Wizje i modele wojny informacyjnej

Piotr Sienkiewicz

Wszczyna się wojnę, kiedy się chce,
a kończy, kiedy można.
N. Machiavelli

Gdy podsumowywano wpływ nowoczesnych technologii na rezultat wojny w Zatoce Perskiej, posłużono się skrótem „4S", co miało oznaczać: niewidzialne samoloty (Stealth), manewrujące rakiety wystrzeliwane z okrętów (*Sea Launched Cruise Missiles*), obronę zorganizowaną zgodnie z założeniami Strategicznej Inicjatywy Obronnej (*SDI Like Defense*) oraz systemy rozpoznania kosmicznego (*Space. System Spy Satelites*). Następnie dodano piąte S – *Semiconductors*, czyli po prostu półprzewodniki, słusznie podkreślając podstawę rozwoju technologii informacyjnych, od których zależał rozwój pozostałych czterech „S". Słynny publicysta Alvin Toffler pisał, nie bez pewnej przesady, że wojnę w Zatoce wygrała inteligencja ukryta w mikroprocesorach systemów uzbrojenia oraz w systemach dowodzenia, łączności i rozpoznania.

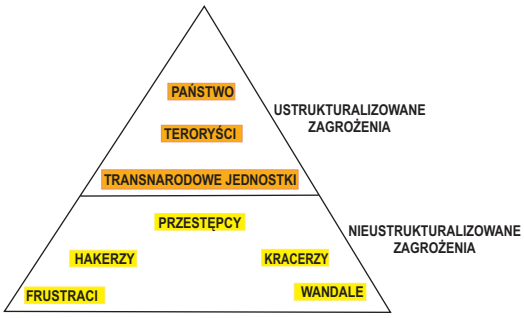
Wśród głównych przyczyn klęski armii irackiej, o znaczącym potencjale bojowym, uznano przestarzałą elektronikę. Była ona bowiem mało wydajna, oparta na łatwo zakłócalnej technice analogowej, uniemożliwiającej efektywną, kompleksową automatyzację systemów dowodzenia, łączności, rozpoznania i sterowania środkami walki. Na przegranej Irakijczyków zaważył również zbyt mały i przestarzały potencjał systemów informacyjnych, które nie były w stanie dostarczyć danych niezbędnych do planowania i wykonania uderzeń na obiekty przeciwnika. Obrazu przyczyn klęski dopełnił mało elastyczny system kierowania i dowodzenia (o sztywnej hierarchicznej strukturze). W tych obszarach wyraża się druzgocąca wprost przewaga aliantów, co można wyrazić jako konfrontację systemów należących do dwóch różnych generacji technologicznych.

Od czasów wojny w Zatoce, którą uznano za „I wojnę informacyjną", rozstrzygająca przewaga informacyjna traktowana jest jako istota współczesnych koncepcji prowadzenia działań (operacji) informacyjnych typu „Infowar" i „Cyberwar".

Konceptualizacja

Za punkt wyjścia należy przyjąć pojęcie bezpieczeństwa informacyjnego jako integralnej części bezpieczeństwa narodowego, a następnie zagrożeń informacyjnych (rys. 1).

Warto zauważyć związek „hierarchii informacji" (*Data – Information – Knowledge – Wisdom*) z ogólnym modelem „OODA" (*Observe – Orient – Decide – Act*; rys. 2).



Rys. 1

Hierarchia zagrożeń

Źródło: opracowanie własne na podstawie [7].

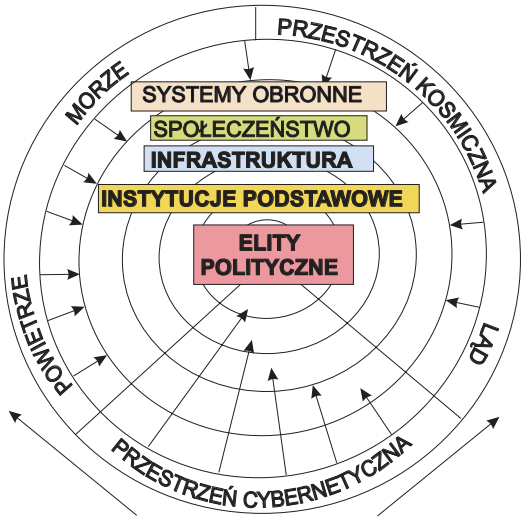
Innym, nowym, bo sformułowanym w latach 90. ujęciem współczesnej walki jest tzw. Model Wardena (rys. 3), w którym piątym „wymiarem" walki jest „przestrzeń cybernetyczna" (*Cyberspace*).

Rys. 2

Hierarchia informacji

Źródło: opracowanie własne na podstawie Sienkiewicz, 1995.

U podstaw tych koncepcji legło przekonanie, że zastosowanie systemów informacyjnych w celu osłabienia zdolności obronnych przeciwnika może prowadzić w szczególności do uniknięcia wybuchu klasycznego konfliktu zbrojnego. Z tego powodu zaliczono do arsenału środków walki, np. wirusy komputerowe i bomby logiczne (unieszkodliwiające), wykorzystanie impulsów elektromagnetycznych o dużym natężeniu (w celu zniszczenia struktur układów scalonych, powodujących nieodwracalne uszkodzenia komputerów i innych urządzeń elektronicznych), wytworzenie szczepów bakterii mogących żywić się materiałami stosowanym do produkcji układów elektronicznych, środki penetracji systemów teleinformatycznych przeciwnika, itp. „Walka na bity" polegać więc będzie na niszczeniu zasobów informacyjnych przeciwnika, sieci komputerowych jego instytucji finansowych, systemów telekomunikacji publicznej i kontroli ruchu powietrznego, włamaniach do komputerów instytucji rządowych, itp.



Rys. 3

Model „pięciu wymiarów" walki Wardena

Źródło: J. Warden, *The Enemy as System*, wiosna 1995.

Konsekwencją analizy systemowej procesów informacyjnych na współczesnym polu walki jest wprowadzenie „stosunku wiedzy" (*relative knowledge*) stron walczących jako czynnika decydującego w rezultatach walki.

Walką informacyjną (*information warfare, infowar*) nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych).

Istotą tak rozumianej walki informacyjnej jest:

1) zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych,
2) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystanych systemów informacyjnych.

Przewaga informacyjna

Nowoczesne koncepcje walki zbrojnej bazują na tworzeniu wieloczynnikowej przewagi militarnej (*multifactor military superioritly*) w oparciu o kontrolowaną, rozstrzygającą przewagę informacyjną (*information superiority*) i technologiczną (*technological superiority*). Jakkolwiek potencjał informacyjny stanowił zawsze istotny czynnik potencjału bojowego, to w rozważaniach dotyczących sposobów tworzenia przewagi na polu walki był on raczej pomijany. W szczególności w matematycznych modelach walki (typu modele Lanchestera) uwaga koncentrowała się na „stosunku sił" uwzględniającym przede wszystkim „potencjały rażenia" stron walczących.

Potencjał informacyjny jako czynnik potencjału militarnego tworzą zasoby informacyjne systemu obronnego państwa oraz systemy informacyjne kształtujące infrastrukturę informacyjną państwa. Oznacza to, że potencjał informacyjny to wszelkie zasoby informacyjne (dane, informacje, wiedza), które tworzą infosferę określonego systemu działania (organizacji, instytucji), ale także systemy informacyjne (informatyczne, telekomunikacyjne) niezbędne do efektywnego prowadzenia określonych, zamierzonych działań.

W ostatnich latach wyróżniono informacyjne operacje (działania) ofensywne i defensywne.

Do operacji ofensywnych zalicza się takie działania, jak:
- osłona operacji (*operations security*),
- operacje psychologiczne (*psychological operations*),
- pozoracja (*military deception*),
- destrukcja (*physical attack*),
- walka elektroniczna (*electronic warfare*).

Warunkiem powodzenia powyższych działań jest uzyskanie przewagi informacyjnej (*information superiority*), rozumianej jako: „zdolność do zbierania, przetwarzania i udostępniania informacji przy wykorzystaniu (lub deprecjonowaniu) zdolności przeciwnika do wykonania tego samego". Z kolei dominacja informacyjna (*information dominance*) obejmuje zarówno wysiłki ofensywne, jak i defensywne, których celem jest stworzenie różnicy „między tym, co my wiemy o naszej przestrzeni bojowej i operacjach w niej prowadzonych, a tym, co nieprzyjaciel wie o swojej przestrzeni bojowej".

Przyjęcie powyższych koncepcji prowadzenia działań zmusza do poszukiwania nowych miar (kryteriów) oceny efektywności. Jedną z nich jest tzw. stosunek wiedzy, określony dla następujących założeń:

1) dowolna jednostka kontroluje dowolny obszar, gdy jest ona zdolna do działania „wewnątrz" tego obszaru w sposób dowolny,
2) promień kontrolowanego przez daną jednostkę obszaru jest równy najmniejszej z trzech wielkości: maksymalnego, skutecznego zasięgu systemów ognia pośredniego jednostki, maksymalnego skutecznego zasięgu jej systemów rozpoznania („sensorów"), promienia przydzielonego obszaru operacji,
3) wiedza to stopień posiadanej przez dowódcę jednostki znajomości dyspozycji sił własnych i nieprzyjaciela wewnątrz obszaru wyznaczonego przez promień kontroli tej jednostki (tzw. stopień posiadanej „świadomości sytuacyjnej").

Wojna cybernetyczna

Współczesne koncepcje walki informacyjnej, obejmujące nowe modele operacji, w których kluczową rolę spełniają pojęcia „przewagi informacyjnej" i „przewagi wiedzy", nie wyczerpują pojęcia wojny cybernetycznej, czyli różnych form walki prowadzonej w „przestrzeni cybernetycznej". Jakkolwiek pojęcie „cyberprzestrzeni" wprowadził W. Gibson w powieści *Neuroromancer*, to obecnie najczęściej określa ono globalną infor-

macyjną (teleinformatyczną) infrastrukturę. A zatem istotą wojny cybernetycznej jest realizacja określonych celów politycznych dzięki działaniom podejmowanym w przestrzeni cybernetycznej.

Do swoistych cech wojny cybernetycznej należy zaliczyć następujące:
– misją jest uzyskanie przewagi informacyjnej,
– przeciwnik jest „niewidzialny",
– terenem działań jest cyberprzestrzeń,
– czynnikiem krytycznym jest czas.

Istnieje kilka poziomów wojny cybernetycznej, z których można wyróżnić trzy:
– wojna cybernetyczna towarzysząca operacjom wojskowym,
– ograniczona wojna cybernetyczna,
– nieograniczona wojna cybernetyczna.

W ograniczonej wojnie cybernetycznej teleinformatyczna infrastruktura państwa jest środkiem i celem działań towarzyszących realnemu atakowi. Może być prowadzona w celu np. opóźniania przygotowań przeciwnika do interwencji zbrojnych. Nieograniczoną wojnę cybernetyczną charakteryzuje rozległy zasięg, zaś celami działań destrukcyjnych są zarówno wojskowe, jak i cywilne systemy informacyjne, funkcjonujące w każdej sferze życia społecznego.

Zakończenie

Współczesne myślenie o pokoju, bezpieczeństwie narodowym, musi obejmować analizy systemowe zjawiska wojny cybernetycznej oraz związane z nim zagrożenia i szanse bezpiecznego rozwoju. Bezpieczeństwo informacyjne jest trwałym elementem bezpieczeństwa narodowego (międzynarodowego), tak, jak społeczeństwo globalnej informacji jest immanentnym elementem (czynnikiem) procesu globalizacji.

Być może w przyszłości cele polityczne będą mogły być osiągane dzięki użyciu ofensywnych środków informacyjnych. A zatem wojna (nawet w rozumieniu clausewitzowskiego aforyzmu, bo nie definicji przecież) cybernetyczna jawi się jako wojna „nowej generacji". Operacja w Afganistanie i wojna z Irakiem są konfliktami zbrojnymi nowego wieku (tj. XXI), ale były wojnami cybernetycznymi. Te zaś nie są już kreacjami z kręgu science fiction, lecz projekcjami przyszłości, o której wiemy tyle, że będzie odmienna od tej, którą dziś sobie wyobrażamy.

Ogłoszona po wydarzeniach z 11 września 2001 roku „wojna z terroryzmen" nie jest, jak tradycyjne wojny, zmaganiami z kimś, lecz z czymś. Wojny z czymś nie rozgrywają się między państwami albo koalicjami krajów. Tradycyjne wojny będą zapewne towarzyszyć ludzkim losom, choć nie ma dobrych wojen, jak nie ma złego pokoju, co podkreślał George Washington. Wydarzenia z 11 września 2001 roku uświadomiły, że ład postzimnowojenny nie przyniósł ani „końca historii", ani nadziei na „trwały pokój".

Atak na WTC i Pentagon niemal cały świat oglądał w czasie rzeczywistym – na ekranach telewizyjnych, niczym *reality show*. Terroryści starają się rozbudzić strach i za po-

mocą strachu zdobyć dominację i kontrolę. Grają swoisty spektakl strachu domagając się udziału publiczności.

Dzięki globalnym systemom masowego komunikowania to im się udaje.

W warunkach globalnego społeczeństwa informacyjnego objawiają się nowe zagrożenia dla bezpieczeństwa i nowe ich „medialne" oblicza.

Błędne skaterygoryzowanie zagrożeń, wojny, bezpieczeństwa jest podobne do wadliwie zaprojektowanego gmachu, który grzebie pod swoimi gruzami projektanta. Natomiast dobra kategoryzacja tych zjawisk promuje politykę i maksymalizuje dla niej poparcie.

Stanisław Lem omawiając militarne zastosowania sztucznej inteligencji (a także „sztucznej nieinteligencji") napisał: „Kiedy w każdym «dziś» przychodzi decydować o tym, co było «wczoraj», decydowanie przesuwa się z teraźniejszości w przeszłość i tym samym staje się pustą grą pozorów".

Bibliografia

[1] Campen A. 1992: *The First Information War*, AFCEA.

[2] Waltz E. 1998: *Information Warfare*, Artech House, Inc.

[3] Darilek R. i in., 2001: *Measures of Effectiveness for the Information Age Army*, RAND.

[4] Balcerowicz B. 2002: *Pokój i nie-pokój*, Bellona, Warszawa.

[5] Goban-Klas T., Sienkiewicz P. 1999: *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków.

[6] Hoffman B. 1995: *Oblicza terroryzmu*, Warszawa.

[7] Sienkiewicz P. 1995: *Analiza systemowa*, Bellona, Warszawa.

[8] Lem S. 1985: *Biblioteka XXI wieku*, WL.