyfikację istniejących norm prawa zwyczajowego i ich rozwój lub tworzenie nowych norm konwencyjnych.

Zespół ekspercki NATO CCD COE poszedł inną drogą, a mianowicie dokonał interpretacji obowiązujących norm prawa międzynarodowego, dążąc do ustalenia: czy, które z nich i w jaki sposób można zastosować do sfery cyberprzestrzeni. Wynikiem tych prac stał się *Tallinn Manual on the International Law Applicable to Cyber Warfare*[37].

Twórcy *Tallinn Manual…* za punkt wyjścia przyjęli koncepcję suwerenności terytorialnej państwa. Rzecz jasna, trudno odnieść ją do cyberprzestrzeni jako takiej, znaj-

---

[34] http://www.icrc.org/ihl/385ec082b509e76c41256739003e636d/7694fe2016f347e1c125641f002d49ce [dostęp: 8 V 2013].

[35] http://www.ihlresearch.org/amw/manual/ [dostęp: 8 V 2013].

[36] Zob. na ten temat: T. Aleksandrowicz, *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, s. 39 i nast.

[37] *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 2013. Tekst dostępny również na stronach internetowych NATO CCD COE – http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=window [dostęp: 8 V 2013].

duje ona jednak zastosowanie do infrastruktury (tj. serwerów, komputerów itp.) znajdujących się na terytorium państwa, które ponosi odpowiedzialność za ich bezpieczeństwo i wykorzystanie zgodne z prawem międzynarodowym. Stąd i jurysdykcja państwa – wobec sprawców przebywających na jego terytorium oraz 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).

Przyjęcie takiego punktu wyjścia oznacza przyznanie państwu prawa kontroli nad własną cyberprzestrzenią (tj. istniejącą w ramach infrastruktury znajdującej się na jego terytorium), nie może ona bowiem być wykorzystywana do działań wrogich przeciwko innemu państwu. Państwo ponosi prawnomiędzynarodową odpowiedzialność za cyberoperacje naruszające prawo międzynarodowe, które mogą być mu przypisane. Sam fakt, że takie operacje zostały przeprowadzone z rządowej infrastruktury nie jest jednak traktowane jako wystarczający dowód do przypisania ich danemu państwu.

Drugim założeniem jest uznanie, że cyberoperacja może być traktowana jako użycie siły w rozumieniu Karty Narodów Zjednoczonych wówczas, gdy jej skutki 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 skutki fizyczne, to podlegają obowiązującemu prawu międzynarodowemu regulującemu kwestie *ius ad bellum*. Mają do nich zatem zastosowanie normy dotyczące agresji, zakazu użycia siły i samoobrony w trybie art. 51 Karty Narodów Zjednoczonych. Równocześnie, jeśli cyberoperacje spełniają kryterium użycia siły i są prowadzone w ramach konfliktu zbrojnego, podlegają międzynarodowemu prawu konfliktów zbrojnych, czyli *ius in bello*.

Konsekwencją przyjęcia takiego rozwiązania jest zastosowanie do aktów cyberwojny obowiązujących przepisów *ius in bello*, dotyczących np. udziału w działaniach zbrojnych, statusu kombatanta, ochrony ludności cywilnej i dóbr kultury. Analogicznie do *ius ad bellum*, także w *ius in bello* za kryterium przyjęto konsekwencje ataku. Tak więc za atak cybernetyczny uznaje się taką operację w cyberprzestrzeni, co do której można zasadnie przypuszczać, że spowoduje śmierć lub uszkodzenie ciała osób, szkody lub zniszczenie obiektów fizycznych (np. atak na systemy sterujące siecią energetyczną, których konsekwencją jest wybuch pożaru).

Wyniki pracy twórców *Tallinn Manual*... bez wątpienia zasługują na uznanie. Stanowią one doktrynalną wykładnię obowiązujących norm prawa międzynarodowego, pozwalającą na zastosowanie obowiązujących norm do nowej sytuacji i nowych zjawisk, jakie pojawiły się w związku z rozwojem współczesnych technologii informacyjnych. Trudno jednak uznać, że rozważania i propozycje zawarte w omawianym opracowaniu rozwiązują istniejący problem.

Po pierwsze mamy do czynienia z doktryną prawa międzynarodowego, a nie z jego źródłem. Przyjęcie prezentowanych powyżej interpretacji nie musi znaleźć odbicia ani w praktyce międzynarodowej państw, ani w orzecznictwie sądów międzynarodowych. Po drugie normy prawa międzynarodowego regulują m.in. kwestie odpowiedzialności państw i osób fizycznych za naruszenia prawa (np. agresję i zbrodnie wojenne). W takim przypadku nie jest możliwe uznanie odpowiedzialności przez ana-

logię, wymagana jest konkretna norma pozwalająca na wyegzekwowanie tej odpowiedzialności. Po trzecie cechy cyberprzestrzeni jako środowiska walki są na tyle specyficzne, że wymagają stworzenia norm prawa międzynarodowego uwzględniających tę specyfikę. Cyberprzestrzeń pozwala na przeprowadzenie np. ataku anonimowego, a przynajmniej takiego, który aby zidentyfikować napastnika, będzie wymagać określonego czasu. Jak w takim razie zastosować przepisy dotyczące kontrśrodków czy samoobrony? Należy też wskazać, że cyberprzestrzeń niejako zrównuje pozycję państwa z pozycją i możliwościami podmiotów niepaństwowych.

Chociaż z formalnego punktu widzenia *Tallinn Manual…* jest klasyczną formą rozważań *te lege lata*, to jednak – mając na uwadze rozwój prawa międzynarodowego, perspektywy rozwoju technologicznego oraz skalę i potencjalne konsekwencje cyberkonfliktów – wypada postulować traktowanie go jako uwag *de lege ferenda*, a zatem uznać za podstawę działań zmierzających do wykreowania nowych norm prawa międzynarodowego regulujących cybernetyczne aspekty *ius ad bellum* i *ius in bello*[38].

Podsumowanie

Powstanie i rozwój społeczeństwa informacyjnego przyniosły ze sobą – poza bezspornymi korzyściami – także wiele zagrożeń bezpieczeństwa państwa i jego obywateli. Większość z nich jest związana z rozwojem cyberprzestrzeni, a także z coraz większą i dziś już zasadniczą rolą informacji, rozumianą jako zasób strategiczny. Nic zatem dziwnego, że te zagrożenia sytuują się w kategorii walki informacyjnej.

Rodzi to nowe wyzwania dla służb odpowiedzialnych za bezpieczeństwo państwa. Podejmując walkę informacyjną w cyberprzestrzeni, muszą one mieć zdolności zarówno defensywne, jak i ofensywne, a zatem – innymi słowy – także zdolności do odstraszania potencjalnego napastnika, niezależnie od tego, czy mamy do czynienia z atakiem cybernetycznym ze strony państwa, podmiotu pozapaństwowego, czy stoimy wobec przestępstwa szpiegostwa w cyberprzestrzeni, czy też mamy do czynienia z przestępcą wykorzystującym nowoczesne technologie komunikacyjne.

Z punktu widzenia służb specjalnych stanowi to nie lada problem. Widać bowiem wyraźnie, że prawo z trudnością nadąża za przebiegającą dynamicznie rewolucją naukowo-techniczną. To poważny problem, gdyż służby specjalne demokratycznego państwa prawnego, jakim jest Rzeczpospolita Polska, muszą działać na podstawie i w granicach prawa. Zasadna wydaje się propozycja przeprowadzenia gruntownej analizy zmian warunków, w jakich przyszło działać polskim służbom specjalnym, aby na tej podstawie sformułować propozycje zmian w obowiązującym prawie uwzględniających realia współczesnego środowiska bezpieczeństwa.

Bibliografia:

Publikacje zwarte:

1. Aleksandrowicz T., *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, Difin.

[38] Zob. na ten temat: T. Aleksandrowicz, *Świat w sieci…*, s. 168 i nast.

2. Aleksandrowicz T., *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, Difin.
3. Arguilla J., Ronfeldt D., *Cyberwar is Coming!*, w: *In Athena's Camp:Preparing for Conflict in the Information Age,* Santa Monica 1993, RAND; http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [dostęp: 6 IV 2012].
4. Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, Scholar.
5. Barcik J., Srogosz T., *Prawo międzynarodowe publiczne*, Warszawa 2007, C.H. Beck.
6. Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, ASPRA-JR.
7. Czapliński W., Wyrozumska A., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2004, C.H. Beck.
8. Gibson W., *Neuromancer*, Poznań 1999, Książnica.
9. Głowacka D., *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji* [online], http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf [dostęp: 3 VII 2014].
10. Lichocki E., *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP*, Warszawa 2009, AON (rozprawa doktorska).
11. Liedel K., *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, Difin.
12. Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17, s. 15–28.
13. Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, PISM.
14. Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, Difin.
15. Pacek B., Hoffman R., *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, AON.
16. Pielesiek K., *Światowa cyberwojna – nie zobaczysz jej w telewizji*, Gazeta pl. Technologie [online], 19 IV 2012, http://technologie.gazeta.pl/internet/1,104530,11557651,Swiatowa_cyberwojna_nie_zobaczysz_jej_w_telewizji.html [dostęp: 19 IV 2012].
17. Sienkiewicz P., *Wizje i modele wojny informacyjnej* [online], s. 373–374, http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf [dostęp: 5 IV 2012].
18. Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, PISM.
19. Tekielska P., Czekaj Ł., *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (red.), Warszawa 2014, Difin.

Akty prawne:

1. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (tekst jednolity: Dz.U. z 2016 r. poz. 1137).
2. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (tekst jednolity: Dz.U. z 2013 r. poz. 1166).

3. *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. z 2014 r. poz. 1815 dla ustawy: Dz.U. z 2002 r. Nr 156 poz. 1301).
4. *Ustawa z dnia 21 czerwca 2001 r. o stanie wyjątkowym* (tekst jednolity: Dz.U. z 2014 r. poz. 1191).
5. *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. z 2014 r. poz. 1815. ze zm.).
6. *Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r*. (Dz.U. z 2014 r. poz. 1514).
7. *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiS* (Dz.Urz. UE L 218 z 14 VIII 2013 r.).
8. *Convention of Cybercrime* [online], Budapest, 23 XI 2001 r., European Treaty Series nr 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [dostęp: 3 VII 2014].
9. *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy* [online], April 2011: *Cyberspace is the interdependent network of information technology components that underpins many of our communications; the Internet is one component of cyberspace,* http://www.hsdl.org/?view&did=7010 [dostęp: 15 III 2012].
10. *The National Strategy to Secure Cyberspace* [online], February 2003, http://www.hsdl.org/?view&did=1040 [dostęp: 15 III 2012].
11. *International Strategy for Cyberspace. Prosperity, Secirity, and Openess in a Networked World* [online], May 2011, http://www.hsdl.org/?view&did=5665 [dostęp: 15 III 2012].
12. *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia* [online], Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Bruksela 1 VI 2005, COM(2005) 229 końcowy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PL:PDF [dostęp: 5 IV 2012].
13. *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 2013. Tekst dostępny również na stronach internetowych NATO CCD COE, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=window [dostęp: 8 V 2013].

Abstrakt

Artykuł jest poświęcony analizie zagrożeń w cyberprzestrzeni odnoszących się do bezpieczeństwa państwa. Autor bada ten problem z punktu widzenia prawa międzynarodowego publicznego oraz prawa Unii Europejskiej i polskiego prawa karnego.

Na podstawie przeprowadzonej analizy autor stwierdza, że walka informacyjna toczona w cyberprzestrzeni rodzi nowe wyzwania dla służb odpowiedzialnych za bezpieczeństwo państwa, które, operując w tej sferze, muszą mieć zdolności zarówno defensywne, jak i ofensywne. Jednocześnie trzeba zauważyć, że prawo z trudem nadąża za dynamicznie przebiegającą rewolucją naukowo-techniczną. To poważny problem, gdyż służby specjalne demokratycznego państwa prawnego, jakim jest Rzeczpospolita Polska, muszą działać na podstawie i w granicach prawa. Zasadna wydaje się propozycja przeprowadzenia gruntownej analizy zmian warunków, w jakich przyszło działać polskim służbom specjalnym, aby na tej podstawie sformułować propozycje zmian w obowiązującym prawie, które uwzględnia realia współczesnego środowiska bezpieczeństwa.

Słowa kluczowe: cyberprzestrzeń, prawo międzynarodowe, walka informacyjna.

Abstract

The paper treats cyberspace as a source of threats for national security. The Author analyses this issue from the point of view of international public law, European Union law and polish penal code. The Author states that information war in cyberspace creates new challenges for the institutions responsible for the national security. Those institutions should have both offensive and defensive capabilities. On the other hand the Author recommends changes in the contemporary law according to the changes in the security environment.

Keywords: cyberspace, international law, information warfare.