S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 1 ss. 5–32 ROK 2016

ISSN 2543–7321

Andrzej Urbanek
Akademia Pomorska
Słupsk
andrzej.urbanek@apsl.edu.pl

CYBERWOJNA – ZAGROŻENIE ASYMETRYCZNE WSPÓŁCZESNEJ PRZESTRZENI BEZPIECZEŃSTWA

CYBERWAR – ASYMMETRIC THREAT OF CONTEMPORARY SPACE OF SECURITY

***Zarys treści*:** W związku z postępującą rewolucją informatyczną zmienia się oblicze współczesnych konfliktów. Ich areną staje się cyberprzestrzeń, do której dostęp mają różni aktorzy: siły zbrojne, organizacje przestępcze i terrorystyczne czy hakerzy. W artykule autor zajął się analizą cyberwojny jako konfliktu o asymetrycznym charakterze. Wyjaśnił w nim istotę asymetryczności współczesnych zagrożeń, dokonał analizy terminu „cyberprzestrzeń", a także omówił pojęcie i charakterystyczne cechy wojny cybernetycznej.
***Słowa kluczowe*:** cyberwojna, cyberkonflikt, netwojna, wojna informacyjna, zagrożenie asymetryczne
***Key words*:** cyberwar, cyber conflict, netwar, information warfare, asymmetric threats

Wstęp

Cyberwojna to nowe zjawisko, które wyrosło na fali rewolucji informacyjnej i powszechnego już obecnie dostępu do technologii związanych z cyberprzestrzenią. Powszechność zastosowania mediów elektronicznych i korzystania z zasobów internetowych nie ominęła również sfery militarnej. Współczesne siły zbrojne nie opierają się wyłącznie na zasobach ludzkich i konwencjonalnych środkach walki. Sięgają coraz częściej po nowe, zaawansowane technologicznie środki walki, broń inteligentną, zinformatyzowane środki dowodzenia i łączności, inteligentne systemy rozpoznania i kierowania działaniami operacyjnymi oraz taktycznymi. Zagospodarowują w ten sposób i wykorzystują do własnych celów cyberprzestrzeń, przenosząc do niej konflikty, traktując ją jako nowy wymiar współczesnego pola walki.

Powszechność Internetu i związanych z nim elektronicznych mediów powoduje jednak, że dostęp do cyberprzestrzeni mają nie tylko podmioty państwowe, w tym

militarne, ale i pozapaństwowe. Stają się one nowymi aktorami w globalnej grze rozgrywającej się w cybernetycznej przestrzeni bezpieczeństwa. Organizacje terrorystyczne, zorganizowane grupy przestępcze czy korporacje transnarodowe, atakując wrażliwe elementy infrastruktury informatycznej czy infrastruktury krytycznej zarządzanej przez technologie informatyczne, mogą w coraz większym zakresie wywierać wpływ na działalność nie tylko różnego rodzaju instytucji narodowych, ale również całych państw, a nawet społeczności międzynarodowej. Hakerzy stają się powoli „dywersantami" cyberprzestrzeni i mogą być wykorzystywani jako „narzędzie" nowej jakościowo wojny – wojny cybernetycznej.

W 1993 roku John Arquilla i David Ronfeld przeprowadzili na zlecenie RAND Corporation analizę perspektywicznych konfliktów zbrojnych ery informacyjnej[1]. Już ponad dwadzieścia lat temu prognozowali, że o obliczu konfliktów zbrojnych nowej ery decydować będzie postęp w dziedzinie technologii informatycznych, a także rozwój takich dziedzin, jak: pirotechnika, broń inteligentna, samoloty szpiegowskie, nowe metody i techniki wywiadu technicznego czy metody dowodzenia i łączności (komunikacji). Przyszłość wojny, ich zdaniem, zależy od tego, jak technologie te będą wykorzystywane, a nie od poziomu ich rozwoju i technologicznego zaawansowania. Organizacja i technologia tworzą ramy wojny, a to, jakie będzie miała oblicze, decydują dowódcy i stratedzy[2].

W tym kontekście warto zastanowić się nad obliczem współczesnej cyberwojny i ujmowania jej jako zagrożenia o typowo asymetrycznym charakterze.

Istota zagrożeń asymetrycznych

Problematyka zagrożeń asymetrycznych budzi dzisiaj wiele kontrowersji, jakkolwiek sama koncepcja rozwija się stosunkowo dynamicznie głównie w ramach wojskowej myśli strategicznej. O dyskusyjności powyższego zagadnienia decyduje dzisiaj kilka istotnych związanych z nią problemów z pogranicza teorii i praktyki bezpieczeństwa[3].

Po pierwsze nie doczekaliśmy się jeszcze jednoznacznej i powszechnie uznanej definicji asymetrii (asymetryczności) bezpieczeństwa. Podejmowane są pod tym względem różne próby, ustalono pewne charakterystyczne cechy tego zjawiska, ale wynikające z nich implikacje trudno uznać za paradygmaty pozwalające na dalszą i dogłębną analizę problemu.

Po drugie pojęcia tego używa się coraz częściej w wielu pracach naukowych i publikacjach, ale jest to bardziej wynikiem „mody", traktowania asymetrii jako swoistej

---

[1] Zob.: J. Arquilla, D. Ronfeldt, *Cyberwar is coming!*, [w:] *In Athena's Camp: Preparing for conflict in the information age*, red. J. Arquilla, D. Ronfeldt,Washington: RAND Corporation, 1993, a także J. Arquilla, D. Ronfeld, *Networks and Netwars*: *The Future of Terror, Crime, and Militancy*, Santa Monica 2001. Pełny raport z projektu badawczego z 1993 r. dostępny jest na stronie internetowej: www.rand.org.

[2] J. Arquilla, D. Ronfeldt, *Cyberwar is coming!...*, s. 24–25, zob. też: K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr I (17), s. 15.

[3] Zob.: A. Urbanek, *Podstawy bezpieczeństwa państwa. Wymiar społeczno-polityczny*, Słupsk 2013, s. 237–248, a także A. Urbanek, *Zagrożenia asymetryczne czy asymetryczność zagrożeń*, [w:] *Wyzwania i zagrożenia w XXI wieku. Aspekty militarne i niemilitarne*, red. M. Borkowski, M. Stańczyk-Minkiewicz, I. Ziemkiewicz-Gawlik, Poznań 2013.

etykiety, której używa się do określenia nowych zagrożeń w celu uatrakcyjnienia problemu, niż wynikiem szczegółowych prac badawczych i przemyślanych koncepcji opartych na solidnej podbudowie teoretycznej[4].

Po trzecie koncepcja ta rozwija się głównie w kręgach amerykańskich wojskowych i dotyczy przede wszystkim bezpieczeństwa USA jako światowego mocarstwa, stąd też trudno na podstawie tych przemyśleń i podejmowanych w tym zakresie działań dokonywać daleko idących uogólnień i uniwersalizacji całej idei[5].

Po czwarte koncepcja ta rozwija się głównie w obrębie wojskowej myśli strategicznej, gdzie rozpatrywana jest z perspektywy wojny, konfliktów zbrojnych i innych zagrożeń militarnych, dlatego nie da się jej w prosty sposób przełożyć na analizę innych, pozamilitarnych zagrożeń, a takie próby czynione są coraz częściej.

Po piąte w wielu kręgach ekspertów od spraw bezpieczeństwa narodowego zagrożenia tego rodzaju utożsamiane są z terroryzmem, co zawęża perspektywę ich badań i analizy.

Wreszcie po szóste, przyjmując współczesne rozumienie asymetrii, łatwo zauważyć, że nie jest to zjawisko nowe, charakterystyczne dla zagrożeń wyrosłych z rozwoju cywilizacyjnego i procesów globalizacyjnych, ale towarzyszyło człowiekowi od zarania dziejów. W historii znajdujemy bowiem wiele przykładów wojen i konfliktów, w których stosowano techniki asymetryczne, co nie do końca koresponduje z tezą o ich współczesnej genezie.

Niektórzy eksperci i naukowcy idą jeszcze dalej w swoich poglądach, negując całkowicie koncepcję zagrożeń asymetrycznych. Przykładem tego jest stanowisko Ryszarda Zięby, który postawił tezę, że wszystkie zagrożenia mają charakter asymetryczny, dlatego też

> […] wątpliwy z logicznego punktu widzenia wydaje się rozpowszechniony przez wielu autorów pogląd o występowaniu po zimnej wojnie tzw. zagrożeń asymetrycznych dla bezpieczeństwa państw. Gdyby uznać tę rację, to należałoby zapytać, czy istnieją zagrożenia symetryczne, a więc czy występowanie symetrii np. w posiadanym potencjale obronnym dwóch państw tworzy zagrożenie[6].

Nie wdając się w dalsze próby rozstrzygnięcia tych spornych kwestii, należałoby jednak zaznaczyć, że omawiana koncepcja zyskuje coraz więcej zwolenników. Ich przemyślenia mają swój wymiar nie tylko teoretyczny, ale i praktyczny, stąd też warto jej poświęcić nieco więcej uwagi.

Słowa „symetria" i „asymetria" są wyrazami pochodzenia greckiego i oznaczają odpowiednio – ‘proporcję, współmierność’ oraz ‘naruszenie lub brak symetrii’[7].

---

[4] Por.: V.L. Goulding, *Back to the Future with Asymmetric Warfare*, „Parameters" 2000, t. 30, nr 4, s. 21–22; M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007, s. 32.

[5] Por.: T.L. Thomas, *Deciphering Asymmetry's Word Game*, „Military Review" 2001, t. 81, nr 4, s. 32–37; M. Madej, *Zagrożenia asymetryczne bezpieczeństwa...*, s. 33.

[6] R. Zięba, *Pozimnowojenny paradygmat bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, red. R. Zięba, Warszawa 2008, s. 25–26.

[7] Por.: W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1989.

Używając terminu „asymetria" do opisu nowych zagrożeń, przypisuje się mu między innymi następujące znaczenia[8]:

- nieuczciwa walka,
- uderzenie w słaby punkt,
- walka informacyjna,
- walka w sferze opinii publicznej,
- groźba wykorzystania lub użycie broni masowego rażenia,
- walka w cyberprzestrzeni.

Jak widać z tego zestawienia, istnieją duże rozbieżności w interpretacji pojęcia asymetryczności i odniesienia go do współczesnego środowiska bezpieczeństwa. W najogólniejszym znaczeniu asymetria (asymetryczność) odnosi się do sytuacji, w której mamy do czynienia z nieprzystosowalnością, niewspółmiernością, odmiennością czy też nieproporcjonalnością obiektów będących przedmiotem porównania[9]. Asymetryczność jest antonimem hipotetycznego stanu symetrycznej równowagi, odnoszącej się do całokształtu zjawisk o charakterze społeczno-kulturowym i cywilizacyjnym oraz ich wzajemnych związków, powiązań i relacji. Symetria jest przez to czynnikiem determinującym trwałość i stabilność zmian zachodzących w procesach ewolucyjnych[10].

Dysproporcja, zróżnicowanie i dysharmonia wywołane czynnikiem asymetrycznym dotyczą zarówno sfery materialnej, to jest gospodarczej, ekonomicznej, technicznej, naukowej, informacyjnej, jak i duchowej, obejmującej aspekty kulturowe, religijne, etyczne i inne[11]. Asymetryczność pomiędzy zantagonizowanymi stronami, po przekroczeniu określonego poziomu ryzyka, gdy zagrożenia przybierają realny kształt, prowadzi w konsekwencji do konfliktów i konfrontacji zarówno w sferze materialnej, jak i duchowej[12].

Asymetryczność zantagonizowanych stron oraz wynikające z niej zagrożenia są warunkowane czynnikami ilościowymi i jakościowymi. Czynniki ilościowe, które mogą przybrać postać zróżnicowania w liczebności wojsk, posiadanych środków walki (broni), zasobów logistycznych i ekonomicznych, powodują powstanie asymetrycznej przewagi ilościowej jednej ze stron konfliktu. Asymetryczna przewaga jakościowa jest z kolei wynikiem dostępu przez jedną ze stron do nowszych technologii, nowszej generacji broni, zdolności wykorzystania swojego potencjału technologicznego i cywilizacyjnego do zapewnienia w krótkim okresie przewagi nad drugą ze stron. Zatem asymetryczność ma nie tylko wymiary materialny i duchowy, ale również ilościowy i jakościowy oraz militarny i pozamilitarny. Dodatkowo asymetria działa niejako w dwie strony i ma swój aspekt pozytywny (*positive high*) i negatywny (*negative low*)[13]. Aspekt

---

[8] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, Warszawa 2003, s. 11.

[9] Por.: M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 33; P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne…*, s. 11; K. Piątkowski, *Wojna nowego typu?*, „Polska w Europie" 2002, nr 1, s. 24.

[10] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 11.

[11] Tamże.

[12] Tamże, s. 12.

[13] Por.: M.V. Rasmussen, *A New Kind of War: Strategic Culture and the War of Terrorism*, „IIS Working Paper" 2003, nr 3; S. Metz, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*, Carlise 2000.

pozytywny oznacza uzyskiwanie przewagi przez wykorzystywanie odmienności w danym rodzaju działań wojskowych (np. posługiwanie się bardziej zawansowanymi technologicznie środkami walki, lepiej wyszkolonymi siłami). Z kolei aspekt negatywny sprowadza się do wykorzystywania słabości przeciwnika, pozbawienia go atutów itp.

Ze względu na wielowymiarowość zagrożeń trudnym zadaniem staje się zdefiniowanie ich asymetryczności. Najbardziej rozwinięte koncepcje możemy odnaleźć w pracach strategów i dokumentach NATO. W *Słowniku terminów i definicji NATO* możemy przeczytać, że zagrożenie asymetryczne to takie „wynikające z możliwości zastosowania różnych środków i metod w celu obejścia lub neutralizacji silnych punktów przeciwnika, wykorzystując jednocześnie jego słabości, w celu uzyskania niewspółmiernych wyników”[14].

Według klasyfikacji NATO typowe działania asymetryczne, które mogą być podejmowane w okresach zwiększonego napięcia i ryzyka, organizowania ataków terrorystycznych, w wojnach partyzanckich czy też otwartych konfliktach, polegają przede wszystkim na[15]:

- wprowadzaniu zamieszania lub obezwładniania kluczowych elementów infrastruktury cywilnej lub wojskowej przeciwnika;
- uniemożliwianiu przeciwnikowi rozwinięcia jego wojsk w okresie otwartego konfliktu zbrojnego;
- zrywaniu interoperacyjności w celu uniemożliwienia prowadzenia działań koalicyjnych;
- osłanianiu skuteczności wojskowej przeciwnika głównie poprzez ograniczenie możliwości użycia techniki wojskowej;
- zwiększaniu kosztów operacji w wymiarze politycznym i ekonomicznym;
- ograniczaniu tempa prowadzenia operacji;
- uniemożliwianiu przeciwnikowi osiągnięcia przewagi informacyjnej i prawidłowej oceny sytuacji bojowej;
- osłabianiu poparcia politycznego udzielanego przeciwnikowi przez jego sojuszników.

W koncepcji Sojuszu zwraca się ponadto uwagę na dużą różnorodność współczesnych środków asymetrycznych, do których zalicza się między innymi: walkę informacyjną, broń masowego rażenia, technikę antysatelitarną, tanie uzbrojenie i amunicję, broń obezwładniającą, środki antymateriałowe, broń psychotroniczną, broń etniczną, środki wpływające na środowisko naturalne oraz broń geofizyczną[16].

Szerszą definicję asymetryczności proponują Steven Metz i Douglas Johnson. Ich zdaniem asymetria jest działaniem, organizacją i myśleniem innym niż przeciwnika w celu maksymalizacji własnych korzyści odniesienia zwycięstwa, uwypuklenia słabości przeciwnika, przejęcia inicjatywy lub osiągnięcia większej swobody działania. Może być ona polityczno-strategiczna, wojskowo-strategiczna, operacyjna

---

[14] Zob.: AAP-6, *Słownik terminów i definicji NATO, NATO Glossary of terms and definitions*, NATO 2005, gdziewojsko.files.wordpress.com/2011/05/slownik_terminow_i_definicji_nato.pdf (dostęp: 15.03.2014), s. 54.

[15] Zob.: P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 18.

[16] Tamże, s. 41–42.

lub stanowić kombinację wyżej wymienionych. Bywa krótkoterminowa albo długoterminowa, dyskretna lub występuje w połączeniu z działaniem symetrycznym. Może wreszcie obejmować wymiar psychiczny i psychologiczny[17].

W Polsce przyjmuje się najczęściej, nawiązując do koncepcji NATO, że zagrożenia asymetryczne dotyczą zarówno sfery militarnej, jak i niemilitarnej. Obejmują myślenie, organizowanie i działanie odmienne od przeciwnika, w tym wykorzystywanie wszelkiego rodzaju różnic w szeroko rozumianych potencjałach stron.

Celem asymetrii jest maksymalizowanie własnej przewagi, wykorzystywanie słabości przeciwnika dla uzyskania dominacji nad nim oraz większej swobody operacyjnej[18]. Z tego punktu widzenia asymetria i zagrożenia asymetryczne stają się wartościowym elementem taktyki działań militarnych i nie jest to wcale nowy sposób myślenia. Jak napisał Tadeusz Kotarbiński, „[…] dobra rada, by próbować osiągnąć swoje cele drogą zagrożenia […] przecież na ogół zagrożenie mniejszych wymaga starań własnych niż wykonanie faktyczne czynów, których wykonaniem grozimy przeciwnikowi"[19]. Na przykład bywa tak, że nie potrzeba strzelać, lecz wystarczy zagrozić strzałem, aby przeciwnik ustąpił z placu.

Współcześnie najwięcej uwagi poświęca się asymetrii w aspekcie konfliktów zbrojnych. Patrząc z tej perspektywy, dzieli się je na symetryczne i asymetryczne. Symetryczność konfliktu oznacza, że jego uczestnicy mają w dużym stopniu zbliżone do siebie potencjały i koncepcje ich wykorzystania, zbliżone sposoby lub środki walki, jak również akceptują powszechnie obowiązujące normy i zasady prowadzenia walki[20]. Pojęcie konfliktu asymetrycznego pojawiło się już w latach dziewięćdziesiątych ubiegłego wieku. Określano nim taki konflikt zbrojny, w którym

> państwo i jego siły zbrojne konfrontowane są z przeciwnikiem, którego cele, organizacja, środki walki i metody działania nie mieszczą się w konwencjonalnym pojęciu wojny. […] Wojna asymetryczna nie zna pojęcia pola walki, frontu, odbywa się w rozproszeniu bez zachowania ciągłości geograficznej i chronologicznej[21].

Zdaniem Krystiana Piątkowskiego wojny asymetryczne odróżniają od klasycznych cele, organizacja, technika, metody działania oraz zasięg[22]. Podobnego zdania jest Bolesław Balcerowicz, który uważa, że zasadnicze różnice między obydwoma rodzajami konfliktów kryją się w obszarze celów wojny (konfliktu zbrojnego), metod prowadzenia działań, sposobów i źródeł finansowania oraz stosowanych form przemocy[23]. Zdaniem niektórych autorów z asymetrycznością mamy do czynienia

---

[17] Por.: S. Metz, D.V. Johnson, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concept*, Carlise 2001, s. 5–6; M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 41; P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 57.

[18] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 18.

[19] T. Kotarbiński, *Dzieła wszystkie, Prakseologia*, cz. II, Wrocław–Warszawa–Kraków 2003, s. 337–338.

[20] J. Russel, *Asymmetric Warfare*, [w:] *The Big Issue: Command and Combat in the Information Age*, red. D. Potts, Shrivenham 2002, s. 19; P.F. Herman, *Asymmetric Warfare: Sizing the Threat*, „Low Intensity Conflict and Law Enforcement" 1997, t. 6, nr 1, s. 176.

[21] K. Piątkowski, *Wojna nowego typu?...*, s. 23–24.

[22] Tamże, s. 24–26.

[23] B. Balcerowicz, *Wojna. Kwestie nie tylko terminologiczne*, „Myśl Wojskowa" 2003, nr 3, s. 70–71.

wówczas, gdy strony konfliktu mają różny status prawno-międzynarodowy (jedna ze stron nie jest podmiotem prawa międzynarodowego)[24]. Ponadto zdaniem Herfrieda Münklera cechą asymetrycznej wojny jest uznanie za nadrzędne podrzędnych dotąd technik stosowania przemocy, to jest partyzantki i terroryzmu[25]. Przykładem tego typu działań są obecnie regularne wręcz starcia z kartelami narkotykowymi prowadzone przez siły zbrojne państw Ameryki Środkowej, Południowej czy też obszaru „Złotego Trójkąta" w Azji Południowo-Wschodniej. Cechą wyróżniającą tego typu konflikty jest asymetryczny przeciwnik. Zdaniem Krzysztofa Rokicińskiego przeciwnika asymetrycznego można zdefiniować następująco[26]:

- nie jest stroną w świetle prawa międzynarodowego;
- jako uczestnik walk nie ma statusu kombatanta;
- obszar prowadzenia walk nie jest dla niego określony;
- prowadzi działania za pomocą wszystkich dostępnych i wygodnych dla siebie środków walki;
- nie dostosowuje się do norm prawa międzynarodowego.

Rozpatrywanie zagrożeń asymetrycznych w ramach wojskowej myśli strategicznej to nie jedyne dzisiaj próby poznania istoty tych zjawisk. Według Marka Madeja na gruncie *security studies* obserwujemy dzisiaj dwa wyraźne podejścia do ich rozumienia: ujęcie wojskowe i ujęcie politologiczne.

W ujęciu wojskowym zwraca się uwagę przede wszystkim na to, że ich źródłem mogą być zarówno państwa, jak i podmioty pozapaństwowe (między innymi ugrupowania terrorystyczne). W podejściu tym, o czym wspomniano wcześniej, przez asymetrię rozumie się najczęściej umiejętność wykorzystania wszelkiego rodzaju różnic w szeroko pojmowanych potencjałach stron konfliktu w celu osiągnięcia przewagi nad przeciwnikiem. Ujęcie wojskowe jest ujęciem szerokim, co w konsekwencji utrudnia próby wykorzystania go do analiz współczesnego środowiska bezpieczeństwa, bowiem, jak uważa M. Madej,

> rozumienie zagrożeń asymetrycznych jako określone metody lub techniki (taktyki) działania nie wydaje się w pełni uzasadnione, choć niewątpliwie główną płaszczyzną, na której przejawia się odmienność między stronami danego konfliktu, jest właśnie nieprzystawalność ich sposobów operowania. Zagrożenie dla jednego podmiotu stanowi nie sama metoda, lecz inny podmiot ją stosujący[27].

Podmiotowe pojmowanie tego terminu jest bardziej użyteczne niż definiowanie go w kategoriach metod i technik działania, głównie w sytuacji, gdy odnosi się do problemów innych niż militarne. W raporcie *Strategic Assessment* z 1998 roku wyróżniono cztery podstawowe opcje asymetryczne, czyli: użycie broni masowego rażenia, wysoko zaawansowanej technologicznie broni konwencjonalnej, tech-

---

[24] Por.: T. Szubrycht, *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizować zagrożenia asymetryczne*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2006, nr 1 (164), s. 141; H. Münkler, *Wojny naszych czasów*, Kraków 2004, s. 10.

[25] H. Münkler, *Wojny naszych czasów*…, s. 10.

[26] K. Rokociński, *Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1, s. 153.

[27] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa*…, s. 45.

nologii informatycznych oraz metod wykorzystujących specyfikę środowiska geograficznego konfliktu. Wskazano tam również podmioty mogące nimi się posługiwać, czyli państwa w fazie transformacji, państwa hultajskie[28], państwa upadłe oraz transnarodowe grupy przestępcze[29]. Ciekawą koncepcję podmiotowego ujęcia zagrożeń asymetrycznych przedstawił Robert D. Steele. Jego zdaniem wyłania się dzisiaj nowy paradygmat zagrożeń, który cechuje dynamika i nieliniowość, brak jakichkolwiek ograniczeń i reguł działania. Stąd też przed siłami zbrojnymi w XXI wieku pojawiają się cztery typy zagrożeń, przeciwników (podmiotów), którym muszą stawić czoło[30]:

1. przeciwnik kategorii 1 (ang. *high-tech brutes, the violent state threat*) – czyli siły zbrojne konkretnego kraju dysponujące kompleksowymi systemami uzbrojenia i pełnym zapleczem logistycznym;
2. przeciwnik kategorii 2 (ang. *low-tech brutes, the violent nonstate threat*) – czyli kombinacja grup kryminalnych i terrorystycznych (podmioty pozapaństwowe);
3. przeciwnik kategorii 3 (ang. *low-tech seers, the nonviolent nonstate threat*) – czyli nieuzbrojone masy wyznawców jakiejś religii, ideologii;
4. przeciwnik kategorii 4 (ang. *high-tech seers, the volatile mixed threat*) – czyli grupy przestępców informatycznych i szpiegów gospodarczych.

Z kolei wąskie rozumienie zagrożeń asymetrycznych – charakterystyczne dla podejścia politologicznego – odnosi się przede wszystkim do zagrożeń wywołanych aktywnością podmiotów pozapaństwowych, trans- lub subnarodowych[31]. Jak podkreśla M. Madej, w takiej sytuacji

> odmienność metod działania i sposobów prowadzenia konfliktu oraz dysproporcja potencjałów (zwłaszcza militarnych) stron układu wynika z faktu, iż podmiot zagrożony (państwo) i stanowiący zagrożenie należą do różnych kategorii uczestników stosunków międzynarodowych[32].

Wśród tak rozumianych zagrożeń asymetrycznych wyróżnia się zazwyczaj ich cztery podstawowe rodzaje: terroryzm międzynarodowy, transnarodową przestępczość zorganizowaną (uwzględniającą między innymi handel narkotykami, wyróżniany przez niektórych znawców przedmiotu jako odrębny rodzaj zagrożeń), użycie przez podmioty pozapaństwowe broni masowego rażenia oraz wykorzystanie przez nie, dla osiągnięcia

---

[28] Terminem tym określa się takie państwa, jak Iran czy Korea Północna.

[29] Por.: *Strategic Assessment* 1998, s. 169–178, 205–216.

[30] Zob.: R.D. Steele, *New craft of the intelligence: achieving asymmetric avantage in the face of nontraditional threats*, US Army War College, Carlisle 2002, www.strategicstudiesinstitute.army.mil/pdffiles/pub217.pdf (dostęp: 15.03.2014); P. Gawliczek, *Istota zagrożeń i działań asymetrycznych*, [w:] *Bezpieczeństwo polityczne i wojskowe*, red. A. Ciupiński, K. Malak, Warszawa 2004.

[31] Por.: R. Kuźniar, *Niebezpieczeństwa nowego paradygmatu bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe czasu przemian. Zagrożenia – koncepcje – instytucje*, red. R. Kuźniar, Z. Lachowski, Warszawa 2003, s. 216; D.A. La Carte, *Asymmetric Warfare and the Use of Special Operation Forces in North American Law Enforcement*, „Canadian Military Journal" 2001, t. 2, nr 4, s. 23–27.

[32] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 50.

własnych celów, nowoczesnych technologii informatycznych[33]. Należy zauważyć, że lista ta nie jest pełna i zamknięta oraz nie obejmuje wszelkich możliwych form zagrożeń asymetrycznych w węższym i jeszcze bardziej szczegółowym zestawieniu.

Cechą charakterystyczną zagrożeń asymetrycznych w ujęciu politologicznym jest nie tylko fakt, że ich źródłem są podmioty pozapaństwowe, lecz również:

- ich **quasi-militarny charakter** (zagrożenia ze strony podmiotów pozapaństwowych nie przybierają postaci ataku regularnych sił zbrojnych, co nie pozwala uznać ich za zagrożenia militarne w tradycyjnym znaczeniu, jakkolwiek podmioty pozapaństwowe mogą używać do swoich celów typowych środków walki zbrojnej wyprodukowanych dla wojska);
- **transnarodowość i aterytorialność** (podmioty pozapaństwowe stanowiące zagrożenie mogą rozwijać swoje struktury na terytorium więcej niż jednego państwa[34], a w przypadku wystąpienia samego zagrożenia trudno im przypisać konkretny obszar działań, teatr walki czy front, przez co zaciera się rozróżnienie między groźbami o charakterze zewnętrznym a wewnętrznym[35]);
- **nieprzewidywalność miejsca i czasu wystąpienia oraz formy i sposobu realizacji konkretnych działań** podejmowanych przez podmioty pozapaństwowe stanowiące zagrożenie[36];
- **niska podatność podmiotów będących źródłem zagrożeń na odstraszanie** czy też inne strategie zapobiegania i zwalczania niebezpieczeństw przez przymus lub groźbę jego zastosowania[37].

Zagrożenia asymetryczne to istotna kategoria niebezpieczeństw, która nie pozostaje obojętna dla współczesnego państwa i tworzonego przez niego systemu bezpieczeństwa. Zagrożenia tego typu pochłaniają ogromne ilości środków finansowych i angażują znaczne siły przy niewspółmiernie niskich siłach i środkach często wirtualnego przeciwnika. Stąd też przy neutralizacji tego typu zagrożeń istotna staje się współpraca międzynarodowa, zaangażowanie w nią instytucji międzynarodowych i przygotowanie procedur działania na tyle skutecznych, by chronić państwo przed ich następstwami. Sam termin „zagrożenia asymetryczne" zyskał sobie już pełne prawo w nauce i praktyce. Jego kwestionowanie nie wydaje się uzasadnione.

Należy zauważyć, że współczesne konflikty asymetryczne mogą rozgrywać się nie tylko w materialnej rzeczywistości, ale i w świecie wirtualnym. Warto w tym miejscu przytoczyć opinię Winna Schwartaua, konsultanta do spraw komunikacji firmy Inter-Pactu, który stwierdził, powołując się na A.H. Toflera, że

> ponad 100 milionów komputerów łączy nas wzajemnie przez niesłychanie złożony system układów komunikacyjnych, zarówno naziemnych jak i satelitarnych. […] rządowe

[33] Zob.: D.A. La Carte, *Asymmetric Warfare…*; R. Kuźniar, *Bezpieczeństwo – realizm oceny, dylematy polityki*, „Polska w Europie" 2002, nr 3; M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*

[34] Zob.: S. Koziej, *Powrześniowe wyzwania w dziedzinie bezpieczeństwa*, „Polska w Europie" 2002, nr 1.

[35] Zob.: R. Kuźniar, *Niebezpieczeństwa nowego paradygmatu…*, s. 225–226.

[36] Zob.: tenże, *Bezpieczeństwo – realizm oceny...*, s. 15.

[37] Zob.: M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 58.

i komercyjne systemy komputerowe są tak słabo dziś chronione, że można je praktycznie uznać za bezbronne. Czeka nas zatem elektroniczne Pearl Harbour[38].

Cyberprzestrzeń – aspekty definicyjne i charakterystyka

Wiek XX, a właściwie jego druga połowa, stał się areną dynamicznego rozwoju nowoczesnych mediów. Rozwinęły się techniki video, telewizja satelitarna, sieci komputerowe, a w tym globalna sieć Internetu. Upowszechnienie się multimediów i technologii informatycznych, zastosowanie ich w wielu dziedzinach życia człowieka, a także olbrzymie już obecnie zasoby internetowe nie pozostają obojętne wobec kształtowania się zupełnie nowej jakościowo przestrzeni istotnej z perspektywy życia współczesnego człowieka, a mianowicie cyberprzestrzeni.

Szczególnie ważny w perspektywie cyberprzestrzeni okazuje się dynamiczny rozwój Internetu. Jeszcze w 1995 r. dostęp do niego miało jedynie 16 milionów użytkowników na świecie. Pięć lat później było ich już 361 milionów, w grudniu 2005 r. 1,018 miliarda, w czerwcu 2010 r. niemal 2 miliardy, a obecnie blisko 3 miliardy (dokładnie 2,937 miliarda – szacunek z marca 2014)[39].

O istocie cyberprzestrzeni decyduje wykreowana w niej wirtualna rzeczywistość. Pojęcie „rzeczywistość wirtualna" (ang. *virtual reality* – VR) pojawiło się pod koniec lat osiemdziesiątych ubiegłego wieku. Wirtualny to według *Słownika języka polskiego* „tworzony sztucznie za pomocą techniki komputerowej; wykorzystujący rzeczywistość tworzoną w ten sposób"[40]. Według Komitetu Definicji i Terminologii Amerykańskiego Towarzystwa Komunikacji i Terminologii Edukacyjnej wirtualny oznacza „funkcjonalny i efektywny bez rzeczywistego istnienia w tradycyjnej formie"[41], a zgodnie ze *Słownikiem wyrazów obcych* wirtualny znaczy tyle, co „mogący zaistnieć, (teoretycznie) możliwy"[42]. Rzeczywistość wirtualna oznacza zatem nierzeczywisty świat stworzony za pomocą komputera i dodatkowych akcesoriów multimedialnych, zgromadzony w zasobach internetowych i na innych nośnikach informacji. Jej celem jest stworzenie sztucznego środowiska, które w jak największym stopniu przypominałoby realny świat.

Wirtualna rzeczywistość jest wytworem technologii informatycznej, która umożliwia wejście i przebywanie w świecie wytworzonym przez komputer. Jest to swoista kombinacja emocji, wrażeń i sposobu ich odbioru przez poszczególnych użytkowników. Otwiera przed nimi ogromne możliwości: daje im dostęp do zasobów informacyjnych

---

[38] Za: R. Kwećka, *Informacja w walce zbrojnej*, Warszawa 2001, s. 82. Teza ta zawarta jest w książce: H.A. Tofler, *Wojna i antywojna*, Warszawa 1997, s. 218.

[39] Internet World Stats, *Internet Growth Statistics*, www.internetworldstats.com/emarketing.htm (dostęp: 14.06.2014).

[40] *Słownik współczesnego języka polskiego*, t. 2, red. A. Sikorska-Michalak, O. Wojniłko, Warszawa 1998, s. 31.

[41] Podaję za: J. Bednarek, *Teoretyczne i metodologiczne podstawy badań nad człowiekiem w cyberprzestrzeni*, [w:] *Cyberświat. Możliwości i zagrożenia*, red. J. Bednarek, A. Andrzejewska, Warszawa 2009, s. 28.

[42] Por.: *Słownik wyrazów obcych PWN*, red. J. Tokarski, Warszawa 1980.

niemalże na całym świecie, sprowadza odległość w tradycyjnym znaczeniu do roli nieistotnego czynnika, zmieniając jednocześnie sposób tradycyjnego pojmowania czasu i przestrzeni. Z technicznego punktu widzenia to nic innego, jak komputerowa symulacja obrazu, dźwięku, ale także realnej rzeczywistości, do której „wejść" i z której „wyjść" można w każdej chwili, której jest się w stanie doświadczać, a nawet „dotknąć"[43].

W cyberprzestrzeni pojawia się obecnie wiele wirtualnych światów. Dla wielu ludzi staje się ona nieodłączną częścią codzienności. Ludzie znajdują się w cyberprzestrzeni, gdy czytają elektroniczną korespondencję, korzystają z e-booków, elektronicznych mediów, kiedy rezerwują bilet na samolot czy pociąg, dokonują przelewów środków finansowych z osobistego konta. W cyberprzestrzeni można prowadzić rozmowy telefoniczne, wideokonferencje, oglądać filmy, słuchać muzyki i korzystać z gier komputerowych. Stwarza ona możliwość budowania nowych, czasami silnych więzi w ramach wirtualnych społeczności, pomimo że wirtualnych znajomych zazwyczaj nie spotyka się fizycznie w realnym świecie. Rzeczywistość wirtualną można wykorzystywać w wielu dziedzinach życia publicznego i gospodarczego: do kontroli ruchu drogowego, w medycynie, rozrywce, jako narzędzie w pracy zawodowej czy w różnych gałęziach przemysłu. Cyberprzestrzeń pełni przez to funkcje edukacyjną, usługową, rozrywkową, społeczną, ekonomiczną czy kulturotwórczą, ale również i militarną.

Cyberprzestrzeń to jednak nie tylko pole nowych jakościowo możliwości, które mogą ułatwiać współczesnemu człowiekowi życie, to także przestrzeń nowych jakościowo zagrożeń nie tylko w wymiarze personalnym, ale i narodowym, a nawet międzynarodowym. Może być przyczyną uzależnień, nośnikiem zachowań i wartości niezgodnych ze społecznie akceptowanymi wzorcami, narzędziem nowych jakościowo form przestępczości, przestrzenią działań terrorystycznych, a także areną cyberwojny, gdy postrzegamy ją w perspektywie zagrożeń militarnych.

Brak jednoznacznej definicji cyberprzestrzeni powoduje pewne trudności w jej analizie z perspektywy bezpieczeństwa. Cyberprzestrzeń to w ujęciu ogólnym cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[44]. Traktuje się ją również jako mającą charakter wirtualny (nieprzestrzenny w sensie fizycznym, aterytorialny, ageograficzny) całość istniejących w świecie powiązań powstałych i realizowanych bądź przez technologie informatyczne i ich fizyczne manifestacje, bądź też na ich podstawie[45].

Cyberprzestrzeń powstała w wyniku upowszechniania się technologii informatycznych, jest dla jej użytkowników zupełnie nową płaszczyzną aktywności i środowiskiem działań o bardzo specyficznym charakterze. Dotyczy to nie tylko podmiotów korzystających z zasobów informatycznych zgodnie z obowiązującymi zasadami i literą prawa, ale również tych, którzy mogą wykorzystać technologie informatyczne w celach przestępczych, terrorystycznych czy militarnych. Warto zatem w tym miejscu

---

[43] Por.: J. Bednarek, *Media w nauczaniu*, Warszawa 2002, s. 278.

[44] *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, Warszawa 2010, s. 6.

[45] A. Bógdał-Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 37–39.

zwrócić uwagę na te jej cechy, które pozwalają na wykorzystywanie jej do działań zagrażających bezpieczeństwu.

Najbardziej oczywistą właściwością aktywności podejmowanej w cyberprzestrzeni, wynikającą bezpośrednio z jej aterytorialności i amaterialności, jest pełne uniezależnienie się od ograniczeń przestrzennych, głównie geograficznych. Działania w cyberprzestrzeni można zainicjować praktycznie z każdego miejsca na świecie, a jedynym wymogiem jest techniczna możliwość połączenia się z siecią internetową[46]. Z aterytorialności cyberprzestrzeni, a także z szybkiego tempa rozwoju technologii informatycznych wynika stosunkowo niski koszt rozpoczęcia i prowadzenia w niej działań. W praktyce nakłady wymagane do ich podjęcia ograniczają się do zakupu odpowiedniego sprzętu i oprogramowania, zapewnienia dostępu do Internetu oraz zdobycia wiedzy i umiejętności niezbędnych w tego typu działaniach[47].

Istotną cechą funkcjonowania w cyberprzestrzeni jest możliwość zachowania anonimowości. Nie wynika to jednak z istoty cyberprzestrzeni, ale z jej konstrukcji i istniejącej w niej sieci powiązań oraz możliwości technologicznych. Dostęp do sieci internetowej nie wymaga obowiązkowej autoryzacji, dodatkowo ograniczone są możliwości śledzenia wszelkich czynności podejmowanych w sieci. Trudność identyfikacji sprawców oznacza również małe prawdopodobieństwo ich wykrycia, przeciwdziałania skutkom ich działalności, niewielkie możliwości podejmowania odwetu czy ich ukarania[48]. Powoduje to, że sprawcy cybernetycznych przestępstw czują się nie tylko anonimowo, ale i bezkarnie.

Działania te są ponadto nieprzewidywalne pod kątem miejsca i czasu ich wystąpienia. Niemożliwe jest również wykrycie przygotowań jakiegokolwiek użytkownika Internetu do podjęcia niezgodnych z prawem czynów. W praktyce trudno jest też odróżnić awarie sieci od działań zamierzonych. Wszystko to w konsekwencji ogranicza możliwości obrony ewentualnych ofiar przed zagrożeniami i redukuje zdolności zapobiegania ich urzeczywistnieniu[49].

Kolejną istotną cechą działań w cyberprzestrzeni, a konkretniej ich następstw, jest systemowy charakter i szeroki zasięg. Podmioty działające w sieci mogą teoretycznie uzyskiwać równoczesny dostęp do bardzo wielu elementów sieci, a następnie wpłynąć na ich bezpieczeństwo. Skutki mogą być złożone, objąć swoim zasięgiem wiele składników i wielu użytkowników cyberprzestrzeni, nawet w najodleglejszych zakątkach świata, mogą być długotrwałe i kosztowne. Zasięg ewentualnych konsekwencji tego typu operacji potęguje monokulturowość cyberprzestrzeni, polegająca na daleko idącej standaryzacji stosowanych w niej procedur oraz ujednoliceniu stosowanego oprogramowania w globalnej sieci[50]. Podkreślenia wymaga fakt, że taka

---

[46] A.D. Sofaer, S.E. Goodman, *Cyber Crime and Security: The Transnational Dimension*, [w:] *The Transnational Dimension of Cyber Crime and Terrorism*, red. A.D. Sofaer, S.E. Goodman, Stanford 2001, s. 6–7.

[47] Por.: M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 330.

[48] Por.: K. Soo Hoo, S. Goodman, L. Greenberg, *Information Technology and Terrorist Threat*, „Survival" 1997, t. 39, nr 3, s. 142–143.

[49] Por.: G. Weimann, *Cyberterrorism, How Real is The Threat?*, Washington 2004, s. 6; Ow Kim Meng, *Cyber-Terrorism: An Emerging Threat of The New Millennium*, „Pointer" 2002, t. 28, nr 3, s. 100–102; M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 332.

[50] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 333.

działalność może przynieść niewspółmiernie wysokie efekty przy stosunkowo niewielkim zaangażowaniu sił i środków oraz niskich nakładach finansowych. Michael McConnel uważa, że „atak cyfrowy na pojedynczy bank amerykański spowodowałby większe straty materialne niż zamachy z 11 września 2001 roku”[51].

Wszystkie z przedstawionych powyżej cech są przesłankami do tego, żeby zagrożenia cyberprzestrzeni traktować w kategorii zagrożeń asymetrycznych.

Warto zauważyć, że sieci informatyczne już od momentu powstania były polem pierwszych, jeszcze niezbyt spójnych, prób ich wykorzystania do celów politycznych bądź militarnych. Chronologicznie pierwsza była prawdopodobnie operacja przeprowadzona przez amerykańską CIA w 1982 r. W kanadyjskim programie przemysłowym, skradzionym przez radzieckich szpiegów amerykańskim agentom, udało się umieścić tzw. bombę logiczną.

W chwili obecnej ataki cybernetyczne

> […] stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej, mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności[52].

Przykłady najbardziej spektakularnych ataków cybernetycznych zestawiono w tabeli nr 1.

Tabela 1

Przykłady ataków cybernetycznych

Table 1

Examples of cyber attacks

Rok	Cel ataku	Szczegóły ataku
1998–2000	instytucje w USA	Afera znana pod nazwą Moonlight Maze, która rozpoczęła się w 1998 roku i trwała dwa lata. Był to skoordynowany atak rosyjskich hakerów na serwery wielu amerykańskich instytucji rządowych i prywatnych, w tym m.in. Pentagonu, NASA, Departamentu Energii, uniwersytetów oraz instytutów badawczych.
1999	infrastruktura teleinformatyczna Serbii	Podczas operacji NATO w Kosowie informatycy Sojuszu dokonali wielu ataków w cyberprzestrzeni, których celem było zablokowanie infrastruktury teleinformatycznej Serbii. W odwecie serbscy hakerzy podjęli wiele prób zablokowania serwerów Paktu Północnoatlantyckiego.

[51] Podaję za: B. Bartoszek, *Cyberwojna – wojna XXI wieku*, www.mojeopinie.pl/cyberwojna_wojna_xxi_ wieku,3,1215862210 (dostęp: 15.04.2014).

[52] *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie*, tłumaczenie robocze BBN, www.bbn.gov.pl/pl/wydarzenia/2694,dok.html (dostęp: 14.03.2014).

Rok	Cel ataku	Szczegóły ataku
2003	amerykańskie serwery rządowe i korporacyjne	Afera znana jako Titan Rain. Seria skoordynowanych ataków chińskich hakerów w celu pozyskania poufnych informacji m.in. z NASA, Lockheed-Martin czy Redstone Arsenal. Chińczycy zdobyli informacje m.in. na temat programu F-35 Joint Strike Fighter.
2007	instytucje rządowe, sieci energetyczne, banki w Estonii	Akcja rosyjskich hakerów określana jako **pierwsza cyberwojna**. Szczególnie groźne okazały się ataki na system bankowy. Ze względu na fakt, że około 90% transakcji bankowych odbywało się tam za pomocą Internetu, system ten został w zasadzie sparaliżowany. Był to pierwszy przypadek w historii, kiedy za pomocą ataku cybernetycznego obcemu państwu udało się sparaliżować na pewien czas funkcjonowanie ważnych instytucji państwowych i prywatnych.
2007	sieć informatyczna syryjskiego systemu obrony przeciwlotniczej	Izraelczycy wykorzystali wirusa komputerowego Suter, który pozwolił nie tylko na atak na sieci komputerowe i telekomunikacyjne przeciwnika, ale jednocześnie na monitorowanie i przejęcie kontroli m.in. nad systemami radarowymi obrony powietrznej. Dzięki temu dokonano bombardowania syryjskiego ośrodka wojskowego, w którym prowadzono prace nad bronią atomową, bez zaalarmowania syryjskiej obrony przeciwlotniczej. Jest to przykład użycia ataku cybernetycznego w celach militarnych.
2008	Osetia, Gruzja	Tak zwana **druga wojna cybernetyczna** tocząca się równolegle z konfliktem w Osetii Południowej. Przed jego wybuchem gruzińscy hakerzy dokonali dwóch ataków na strony osetyńskiej agencji informacyjnej oraz radia rządowego w Cchinwali. W ich wyniku media te zaczęły nadawać informacje podawane przez Alania TV, gruzińską stację telewizyjną skierowaną do Osetyńczyków. Po zaangażowaniu Rosji w konflikt rosyjscy hakerzy dokonali serii ataków na strony internetowe najważniejszych instytucji państwowych Gruzji, w tym na witrynę prezydenta Micheila Saakaszwiliego, rządu, ministra spraw zagranicznych oraz ministra obrony. Zablokowano również dostęp do serwerów naukowych i komercyjnych.
2008	amerykańskie sieci wojskowe na Bliskim Wschodzie	Za pomocą pamięci USB do sieci wojskowych zostało przeniesione złośliwe oprogramowanie, które błyskawicznie rozprzestrzeniło się m.in. na komputery Pentagonu. Umożliwiło to hakerom m.in. transfer tajnych danych wojskowych poza zabezpieczone serwery. Atak przez długi czas pozostał niewykryty i stanowił największe w historii włamanie do sieci militarnych USA. Przeprowadzony prawdopodobnie przez rosyjskich hakerów.
2009	sieci informatyczne 103 krajów	Chińska grupa cyberszpiegowska, ochrzczona mianem Ghostnet, dokonała włamań do 1295 komputerów należących do instytucji państwowych, polityków, korporacji czy instytucji badawczych w 103 krajach. Według informacji podanych przez Information Warfare Monitor Ghostnet był

Rok	Cel ataku	Szczegóły ataku
		w stanie przez długi okres kontrolować komputery należące do ministerstw spraw zagranicznych m.in.: Iranu, Bhutanu, Indonezji, Bangladeszu, Filipin, Brunei, Barbadosu czy Łotwy. Włamano się również do serwerów ambasad Pakistanu, Korei Południowej, Niemiec, Cypru, Tajlandii oraz Indii. Ponadto chińskim hakerom udało się uzyskać dostęp do komputerów osobistych tybetańskich opozycjonistów, w tym sekretariatu Dalajlamy.
2009	amerykańskie korporacje	Operacja Aurora, przeprowadzona przez chińskich hakerów przeciwko ponad 20 korporacjom amerykańskim w drugiej połowie 2009 r. Wśród zaatakowanych znalazły się m.in.: Google, Adobe Systems, Northrop Grumman, Yahoo i Symantec. Celem ataku było uzyskanie nowoczesnych technologii oraz specjalistycznego oprogramowania używanego przez te firmy.

Źródło: *Cyberwojna jako rzeczywistość XXI wieku*, raport zamieszczony na stronie Europejskiego Centrum Analiz Geopolitycznych, www.geopolityka.org/analizy/1813-cyberwojna-jako-rzeczywistosc-xxi-wieku (dostęp: 15.05.2014).

Zagrożenia w cyberprzestrzeni dotyczą również Polski. O skali tego typu zagrożeń świadczą chociażby dane zawarte w *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*[53]. Zgodnie z Raportem sporządzonym przez Zespół CERT.GOV.PL[54] rok 2013 pod względem liczby otrzymanych zgłoszeń oraz obsłużonych incydentów okazał się rekordowy w stosunku do lat poprzednich. W sumie w 2013 roku zarejestrowanych zostało aż 8817 zgłoszeń, z których 5670 zakwalifikowano jako incydenty.

W obliczu globalizacji ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. W czasach, gdy panuje swoboda przepływu osób, towarów, informacji i kapitału – bezpieczeństwo demokratycznego państwa zależy od wypracowania mechanizmów pozwalających skutecznie zapobiegać zagrożeniom bezpieczeństwa cyberprzestrzeni i je zwalczać. Obecnie w cyberprzestrzeni granica między pokojem a wojną staje się coraz bardziej umowna. Cyberwojna staje się stopniowo rzeczywistością. Co prawda nie doszło jeszcze do otwartego konfliktu międzypaństwowego w tym wymiarze, jednak dotychczasowe wydarzenia wskazują, że można mówić już nie tylko o „zimnej wojnie w cyberprzestrzeni" czy wyścigu zbrojeń, lecz o regularnych starciach między poszczególnymi aktorami na arenie międzynarodowej[55]. Zdaniem Mikko Hypponena państwa „[…] atakują się wzajemnie przy pomocy złośliwego oprogramowania.

[53] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*, CERT.GOV.PL, Warszawa 2014, www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/686,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2013-roku.html (dostęp: 15.05.2014).

[54] Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej. Działalność zespołu finansowana jest przez NASK.

[55] Zob.: *Virtual Criminology Report 2009*, McAfee Corporation, 2009; D. Gardham, *Hackers recruited to fight 'new cold war'*, „The Telegraph" 26 czerwca 2009 r.

Cyberwojenna rewolucja już trwa”[56]. Z tej przyczyny warto przyjrzeć się bliżej zagadnieniom związanym z zagrożeniami militarnymi cyberprzestrzeni zarówno w ich wymiarze międzynarodowym, jak i narodowym.

Oblicza współczesnej cyberwojny

Przestrzeń cybernetyczna jest dzisiaj uważana jako piąty wymiar pola walki[57], istniejący obok trójwymiarowej przestrzeni kartezjańskiej (x, y, z) i wymiaru czasowego (t)[58]. W chwili obecnej, w dobie intensywnego rozwoju sieci internetowej i rozbudowy globalnej sieci informatycznej, problem ten wymaga szczególnej uwagi.

Z perspektywy militarnej światowa infrastruktura informatyczna, czyli realna infrastruktura wymiaru cybernetycznego, to

> […] aspekt strefy konfliktu obejmujący pełny zakres zjawisk elektromagnetycznych i pozaludzki wymiar rozpoznania (wykrywania celów), w którym siły zamaskowane techniczne (*stealth*) – trudne do wykrycia środkami technicznymi – prowadzą operacje zaczepne lub ukrywające się przed takimi operacjami[59].

Zatem globalną sieć informatyczną można rozpatrywać jako pole współczesnej walki prowadzonej z wykorzystaniem narzędzi informatycznych[60].

W cyberprzestrzeni rozgrywać się może, a praktycznie już rozgrywa, nowy rodzaj wojny, czyli wojna informacyjna. Według Amerykańskiego Depratamentu Obrony definiuje się ją jako działania podjęte w celu osiągnięcia informacyjnej przewagi, wspierające narodową strategię militarną poprzez oddziaływania na informację i systemy informacyjne przeciwnika, przy jednoczesnej ochronie własnych informacji i systemów informacyjnych[61]. Z kolei walka informacyjna w ogólnym znaczeniu to sposób działania, którego celem jest zdobycie i wykorzystanie zasobów informacyjnych[62].

Zatem wojna, a właściwie walka informacyjna obejmuje całość czynności podejmowanych przez uczestników danego konfliktu zmierzających do uzyskania kon-

---

[56] M. Hypponen, *Cyberwojna stała się rzeczywistością*, tech.wp.pl/kat,1009785,title,Cyberwojna-stala-sie-rzeczywistoscia,wid,14867034,wiadomosc.html (dostęp: 15.03.2014).

[57] Prekursorem takiego podejścia był John A. Warden, który już w 1995 r. stwierdził, że cyberprzestrzeń jest obok lądu, morza, powietrza i przestrzeni kosmicznej piątym wymiarem walki zbrojnej. J.A. Warden, *Enemy as a System*, „Airpower Journal” 1995, nr 9, s. 40–55. Zobacz także: R. Fry, *Fighting Wars in Cyberspace*, „The Wall Street Journal” 21 lipca 2010 r., s. 45; P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, red. L.H. Haber, Kraków 2003, s. 376–377.

[58] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 49.

[59] Tamże.

[60] Najważniejszym ogniwem cyberprzestrzeni, stanowiącym jej szkielet, jest Internet. Internet to zespół połączonych ze sobą (*interconnected*) sieci komunikacyjnych umożliwionych transfer danych w postaci cyfrowej. B. Schmitt, *Information Security. A New Challenge for the UE*, „Chaillot Paper” 2005, nr 76, podaję za: M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 324.

[61] Podaję za: P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 49.

[62] Zob.: D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 23–25.

troli nad treścią, przepływem i dostępnością istotnych informacji. Tak pojmowana walka informacyjna, będąca przejawem wojny informacyjnej, nie ogranicza się tylko do operacji prowadzonych przy użyciu technologii informatycznych albo przez infrastrukturę zbudowaną na bazie tych technologii, lecz może przybrać postać wielu innych form aktywności, zarówno fizycznych, jak i wyłącznie symbolicznych z wykorzystaniem technologii teleinformatycznych[63].

Martin Libicki zwrócił uwagę na siedem form walki informacyjnej, które mogą przyjąć postać: walki w zakresie systemów dowodzenia i kontroli (*command-and-control warfare*), walki opartej na wywiadzie (*intelligence-based warfare*), wykorzystywania technik radioelektronicznych i kryptografii (*electronic warfare*), działań psychologicznych (*psychological warfare*), operacji hakerskich (*hacker warfare*), ekonomicznej walki informacyjnej (*economic information warfare*) i walki cybernetycznej (*cyberwarfare*)[64].

Jak pokazują liczne przykłady, w działania w cyberprzestrzeni zaangażowane są często podmioty pozapaństwowe, przede wszystkim hakerzy (czasami są przykrywką dla działalności instytucji państwowych, głównie wywiadu), jakkolwiek po technologie te sięgają również organizacje terrorystyczne i zorganizowane grupy przestępcze. Dla tego typu działań trudno jest zastosować pojęcie wojny czy walki informacyjnej, stąd też operuje się coraz powszechniej innym pojęciem, odnoszącym się do działań podmiotów pozapaństwowych, a mianowicie pojęciem cyberkonfliktu.

Cyberkonflikt, czyli konflikt cybernetyczny, określany jest często jako

> […] konflikt angażujący różnorodne systemy ludzi, rzeczy, procesów i postrzegania, które związane są z sieciami komputerowymi, choć niekoniecznie całkowicie skomputeryzowane. Konfliktem cybernetycznym będzie zatem każdy konflikt, w którym sukces lub porażka są dla większości jego uczestników uzależnione od działań prowadzonych w sieciach komputerowych[65].

Cyberkonflikty mogą przybrać postać trzech podstawowych form aktywności[66]:

- **aktywizmu** – niedestrukcyjnej działalności niektórych grup, w ramach której Internet służy do wsparcia prowadzonej kampanii;
- **haktywizmu** – kombinacji aktywizmu i działań przestępczych; haktywizm wykorzystuje metody hakerskie przeciwko określonym celom w Internecie, by zakłócić ich funkcjonowanie, nie powodując przy tym poważnych strat; działalność ta ma na celu nie tyle pozyskanie czy zniszczenie zasobów przeciwnika, ile przede wszystkim zwrócenie uwagi na dany problem;
- **cyberterroryzmu** – politycznie motywowanego ataku lub groźby ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych działań, w szerszym rozumieniu tego słowa, zastosowanych przez organizacje terrorystyczne.

---

[63] Por.: M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 325.
[64] Por.: M. Libicki, *What is Information Warfare?*, Washington 1995.
[65] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie*…, s. 16.
[66] Tamże, s. 17.

Powszechnie stosowaną praktyką jest również użycie cyberprzestrzeni do celów wywiadowczych, w tym do celów o charakterze militarnym. Jak podano w raporcie opracowanym przez służby kontrwywiadowcze Stanów Zjednoczonych[67], niektóre państwa (w domyśle Rosja i Chiny) wykorzystują na szeroką skalę cyberprzestrzeń do zbierania danych wywiadowczych szczególnie danych gospodarczych dotyczących nowoczesnych technologii, przemysłu obronnego, farmaceutycznego itp. Ze względu na niskie koszty i łatwość uniknięcia wykrycia **cyberszpiegostwo** jest niezwykle efektywną i stosowaną coraz powszechniej formą prowadzenia działalności wywiadowczej[68].

Uwzględniając dość szeroki zakres pojęciowy i wymiar pragmatyczny działań w cyberprzestrzeni w celach militarnych, można wyróżnić, zdaniem J. Arquilli i D. Ronfeldta, dwa rodzaje wojny informacyjnej, a właściwie wojny w cyberprzestrzeni[69]:

- **netwar**, czyli konflikt, który toczy się między państwami, społeczeństwami i narodami, polegający na niszczeniu bądź modyfikowaniu informacji w celu zmiany poglądów o państwie będącym celem ataku, o jego społeczeństwie czy otoczeniu; jest to konflikt o charakterze społeczno-kulturowym, a co ważne, dotyczy głównie samej cyberprzestrzeni;
- **cyberwar**, czyli prowadzenie i przygotowanie działań militarnych z wykorzystaniem informacji jako podstawowego elementu uzyskania przewagi lub też innych technologii mogących oddziaływać na cyberprzestrzeń, a w konsekwencji zakłócających procesy informacyjne w niej zachodzące.

Netwar można określić jako wojnę idei, której środkiem walki staje się szeroko rozumiana informacja. Działania tego typu określane były w historii jako wojna czy walka propagandowa albo też częściej jako wojna psychologiczna. Wojna psychologiczna, w klasycznym ujęciu, definiowana jest jako „[…] system oparty na specjalnych metodach i sposobach oddziaływania dywersji polityczno-propagandowej na żołnierzy i społeczeństwo przeciwnika, w celu osłabienia ich odporności psychicznej”[70] lub też jako „[…] system zabiegów propagandowych w celu pozyskania społeczeństwa do realizacji polityki agresywnej”[71]. Wojna psychologiczna, w klasycznym ujęciu, charakteryzuje się: całkowitym lub pozornie całkowitym zsynchronizowaniem zadań politycznych, propagandowych i wojskowych, a także zastosowaniem zdobyczy nowoczesnej psychologii do osiągnięcia celów militarnych[72]. Jeżeli powyższe cechy uzupełnimy jeszcze o jedną, czyli wykorzystanie nowoczesnych technologii informatycznych, to mamy do czynienia z niemal wszystkimi istotnymi cechami współczesnej netwojny.

---

[67] Chodzi tu o raport: *Foreign Spies Stealing US Economic Secrets in Cyberspace*, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011, October 2011 r., www.ncix.gov/publica tions/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (dostęp: 20.05.2013).

[68] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe” 2012, nr II (22), s. 127 (szerzej: tamże, s. 125–137). Zobacz też: M. Grzelak, *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe” 2013, nr II (26), s. 111–127.

[69] Podaję za: K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 21.

[70] *Leksykon wiedzy wojskowej*, red. M. Laprus, Warszawa 1979, s. 482.

[71] Tamże.

[72] P.M.A. Linebarger, *Wojna psychologiczna*, Warszawa 1959, s. 61.

Netwojna sprowadza się przede wszystkim do wszelkich działań zmierzających do dezintegracji więzi łączącej państwo i społeczeństwo, podważenia zaufania społeczeństwa do instytucji państwa czy też manipulowania opinią społeczną we własnych celach, zarówno militarnych, jak i pozamilitarnych[73]. Netwojna to zatem konflikt skierowany przeciwko komunikacji i przepływowi informacji, wykorzystujący nowoczesne rozwiązania technologiczne, do osiągnięcia własnych celów. Netwojny mogą przybierać różne formy i dotyczyć działań podejmowanych pomiędzy[74]:

- rządami skonfliktowanych państw;
- rządami państw a aktorami niepaństwowymi;
- rządem a aktywnymi społecznie grupami obywateli, którzy mogą protestować przeciwko całej, polityce rządu lub jej części.

W przypadku działań o charakterze militarnym netwojna sprowadza się do walki informacyjnej, którą w NATO definiuje się jako „[…] działania informacyjne prowadzone w okresie kryzysu lub konfliktu zbrojnego z zamiarem promowania określonego celu politycznego i lub wojskowego w odniesieniu do wskazanego przeciwnika bądź przeciwników”[75]. Walka informacyjna prowadzona jest poprzez podejmowanie operacji informacyjnych obejmujących działania wspierające

> […] wyselekcjonowane cele polityczne i wojskowe, podejmowane z zamiarem wpłynięcia na decydentów i polegające na oddziaływaniu na procesy oparte na informacji oraz systemy dowodzenia, łączności i rozpoznania, przy równoczesnym zapewnieniu ochrony własnemu systemowi informacyjnemu[76].

W ujęciu militarnym można wyróżnić cztery podstawowe formy ataku informacyjnego:

- zrywanie procedur wymiany informacji;
- manipulowanie informacją (dezinformacja, zatajanie, przekształcanie informacji);
- nieautoryzowane korzystanie z zasobów informacyjnych (np. baz danych) oraz kopiowanie i niszczenie danych;
- masowe niszczenie oprogramowania systemowego.

Ataki tego typu mogą być prowadzone z wykorzystaniem następujących metod i narzędzi:

- wirusów komputerowych;
- bomb logicznych;
- blokowania wymiany informacji w systemach łączności;
- fałszowania informacji znajdujących się w bazach danych w systemach informatycznych przeciwnika;
- wprowadzania w obieg – z wykorzystaniem różnych technologii komunikowania – spreparowanych informacji[77].

Analizując możliwości wykorzystania nowoczesnych technologii informatycznych jako środków ataków przez podmioty niepaństwowe, Marek Madej dzieli je

---

[73] Por.: K. Liedel, *Bezpieczeństwo informacyjne w dobie…*, s. 22.
[74] Szerzej: J.J. Arquilla, D.F. Ronfeldt, *Cyberwar is coming*, „Comparative Strategy” 1993, vol. XII, s. 141–165.
[75] Podaję za: P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 42.
[76] Tamże.
[77] Tamże, s. 42–43.

na dwie zasadnicze grupy: operacje o skutkach ograniczonych wyłącznie do cyberprzestrzeni oraz działania o bezpośrednich następstwach również w świecie rzeczywistym[78]. Do działań pierwszej grupy można jego zdaniem zaliczyć następujące działania:

- wymierzone w strony internetowe atakowanego podmiotu (*website defacement*);
- uniemożliwiające albo korzystanie z określonej usługi sieciowej, albo jej świadczenie na własnych zasadach bądź też blokujące pracę urządzeń podłączonych do Internetu, co dokonuje się głównie przez tzw. *flooding* (przepełnienie, czyli przeciążenie pracy urządzeń wskutek przesyłania do nich nadmiernej liczby informacji);
- polegające na włamaniu się do komputerów pracujących w sieci w celu zniszczenia, pozyskania lub zmiany przechowywanych w nich zasobów informacyjnych[79].

Zatem działania zaliczane do pierwszej grupy są typowe dla zaliczanych do netwojny. Drugą grupę, czyli działania o bezpośrednich skutkach nieograniczonych wyłącznie do cyberprzestrzeni, ale powodujących też zniszczenia fizyczne, można z kolei zaliczyć do działań charakterystycznych dla kolejnego rodzaju wojny informacyjnej, a mianowicie do cyberwojny (*cyberwar*).

W ujęciu słownikowym *cyberwar* to wykorzystanie technologii komputerowej do zakłócenia działalności państwa lub organizacji, w szczególności zamierzonego atakowania systemów komunikacyjnych przez inne państwo lub organizację[80]. Zdaniem Richarda A. Clarka cyberwojna jest „działalnością państw, mającą na celu penetrację systemów i sieci komputerowych innych podmiotów międzynarodowych dla dokonania określonych zniszczeń lub zakłóceń"[81]. W ramach wojny cybernetycznej napastnik może dążyć do osiągania rozmaitych celów, od rozpowszechniania propagandy lub wywoływania paniki pośród ludności cywilnej po trwałe uszkodzenie kluczowych elementów infrastruktury technologicznej (elektrownie, systemy komunikacyjne itp.). Ataki mogą też być narzędziem wywiadu i pozyskiwania wrażliwych i chronionych informacji. Może wykorzystywać również inne technologie przełamujące tradycyjne ograniczenia przestrzeni fizycznej (np. promieniowanie elektromagnetyczne czy neutronowe).

Zgodnie z teorią RAND wojna cybernetyczna jest konfliktem o wysokiej intensywności i szerokim spektrum działań. Może ona angażować różnorodne technologie (nie tylko informatyczne), m.in.[82]:

- dowodzenia i kontroli,
- gromadzenia informacji wywiadowczych,

---

[78] Zob.: M. Libicki, *What is Information Warfare?...*, s. 50-51; M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 444.

[79] Zob.: J.D. Howard, T.A. Longstaff, *A Common Language for Computer Security Incidents*, Sandia Report, Sandia National Laboratories, Albuquerque-Livermore 2002; M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 446.

[80] English Oxford Living Dictionary, *Cyberwar*, [hasło], oxforddictionaries.com/definition/english/cyberwar (dostęp: 15.03.2014).

[81] R.A. Clarke, R. Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, New York 2010.

[82] J. Arquilla, D. Ronfeldt, *Cyberwar is coming!*, [w:] *In Athena's Camp…*, s. 30.

- przetwarzania i dystrybucji informacji,
- identyfikacji „przyjaciel–wróg”,
- systemy „inteligentnej” broni.

O istocie cyberwojny w sensie militarnym decyduje nie tylko użycie różnorodnych technologii, ale również możliwość przezwyciężenia w cyberprzestrzeni ograniczeń czasoprzestrzennych, takich jak[83]:

- fizyczna odległość i położenie obiektów w przestrzeni – wymiar cybernetyczny zniekształca tradycyjne relacje czasoprzestrzenne poprzez powiększanie lub pomniejszanie istniejącej przestrzeni;
- czas konieczny do przebycia odległości między obiektami – wymiar cybernetyczny może powodować kompresję przestrzeni czasowej, a nawet eliminację czasu (na przykład przy użyciu broni wiązkowej, w tym laserowej, wykorzystującej ukierunkowaną energię, eliminuje się nią takie pojęcia, jak „czas lotu do celu”, gdyż „wystrzał” i „trafienie” są w jej przypadku prawie równoczesne);
- fizyczna struktura i wymiar obiektów wojskowych – wymiar cybernetyczny pozwala chociażby poprzez użycie energii elektromagnetycznej czy promieniowania neutronowego (mających właściwości przenikania przez różnego rodzaju materiały) na przezwyciężenie ograniczeń dostępności do celu ukrytego w obronnych konstrukcjach wojskowych.

Z cybernetycznym wymiarem współczesnego pola walki wiążą się różne koncepcje prowadzenia działań zarówno ofensywnych, jak i defensywnych, wśród których na uwagę zasługują: koncepcja atakowania powiązań oraz idea tarczy cybernetycznej.

Pierwsza z powyższych, czyli **atakowania powiązań**, pozwala w swojej istocie na uniknięcie masowych zniszczeń towarzyszących tradycyjnym konfliktom zbrojnym. Zgodnie z jej podstawowymi założeniami celem ataku nie są same obiekty, a powiązania między nimi. W praktyce oznacza to, że podjęcie tego typu działań w stosunku do wrogiego państwa, miasta czy społeczności wyłącznie w przestrzeni cybernetycznej ma doprowadzić je stanu rzeczywistego chaosu wewnętrznego[84].

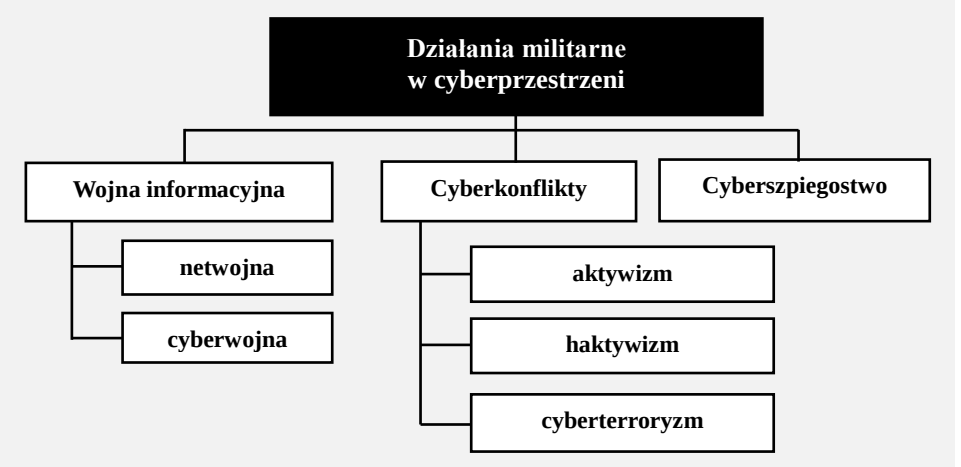
Z kolei **tarcza cybernetyczna** oznacza zdolność do przezwyciężania uderzenia broni precyzyjnego rażenia (np. broni rakietowej, pocisków samosterujących) w wyniku utworzenia niewidzialnej tarczy wokół wojsk (innych obszarów). Tarcza ta, w zależności od zastosowanej technologii, może spowodować przedwczesną detonację środka ogniowego rażenia, „oślepienie” urządzeń nawigacyjnych samolotów i latających środków bezzałogowych, stworzenie kurtyny akustycznej, holograficznej czy bariery optycznej[85].

Cyberprzestrzeń rozszerza dzisiaj w sposób wyraźny pojęcie pola walki. Stawarza nowe jakościowo możliwości wykorzystania jej do celów militarnych, ale również może stać się areną zmagań z udziałem aktorów niepaństwowych jako uczestników międzynarodowego środowiska bezpieczeństwa. Te możliwości cyberprzestrzeni powodują, że staje się ona ważnym czynnikiem kształtowania bezpieczeństwa poszczególnych państw, jak również podmiotów ponadnarodowych.

---

[83] Szerzej: P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 49–52.
[84] Tamże, s. 52–54.
[85] Tamże, s. 55–56.

Reasumując dotychczasowe rozważania, można przyjąć, że działania militarne w cyberprzestrzeni można podzielić na trzy kategorie: wojnę informacyjną (w tym netwojnę i cyberwojnę), cyberszpiegostwo oraz cyberkonflikty. Podział ten ilustruje rycina 1.



Ryc. 1. Klasyfikacja działalności o charakterze militarnym w cyberprzestrzeni
Fig. 1. Classification of activities of a military nature in cyberspace

Źródło: opracowanie własne.

Warto w tym miejscu wspomnieć, że w 2011 r. pojawiły się informacje na temat wynalezienia tzw. ostatecznej broni w Internecie. Naukowcom z University of Minnesota udało się opracować metodę ataku w cyberprzestrzeni, której skutkiem byłoby sparaliżowanie Internetu na całym świecie. Nowy sposób polega na ataku na węzły sieci – routery – za pomocą bardzo dużej sieci botnet, liczącej około 250 tysięcy komputerów (typowy atak na powiązania sieci). Według specjalistów obecna struktura Internetu nie pozwala na obronę przed taką metodą ataku, jednak jest on mało prawdopodobny. Sposób ten może być jednak potencjalnie użyty jako „broń ostateczna" w cyberwojnie[86].

Współczesne dylematy cyberobrony

Obecnie można zaobserwować, jak zmieniają się zagrożenia w cyberprzestrzeni i działania, które podejmowane są w celu jej militarnego wykorzystania. Pomimo powszechności dostępu do cyberprzestrzeni najbardziej niebezpiecznymi podmiotami w tym zakresie pozostają nadal państwa narodowe, często ukrywające swoje działania pod przykrywką hakerów czy haktywistów[87]. Zorganizowane ataki cyber-

[86] *The Cyberweapon That Could Take Down the Internet*, „Financial News Now!" 14 lutego 2011 r., podaję za: *Cyberwojna jako rzeczywistość...*

[87] Największym zagrożeniem w tym zakresie są dzisiaj Rosja i Chiny.

netyczne na szeroką skalę, cyberszpiegostwo lub sabotaż w sieci wymagają stosunkowo dużych nakładów finansowych, dysponowania odpowiednim potencjałem technologicznym, a także zaangażowania wysokiej klasy specjalistów, stąd też w najbliższym czasie tego typu działania nie będą podejmowane przez podmioty pozapaństwowe, w tym organizacje terrorystyczne czy zorganizowane grupy przestępcze. Nie doszło jak dotąd do otwartej wojny informacyjnej (można mówić jedynie o cyberkonfliktach, w których korzystano z usług hakerów) ani do fizycznych zniszczeń czy zakrojonych na szeroką skalę cybernetycznych ataków terrorystycznych. Jednakże możliwe do wykorzystania w tym zakresie technologie ewoluują, wiedza na temat ich stosowania jest powszechnie dostępna, a szkodliwe oprogramowanie możliwe do wykorzystania w cyberatakach jest dostępne na rynku (można je zakupić), stąd ochrona wrażliwych na ataki sieci teleinformatycznych, infrastruktury krytycznej, a także budowa infrastruktury służącej do cyberobrony własnych, rządowych czy militarnych systemów teleinformatycznych i komunikacyjnych wymaga podejmowania odpowiednich, zorganizowanych działań, również w ramach współpracy międzynarodowej.

Wydarzenia w Estonii w 2007 r. stały się przesłanką do podjęcia stosownych działań ze strony NATO. W 2008 r. Sojusz wypracował pierwsze założenia wspólnej polityki sojuszniczej w dziedzinie cyberobrony. Na szczycie NATO w Lizbonie (19–20 listopada 2010 r.) przyjęto z kolei nową Koncepcję Strategiczną[88], a w czerwcu 2011 r. założenia nowej polityki w zakresie *Cyber Defence*. Zgodnie z przyjętą polityką Sojusz definiuje zagrożenia cybernetyczne jako potencjalny powód do podjęcia obrony wspólnej zgodnie z art. 5 Traktatu Waszyngtońskiego[89]. NATO zwraca szczególną uwagą na ochronę infrastruktury Sojuszu, pozostawiając zabezpieczenie wewnętrznej infrastruktury krytycznej w gestii władz krajowych. Wyrazem działań Sojuszu na rzecz cyberbezpieczeństwa jego państw członkowskich jest także stworzenie w stolicy Estonii **Kooperacyjnego Centrum Doskonalenia Cyberobrony** (Cooperative Cyber Defence Centre of Excellence, CCDCOE), którego misją jest wzmacnianie zdolności, współpracy i wymiany informacji w ramach NATO, krajów członkowskich i partnerów Sojuszu przez edukację, badania i rozwój oraz konsultacje[90]. Unia Europejska powołała z kolei do życia „2CENTRE" – **Centrum do spraw Cyberprzestępczości w zakresie Doskonalenia Szkoleń, Badań i Edukacji** (Cybercrime Centres of Excellence Network for Training, Research and Education)[91].

Działania na rzecz budowania zdolności w zakresie cyberobrony i cyberbezpieczeństwa trwają także w Polsce. W Białobrzegach działa Centrum Bezpieczeństwa Cybernetycznego, którego zadaniem jest ochrona polskiej armii przed atakami w cyberprzestrzeni. Jest to pierwszy krok na drodze do utworzenia cyfrowych jednostek wojskowych, których żołnierze i dowódcy będą wyposażeni w najnowsze technolo-

---

[88] *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, Lizbona 19–20 listopada 2010, www.nato.int/cps/en/natolive/topics_82705.htm (dostęp: 15.06.2014).

[89] O. Theiler, *Nowe zagrożenia: wymiar cybernetyczny*, „Przegląd NATO", 11 września 2011, www.nato.int/docu/review/2011/11-september/Cyber-Threads/PL/index.htm (dostęp: 15.06.2014).

[90] The Cooperative Cyber Defence Centre of Excellence (CCDCOE), *About Cyber Defence Centre*, www.ccdcoe.org/about-us.html (dostęp: 15.06.2014).

[91] Cybercrime Centres of Excellence Network for Training, Research and Education, www.2centre.eu/ (dostęp: 15.06.2014).

gie informacyjne[92]. Polska przystąpiła w 2011 r. do projektu Centrum Doskonalenia Cyberobrony w Tallinie[93]. Opracowano również w 2010 r. **Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016**.

Dobrze, że takie działania zostały dostrzeżone i są podejmowane. Rodzi się jednak w tym miejscu pytanie: czy i na ile są one skuteczne?

W działaniach w zakresie cyberobrony pojawiają się dylematy polityczno-prawne. Działania militarne w cyberprzestrzeni nie mieszczą się bowiem w prawnym rozumieniu wojny. Według tradycyjnej definicji wojny przyjmuje się, że obejmuje ona działania na lądzie, morzu, w powietrzu i przestrzeni kosmicznej. W takim wypadku ataki w cyberprzestrzeni nie powinny być uznawane za wojnę, bowiem nie obejmują jej zapisy Karty Narodów Zjednoczonych oraz konwencji genewskich. Zdaniem Bryana W. Ellisa wojna w cyberprzestrzeni jest wyzwaniem dla prawa międzynarodowego z trzech powodów. Po pierwsze ataki za pomocą sieci teleinformatycznych mogą poczynić szkody o zupełnie innym charakterze niż tradycyjne działania zbrojne, których skutki obejmuje prawo wojenne. Po drugie sygnał elektroniczny przekraczający granice państw jest wyzwaniem dla pojęcia granic, suwerenności czy integralności terytorialnej. Dzięki temu nie tylko państwa, ale także jednostki i ich grupy mogą dokonywać ataków wpływających na działania systemów na całym świecie, nie podlegając przy tym porządkowi prawnemu zaatakowanego kraju. Po trzecie wreszcie problematyczne jest nie tylko uznanie cyberataku za akt wojny, ale także określenie, w którym momencie cele tych ataków mają charakter wojskowy, czyli dozwolony przez prawo międzynarodowe, a kiedy cywilny – więc zabroniony[94].

Podsumowanie

Problematyka cyberwojny, cyberkonfliktów, cyberszpiegostwa, cyberprzestępczości, cyberterroryzmu i innych zagrożeń w cyberprzestrzeni nabiera coraz większego znaczenia w całokształcie polityki bezpieczeństwa narodowego. Cyberwojna staje się faktem. W cyberprzestrzeni granica między pokojem a wojną staje się coraz bardziej umowna. Przedmiotem ataków cybernetycznych mogą stać się zarówno obiekty wojskowe, jak i cywilne, a zaangażowane w nią mogą być podmioty państwowe oraz pozapaństwowe.

Z przedstawionego w niniejszym artykule materiału wynika kilka istotnych konkluzji:

1. Działania o charakterze militarnym w cyberprzestrzeni to typowe działania asymetryczne. Decydują o tym między innymi: niskie koszty działalności, brak tradycyjnych granic, brak potrzeby wykorzystania wywiadu strategicznego, ła-

[92] W. Lorenz, *Polska na cyberfroncie*, www.rp.pl/artykul/572005.html (dostęp: 15.06.2014).

[93] Noty akcesyjne w tym zakresie Polska podpisała 15 listopada 2011 roku w siedzibie Naczelnego Dowództwa Transformacji NATO (HQ SACT) w Norfolk (USA).

[94] B.W. Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?*, Pennsylvania 2001, s. 3. Zob. także: J. Kulesza, *New Technologies and the Need of a Uniform Legal System*, Social Science Research Network – Working Paper Series, 12 listopada 2007 r., https://ssrn.com/abstrakt=1446768 (dostęp: 15.03.2014).

twość w osiągnięciu anonimowości czy wreszcie niewspółmierne do działań potencjalnego przeciwnika zaangażowanie własnych sił i środków. Asymetryczność decyduje o ich złożoności i trudnościach w znalezieniu skutecznych metod i środków ochrony przed cyberatakami.

2. Istnieje pilna potrzeba jednoznacznego zdefiniowania cyberprzestrzeni, poznania rządzących nią prawidłowości i ujednolicenia pojęć związanych z pojawiającymi się w niej zagrożeniami.
3. Zachodzi istotna zmiana w postrzeganiu współczesnego pola walki, które rozszerzyło się o piąty wymiar – cyberprzestrzeń. Warto zatem prowadzić dalsze szczegółowe prace analityczne i koncepcyjne, które pozwolą na jej dokładniejsze rozpoznanie, wypracowanie skutecznych metod działania w cyberprzestrzeni podczas osiągania własnych celów militarnych, ale również sposobów obrony przed atakami w cyberprzestrzeni.
4. Pomimo podjęcia szeregu inicjatyw na arenie międzynarodowej, głównie przez NATO i Unię Europejską, otwarte pozostają pytania, czy i na ile są one skuteczne? czy pozostawienie w gestii rządów poszczególnych krajów ochrony własnej infrastruktury krytycznej nie przekracza ich możliwości działania w tym zakresie w sytuacji, gdy sieci mają charakter globalny?
5. Obecne zapisy prawa międzynarodowego publicznego nie dają jasnej odpowiedzi na pytanie, jakie środki mogą podjąć państwa w celu zwalczania działań militarnych w cyberprzestrzeni. Podobnie wyglądają obecne rozwiązania polityczne. Od lat rządy państw zastanawiają się nad odpowiednimi rozwiązaniami politycznymi, które stanowiłyby właściwą odpowiedź na cyberataki. W dobie wzrastającej ich liczby jest to kwestia wymagająca dość pilnego uregulowania.

Bibliografia

Arquilla J., Ronfeldt D., *Cyberwar is coming!*, [w:] *In Athena's Camp: Preparing for conflict in the information age*, red. J. Arquilla, D. Ronfeldt, Washington 1993.

Arquilla J., Ronfeldt D., *Cyberwar is coming*, „Comparative Strategy" 1993, vol. XII.

Arquilla J., Ronfeldt D., *Networks and Netwars*: *The Future of Terror, Crime, and Militancy*, Santa Monica 2001.

Balcerowicz B., *Wojna. Kwestie nie tylko terminologiczne*, „Myśl Wojskowa" 2003, nr 3.

Bednarek J., *Media w nauczaniu*, Warszawa 2002.

Bednarek J., *Teoretyczne i metodologiczne podstawy badań nad człowiekiem w cyberprzestrzeni*, [w:] *Cyberświat. Możliwości i zagrożenia*, red. J. Bednarek, A. Andrzejewska, Warszawa 2009.

Bógdał-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Clarke R.A., Knake R., *Cyberwar: The Next Threat to National Security and What to Do About It*, New York 2010.

Denning D., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
Ellis B.W., *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?*, Pennsylvania 2001.
Fry R., *Fighting Wars in Cyberspace*, „The Wall Street Journal" 21 lipca 2010 r.
Gardham D., *Hackers recruited to fight 'new cold war'*, „The Telegraph" 26 czerwca 2009 r.
Gawliczek P., *Istota zagrożeń i działań asymetrycznych*, [w:] *Bezpieczeństwo polityczne i wojskowe*, red. A. Ciupiński, K. Malak, Warszawa 2004.
Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Warszawa 2003.
Goulding V.L., *Back to the Future with Asymmetric Warfare*, „Parameters" 2000, t. 30, nr 4.
Grzelak M., *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" 2013, nr II (26).
Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr II (22).
Herman P.F., *Asymmetric Warfare: Sizing the Threat*, „Low Intensity Conflict and Law Enforcement" 1997, t. 6, nr 1.
Howard J.D., Longstaff T.A., *A Common Language for Computer Security Incidents*, Sandia Report, Sandia National Laboratories, Albuquerque–Livermore 2002.
Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1989.
Kotarbiński T., *Dzieła wszystkie, Prakseologia*, cz. II, Wrocław–Warszawa–Kraków 2003.
Koziej S., *Powrześniowe wyzwania w dziedzinie bezpieczeństwa*, „Polska w Europie" 2002, nr 1.
Kuźniar R., *Bezpieczeństwo – realizm oceny, dylematy polityki*, „Polska w Europie" 2002, nr 3.
Kuźniar R., *Niebezpieczeństwa nowego paradygmatu bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe czasu przemian. Zagrożenia – koncepcje – instytucje*, red. R. Kuźniar, Z. Lachowski, Warszawa 2003.
Kwećka R., *Informacja w walce zbrojnej*, Warszawa 2001.
La Carte D.A., *Asymmetric Warfare and the Use of Special Operation Forces in North American Law Enforcement*, „Canadian Military Journal" 2001, t. 2, nr 4.
Leksykon wiedzy wojskowej, red. M. Laprus, Warszawa 1979.
Libicki M., *What is Information Warfare?*, Washington 1995.
Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008.
Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr I (17).
Linebarger P.M.A., *Wojna psychologiczna*, Warszawa 1959.
Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.
Metz S., *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*, Carlise 2000.
Metz S., Johnson D.V., *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concept*, Carlise 2001.
Münkler H., *Wojny naszych czasów*, Kraków 2004.

Ow Kim Meng, *Cyber-Terrorism: An Emerging Threat of The New Millennium*, „Pointer" 2002, t. 28, nr 3.
Piątkowski K., *Wojna nowego typu?*, „Polska w Europie" 2002, nr 1.
Rasmussen M.V., *A New Kind of War: Strategic Culture and the War of Terrorism*, „IIS Working Paper" 2003, nr 3.
Rokociński K., *Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1.
Russel J., *Asymmetric Warfare*, [w:] *The Big Issue: Command and Combat in the Information Age*, red. D. Potts, Shrivenham 2002.
Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Warszawa 2010.
Schmitt B., *Information Security. A New Challenge for the UE*, „Chaillot Paper" 2005, nr 76.
Sienkiewicz P., *Wizje i modele wojny informacyjnej*, [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, red. L.H. Haber, Kraków 2003.
Słownik współczesnego języka polskiego, t. 2, red. A. Sikorska-Michalak, O. Wojniłko, Warszawa 1998.
Słownik wyrazów obcych PWN, red. J. Tokarski, Warszawa 1980.
Sofaer A.D., Goodman S.E., *Cyber Crime and Security: The Transnational Dimension*, [w:] *The Transnational Dimension of Cyber Crime and Terrorism*, red. A.D. Sofaer, S.E. Goodman, Stanford 2001.
Soo Hoo K., Goodman S., Greenberg L., *Information Technology and Terrorist Threat*, „Survival" 1997, t. 39, nr 3.
Strategic Assessment, 1998.
Szubrycht T., *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizować zagrożenia asymetryczne*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2006, nr 1 (164).
The Cyberweapon That Could Take Down the Internet, „Financial News Now!" 14 lutego 2011 r.
Thomas T.L., *Deciphering Asymmetry's Word Game*, „Military Review" 2001, t. 81, nr 4.
Tofler H.A., *Wojna i antywojna*, Warszawa 1997.
Urbanek A., *Podstawy bezpieczeństwa państwa. Wymiar społeczno-polityczny*, Słupsk 2013.
Urbanek A., *Zagrożenia asymetryczne czy asymetryczność zagrożeń*, [w:] *Wyzwania i zagrożenia w XXI wieku. Aspekty militarne i niemilitarne*, red. M. Borkowski, M. Stańczyk-Minkiewicz, I. Ziemkiewicz-Gawlik, Poznań 2013.
Warden J.A., *Enemy as a System*, „Airpower Journal" 1995, nr 9.
Weimann G., *Cyberterrorism, How Real is The Threat?*, Washington 2004.
Zięba R., *Pozimnowojenny paradygmat bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, red. R. Zięba, Warszawa 2008.

AAP-6, *Słownik terminów i definicji NATO, NATO Glossary of terms and definitions*, NATO 2005, gdziewojsko.files.wordpress.com/2011/05/slownik_terminow_i_definicji_nato.pdf (dostęp: 15.03.2014).
Bartoszek B., *Cyberwojna – wojna XXI wieku*, www.mojeopinie.pl/cyberwojna_wojna_XXI_ wieku,3,1215862210 (dostęp: 15.04.2014).
Cybercrime Centres of Excellence Network for Training Research and Education, www.2centre.eu/ (dostęp: 15.06.2014).

Cyberwojna jako rzeczywistość XXI wieku, raport zamieszczony na stronie Europejskiego Centrum Analiz Geopolitycznych, www.geopolityka.org/analizy/1813-cyberwojna-jako-rzeczywistosc-xxi-wieku (dostęp: 15.06.2014).

English Oxford Living Dictionary, *Cyberwar*, [hasło], oxforddictionaries.com/definition/english/cyberwar (dostęp: 15.03.2014).

Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011, October 2011 r., www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (dostęp: 20.05.2013).

Internet Growth Statistics, *Internet Growth and Stats*, www.internetworldstats.com/emarketing.htm (dostęp: 14.06.2014).

Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie, tłumaczenie robocze BBN, www.bbn.gov.pl/pl/wydarzenia/2694,dok.html (dostęp: 14.03.2014).

Kulesza J., *New Technologies and the Need of a Uniform Legal System*, Social Science Research Network – Working Paper Series, 12 listopada 2007 r., https://ssrn.com/abstract=144768 (dostęp: 15.03.2014).

Lorenz W., *Polska na cyberfroncie*, www.rp.pl/artykul/572005.html (dostęp: 15.06.2014).

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku, CERT.GOV.PL, Warszawa 2014, cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/686,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2013-roku.html (dostęp: 15.05.2014).

Steele R.D., *New craft of the intelligence: achieving asymmetric avantage in the face of nontraditional threats*, US Army War College, Carlisle 2002, www.strategicstudiesinstitute.army.mil/pdffiles/pub217.pdf (dostęp: 15.03.2014).

Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Lizbona 19–20 listopada 2010, www.nato.int/cps/en/natolive/topics_82705.htm (dostęp: 15.06.2014).

The Cooperative Cyber Defence Centre of Excellence (CCD COE), www.ccdcoe.org (dostęp: 15.06.2014).

Theiler O., *Nowe zagrożenia: wymiar cybernetyczny*, Przegląd NATO, 11 września 2011, www.nato.int/docu/review/2011/11-september/Cyber-Threads/PL/index.htm (dostęp: 15.06.2014).

Virtual Criminology Report 2009, McAfee Corporation, 2009, img.eu25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRYMINOLOGY_RPT_NOREG.pdf (dostęp: 20.05.2013).

Summary

In connection with the progressive revolution that is changing the face of contemporary conflicts. This arena is becoming cyberspace, which is accessible to different actors: armed forces, criminal and terrorist organizations and hackers. In the article, the author deals with the analysis of cyberwar as an asymmetric conflict. He explains the essence of today's asymmetric threats, analyzes the concept of cyberspace and also explains the concept and characteristics of cyberwar.