FOLIA 250

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate et Educatione Civili 7 (2017)
ISSN 2082-0917
DOI 10.24917/20820917.7.7

Danuta Kaźmierczak
Uniwersytet Pedagogiczny im. KEN w Krakowie
Instytut Bezpieczeństwa i Edukacji Obronnej

Walka informacyjna we współczesnych konfliktach i jej społeczne konsekwencje

Wstęp

Informacja od zawsze była istotnym zasobem, a wraz z rozwojem technologii komunikacyjnych umożliwiających efektywniejsze jej wykorzystanie klasyfikowana jest, jako zasób strategiczny. Zdecydowały o tym między innymi następujące zjawiska. Zwiększa się liczba dostępnych informacji, liczba źródeł a ich dostępność nie jest ograniczona ani czasowo ani przestrzennie. Szybkość przekazu i konkurencja na rynku sprawia, ze informacja jest coraz bardziej powierzchowna i zinterpretowana. Dostęp do *raw data* coraz trudniejszy a korzystanie z nich wymaga wiedzy eksperckiej.

We współczesnej cywilizacji niemożliwe jest funkcjonowanie bez dostępu do informacji. Ilość danych niezbędnych do podjęcia optymalnych decyzji ciągle rośnie. Informacja posiada swoją wartość, jest podstawowym elementem procesów zarządzania, dowodzenia. Przerwanie lub zafałszowanie obiegu informacji powoduje straty dla firmy mogące skończyć się bankructwem, a dla państwa niepokojami społecznymi, zaburzeniami w gospodarce, osłabieniem pozycji na arenie międzynarodowej[1] i przesądza o klęsce na współczesnym polu walki. Dążenie do przewagi informacyjnej stało się, więc warunkiem koniecznym dla funkcjonowania państwa i powodzenia wszelkich operacji militarnych.

Przewaga w teorii sztuki wojennej to „zasada zasad" czy też „super zasada" lub podstawowa zasada, stanowi sens wszelkich zabiegów koncepcyjnych i organizacyjnych. Definiowana jest, jako górowanie nad nieprzyjacielem pod względem intelektualnych możliwości dowódców i oficerów sztabu, taktyki i sztuki operacyjnej, lepszego uzbrojenia, doskonalszych środków walki, skuteczniejszego wykorzystania warunków terenowych, większej liczby wojsk w ogóle lub tylko w określonym miejscu i czasie, które zapewni narzucenie przeciwnikowi własnej woli i sposobu realizacji zamiaru walki, bitwy lub operacji przy jak najmniejszych stratach własnych[2]. Przewaga decyduje o przebiegu i wynikach starć zbrojnych[3].

[1] K. Liederman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 17.

[2] K. Nożko, *Walka o przewagę*, Warszawa 1985, s. 7, [w:] S. Koziej, *Teoria sztuki wojennej*, Warszawa 2010.

[3] S. Koziej, *Teoria sztuki wojennej*..., s. 69.

Współcześnie kluczowym elementem przewagi stały się jej pozamaterialne składniki, tj. działania w sferze informacyjnej: wiarygodne rozpoznanie, fortel (maskowanie, mylenie), oddziaływanie psychologiczne zmniejszające wolę walki nieprzyjaciela stanowią pozamaterialne składniki przewagi. Sun Tzy nazwał je „mnożnikami siły" a obecnie definiowane są, jako przewaga informacyjna, czyli zdolność do zbierania, gromadzenia, przetwarzania i dystrybucji informacji, utrzymania nieprzerwanego strumienia ich przepływu oraz pełnego jej wykorzystania, przy jednoczesnym posiadaniu możliwości wzbraniania przeciwnikowi prowadzenia podobnej działalności informacyjnej[4]. Przy czym zdobycie przewagi informacyjnej nad przeciwnikiem, jak twierdzą John Arguilla i David Ronfeldt, nie polega na zdobyciu wszystkich informacji dotyczących przeciwnika, jakie są możliwe do zdobycia, a raczej zdobyciu ilości informacji wystarczającej do osiągnięcia zakładanych efektów w prowadzonym konflikcie; dominacja informacyjna ma charakter względny, nie absolutny[5].

Uzyskanie przewagi informacyjnej, dzięki nowym możliwościom, jakie dają nowoczesne rozwiązania telekomunikacyjne nabrało formy walki informacyjnej. Informacja jest zasobem strategicznym, celem ataku, środkiem walki i przekazu pozwalającym na koordynację działań[6], przesądzającym o wyniku końcowym konfliktu. Należy jednak zaznaczyć, że rezultatu wojny nie da się uzależnić od jednego tylko czynnika, np. informacji. Taki jeden absolutny czynnik w sprawach wojskowych nie istnieje, podkreśla Bolesław Balcerowicz[7]. Jednak podobnie jak inni eksperci zauważa powstanie i specjalizację oddziałów wojsk informacyjnych i co w praktyce zwiększa rolę przewagi informacyjnej.

Walka informacyjna może być:

- zjawiskiem autonomicznym,
- komponentem wspierającym działania militarne,
- głównym komponentem wspieranym działaniami militarnymi.

Zgodnie z definicją Kolegium Szefów Sztabów Połączonych[8], walka informacyjna to działania podjęte w celu osiągnięcia dominacji informacyjnej poprzez wpływ na informację przeciwnika, jego procesy oparte na informacji, systemy informacyjne i sieci komputerowe[9].

Dominacja informacyjna obejmuje wysiłki ofensywne i defensywne, których celem jest stworzenie różnicy „miedzy tym, co my wiemy o naszej przestrzeni bojowej i operacjach w niej prowadzonych, a tym, co nieprzyjaciel wie o swojej przestrzeni

---

[4] *JP3-13 Joint Doctrine for Information Operations*, Department of Defense, Washington 1998, [w:] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 107.

[5] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*…, s. 107.

[6] Tamże, s. 56–58.

[7] T.R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa*, *ludzie*, Warszawa 2014, s. 153.

[8] Siedzibę ma w Pentagonie. W skład tego gremium wchodzi przewodniczący, wiceprzewodniczący, szefowie sztabów: Armii (Wojsk Lądowych), Sił Powietrznych oraz Szef Operacji Morskich (będący odpowiednikiem szefa sztabu w U.S. Navy) i komendant Korpusu Piechoty Morskiej (Marines) https://pl.wikipedia.org/wiki/Przewodnicz%C4%85cy_Kolegium_Po%C5%82%C4%85czonych_Szef%C3%B3w_Sztab%C3%B3w.

[9] K. Giles, *Handbook of Russian Information Warfare*, NATO 2016.

bojowej" Elementami walki informacyjnej są: destrukcja fizyczna, operacje bezpieczeństwa, operacje psychologiczne, sabotaż, walka elektroniczna.

Narzędzia wykorzystywane w walce to:

- dyplomacja,
- propaganda,
- kampanie psychologiczne,
- działania na poziomie wpływania na procesy polityczne lub kulturowe,
- dezinformację, manipulowanie lokalnymi mediami,
- infiltrację sieci komputerowych i baz danych[10].

Walka informacyjna, jako element współczesnych konfliktów

Przewagę informacyjną skonfliktowane strony uzyskują dobierając narzędzia w zależności od rodzaju działań i warunków ich prowadzenia.

W działaniach sieciocentrycznych regularnych armii, wykorzystujących cykl dowodzenia *Observe Orient Decide Act,* przewaga informacyjna ma przekładać się na przewagę decyzyjną a w konsekwencji na przewagę efektów działania a także dać możliwość działania wewnątrz cyklu dowodzenia przeciwnika.

Jak wyjaśnił twórca cyklu John Boyd, cykl OODA to sekwencja działań w każdej operacji militarnej. Przeciwnik jest obserwowany w celu zebrania informacji na jego temat. Napastnik musi zorientować swoją pozycję, następnie podjąć decyzję i działać. Dodaje, że taki cykl decyzyjny był stosowany już 25,000 lat temu w wojnach plemiennych a w przyrodzie jest podstawową zasadą, na której opierają się relacje drapieżnik – ofiara.

Trzy pierwsze etapy cyklu dotyczą zbierania, przetwarzania, analizowania informacji i podejmowania decyzji. Czym szybciej informacje zostaną zebrane i przeanalizowane tym szybciej podejmiemy optymalne decyzje – zyskamy przewagę informacyjną. Ostatni, czwarty etap to ruch i precyzja rażenia. Carlo Copp uważa, że właśnie trzy etapy cyklu budujące przewagę informacyjną praktycznie decydują o przyspieszeniu całego cyklu dowodzenia

Rewolucja w obszarze technologii informacyjnych dała nowe możliwości tworzenia wielowymiarowych sieci przepływu informacji a przez to przyspieszenia etapów *Observe Orient Decide*. Sieć jest korzystna na wiele sposobów. Ułatwia i przyspiesza proces decyzyjny poprzez zebranie odpowiednich informacji a także przesyłanie ich do pojedynczych żołnierzy, dzięki czemu zyskują większa swobodę i skuteczność działania. Jednak ciągle elementem spowalniającym jest etap *Act*, gdzie musi zostać zachowana sztywna kolejność działań: dowódca najpierw czeka na odpowiedź by następnie rozlokować siły i doprowadzić do uderzenia. Ponadto zastosowanie bardziej destrukcyjnej broni powodującej obustronne zniszczenia czy szybszych platform oznacza zwiększenie kosztów. Większość sprzętu ciągle produkowana jest na podstawie prototypów z lat 50. ubiegłego stulecia. Przykładem może być amerykański bombowiec B-52.

Koncepcję działania sieci zilustrowano na rysunku 1. Płaszczyzny (grids) są połączone na zasadzie „każdy z każdym". Siatki sensorów (sensor grids) – składają się

[10] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*…, s. 133.

z sensorów pracujących na lądzie, w powietrzu, na morzu, w przestrzeni kosmicznej oraz w cyberprzestrzeni. Siatka informacyjna centrum dowodzenia (C2 grids) – to sieć zasobów obliczeniowych umożliwiająca wykorzystanie najświeższych danych dla wspólnego planowania, analiz i podejmowania decyzji. Siatki środków walki (shooter grids) – to system skoordynowanych środków walki, umieszczonych na różnorakich platformach (okręty, samoloty, czołgi), umożliwiający jak najszybsze przeciwstawienie się zagrożeniom.

Płaszczyzny te mogą być odpowiednikiem poziomów dowodzenia (strategicznego, taktycznego i operacyjnego). Elementarnym składnikiem sieci może być nawet pojedyncza osoba – filar koncepcji – jest ona jednocześnie źródłem i odbiorcą informacji znajdującej się w sieci. Taka sieć jest „niezniszczalna" – wyeliminowanie któregoś z węzłów (hubów) decyzyjnych, lub kanałów informacyjnych, spowoduje jedynie, że ich funkcje przejmie inny węzeł decyzyjny, czy inny kanał informacyjny[11].

Rys. 1. Idea koncepcji sieciocentryczności

Source: https://www.google.pl/search?q=network+centric+warfare&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwibt_Cd54fZAhUMJlAKHcdWAX0QsAQIOQ&biw=1366&bih=637#imgrc=pCg3QZhS8M369M

„Pustynna Burza" jest przykładem operacji, w której o skuteczności działań zdecydowała przewaga informacyjna uzyskana dzięki działaniom sieciocentrycznym przy zastosowaniu zautomatyzowanych, opartych na technologiach cyfrowych systemów wspomagania dowodzenia. Jednym z takich systemów był kompleks JSTARS – radarowy system monitorowania pola walki i wskazywania celów. Składał się z samolotu E-8, czyli Boeinga 707 wyposażonego w georadar oraz naziemnych centrów przetwarzania i dystrybucji informacji. Zasada działania JSTARS była następująca: obraz radarowy wstępnie przetworzony na pokładzie samolotu, był przesyłany do centrów naziemnych, gdzie poddawano go dalszej obróbce, a uzyskane dane przekazywano do sztabów związków taktycznych. System wykrywał cel wielkości

[11] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf [dostęp: 21.08.2017].

śmigłowca, co dało dowódcom całościowe spojrzenie na rejon prowadzenia operacji i zapewniło zdecydowaną przewagę nad przeciwnikiem.

Na szczeblu taktycznym wykorzystano LTACFIRE – system kierowania ogniem, składający się z radarów obserwacji pola walki zintegrowanych z komputerami oraz radiowymi systemami przekazu informacji. Radar wykrywał wystrzelone pociski irackie, na podstawie obserwacji trajektorii ich lotu komputery wyliczały położenie baterii przeciwnika i przekazywały dane do amerykańskich baterii pocisków rakietowych. Rakiety były odpalone już po 30 sekundach i skutecznie obezwładniały irackie armaty, gdyż ich obsługa nie mogła w tak krótkim czasie zmienić stanowisk ogniowych[12].

Jednak, jak ocenia Tomasz R. Aleksandrowicz, pokonanie przeciwnika w wymiarze militarnym przebiegło szybko i przy minimalnych stratach własnych, jednak nie zapanowano nad sytuacją po zakończeniu działań wojennych – zwycięstwo operacyjne nie przełożyło się na zwycięstwo strategiczne[13].

S. Koziej twierdzi, że nie doceniono wagi niektórych aspektów walki informacyjnej i zaniedbano współpracę z ludnością cywilną, której przychylność mogła udaremnić działania terrorystów[14].

Urlich Beck wyjaśniając socjologiczne mechanizmy wojny w Iraku posłużył się terminem Micheala Ignatieffa „wojna wirtualna". Wirtualność ma tutaj dwa znaczenia.

Pierwsze znaczenie odnosi się do strategii. Teren zostaje opanowywany nie przez klasyczne działania oddziałów naziemnych, ale działania sieciocentryczne. W ten sposób, ryzyko utraty własnych żołnierzy zostało przerzucone na straty wśród ludności cywilnej innych. Działa mit „czystej", „chirurgicznej" wojny bez własnych ofiar. Wojna była czymś rozgrywającym się „tam", „ofiary nie były „naszymi" ofiarami, a „nasze" ofiary dzięki nieprzedstawianiu ich pozostały „niewidoczne" Zastosowano zasadę redystrybucji ryzyka (*risk-transfer war*)[15]. Redaktorzy telewizji CNN – Cable News Network pokazali politykom obu stron, jaką siłę oddziaływania ma technika satelitarna i nadawanie wiadomości w czasie rzeczywistym (*real time reporting*). Około stu milionów widzów w stu trzech krajach mogło na bieżąco śledzić wydarzenia w Iraku. Jednak armia amerykańska tak dobrze kontrolowała przepływ informacji, iż w dzienniku *Frankfurter Allgemeine Zeitung* w numerze z 21.01.1991 r. stwierdzono, że jeszcze nigdy tak wielu dziennikarzy przy użyciu tak wielu słów i obrazów nie przekazało tak skąpych treści, jak podczas wojny w Zatoce[16].

---

[12] K. Kubiak, *Wojna sieciocentryczna*, [w:] rp.pl Historia 11.01.2008, http://www.rp.pl/artykul/83102-Wojna-sieciocentryczna.html#ap-1 [dostęp: 18.08.2017].

[13] T.R. Aleksandrowicz, ……, s. 98.

[14] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*…, s. 137.

[15] U. Beck, *Społeczeństwo światowego ryzyka*, Warszawa 2012, s. 215.

[16] A. Osińska, *Afganistan. Konflikty wojenne w mediach – relacjonowanie*, fragmenty pracy dyplomowej *Obraz konfliktów wojennych w mediach na przykładzie wojny w Afganistanie* PWSZ w Wałbrzychu, http://www.reporterzy.info/321,afganistan-konflikty-wojenne-w-mediach---relacjonowanie.html [dostęp: 20.08.2017].

Drugie znaczenie wirtualności odnosi się do oddziaływania mediów na społeczeństwo. Dla społeczeństw zachodnich wojna nabrała charakteru „widowiska sportowego". Mass media stały się kluczową sceną a dowódcy wojskowi wiedzą, że sukces zależy od przygodnej publicznej akceptacji[17].

15 kwietnia 2003 – choć wojna jeszcze trwała, to badania opinii publicznej przeprowadzone przez New York Times i CBS News pokazały, że 62 procent Amerykanów uznała wojnę w Iraku za sukces, nawet, jeśli Saddam Hussein pozostanie na wolności lub nie zostanie znaleziona broń chemiczna czy jądrowa. Jednocześnie większość jest przeciwna atakowi prewencyjnemu wobec kolejnego państwa. 73 procent badanych aprobowało dokonania Busha. 56 procent respondentów wyraziło pogląd, że Ameryka zmierza w dobrym kierunku, o 20 procent więcej niż w lutym 2003 r. Badania przeprowadzono 2 dni po tym, jak grupa marines obaliła statuę Saddama Husseina na placu Firdos w Bagdadzie. Wielu Amerykanów uznało wówczas, że wojna się skończyła[18].

Trzy lata później, latem 2006 r. w przeprowadzonej i opublikowanej przez CBS ankiecie tylko 9% osób uznało, że wojna w Iraku przyczyniła się do ograniczenia terroryzmu[19].

Oficjalne zakończenie wojny w Iraku prezydent Barack Obama ogłosił 1 września 2010 roku. Według skrajnych wyliczeń wojna w Iraku kosztowała Stany Zjednoczone od 800 mld dolarów do 3 bilionów dolarów.

W przypadku działań organizacji terrorystycznych przeciwko państwu, Stanisław Koziej twierdzi, że to organizacja terrorystyczna ma zawsze przewagę czasu i miejsca[20]. Jest to możliwe dzięki skutecznie prowadzonym działaniom wywiadowczym. Wykorzystywanym w tym celu narzędziem jest Internet, który tworzy anonimowe i bezpieczne środowisko. Zapewnia swobodny i pewny przepływ informacji, co do wyboru celu zamachu, rozpoznania, określenia drogi dojścia, wyboru najbardziej optymalnego *modus operandi*.

Grupa terrorystyczna zainteresowana jest w szczególności informacjami dotyczącymi:

- ogólnej sytuacji przeciwnika – państwa – celu: politycznej, ekonomicznej, społecznej,
- poglądów, planów i zamierzeń władz dotyczących sprawy, o którą walczą terroryści,
- możliwych i potencjalnych celów – osoby, instytucje, obiekty,
- działań władz w stosunku do terrorystów – infiltracja grupy przez policję.

W państwach demokratycznych generalnie wszystkie informacje dotyczące sytuacji ogólnej państwa – celu, są możliwe do pozyskania poprzez jawne źródła informacji (prasa, książki, media elektroniczne, Internet – tzw. „biały wywiad"). Pozyskiwanie informacji niejawnych odbywa się poprzez rozpoznanie osobowe

[17] U. Beck, *Społeczeństwo światowego ryzyka*..., s. 226.

[18] M. Palczewski, W*ojna w Iraku w amerykańskich mediach*, http://www.sdp.pl/analizy/85, wojna-w-iraku-w-amerykanskich-mediach-opracowanie-marka-palczewskiego-,1365173562 [dostęp: 20.08.2017].

[19] U. Beck, *Społeczeństwo światowego ryzyka*..., s. 227.

[20] T.R. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2010, s. 45.

(HUMINT). Nie wymaga ono dużych nakładów finansowych, ani zaawansowanego sprzętu. Najczęściej stosowane formy rozpoznania osobowego to:

- prowadzenie obserwacji potencjalnych celów,
- werbowanie agentów (zbierających informacje oraz pomocniczych),
- przenikanie członków organizacji terrorystycznych do interesujących ich miejsc (np. potencjalnych celów),
- prowadzenie działań kontrwywiadowczych (np. zabezpieczających przed obserwacją).

Możliwości rozpoznania poprzez środki techniczne są ograniczone. Terroryści nie są w stanie rozwinąć np. rozpoznania satelitarnego czy radioelektronicznego na dużą skalę, dlatego też są zmuszeni do stosowania prostszych i łatwiej dostępnych (co nie znaczy, że mniej skutecznych) metod. Metody te to m.in.:

- umieszczanie urządzeń podsłuchowych w określonych miejscach (np. celu przyszłego ataku),
- podsłuchiwanie środków łączności (np. łączności radiowej sił policyjnych),
- stosowanie włamań do systemów informatycznych (*hacking*) w celu pozyskania potrzebnych informacji[21].

Terroryści wykorzystują głównie Internet, jako narzędzie do neutralizacji zabezpieczeń, doprowadzenia do zakłóceń w funkcjonowaniu instytucji wybranej, jako cel – czyli tworzenia planu ataku, który przekazywany w sieci wspiera koordynację działań z uczestniczącymi podmiotami. T.R. Aleksandrowicz wskazuje na podobieństwo tych działań z działaniami sieciocentrycznymi[22].

Gra psychologiczna i propaganda to kolejne metody budowania i wykorzystywania przewagi informacyjnej.

Działania propagandowe są dwojakiego rodzaju mają wywołać pozytywny efekt i pozyskać sympatyków, a inne wywołać strach.

Propagowanie swoich idei, podtrzymanie zapału i poparcia miał uzyskać, na przykład Anders Breivik – zamachowiec z Oslo, publikując w Internecie swój manifest *2083. Europejska Deklaracja Niepodległości*.

Inny rodzaj propagandy ma na celu indoktrynację dzieci: rozpowszechnienie informacji na stronie FriendFeed o nieoficjalnych klockach LEGO – terrorystach produkowanych przez firmę BrickArms, czy też wykorzystanie Mickey Mouse w celu propagowania ideologii Hamasu (rys. 2).

Wojnę psychologiczną terroryści prowadzą poprzez samodzielną, niczym nieskrępowaną publikację ekstremalnie drastycznych treści dotyczących przeprowadzonych zamachów na ludności cywilnej. Poprzez rzeczywistość wirtualną, telewizję i możliwość bezpośredniego przekazu audio i wideo na skalę globalną cele stają się widoczne. Cytując Eqbala Ahmada: *Każdy jest dziś w zasięgu strzału. Cały świat jest w zasięgu strzału. To zglobalizowało terror*[23]. Celem jest zastraszenie społeczeństwa i państwa, by narzucić własną wolę.

---

[21] M. Piekarski, *Strategia i taktyka terrorystów*, Konflikty.pl, 19.11.2006, http://www.konflikty.pl/historia/czasy-najnowsze/strategia-i-taktyka-terrorystow/ [dostęp: 20.08.2017].

[22] T.R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa, ludzie*, Warszawa 2014, s. 95.

[23] K. Liedel, *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*, Difin, Warzawa 2010, s. 30.

Rys. 2. Informacja na stronie FriendFeed o nieoficjalnych klockach LEGO produkowanych przez firmę BrickArms. Wykorzystanie Mickey Mouse w celu indoktrynacji dzieci propagandą Hamasu. (Al-Aqsa TV, May 10, pictures courtesy of Palestinian Media Watch)

Źródło: https://www.google.pl/search?q=mickey+mouse+terrorist&tbm=isch&tbo=u&source=univ&-sa=X&ved=0ahUKEwiQ0Kbf_ePVAhUGDJoKHcDlC-0QsAQIJg&biw=1366&bih=638#imgrc=_

Krzysztof Liedel wprost wskazuje, że terroryzm należy postrzegać, jako działania przejawiające cechy walki informacyjnej. Większość definicji terroryzmu akcentuje rozgłos, reklamowy charakter przemocy, demonstrowanie siły innym, aby wywołać określone reakcje opinii publicznej – przede wszystkim strach[24].

Powtarzając za Walterem Laqueur'em, „dążeniem terroryzmu jest zastraszenie państwa poprzez ofiary [...] i, rozgłos (publicity) jest istotnym czynnikiem strategii terrorystycznej"[25].

Zaś Brian Jenkins pisze: „Terroryzm jest teatrem [...] jest przeznaczony dla tych, którzy patrzą [...] akty terrorystyczne są często starannie wyliczone i zaplanowane tak, by przyciągnąć uwagę międzynarodowych mediów elektronicznych i prasy"[26].

Terroryzm to proces komunikacji oparty na przemocy, wywieraniu wpływu i manipulacji. Aby osiągnąć własne cele terroryści muszą przyciągnąć uwagę opinii publicznej wykorzystując istniejące kanały komunikacji: telewizja, prasa, lub stworzyć własne w Internecie[27].

15 kwietnia 2013 roku – dokonano zamachu podczas maratonu w Bostonie. W czasie trwania imprezy doszło do wybuchu dwóch bomb. Zginęły 3 osoby, a 264 zostały ranne. Był to najkrwawszy zamach w Stanach Zjednoczonych od 11 września 2001 roku. W mediach pojawiły się informacje i drastyczne zdjęcia z miejsca tragedii (rys. 3).

---

[24] K. Liedel, *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011, s. 97.

[25] W. Laqueur, *Reflection on Terrorism Foreign Affairs Fall 1986*, vol. 65, no. 1, s. 88.

[26] B.M. Jenkins, *International Terrorism*: A New Mode of Conflict, International Terrorism and World Security, https://www.rand.org/content/dam/rand/pubs/papers/2008/P5261.pdf [dostęp: 21.08.2017].

[27] K. Liedel, *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011, s. 98.

Rys. 3. Zamach w Bostonie 15 kwietnia 2013 roku

Źródło: https://wiadomosci.wp.pl/najwieksze-zamachy-terrorystyczne-xxi-wieku-6043602252223617g/11 [dostęp: 20.08.2017)

Działanie medialne to ostatni punkt działań terrorystycznych. Każdy atak terrorystyczny jest wielkim wyzwaniem logistycznym. Operację trzeba zaplanować, sfinansować, przeszkolić wykonawców, przeprowadzić, a przede wszystkim utrzymać w tajemnicy. A potem dopiero, dla oczekiwanego efektu, odpowiednio nagłośnić. Tym oczekiwanym efektem nie ma być tylko strach i panika społeczeństwa. U. Beck wyjaśnia, że terroryści chcą pokazać światu kruchość Zachodu, który dominuje nad światem militarnie, technologicznie. Świat arabski uderza wykorzystując konwencjonalną broń „high tech, i trafia w samo serce supermocarstwa. Ale to nie sam akt terrorystyczny niszczy Zachód, lecz reakcja na antycypację tego aktu. Rozbudza ona odczucie wojny w głowach i centrach Zachodu. […] Zagrożenie jest dominującym oczekiwaniem, ogarnia umysł, myślenie pozostaje otwarte na inscenizacje”[28].

W powyżej opisanych przykładach działań sieciocentrycznych i działań terrorystycznych walka informacyjna (dążenie do przewagi informacyjnej) była komponentem wspierającym. Rosjanie walkę informacyjną traktują, jako samodzielne, długofalowe działanie w kategoriach „pokojowej wojny” (*peaceful war*) niekoniecznie angażującej środki militarne[29].

Michał Wojnowski zwraca uwagę na fakt, że we współczesnej rosyjskiej literaturze przedmiotu powszechne stało się używanie zachodnich terminów i określeń: „działania pośrednie”, „soft power”, „działania asymetryczne”, „wojna informacyjna”, „wojna sieciowa”. Jednak, adaptując zachodnie terminy Rosjanie kierują się własnymi założeniami i logiką.

Problematyka rozróżnienia istoty walki i wojny informacyjnej w poglądach NATO i FNP również była przedmiotem badań w literaturze fachowej.

---

[28] U. Beck, *Społeczeństwo światowego ryzyka*…, s. 219–229.

[29] T. Thomas, *Psycho Viruses and Reflexive Control. Russian Theories of Information – Psychological War*, [w:] *Information at War: From China's Three Warfares to NATO's Narratives*, Legatum Institute, 2015, s. 16–20.

W myśli strategicznej USA wojna informacyjna nie jest traktowana, jako samodzielne zjawisko, lecz element coraz silniej wykorzystywany w konfliktach zbrojnych, pozwalający ograniczyć użycie przemocy zbrojnej i uniknięcia strat w ludziach.

Operacje informacyjne i psychologiczne prowadzone są w otoczeniu informacyjnym, na które składają się osoby fizyczne, organizacje i systemy pozyskujące, przetwarzające i dystrybuujące informacje oraz działające na ich podstawie. Operacje informacyjne prowadzone są w 3 wymiarach:

- poznawczym – celem jest człowiek,
- informacyjnym – celem są dane,
- fizycznym – system informacyjny.

W Doktrynie Wojennej Federacji Rosyjskiej z 2014 r. mówi się nie o środkach prowadzenia walki/wojny/konfliktu, lecz wprost o wojnie informacyjnej:

> […] główne zewnętrzne niebezpieczeństwo wojenne to wykorzystywanie technologii informacyjnych i komunikacyjnych w celach wojskowo-politycznych do prowadzenia działań sprzecznych z prawem międzynarodowym, skierowanych przeciwko suwerenności, niezawisłości politycznej, integralności terytorialnej…

Rosyjska wojna informacyjna stanowi całokształt różnorodnych czasowo skoordynowanych działań prowadzonych przez wojsko jak i cywilne służby specjalne na wielu obszarach, w celu zneutralizowania przeciwnika przy pomocy narzędzi informacyjno-technicznych i informacyjno-psychologicznych[30].

Na wojnę informacyjna składa się wiele koncepcji i działań, niektóre z nich czerpią z radzieckich wzorców. Przykładem może być polityka „miękkiej siły", określająca politykę walki o kulturę postulowaną przez Aleksandra Dugina, która zakłada zdobycie władzy politycznej poprzez wcześniejsze narzucenie swojej kultury i systemu wartości. Mechanizm jej funkcjonowania bliski jest radzieckiej koncepcji „aktywnych działań" (ros. активные мероприятия), która oznacza tajne, ofensywne przedsięwzięcia o charakterze dezinformacyjnym, destabilizującym i agenturalnym, wynikające z aktualnych priorytetów polityki ZSRR, których zamierzeniem było uzyskanie wpływu na szerokie sfery działalności politycznej i społecznej w innych państwach. Jednym z elementów aktywnych działań była dywersja ideologiczna (ros. идеологическая диверсия), określana także mianem „przewrotu ideologicznego".

Pojęcie „dywersji ideologicznej" oznaczało odwrócenie uwagi społeczeństwa danego kraju od wrogiej działalności skierowanej przeciwko niemu, mającej na celu dokonanie rozkładu jego tradycji, religii, kultury, nauki i ideologii lub przeformatowanie tych czynników w taki sposób, aby ofiara agresji przyjęła wrogie treści, afirmując je, jako własne.

Według Bezmienowa, przewrót ideologiczny to długotrwały proces przebiegający w czterech etapach:

1) Demoralizacji. Na tym etapie prowadzono działania zmierzające do jak największego rozbicia i podzielenia społeczeństwa. Za ich pośrednictwem ekstremalnych ruchów politycznych, ideologicznych, sekt, organizacji przestępczych,

[30] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 158–165.

związków zawodowych, oddziaływano na takie obszary, jak administracja, wymiar sprawiedliwości, siły zbrojne oraz religia i gospodarka. Działania te miały doprowadzić do relatywizmu moralnego, zdyskredytowania religii oraz osłabienia systemu edukacji przez jego komercjalizację i zideologizowanie a także osłabienia autorytetu władzy państwowej, wojska. Efektem miały być podziały społeczne i powstawanie grup będących łatwym celem manipulacji.

2) Destabilizacji. Demoralizacja społeczeństwa powinna doprowadzić do jego destabilizacji. Wszelkie konflikty w najważniejszych dziedzinach życia, takich jak relacje rodzinne, gospodarka, porządek publiczny i media, powinny prowadzić do przemocy. W tej sytuacji agenci wpływu zdobywali pozycję polityczną, uzyskując realny wpływ na sfery funkcjonowania państwa.
3) Kryzysu. Rozumianego, jako gwałtowne załamanie gospodarki, wybuch społecznego niezadowolenia przybierający postać intensywnych rozruchów, które miały wywołać zdezorientowanie społeczeństwa, stan psychozy, wzmożonej czujności i rozdrażnienia, na co nakładały się dodatkowo akty terroru. Zastraszone społeczeństwo na granicy wojny domowej w zamian za gwarancję pokoju i bezpieczeństwa było w stanie podporządkować się czynnikom zdolnym do ich zapewnienia. Wówczas, za pośrednictwem zbrojnej interwencji lub bratniej pomocy wprowadzano sprzyjający Kremlowi rząd.
4) Normalizacji. Czyli pacyfikacji czynników stanowiących narzędzia przewrotu ideologicznego. Nastanie „nowego ładu", któremu podporządkowano wszystkie dziedziny życia społecznego, politycznego i kulturalnego[31].

M. Wojnowski uważa, że za przykład użycia „miękkiej siły" można uznać działania w czasie konfliktu ukraińskiego ukierunkowane na:

> […] dyskredytację stanowiska Polski i innych państw członkowskich NATO w kwestii kryzysu ukraińskiego, a także na akcentowanie polsko-ukraińskich skomplikowanych doświadczeń historycznych w celu wywoływania antagonizmów pomiędzy społeczeństwami obu tych krajów.[…] uwypuklanie i niekiedy także kreowanie podziałów wśród państw UE oraz NATO. Eksponowano wszelkie antyunijne i antyamerykańskie wypowiedzi.[…] Do realizacji tego typu przedsięwzięć Rosjanie wykorzystywali zarówno rosyjskie media, jak i obywateli RP opłacanych przez instytucje Federacji Rosyjskiej. Miały one wielopłaszczyznowy charakter i były realizowane m.in. przy wykorzystaniu internetu. […] Rosjanie wraz z wybuchem konfliktu na Ukrainie aktywnie zaangażowali się w działania wspierające przedsięwzięcia inspiracyjno-propagandowe […] kreujących jednoznacznie pozytywny wizerunek Rosji, a zarazem ukazujących w negatywnym świetle oponentów polityki Kremla[32].

Idee wojny informacyjnej znajdują odzwierciedlenie w koncepcji zarządzania refleksyjnego.

---

[31] M. Wojnowski, *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, Przegląd Bezpieczeństwa Wewnętrznego 13/15, www.abw.gov.pl/download/1/1989/Wojnowski.pd.

[32] Cyt. za: Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r., Warszawa 2015, s. 15 (raport jest dostępny również w wersji elektronicznej na oficjalnej stronie ABW pod adresem: http:// www.abw.gov.pl/pl/pobierz/raporty/575,Raporty.html).

Władimir Lefewr opisując koncepcję *zarządzania refleksyjnego* przekonuje, że można dokonać głębokiej transformacji masowej świadomości ludności cywilnej i zmienić moralno-psychologiczny stan narodu poprzez wykorzystanie kompleksu technik i sposobów manipulacji emocjami, percepcją i świadomością sił zbrojnych, elit i grup społecznych w państwie nieprzyjacielskim.

Mieści się one również w kategorii – *maskirowka (maskowanie)* – prowadzenie operacji mających na celu wprowadzenie w błąd przeciwnika i ukrycie przed nim faktu, charakteru, celu, bądź istoty działań własnych, np. operacje pozorowane[33].

Wszystkie te działania zostały określone jednym pojęciem *broni poznawczej (cognitive weapon)* i oznaczają wprowadzenie do intelektualnego środowiska zaatakowanego społeczeństwa fałszywych teorii naukowych, paradygmatów, koncepcji i strategii, które wpływają na administrację państwową w sposób znacząco osłabiający narodowy potencjał obronny.

Rosyjska koncepcja zarządzania refleksyjnego (*reflexive control*) jest bliska amerykańskiej koncepcji zarządzania percepcją „perception management"[34].

Ukraina okazała się optymalnym środowiskiem tego typu działań Federacji Rosyjskiej mających na celu utrzymanie wpływów (wojna w Donbasie, aneksja Krymu) ze względu na następujące czynniki: bliskość kulturowa, brak bariery językowej, duża liczba etnicznych Rosjan i rosyjskojęzycznych Ukraińców, wysoki poziom penetracji struktur państwowych, wynikający z wieloletnich powiązań polityczno-gospodarczych. Przewaga drukowanych mediów rosyjskojęzycznych oraz ogólnie języka rosyjskiego w przestrzeni informacyjnej decydują o powodzeniu rosyjskiej propagandy. Walka z tym zjawiskiem polegająca na ograniczeniu języka rosyjskiego prowadzi do antagonizmów społecznych podsycanych przez rosyjskie głosy o tolerancji językowej, pokojowym współistnieniu i ekonomicznej racjonalności (sami właściciele mediów podejmują te decyzje, co ma zwiększać grono odbiorców, a przez to i zyski).

Powodzenie działań strony rosyjskiej jest również wynikiem braku skutecznej komunikacji pomiędzy strukturami władzy a społeczeństwem, jasnego przekazu o planach czy nawet uwarunkowaniach dla podejmowania danych decyzji, istotnych z punktu widzenia poszczególnych grup społecznych. Braki te kompensują spekulacje i informacyjne z rosyjskich lub prorosyjskich mediów. Ten błąd oceniany jest w kategorii błędu strategicznego polegającym na niedocenieniu czynnika społecznego.

Opisywany stan pogłębiany jest przez słabą jakość ukraińskiego dziennikarstwa: Słaba znajomość języków obcych powoduje błędy w interpretacji wydarzeń europejskich a plagiaty i naruszanie praw autorskich odbijają się na wiarygodności poszczególnych mediów.

---

[33] S.S. Sulakshin, *„Kognitivnoe oruzhie – novoe pokolenie informatsionnogo oruzhiya" ("Cognitive Weapons – A New Generation of Information Weapon"*), Vestnik Akademii Voyennykh Nauk (Journal of the Academy of Military Science), 1 (2014), s. 57–65.

[34] T. Thomas, *Psycho Viruses and Reflexive Control. Russian Theories of Information – Psychological War*, [w:] *Information at War: From China's Three Warfares to NATO's Narratives*, Legatum Institute, 2015, s. 16–20.

Ważną rolę odgrywają również aktywiści internetowi wzywający do „buntu", czy „obalenia rządu". Działają pod fikcyjnymi nazwiskami i piszą z Petersburga lub Moskwy, udając ukraińskich patriotów. Wykorzystują niechęć coraz szerszych kręgów społecznych do rządu i prezydenta a ich działania są ukierunkowane krytykę działań władzy, oskarżenia i próby rozliczeń. Ich tropienie jest jednak kosztowne i czasochłonne, podobnie jak popularyzacja wiedzy na temat zagrożeń[35].

Społeczne konsekwencje walki

Powyższe przykłady konfliktów ilustrują całe spektrum działań nakierowanych na zdobycie przewagi informacyjnej, czyli na walkę informacyjną. Działania te to warunek konieczny powodzenia konfliktu. Wykorzystując najnowsze technologie i czerpiąc z wojskowych zasobów doświadczeń i metod zwiększyły swą skuteczność i rangę. Każde z nich angażowały społeczeństwo, ludność cywilną, jako narzędzie. W konflikcie w Zatoce Perskiej dzięki zaawansowanym technologiom i profesjonalnemu systemowi dowodzenia minimalizowano straty własne a za pomocą mediów ukrywano cierpienia ludności cywilnej, walcząc w ten sposób z sukcesem o aprobatę społeczeństw zachodnich; działania terrorystyczne nastawione są nie tyle na ilość ofiar, co na skutek: ofiary te są narzędziem wzbudzania strachu; rosyjska wojna informacyjna zaś ma na celu zmianę moralno-psychologicznego stanu ludności.

Opinia B. Balcerowicza, że, *rezultatu wojny nie da się uzależnić od jednego tylko czynnika. Taki jeden „absolutny" czynnik w sprawach wojskowych nie istnieje. To podejście utopijne*[36], daje autorce pewne podstawy do formułowania poglądu, że obok informacji, społeczeństwo stało się kolejnym zasobem strategicznym, celem ataku, środkiem walki i przekazu propagandowych treści. Jego kondycja i postawa może przesądzić o wyniku konfliktu.

Walka informacyjna i angażowanie w konflikt ludności cywilnej zmieniła charakter tych konfliktów w takim stopniu, że eksperci dostrzegli problem w ich definiowaniu i kategoryzacji.

B. Balcerowicz zauważa, że dzisiaj został zamazany czytelny podział między tym, co cywilne, i tym, co wojskowe: wewnętrznym prawnym współżyciem wewnętrznym i użyciem siły na zewnątrz, przez co konieczne staje się zdefiniowanie pojęcia przemocy zbrojnej na nowo: granice między trzema podstawowymi typami przemocy zorganizowanej: wojną, przestępczością międzynarodową i gwałceniem praw człowieka, zdają się ostatnio coraz bardziej zacierać[37].

Zamazany został również podział między wojną a pokojem. U. Beck wyróżnił stany: *odczuwanej wojny, odczuwanego pokoju*, wyjaśniając je na przykładzie słonecznego dnia zimą w Monachium i nagłego śniegu w sierpniu. Temperatury odczuwane i realne są zupełnie inne.

Scenariusz *odczuwanego pokoju* jest następujący: Wojna toczy się dla innych, a nie w kraju narodu prowadzącego wojnę (wojna w Iraku). *Odczuwany pokój*

[35] A. Lelonek*, Rosyjska wojna informacyjna na Ukrainie, w Defence 24 z* 30 kwietnia 2016; http://www.defence24.pl/rosyjska-wojna-informacyjna-na-ukrainie [dostęp: 2.02.2018].

[36] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*…, s. 153.

[37] Tamże, s. 133.

i faktyczna wojna istnieją jednocześnie obok siebie, oddzielone przestrzennie i społecznie, ale powiązane według określonego wzorca inscenizacji i legitymizacji.

Terroryści zaś kierują się scenariuszem *odczuwanej wojny*:

> Patrząc z perspektywy ofiar, chodzi o strategię maksymalizacji zagrożenia [...] Przy wciąż jeszcze relatywnie „małej" liczbie zabitych i zamachów odczuwana przemoc, odczuwana wojna ulega maksymalizacji, a w centrach odczuwanego pokoju doprowadza się do jej wybuchu w medialnym i realnym sensie[38].

Rola rządu i edukacji w warunkach walki informacyjnej

Życie i funkcjonowanie w tak zorganizowanym środowisku bezpieczeństwa jest dla ludności cywilnej wyzwaniem. Wciągnięte w konflikt w charakterze ofiary krwawego ataku, ofiary manipulacji psychologiczno-medialnej lub dywersji ideologicznej nie posiada wypracowanych sposobów obrony i samoobrony. Nasuwa się, więc pytanie:, jakie powinny być te mechanizmy i kto powinien ludność cywilną w nie wyposażyć?

Ogromną rolę ma do odegrania w tej kwestii edukacja, w szczególności edukacja dla bezpieczeństwa i obronności.

W jednej z wielu dostępnych w literaturze przedmiotu definicji stwierdza się, że edukacja dla obronności i pokoju służyć powinna zdobywaniu odpowiedniej wiedzy, kształtowaniu umiejętności, postaw i systemów wartości, sprzyjających budowaniu i ochronie bezpiecznego i pokojowego świata[39].

Wartości i postawy, które można uznać za uniwersalne niezbędne dla rozwoju i harmonijnego funkcjonowania każdego społeczeństwa to: wolność, odpowiedzialność, godność, uczciwość, samostanowienie. W sytuacji, kiedy młode pokolenie, na co dzień bombardowane jest informacjami, jest świadkiem lub samo doświadcza łamania praw człowieka, krwawych ataków terrorystycznych, wyzysku i ucisku ekonomicznego, politycznego, czy dyskryminacji, wpajanie tych wartości i kształtowanie postaw tolerancji, umiejętności negocjacji, współistnienia i przeciwstawienia się wszelkim formom dyskryminacji niewątpliwie jest trudnym zadaniem.

Uczeń, student, obywatel powinien zdobywać wiedzę ogólną i specjalistyczną umożliwiającą ocenę procesów zachodzących w świecie, informacje na temat zagrożeń i jednocześnie rozwijać umiejętności przeciwdziałania tym zagrożeniom w kontekście lokalnym i globalnym.

Biorąc pod uwagę opisane powyżej zagrożenia manipulacji, dezinformacji, wpływów „soft power", demoralizacji i indoktrynacji, które można określić, jako *broń poznawcza (cognitive weapon),* zdolności, które pomogą się nim przeciwstawić to zdolności poznawcze*(cognitive skills):* spostrzegawczość, wyciąganie wniosków, przetwarzanie informacji podanych w formie werbalnej i numerycznej, orientacja przestrzenna, pamięć i koncentracja.

---

[38] U. Beck, *Społeczeństwo światowego ryzyka*..., s. 224.

[39] http://stosunki-miedzynarodowe.pl/bezpieczenstwo/1058-filozofia-i-edukacja-dla-bezpieczenstwa-w-obliczu-szans-zagrozen-i-wyzwan-przelomu-xx-i-xxi-wieku [dostęp: 4.10.2014].

Zdolności te są dla żołnierzy również niezbędne na polu walki, jeżeli model dowodzenia OODA ma się sprawdzić.

W dzisiejszym świecie doświadczamy przesytu informacją. Informacja, jak zauważył Herbert Simon, konsumuje uwagę tych, którzy ją przyjmują. Niemożność opanowania ich natłoku sprawia, że doświadczamy syndromu zmęczenia informacją (*attention crash*) zdiagnozowanego przez psychologa Davida Lewisa: nie jesteśmy w stanie przyswoić nowych wiadomości, mamy problem ze zrozumieniem prostych komunikatów, nie mówiąc już o ich selekcji[40]. Ilość danych rośnie szybciej niż zdolność ich przetwarzania. Nie analizując danych nie wiemy, które są naprawdę ważne.

Co więcej, walka informacyjna ma miejsce nie tylko w sferze militarnej. Ma również zastosowanie w polityce, kulturze, gospodarce w formie:

- kampanii informacyjnych i propagandowych partii politycznych,
- wyłudzania, kradzieży danych niezbędnych do posługiwania się kontem bankowym ofiary,
- aktywizmu, haktywizmu,
- fizycznego zniszczenia central telefonicznych i sterowni[41].

Dlatego też tak ważna jest już nie sama informacja, ale umiejętność jej selekcji i analizy. Analiza daje nam coś więcej niż opis i interpretację informacji, daje możliwość prognozowania, określenia bieżących i przyszłych konsekwencji.

Przekazywane informacje mogą być deformowane i zniekształcane, wówczas mamy do czynienia z dezinformacją. Dezinformacja, dla uściślenia oznacza taki sposób przekazania informacji – prawdziwej lub fałszywej, aby wprowadzić w błąd przeciwnika/konkurenta i skłonić go do zachowania zgodnego z naszymi oczekiwaniami i korzystnego dla nas. Dezinformacja nie jest prostym kłamstwem. Jest podstępem. Efektem działań dezinformacyjnych jest propaganda.

Rozpoznanie dezinformacji nie jest prostym zabiegiem, należy ocenić daną informacji w różnych kontekstach, ale zawsze istnieją wątpliwości, czy nasze wnioski są całkowicie słuszne[42].

Walka z dezinformacją to również zadanie dla rządu i mediów by mogły zachować wiarygodność. Może ona polegać na wspieraniu dziennikarstwa, instytucji analitycznych i organizacji pozarządowych. Rząd powinien też skierować swe wysiłki na odbudowę obcojęzycznych publicznych serwisów informacyjnych, monitorowanie mediów społecznościowych i propagandowych, dostarczanie wiarygodnych danych (*raw data*) i obrazów satelitarnych[43].

Doktryna Bezpieczeństwa Informacyjnego RP (Projekt 2015 r.) określa szereg zadań operacyjnych i transsektorowych, mających na celu wsparcie i ochronę ludności cywilnej. Są to między innymi:

---

[40] E. Mistewicz, *Attention Crash*, Forbes 18.08.2012, https://www.forbes.pl/opinie/attention-crash-syndrom-zmeczenia-informacja/pzqmggh [dostęp: 20.08.2017].

[41] T.R. Aleksandrowicz, *Podstawy walki informacyjnej*…, s. 131.

[42] Tamże, s. 84–88.

[43] B. Nimmo, *The Case for Information Defence. A Pre-Emptive Strategy for Dealing with the New Disinformation Wars*, [w:] *Information at War: From China's Three Warfares to NATO's Narratives*, Legatum Institute, 2015, s. 31.

Koncepcja zadań operacyjnych w zakresie bezpieczeństwa informacyjnego RP:

a) Zadania sektora publicznego w wymiarze krajowym:
   - zapewnienie funkcjonowania spójnego systemu monitorowania i dystrybucji informacji w wymiarze cywilnym i wojskowym,
   - wspieranie działań mających na celu umacnianie tożsamości narodowej,
   - prowadzenie kampanii społecznych mających pozytywnie wpłynąć na obraz Polski,
   - działania z zakresu komunikacji społecznej budujące markę RP,
   - wykorzystanie potencjału dyplomacji publicznej,
   - zapobieganie, w ramach działań kontrwywiadowczych, aktywizacji przez obce państwo wybranych grup społecznych, celem realizacji interesów sprzecznych z interesem RP,
   - stworzenie społecznej zdolności do rozpoznawania i neutralizacji dezinformacji,
   - aktywizacja kapitału społecznego,
   - wdrażanie mechanizmów kontrinformacji oraz edukacja i uświadamianie obywateli na poziomie narodowym m.in. poprzez zaangażowanie mediów,
   - planowanie użycia i produkcji środków oddziaływania na środowisko informacyjne.
b) Główne zadania sektora publicznego na poziomie międzynarodowym:
   - objęcie mniejszości polskiej w regionie powszechnym dostępem do wszystkich polskich mediów elektronicznych (radio i tv),
   - tworzenie silnej konkurencji dla mediów rosyjskich, jako głównego przekaźnika informacji (propagandy) dla tej grupy ludności,
   - współdziałanie z krajami regionu w zakresie nadawania programów radiowych i telewizyjnych na Białorusi,
   - dotarcie z polskimi programami informacyjnymi (radiowymi i telewizyjnymi) do mniejszości polskiej w innych krajach,
   - objęcie tej mniejszości programami edukacyjnymi w zakresie historii i współczesnej polityki,
   - stały monitoring przekazu propagandowego ukierunkowanego na Polskę i treści dyskredytujących polską politykę zagraniczną,
   - analiza pozwalająca identyfikować źródła przekazu oraz – na ile to możliwe – eliminowanie źródeł dezinformacji.
c) Główne zadania sektora prywatnego:
   - współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom środowiska informacyjnego,
   - włączenie prywatnych nadawców komercyjnych do realizacji zadań informacyjnych stawianych mediom publicznym wobec mniejszości polskiej np. na Litwie (system zachęt i ulg podatkowych),
   - udział w mechanizmach wymiany informacji, szkoleniach, oraz stosowanie zasad dobrych praktyk; aktywność i rzetelność informacyjna wobec organów odpowiedzialnych za nadzór nad funkcjonowaniem strategicznych organizacji oraz spółek państwa.

d) Główne zadania sektora obywatelskiego:
   - zaangażowanie obywateli oraz udział w przedsięwzięciach i ruchach obywatelskich służących wzmocnieniu bezpieczeństwa informacyjnego,
   - samoorganizacja społeczeństwa obywatelskiego poprzez samokształcenie, podnoszenie świadomości o zagrożeniach i wspieranie obywatelskiego potencjału przeciwdziałania (np. tzw. „dobre trolle"),
   - świadome konsumowanie treści informacyjnych, analiza treści (identyfikacja ataków propagandowych i dezinformacyjnych).

e) Główne zadania transsektorowe:
   - współpraca sektora państwowego (służby, wojsko, administracja na wszystkich szczeblach) z mediami w celu lepszej ochrony interesów państwa w sferze informacyjnej,
   - przeciwdziałanie propagandzie oraz reagowanie kryzysowe z wykorzystaniem potencjału społecznego,
   - właściwe kreowanie postaw społecznych na rzecz bezpieczeństwa narodowego[44].

Działania te mają zapewnić skuteczne wsparcie ludności cywilnej. Umiejętność obrony przed manipulacją, indoktrynacją i propagandą wymaga silnej świadomości swojej tożsamości, osobowości, które zdobywa przez wychowanie i edukację przez całe życie, ale także aktualnej i rzetelnej wiedzy o zachodzących procesach społecznych, a te czerpie w przeważającej mierze ze środków masowego przekazu.

Zakończenie

Przewaga w teorii sztuki wojennej to podstawowa zasada oznacza górowanie nad przeciwnikiem ilościowe (liczebne) i jakościowe (żołnierzy, środków walki, organizowania i kierowania walką), stanowi sens wszelkich zabiegów koncepcyjnych i organizacyjnych, decyduje o wyniku końcowym. Współcześnie kluczowym elementem przewagi stały się jej pozamaterialne składniki, tj. działania w sferze informacyjnej. Uzyskanie przewagi informacyjnej, dzięki wykorzystaniu nowoczesnych rozwiązań telekomunikacyjnych nabrało formy walki informacyjnej, w której stosuje się takie metody jak: destrukcja fizyczna, operacje psychologiczne, sabotaż, walka elektroniczna.

W opisanych przykładach działań sieciocentrycznych i działań terrorystycznych walka informacyjna była elementem wspierającym. Rosjanie zaś walkę informacyjną traktują, jako samodzielne, długofalowe działanie angażującej środki informacyjno-techniczne i informacyjno-psychologicznie, niekoniecznie środki militarne.

Walka informacyjna, jako element konfliktów zmieniła ich charakter a tym samym stan środowiska bezpieczeństwa, który U. Beck opisał, jako stan *odczuwanej wojny i odczuwanego pokoju*, w których wojna jest toczona jest nie na terytorium państwa, które je wypowiada, co daje minimalizację strat własnych i ukrycie strat w ludności cywilnej przeciwnika.

[44] *Doktryna Bezpieczeństwa Informacyjnego* RP, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 24.08.2017].

Każdy z opisanych konfliktów angażował ludność cywilną, jako narzędzie, co pozwoliło na sformułowanie poglądu, że obok informacji, społeczeństwo stało się kolejnym zasobem strategicznym, celem ataku, środkiem walki i przekazu propagandowych treści. Jej kondycja i postawa może przesądzić o wyniku konfliktu. Poddana ciągłej manipulacji, dezinformacji, indoktrynacji musi zostać wyposażona w mechanizmy obronne. Ta odpowiedzialność spoczywa na rządach poprzez dostarczanie wiarygodnej informacji i edukacji by wykształcić odpowiednie postawy i zdolności.

Bibliografia

Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Warszawa 2016.

Aleksandrowicz T.R., *Świat w sieci. Państwa, społeczeństwa*, *ludzie*, Warszawa 2014.

Aleksandrowicz T.R., *Terroryzm międzynarodowy*, Warszawa 2010.

Beck U., *Społeczeństwo światowego ryzyka*, Warszawa 2012.

Giles K., *Handbook of Russian Information Warfare*, NATO 2016.

Koziej S., *Teoria sztuki wojennej*, Warszawa 2010.

Laqueur W., *Reflection on Terrorism Foreign Affairs Fall 1986*, vol. 65, no. 1.

Liedel K., *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011.

Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*, Difin, Warzawa 2010.

Liederman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Nimmo B., *The Case for Information Defence. A Pre-Emptive Strategy for Dealing with the New Disinformation Wars*, [w:] *Information at War: From China's Three Warfares to NATO's Narratives*, Legatum Institute, 2015.

Thomas T., *Psycho Viruses and Reflexive Control. Russian Theories of Information – Psychological War*, [w:] *Information at War: From China's Three Warfares to NATO's Narratives*, Legatum Institute, 2015.

Netografia

Copp C., *Understanding Network Centric Warfare*, Australian Aviation, January/February 2005, http://www.ausairpower.net/TE-NCW-JanFeb-05.html [dostęp: 18.08.2017].

Jenkins B.M., *International Terrorism*: A New Mode of Conflict, International Terrorism and World Security, https://www.rand.org/content/dam/rand/pubs/papers/2008/P5261.pdf [dostęp: 21.08.2017].

Lelonek A., *Rosyjska wojna informacyjna na Ukrainie, w Defence 24 z* 30 kwietnia 2016, http://www.defence24.pl/rosyjska-wojna-informacyjna-na-ukrainie [dostęp: 2.02.2018].

Mistewicz E., *Attention Crash*, Forbes 18.08.2012, https://www.forbes.pl/opinie/attention-crash-syndrom-zmeczenia-informacja/pzqmggh [dostęp: 20.08.2017].

Rokiciski K., *Możliwości zastosowania koncepcji sieciocentryczności na obszarach morskich RP*, Zeszyty Naukowe AMW, rok XLVIII, nr 3(170) 2007, s. 75–90, http://www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2007/Rokicinski_K3.pdf [dostęp: 21.08.2017].

Sienkiewicz P., *Wizje i modele wojny informacyjnej*, http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf [dostęp: 21.08.2017].

Wojnowski M., *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, Przegląd Bezpieczeństwa Wewnętrznego 13/15 www.abw.gov.pl/download/1/1989/Wojnowski.pdf [dostęp: 21.08.2017].

Information warfare in the contemporary conflicts and its social consequences

Abstract

Nowadays, the operation in the area of information has become the key element of military conflicts. Gaining information advantage with use of modern ICT is defined as information warfare. The aim of the paper is to present the examples of networkcentric and terroristic operations in which information warfare is the supportive element. The paper covers also the issue of Russian concept of information war.

Information warfare as the element of conflicts has changed their nature and the conditions of the security environment. Every of the described conflicts involved civilians as the tool. Together with the information civilians has become another strategic asset, target means of warfare and propaganda. Their mindset and wellbeing may determine the outcome of the operation. Thus, the society should be equipped with defensive mechanisms. This is responsibility of governments and institutions of education for security and defense.

Słowa kluczowe: walka informacyjna, wojna informacyjna, ludność cywilna, edukacja dla bezpieczeństwa i obronności

Keywords: information warfare, information war, civilians, education for security and defense

Danuta Kaźmierczak
doktor nauk społecznych w dyscyplinie nauki o bezpieczeństwie, adiunkt w Instytucie Bezpieczeństwa i Edukacji Obywatelskiej Uniwersytetu Pedagogicznego im. KEN w Krakowie. Zajmuje się zagadnieniami bezpieczeństwa społecznego i edukacji dla bezpieczeństwa.