Elżbieta POSŁUSZNA
Lotnicza Akademia Wojskowa
e-mail: e.posluszna@law.mil.pl
ORCID: 0000-0001-8652-5729

DOI: 10.55676/asi.v3i1.20

HIERARCHIE KONTRA SIECI. RZECZ O WALCE SIECIOWEJ I NIESTEROWANYM OPORZE

HIERARCHIES VERSUS NETWORKS. THE IMPORTANCE OF LEADERLESS RESISTANCE IN THE NETWAR

Streszczenie

Artykuł jest polemiką z twierdzeniem, że walka sieciowa, z uwagi na wykorzystywanie niemilitarnych środków (m.in. informacji i narzędzi cybernetycznych) oraz zaangażowanie niescentralizowanych, społecznie rekrutowanych i rekrutujących się jednostek i grup, jest konfliktem o stosunkowo niedużej intensywności, a w związku z tym nie stanowi znaczącego zagrożenia dla bezpieczeństwa państw i społeczeństw. Takie twierdzenie, zdaniem autorki, jest co najmniej ryzykowne. Nie uwzględnia ono bowiem ani silnej społecznej mobilizacji, biorącej się z możliwości pozyskiwania „dla sprawy" szerokiego, globalnego audytorium, ani też wzrastającego znaczenia nowych form organizacyjnych – nowych sieciowych modeli, bardziej bezpiecznych (jeśli brać pod uwagę odporność na inwigilację) i efektywnych (uwzględniając zdolność zadawania wysokich strat przy udziale minimum zaangażowanych środków) niż dotychczasowe, biorące udział w walce hierarchiczne struktury.

Słowa kluczowe: walka sieciowa, opór bez przywództwa (opór niesterowany), rojenie, terroryzm

Abstract

The article is a polemic with the statement that netwar, due to the use of non-military means (including information and cybernetic tools) and the involvement of non-centralized, socially recruited and recruiting themselves individuals and groups, is a conflict of relatively low intensity, and therefore does not pose a significant threat to the security of states and societies. Such statement, according to the author, is at least risky. It does not take into account either the strong social mobilization resulting from the possibility of attracting a broad, global audience "or the issue", or the growing importance of new organizational forms – new network models, more secure (if we take into account resistance to surveillance) and effective (if take into account the ability to inflict high losses with the participation of a minimum of involved resources) than the existing hierarchical structures taking part in the fight.

Keywords: netwar, leaderless resistance, swarming, terrorism

Artykuł wpłynął do redakcji: 13.12.2022 / Zatwierdzono do publikacji: 18.01.2023

OPEN ACCESS This work is licensed under version CC BY-NC-ND 4.0.

1. WPROWADZENIE

Pod koniec lat sześćdziesiątych XX w. dwoje amerykańskich naukowców Virginia H. Hine oraz Luther P. Gerlach przeprowadziło badania nad strukturą organizacyjną kilku nowych ruchów społecznych[1]. Badania te pokazały, że ich struktura nie jest ani biurokratyczna, ani też amorficzna, lecz segmentacyjna (w jej skład wchodzi wiele różnorodnych grup, które pojawiają się i znikają, dzielą się i łączą, powiększają i różnicują), policentryczna (w jej ramach istnieje wielu często tymczasowych i rywalizujących ze sobą liderów oraz ośrodków wpływów) oraz sieciowa (tworzy luźno zintegrowane sieci z różnorodnymi powiązaniami na bazie zachodzącego na siebie członkostwa, wspólnej aktywności, lektur, wspólnych ideałów i przeciwników). Zdaniem wspomnianych badaczy policentryczne, segmentowe i sieciowe formy organizacyjne (w skrócie określane jako SPIN – *segmentary*, *polycentric*, *integrated networked*), ze względu m.in. na ich zdolność do wyzwalania osobistego zaangażowania uczestników oraz adaptacji do zmieniających się warunków zewnętrznych, w o wiele większym stopniu są w stanie sprostać rozmaitym zagrożeniom (tak zewnętrznym, jak i wewnętrznym) niż struktury dawne, zwykle mocno zhierarchizowane i scentralizowane. Dlatego w przyszłości rola tych ostatnich będzie powoli maleć, a pierwszych zwiększać się. Prognozy te okazały się szczególnie trafne. Ich trafność objawiła się szczególnie wtedy, gdy wśród technologii komunikacyjnych znaczącą rolę zaczął odgrywać Internet.

Wpływ Internetu, a także innych technologii komunikacyjnych sięga znacznie głębiej, niż się to zwykle przypuszcza. Jego najbardziej widomym, jak się wydaje, znakiem jest odchodzenie od tradycyjnych hierarchicznych i centralnie zarządzanych struktur organizacyjnych ku „strukturom luźniejszym", możliwie jak najbardziej zdecentralizowanym, często wręcz horyzontalnym – bez wyraźnego kierownictwa czy ośrodków kontroli. Zdaniem wielu badaczy nie jest to jedynie zjawisko nietrwałe, lecz stała tendencja wpisana w przyszłość terroryzmu. Takiego zdania są m.in. analitycy Rand Corporation – John Arquilla, David Ronfeldt i Michele Zanini. Według nich: „Terroryści odchodzić będą od hierarchicznych modeli ku sieciowym modelom ery informacyjnej. W grupach – przywództwo »wybitnej postaci« ustąpi miejsca horyzontalnym, zdecentralizowanym modelom. Więcej wysiłku wkładać się będzie w tworzenie układu grup ponadnarodowo powiązanych w sieć niż grup autonomicznych"[2].

2. WALKA SIECIOWA

Ale rewolucja informacyjna umożliwia coś jeszcze, a mianowicie prowadzenie działań wojennych nowego typu – działań opartych w dużej części na wykorzystaniu społecznego zaangażowania oraz niescentralizowanej formie organizacji i przepływu

[1] L.P. Gerlach, V.H. Hine, *People, Power, Change: Movements of Social Transformation*, Bobbs-Merrill, Indianapolis 1970.

[2] J. Arquilla, D. Ronfeldt, M. Zanini, *Networks*, *Netwar, and Information-Age Terrorism*, [w:] I.O. Lesser, B. Hoffman, J. Arquilla, D. Ronfeldt, M. Zanini, B.M. Jenkins, *Countering the New Terrorism*, RAND Corporation, Santa Monica 1999, s. 41.

 DOI: 10.55676/asi.v3i1.20

informacji. Ten nowy typ działań wojennych, jak również odpowiadająca im nowa forma konfliktu, określane są w literaturze przedmiotu jako „walka sieciowa".

> Termin »wojna sieciowa« odnosi się do wyłaniającej się formy konfliktu (i przestępczości) na poziomie społecznym, w której wykorzystywane są środki mniej intensywne niż wojenne oraz sieciowe formy organizacyjne, doktrynalne, strategiczne i komunikacyjne. Strony uczestniczące w konfliktach o takiej formie składają się zazwyczaj z rozproszonych, często małych grup, którym odpowiada komunikacja, koordynacja i działanie w sposób sieciowy, często bez określonego zcentralizowanego przywództwa oraz ośrodków dowodzenia. Podejmowanie decyzji może być rozmyślnie zdecentralizowane i rozproszone. [...] Podmioty objęte spektrum konfliktów społecznych i przestępczości ewoluują w stronę wojny sieciowej. Dotyczy to znanych podmiotów, które modyfikują swoje struktury i strategie w celu wykorzystania korzyści płynących z rozwoju modeli sieciowych, jak np. międzynarodowe grupy terrorystyczne, czarno-rynkowi handlarze broni masowego rażenia, narkotyków i inne syndykaty przestępcze, ruchy fundamentalistyczne i nacjonalistyczne, złodzieje własności intelektualnej oraz przemytnicy uciekinierów i emigrantów. Niektóre wielkomiejskie gangi, wiejskie organizacje milicyjne, walczące grupy jednej sprawy [...] także rozwijają swój potencjał sieciowy. Ale to nie wszystko. W spektrum wojny sieciowej być może coraz częściej znajdować się będzie nowa generacja rewolucjonistów i aktywistów wyznających postindustrialne ideologie ery informacyjnej, które właśnie dziś nabierają kształtu. W niektórych przypadkach, tożsamości i uczucia lojalności mogą przesunąć się z poziomu narodowego na ponadnarodowy poziom »globalnego społeczeństwa obywatelskiego«. W wojnie sieciowej wziąć udział mogą też nowego typu podmioty, np. członkowie anarchistycznych i nihilistycznych sprzysiężeń wykwalifikowanych informatycznie cybersabotażystów[3].

Uważa się dość powszechnie, że walka sieciowa, z uwagi na wykorzystywanie niemilitarnych środków (m.in. informacji i narzędzi cybernetycznych) oraz zaangażowanie niescentralizowanych, społecznie rekrutowanych (czy może lepiej rekrutujących się) jednostek i grup, jest konfliktem o stosunkowo niedużej intensywności. Taka ocena wydaje się co najmniej ryzykowna. Nie uwzględnia ona bowiem ani silnej społecznej mobilizacji, biorącej się z możliwości pozyskiwania „dla sprawy" (dzięki nowym mediom) szerokiego, globalnego wręcz audytorium, ani też wzrastającego znaczenia nowych form organizacyjnych – nowych sieciowych modeli, bardziej bezpiecznych (jeśli brać pod uwagę odporność na inwigilację) i efektywnych (jeśli brać pod uwagę zdolność zadawania wysokich strat przy udziale minimum zaangażowanych środków) niż dotychczasowe hierarchiczne struktury.

3. MODELE SIECIOWE

„Sieciowe modele" (sieciowe struktury organizacyjne) mogą przyjmować wiele różnych kształtów[4]. Mogą być na przykład powiązane łańcuchowo (*chain network*, *line network*). W takim przypadku komunikacja między poszczególnymi ogniwami

[3] Koncepcję walki sieciowej (zwanej także „wojną sieciową") opracowali analitycy RAND Corporation, m.in. John Arquilla, David Ronfeldt i Michele Zanini w pracach pt.: *The Advent of Netwar, Countering the New Terrorism oraz Networks and Netwars: The Future of Terror, Crime, and Militancy*, red. J. Arquilla, D. Ronfeldt, RAND Corporation, Santa Monica 2001, s. 5–6.

[4] Patrz: J. Arquilla, D. Ronfeldt, *The Advent of Netwar (Revisited)*, [w:] *Networks and Netwars: The Future of Terror, Crime, and Militancy*, red. J. Arquilla, D. Ronfeldt, RAND Corporation, Santa Monica 2001.

(wymiana dóbr i informacji) przebiegać będzie wzdłuż linii ogniw połączonych jedynie ośrodkami sąsiadującymi. Ten typ sieciowej struktury najczęściej spotkać można w gangach przemytniczych. Innym typem powiązań jest sieć węzłowa (*star network*, *hub network*, *wheel network*). Tu komunikacja pomiędzy ośrodkami i koordynacja działań uzależniona jest od ośrodka centralnego, od swoistego węzła pośredniczącego, który pełni funkcję przekaźnika informacji i dóbr. Nie jest to jednak komunikacja zorganizowana hierarchicznie. Bywa i tak, że poszczególne ośrodki nic nie wiedzą o swym wzajemnym istnieniu. Ten typ najczęściej spotkać można zarówno w kartelach czy franczyzach, jak i u ugrupowań terrorystycznych. Kolejnym rodzajem powiązań jest sieć wszechkanałowa (*all-channel network*, *full-matrix network*). W sieci wszechkanałowej wszystkie ośrodki powiązane są ze sobą – każdy z każdym. Nie ma tu jakichkolwiek wyróżnionych węzłów, a komunikacja pomiędzy wybranymi punktami sieci dokonywać się może niezależnie od wszelkich pozostałych powiązań. Najczęściej ten typ powiązań można odnaleźć wśród wojowniczych ugrupowań (w szczególności wśród tzw. „ugrupowań jednej sprawy”[5]), które są w wysokim stopniu zdecentralizowane i zinformatyzowane.

Te trzy modele powiązań sieciowych występują również w rozmaitych układach hybrydycznych, łączących w jednej strukturze organizacyjnej dwie lub trzy formy powiązań sieciowych (bądź też nawet sieciowych i hierarchicznych zarazem). Złożone struktury organizacyjne mogą być zróżnicowane na poszczególnych poziomach funkcjonowania – na poziomie najwyższym, dla przykładu, funkcjonować mogą zgodnie z którąś z sieciowych form organizacji, hierarchizując jednocześnie organizację poszczególnych ośrodków sieci, bądź na odwrót. Hierarchiczne struktury organizacyjne mogą też posługiwać się sieciowymi formami organizacji któregoś ze swoich elementów, mogą to robić stale lub doraźnie, w celu np. wykonania jakiegoś zadania, którego nie mógłby sprawnie wykonać organ ustrukturalizowany hierarchicznie, bądź też na odwrót. Możliwości jest wiele[6].

Spośród wszystkich tych prostych czy hybrydycznych form organizacyjnych zdecydowanie najbezpieczniejszą jest sieć wszechkanałowa. Sieci łańcuchowe łatwo jest sparaliżować, przynajmniej czasowo, uderzeniem w którekolwiek z ogniw, sieci węzłowe można zdestruować uderzeniem w ośrodek centralny. Sieć wszechkanałowa, nawet jeśli zostanie w którymś miejscu zaatakowana, nadal może funkcjonować, zapewne też szybko ulegnie regeneracji.

Mogłoby się wydawać, że strukturalizowanie w sieć wszechkanałową stanowić będzie dla ugrupowań ekstremistycznych najwyższą (i najbezpieczniejszą) formę decentralizacji. Tak jednak nie jest. Współcześnie obserwować możemy rozwój nowej formy aktywizmu, który stanowi najpełniejsze, jak się wydaje, ucieleśnienie koncepcji „zdecentralizowanego modelu”. Istotą tej nowej formy jest zarzucenie wszelkiej formalnej

[5] Tym mianem określa się zwykle radykalne ugrupowania prozwierzęce (np. Animal Liberation Front), prośrodowiskowe (np. Earth First!) oraz antyaborcyjne (np. Armia Boga).

[6] Patrz: A.-L. Barabàsi, E. Bonabeau, *Scale Free Networks and How They Impact Everything*, „Scale Free Networks” may 2003, http://www.scribd.com/doc/6152736/Scale-Free-Networks-and-How-they-impact-everything-by-AlbertLaszlo-Barabasi-and-Eric-Bonabeau [dostęp: 16.12.2009].

 DOI: 10.55676/asi.v3i1.20

czy nieformalnej struktury oraz skrajny indywidualizm w realizowaniu określonych celów. Inaczej mówiąc, powiązania, które zawsze spajały poszczególne ogniwa sieci, przestają już na dobrą sprawę się liczyć. Liczy się jedynie wspólna ideologia oraz zgodne z nią czyny i działania. Nie ma już powiązań pomiędzy ogniwami. Istnieją jedynie źródła emisji idei (źródła te mogą mieć charakter efemeryczny) oraz ci, którzy skłonni są wprowadzać te idee w życie.

W istocie w drugiej połowie lat osiemdziesiątych XX w. wiele organizacji zaczęło powoli odchodzić od centralistycznych i hierarchicznych struktur ku strukturom luźniejszym, bardziej elastycznym i mniej podatnym na dekonstrukcję, choć zarazem bardziej zagrożonym rozpadem. Główną przyczyną takiego stanu rzeczy była duża skuteczność organów ścigania, które po okresie zastoju i nieporadności przypadającym na lata siedemdziesiąte, nauczyły się w sposób sprawny zbierać informacje, infiltrować i likwidować ugrupowania ekstremistyczne i terrorystyczne. Jednak „poluźnienie" struktur nie stanowiło skutecznego zabezpieczenia przed infiltracją. Tymi, którzy jako pierwsi nie tylko zdali sobie z tego sprawę, ale i skłonni byli zaproponować pewne rozwiązanie, byli założyciel International Service of Information pułkownik Ulius Louis Amoss oraz radykalny działacz amerykańskiej prawicy Louis Beam. Obydwaj zasłynęli jako twórcy strategii określanej jako „opór bez przywództwa" (*leaderless resistance*). Strategia ta zakłada rezygnację z wszelkich hierarchicznych struktur organizacyjnych, które winny zostać zastąpione luźną konfiguracją niewielkich, autonomicznych komórek, jednostek bądź małych grup, którymi nie kieruje żaden ośrodek decyzyjny, wyspecjalizowany w zarządzaniu zhierarchizowanymi strukturami organizacyjnymi. Według Beama, który nakreślił swoją koncepcję oporu bez przywództwa w 1983 r., w eseju „Leaderless Resistance", koncepcja ta (inaczej oporu niesterowanego) oznacza całkowite odejście od teorii organizacji[7].

4. OPÓR BEZ PRZYWÓDZTWA

Analizując różnice między klasycznymi organizacjami typu piramidalnego a ugrupowaniami „zorganizowanymi" na wzór „oporu bez przywództwa", rzeczywiście nie sposób nie zauważyć, że te pierwsze w o wiele większym stopniu narażone są na rozmaite formy inwigilacji ze strony policji. W strukturze piramidalnej bowiem skuteczny agent, jeśli przeniknie na określony szczebel hierarchicznej piramidy, bez trudu może zlikwidować wszystkie szczeble znajdujące się poniżej jego własnego poziomu zaczepienia, jak również zagrozić szczeblom znajdującym się powyżej. Niebezpieczeństwo infiltracji jest o wiele mniejsze w przypadku „organizacji", w których pojedyncze indywidua lub niewielkie grupy nie tylko nie posiadają organizacyjnego centrum, lecz również działają bez jakiegokolwiek strukturalnego powiązania między sobą. W organizacjach tego typu podstawowym elementem jednoczącym staje się ideologia, z której członkowie ruchu czerpać będą wiedzę na temat właściwych (tj. skutecznych i moralnie słusznych) metod walki. Ideologia ta musi mieć oczywiście swoje źródło witalne. Tym źródłem jest oczywiście Internet.

[7] L.R. Beam, *Leaderless Resistance*, „The Seditionist" 1992, nr 12, s. 2–3.

Nie sposób przecenić wpływu, jaki wywiera Internet na sposób funkcjonowania rozmaitych grup o charakterze ekstremistycznym, a nawet terrorystycznym. Aktywność takich ugrupowań w sieci internetowej rozpoczęła się, co prawda, w stosunkowo nieodległej przeszłości, szybko jednak zyskała na intensywności[8]. Przykładem takiej aktywności może być internetowa kampania propagandowa IRA, w ramach której podawane są informacje na temat skutecznych sposobów sporządzania koktajlu Mołotowa, podrabiania dokumentów, działania kontrwywiadu oraz stosowania fałszywej tożsamości, czy też inicjatywa środowisk rasistowskich i neonazistowskich Redwatch, polegająca na zbieraniu i zamieszczaniu w Internecie nazwisk, telefonów i adresów osób uznawanych za wrogów białej rasy (działaczy organizacji lewicowych, homoseksualnych, feministycznych czy antyfaszystowskich), wreszcie rozmaite periodyki (np. periodyk Al-Kaidy „Mu'skar al-Battar", opublikowany *online* pod koniec 2003 r., czy radykalny animalistyczny „Bite Back Magazine"), sprawozdania, instrukcje (przykładem może być tu kurs „How to prepare RDX-explosives" umieszczony w 2004 r. na sprzyjającej Al-Kaidzie arabskiej stronie http://al3dad.jeeran.com, czy zamieszczony przez niezależnego nowozelandzkiego naukowca detaliczny projekt wykonania pocisku typu Cruise za 5000 dolarów![9]), filmy video i podręczniki (np. *Anarchist's Cookbook*, *Terrorist's Handbook*, *Big Book on Explosion*, *Encyclopedia of Preparation for Jihad* – zawierający m.in. instrukcje dotyczące broni biologicznej) publikowane przez rozmaitej maści radykałów (również aktywistów środowiskowych i animalistycznych)[10]. Ilość tego rodzaju „publikacji" stale się zwiększa i coraz częściej mają one charakter praktyczno-instruktażowy. I wreszcie, to właśnie dzięki Internetowi indywidua mające wspólne zadania i cele mogą tworzyć podgrupy, spotykać się w wybranym miejscu, modyfikować taktykę, przeprowadzać operacje – a potem z łatwością wygaszać relacje i ponownie się rozpraszać[11].

5. ROJENIE

Internet jednak może być wykorzystany także do celów ofensywnych, pozwala bowiem poszczególnym węzłom sieci na swobodną i bezpieczną komunikację, która w warunkach niehierarchicznej, rozproszonej struktury jest gwarantem skutecznego działania. Tak zorganizowane ugrupowania mają do dyspozycji niezwykle skuteczną taktykę działania, w literaturze strategicznej określaną jako *swarming* (rojenie się).

Taktyka *swarmingu* nie jest niczym nowym. Przykłady jej stosowania z łatwością można odnaleźć w historii[12]. Jednak dopiero XXI w., w związku z szybkim rozwojem nowych

[8] Na temat aktywności ruchu ekologicznego w sieci internetowej patrz: J. Pickerill, *Cyberprotest. Environmental Activism Online*, Manchester University Press, Manchester–New York 2003.

[9] Patrz: B. Lia, *Globalisation and the Future of Terrorism. Patterns and Predictions*, Routledge, London–New York 2005, s. 180.

[10] B. Hoffman, *Oblicza terroryzmu*, Bertelsmann Media, Warszawa 2001, s. 189–195.

[11] Por. M. Zanini, S.J.A. Edwards, *The Networking of Terror in the Information Age*, [w:] *Networks and Netwars: The Future of Terror, Crime, and Militancy*, red. J. Arquilla, D. Ronfeldt, RAND Corporation, Santa Monica 2001, s. 35–36. Por. F. Cohen, *Terrorism and Cyberspace*, „Network Security" 2002, nr 5, s. 18–19.

[12] Patrz: J. Arquilla, D. Ronfeld, *Swarming and the Future*…, dz. cyt.

 DOI: 10.55676/asi.v3i1.20

technologii komunikacyjnych, pozwalających na wykorzystanie inicjatywy małych bojowych jednostek, może stać się ona ważnym elementem strategii, zarówno dla sił centralnie zorganizowanych, jak i dowolnych, nieafiliowanych grup czy ruchów społecznych[13]. *Swarming* można najogólniej zdefiniować jako „pozornie amorficzny", lecz w gruncie rzeczy „ustrukturyzowany i w pewien sposób »skoordynowany« sposób pulsującego uderzania z wielu stron na konkretny punkt lub punkty"[14]. Atak swarmingowy składa się zwykle z wielu, czasowo odseparowanych od siebie pulsów (uderzeń). W każdym z takich pulsów wyróżnić można cztery fazy: ulokowanie (*locate*), skupienie się (*converge*), atak (*attack*) i rozproszenie (*disperse*)[15]. Pulsowanie jest tym, co zasadniczo odróżnia *swarming* od *guerrilli*. Obie taktyki opierają się na małych, mobilnych i trudnych do zlokalizowania jednostkach, które działają na zasadzie „uderz i uciekaj" (*hit and run*). W przypadku ataku swarmingowego dochodzi tu do wielu powtarzających się w krótkim czasie ataków, dokonywanych równocześnie z różnych kierunków przez kilka, a nawet więcej jednostek. W kwestii *guerrilli* ataków takich jest niewiele (zwykle jest to jeden rajd bądź zasadzka) i są przeprowadzane przez jedną lub dwie jednostki.

Decydujące znaczenie w ataku swarmingowym ma szybkość i koordynacja działania. Jak zauważa Sean Edwards:

> Sieci swarmingowe muszą być w stanie zejść się szybko i skrycie nad celem, następnie rozproszyć się i być w stanie połączyć się do nowego »pulsu«. Jest istotne, by jednostki tworzące rój (swarm) skupiały się i atakowały symultanicznie. Każda pojedyncza jednostka roju jest sama w sobie bezbronna, jednakże, gdy jest połączona w konkretnym zadaniu z inną bratnią jednostką, jej siła ulega zwielokrotnieniu, ponieważ potencjał całości swarmingowej jest wyższy niż suma jej części. Jednostki czy niezbyt dobrze zmontowane grupy takich jednostek są bezradne wobec przeważających sił wroga, z jego większą siłą ognia i masą[16].

Zalety ataków swarmingowych trudno przecenić. Jak twierdzą Arquilla i Ronfeld:

> Siły roju są trudne do zlokalizowania, dlatego styl bitwy będzie odznaczał się amorficznością, przynajmniej w oczach wroga. Niewielki rozmiar i rozproszona lokalizacja manewrujących jednostek daje obraz symultanicznej ukradkowości i wszechobecności – »ukrytej wszechobecności«. Tak więc siła roju będzie w dużej mierze niewidzialna i niezauważona, ale będzie w stanie stężeć i uderzyć zdecydowanie, gdzieś w przestrzeni bitwy – bez żadnych ograniczeń narzucanych zwykle przez linię frontu[17].

„Amorficzność i nieuchwytność" to atuty pozwalające na sprawne otoczenie celu (*encirclement*) i w miarę bezpieczne dokonanie symultanicznego (*simultaneity*) ataku z wielu kierunków, szybkie wycofanie zaangażowanych jednostek, w celu

[13] Jako jeden z pierwszych taktykę *swarmingu* opisał marksistowski rewolucjonista i pisarz Carlos Marighella. Patrz: C. Marighella, *Minimanual of the Urban Guerilla*, Paladin Press, Boulder 1975, s. 22, http://www.latinamericanstudies.org/marighella.htm; http://www.investigatingtheterror.com/documents/files/Mini-Manual%20of%20the%20Urban%20Guerrilla%20-%20Carlos%20Marighella%20(1969).pdf [dostęp: 18.02.2011].

[14] J. Arquilla, D. Ronfeld, *Networks and Netwar*, http://radio-weblogs.com/0107127/stories/2002/09/10/networksAndNetwar.html [dostęp: 19.02.2011].

[15] Patrz: S.J.A. Edwards, *Swarming on the Battlefield: Past, Present, and Future*, Rand Corporation, 2000, s. 68, http://www.rand.org/pubs/monograph_reports/MR1100.html [dostęp: 16.02.2011].

[16] Tamże, s. 68–69.

[17] Patrz: J. Arquilla, D. Ronfeld, *Swarming and the Future*…, dz. cyt., s. 46.

przysposobienia ich do ponownego ataku. Należy zauważyć, że podstawowym celem *swarmingu* jest nie tyle fizyczne zniszczenie wroga (w warunkach jego militarnej przewagi byłoby to zresztą niemożliwe), co zakłócenie jego wewnętrznej spójności, szczególnie gdy ta opiera się na szeroko pojętym morale. Ciągły atak z wielu stron, nawet gdy jest przeprowadzany przy niewielkiej „sile ognia", czyni skoordynowaną obronę niezwykle trudną, odcina wroga od zapasów i dróg komunikacji, przede wszystkim jednak wywołuje u atakowanej strony stres, zwątpienie we własne siły oraz przekonanie, że „sprawy nie idą dobrze".

Historycznie rzecz ujmując, taktyka *swarmingu* występowała zwykle w dwóch postaciach, jako *cloud swarms* (*massed swarming*) lub *vapor swarms* (*dispersed swarming*). *Cloud swarms* ma miejsce wówczas, gdy jednostki swarmingowe przybywają na miejsce bitwy jako zwarta masa, a następnie rozpadają się na pojedyncze części, by dokonać zbieżnego ataku z wielu stron na wrogi cel. Z *vapor swarms* mamy zaś do czynienia wówczas, gdy jednostki są od samego początku rozproszone po całym obszarze operacji, następnie zaś zbiegają się w polu bitwy i atakują, nie formując przy tym jednolitej masy[18]. Do XX w. dominującą formą *swarmingu* był *cloud swarming*, który nie wymagał od atakujących jednostek „bycia w nieustannym ze sobą kontakcie". Wynalazek łączności radiowej spowodował, że *swarming* w wykonaniu geograficznie rozproszonych jednostek stał się nie tylko możliwy, ale i niezwykle skuteczny. Patrząc na *vapor swarms* z perspektywy teorii organizacji, należy zauważyć, że jednostki swarmingowe zwykle przyjmowały postać sieci (np. oddziały w Somalii i Czeczenii) lub też były hybrydą sieci i hierarchii (np. U-booty w Bitwie o Atlantyk). Spośród sieciowych form organizacyjnych najbardziej popularną była zwykle sieć węzłowa (*hub network*) – w której jednostki lub grupy tychże tworzyły oddział zawiadywany przez lidera, który sam powiązany był w sposób mniej lub bardziej luźny z innymi liderami (węzłami). Liderzy wraz z podległymi im grupami tworzyli z kolei sieć multiwęzłową, która na poziomie taktycznym zwykle nie posiadała jednego wyróżnionego lidera. Jak słusznie zauważa Edwards, taka sieć, by osiągnąć operacyjną koherencję, musi spowodować, by „wszystkie węzły podzielały wspólne zasady i cele"[19].

Opisywany tu sposób działania jednostek swarmingowych wspomniani wyżej badacze odnosili przede wszystkim do sił funkcjonujących w zhierarchizowanym systemie rozkazów, choć niekoniecznie w sytuacyjnej od nich zależności (w warunkach ataku jednostki takie mogą posiadać nawet wysoki stopień autonomii). Jednak rozwój nowych technologii komunikacyjnych (w tym Internetu) oraz nowych sieciowych form organizacji pozwolił na wykorzystanie *swarmingu* przez siły, które nie tylko nie podlegają wytycznym „z góry", ale nawet nie są w jakiejkolwiek formalnej od siebie zależności. Zaadaptowanie tej taktyki przez rozmaite ugrupowania ekstremistyczne i terrorystyczne nie jest niczym dziwnym. Bez wątpienia można taką adaptację postrzegać nawet jako naturalną reakcję wynikającą z samego charakteru obranej przez nie formy organizacyjnej – sieć wszechkanałowa lub opór bez przywództwa.

[18] Por. S.J.A. Edwards, *Swarming and the Future of Warfare*, RAND Corporation, Santa Monica 2005, s. xvii.

[19] Tamże, s. 93.

 DOI: 10.55676/asi.v3i1.20

Sam mechanizm ataku swarmingowego w wykonaniu tych ugrupowań jest w zasadzie prosty. Informacje o celach (zawierające nazwę tych celów, lokalizację oraz sposób, w jaki powinno się owe cele „nękać") podawane są na najważniejszych portalach pełniących rolę „ideologicznego źródła" danego ruchu. Informacje te są następnie powielane na innych, „bratnich" portalach, silniej lub słabiej powiązanych ze „źródłem". Przepływ informacji dokonuje się tu głównie za sprawą sieci wielowęzłowej (portale internetowe) i wszechkanałowej (bezpośrednie kontakty uczestników ruchu). Po rozpowszechnieniu informacji o „celach i metodach" rozpoczyna się właściwy proces „nękania" (pulsowania), trwający wiele dni, tygodni, a nawet miesięcy (aż do osiągnięcia pożądanego rezultatu). W przypadku ugrupowań ekoekstremistycznych niewirtualny (dokonujący się w „realu") swarmingowy atak polega głównie na rozmaitych uderzeniach sabotażowych lub akcjach typu *sit-in*, które są dokonywane przez sieciowo skomunikowane, autonomiczne grupy lub jednostki i obliczone na sparaliżowanie aktywności przeciwnika poprzez wygenerowanie strat, czyniących jego działalność w znacznym stopniu nieopłacalną.

Wprowadzenie ataków swarmingowych do cyberprzestrzeni nastąpiło najprawdopodobniej na początku lat dziewięćdziesiątych XX w. za sprawą dwóch ugrupowań Critical Art Ensemble (Zespół Sztuki Krytycznej) oraz Electronic Disturbance Theater (Teatr Zakłóceń Elektronicznych). To ostatnie ugrupowanie udostępniło w 1998 r. 20 000 internautom, protestującym przeciw konfliktowi w Chiapas, program FloodNet w jego instalacji SWARM (rój), umożliwiając im przez dwa dni blokowanie stron www urzędu prezydenta Meksyku, amerykańskiego ministerstwa obrony oraz giełdy papierów wartościowych we Frankfurcie. W tym samym roku (16.09.1998 r.) Internetowa Dywizja Animal Liberation Front (Internet Division of the Animal Liberation Front) zapowiedziała zmasowaną kampanię, polegającą m.in. na atakach *denial of service*, atakach z użyciem wirusów, hakowaniu stron internetowych i niszczeniu danych, przeciwko tym, którzy przy użyciu Internetu prowadzą wykorzystujący zwierzęta biznes. Zapowiedź nie była czczą pogróżką. Niedługo po niej nastąpiła seria ataków skierowanych na firmy i instytucje badawcze, którym ALF przypisywała „antyanimalistyczne nastawienie". Dobrym przykładem może tu być zainicjowana przez ALF w latach 1998–1999 internetowa kampania, polegająca na zrzucaniu na serwer szwedzkiego instytutu badawczego Smittskyddinstitute (oskarżanego o prowadzenie eksperymentów na małpach) „bomb e-mailowych", co doprowadziło do całkowitego zawieszenia pracy serwera i w efekcie do sparaliżowania prac jednostki, czy ogólnoświatowa akcja grupy Animal Liberation-Tactical Internet Response Network, która zorganizowała za pośrednictwem Internetu w lutym 2001 r. internetowe *sit-in*[20] z użyciem programu FloodNet wobec największego akcjonariusza Huntingdon Life Sciences – Stephen Inc. of Little Rock z Arkansas, czym doprowadziła do zapchania i zamknięcia jego systemu[21]. We wszystkich tych zdarzeniach (a także w wielu innych)

[20] Istotą internetowego *sit-in* jest zablokowanie dostępu do danej strony internetowej innym użytkownikom sieci.

[21] Patrz: G. Martin, *Understanding Terrorism. Challenges, Perspectives, and Issues*, Thousand Oaks, London–New Delhi 2003, s. 393, patrz także: http://www.freerepublic.com/focus/fr/675422/posts [dostęp: 14.03.2011].

uczestniczyły jednostki i grupy z całego świata (choć głównie z Europy, Kanady i USA). Wydaje się mało prawdopodobne, by mogły znać się bezpośrednio, czy chociażby być ze sobą w bezpośrednim wirtualnym kontakcie.

Bez wątpienia *swarming* w wykonaniu współczesnych ugrupowań ekoekstremistycznych różni się znacznie od *swarmingu* tradycyjnego, opisywanego przez teoretyków wojskowości. Różnic jest co najmniej kilka, choć najważniejsze niewątpliwie dotyczą: własności atakowanego celu, charakteru powiązań jednostek uczestniczących w *swarmingu* oraz sposobu koordynowania przez nie działań. I tak na przykład w klasycznej postaci tej taktyki cel był zwykle celem aktywnym (militarnym) – świadomym zagrożenia, uczestniczącym w walce i co najważniejsze – mogącym wystąpić z bezpośrednią reakcją na atak. Cel ataku nowych swarmingowych jednostek, rekrutujących się spośród ekologicznych radykałów, ma charakter cywilny – z tego też względu nie tylko nie jest w stanie przeprowadzić „na własną rękę" ataku (czy kontrataku), ale nawet zapewnić sobie we własnym zakresie obrony. Z uwagi na nieograniczoną praktycznie ilość możliwych celów ataki swarmingowe nowego typu są w nieporównanie wyższym stopniu bezpieczniejsze dla strony atakującej od tych znanych z przeszłości, w których obydwie strony miały charakter wybitnie militarny i nastawione były na wzajemne zniszczenie. Poziom bezpieczeństwa jeszcze wzrasta, gdy ataki odbywają się za pośrednictwem sieci internetowej i przy użyciu botnetu.

W klasycznym *swarmingu* grupy przeprowadzające atak były powiązane zarówno formalnie, jak i taktycznie. Stosunkowo nieliczne, zorganizowane wokół zastanej struktury rozkazów, wykonywały z góry narzucone zadania i na bieżąco koordynowały przebieg akcji między sobą, jak również, mimo dość znacznej autonomii, porozumiewały się (przynajmniej okresowo) z „centrum". Współczesne jednostki swarmingowe, zorganizowane bądź to w sieć wszechkanałową, bądź też według modelu oporu bez przywództwa, rezygnują zarówno z nadrzędnej struktury rozkazów, jak i z wymogu koordynacji. Dzięki takiej rezygnacji jednostki te zyskują nieosiągalną w zasadzie dla uczestników klasycznego *swarmingu* własność, a mianowicie masowość. Własność ta sprawia, że dla przeciwnika jednostki swarmingowe są przynajmniej przed rozpoczęciem akcji niewidoczne (jednostką taką może być każdy). Ich mobilizacja zależy jedynie od siły ideologicznego impulsu, którego źródłem, jak napisałam wcześniej, jest internetowa sieć wielowęzłowa, niezwykle trudna do skontrolowania (portale pojawiają się i znikają).

6. WALKA Z WALKĄ SIECIOWĄ

Niezwykle trudno wyobrazić sobie skuteczne przeciwdziałanie wyłaniającej się na naszych oczach nowej formy *swarmingu* (opierającej się na bezbronności atakowanego celu i niezhierarchizowanej organizacyjnie strukturze atakujących), czy, ujmując rzecz nieco szerzej, nowej formy terrorystycznej aktywności. Trudno przede wszystkim wyobrazić sobie, by walkę z zdecentralizowanymi, autonomicznymi, sieciowo zorganizowanymi i wysoce zinformatyzowanymi jednostkami terrorystycznymi (grupami lub samotnymi wilkami) można było prowadzić za pomocą tradycyjnych metod

 DOI: 10.55676/asi.v3i1.20

przeciwdziałania, które opierają się w znacznej mierze na organizacyjnej inwigilacji czy wywiadzie agenturalnym (środkach służących rozpoznaniu grupy, rozpracowaniu jej struktur, poznaniu zamiarów) oraz na policyjnych bądź militarnych działaniach operacyjnych (zmierzających do zniszczenia grupy, bądź przynajmniej udaremnienia jej planów). Skoro stare metody nie do końca się już sprawdzają, poszukiwać trzeba metod nowych, bardziej dostosowanych do zmian, jakie w ostatnich czasach nastąpiły.

Opracowanie zestawu tych metod jest oczywiście zadaniem specjalistów. W tym miejscu chciałabym jednak krótko nakreślić kierunki pożądanych przeobrażeń, które winny uwzględniać istotę zmian w sposobie prowadzenia walki oraz w strukturach organizacyjnych przeciwnika. Trzeba wziąć pod uwagę zwłaszcza dwie kwestie:

1. Po stronie przeciwnika zaangażowane są w walkę siły niehierarchiczne, sieciowe, często zorganizowane na wzór oporu bez przywództwa, z którymi trudno sobie poradzić za pomocą klasycznych, hierarchicznych struktur.
2. Siły te zespolone są za sprawą walczących idei w wielowęzłową sieć internetową, od istnienia której w gruncie rzeczy zależą.

Pierwsza z wymienionych kwestii skłania do rozważenia możliwości odejścia od postrzegania walki z terroryzmem jedynie poprzez pryzmat roli, jaką odgrywać w niej mogą siły zorganizowane hierarchicznie. Wiele wskazuje na to, że walka z nowym, sieciowym terroryzmem może być przegrana, jeśli oprzemy się w niej jedynie na hierarchii i odgórnym zarządzaniu. W takim przypadku bowiem nie będziemy w stanie ogarnąć całego spektrum zdarzeń, ani też wystarczająco plastycznie na nie reagować. Problem ten zauważyli już pod koniec lat dziewięćdziesiątych XX w. John Arquilla i David Ronfeld, którzy w tekście poświęconym walce sieciowej, napisali, iż „strukturom hierarchicznym będzie bardzo trudno walczyć z sieciami”[22]. W podobnym tonie wypowiada się Toby Blyth, stwierdzając, że „użycie hierarchicznej siły przeciwko quasi-terrorystycznym sieciom może nie być szczególnie efektywne”[23]. Wiele wskazuje na to, iż rządzący, którzy chcą się obronić przed walką sieciową, muszą przejąć organizacyjny model i strategię swoich przeciwników. Jest to w praktyce zadanie trudne do przeprowadzenia. Trudno sobie bowiem wyobrazić, by siły z natury swej hierarchiczne mogły się przekształcić w swoje zaprzeczenie. Jednak być może „zaadaptowanie struktur przeciwnika” nie musi się odbywać na drodze transformacji hierarchii w sieci. Może wystarczy tu w zupełności struktura hybrydowa, a więc złożenie sieci i hierarchii. Symptomów takiego, spontanicznego jak na razie, złożenia doszukiwać się można chociażby w cyberataku na Estonię z udziałem rosyjskich hakerów (w tym tych związanych z prokremlowską młodzieżówką „Nasi”), we współpracy między cywilnymi ochotnikami a siłami zbrojnymi w Estonii po ataku cybernetycznym na infrastrukturę tego kraju, w działaniach serbskich hakerów podczas wojny w Kosowie, czy w niektórych przykładach kooperacji pomiędzy organizacjami typu „*watchdog*” a rządem Stanów Zjednoczonych.

[22] J. Arquilla, D. Ronfeld, *The Advent of Netwar: Analytic Background*, „Studies in Conflict & Terrorism” 1999, nr 22, s. 199–200.

[23] T. Blyth, *Terrorism as Technology: a Discussion of the Theoretical Underpinnings*, [w:] *Technology and Terrorism*, red. D. Clarke, Transaction Publischers, New Brunswick–London 2004, s. 45.

7. PODSUMOWANIE

Kluczowe znaczenie wielowęzłowej sieci internetowej dla funkcjonowania tajnych sieciowych struktur, przy jednoczesnej niemożności ich destrukcji, każe myśleć o niej jako o potencjalnym celu antyterrorystycznych działań. W grę wchodzą tu zarówno jej monitoring, jak i samo zwalczanie źródeł walczących idei. Taki monitoring opierać się może albo na bezpośrednim badaniu stron i portali internetowych przez odpowiednio wyszkolonych specjalistów, albo na systemach analizy danych teleinformatycznych w Internecie, takich jak: *carnivore*, *keyboarding logging systems* czy *echelon*. Mimo licznych kontrowersji związanych z funkcjonowaniem tych systemów są one źródłem konkretnej wiedzy zarówno na temat aktywności grup ekstremistycznych, jak i krążących w Internecie idei. Zwalczanie źródeł walczących idei jest sprawą o wiele trudniejszą. Samo ich zamykanie na dzień dzisiejszy nie wydaje się być dobrym rozwiązaniem – z uwagi chociażby na łatwość, z jaką mogą się odradzać (choć okresowo takie działanie na pewno ograniczyłoby przepływ idei i środków). Same państwa mają też, z racji specyfiki cyberprzestrzeni oraz problemów prawnych, ograniczoną możliwość dokonywania cenzury internetowych treści czy likwidacji „niepokornych stron". Dlatego czynić to usiłują za nie, często z naruszeniem prawa, rozmaite podmioty pozapaństwowe[24]. Ich aktywność ma jednak, póki co, bardzo ograniczony charakter. W tej sytuacji pewnym rozwiązaniem pozostaje, jak się wydaje, oddziaływanie pośrednie – za pośrednictwem konkurencyjnych źródeł wywierania ideologicznego wpływu, jak również szeregu działań o charakterze prewencyjnym, zmierzających do niwelowania efektów szeroko rozumianego wykluczenia, które współcześnie generowane są w przeważającej mierze przez procesy globalizacji.

BIBLIOGRAFIA

Artykuły i monografie

Arquilla J., Ronfeldt D., *The Advent of Netwar (Revisited)*, [w:] *Networks and Netwars: The Future of Terror, Crime, and Militancy*, red. J. Arquilla, D. Ronfeldt, RAND Corporation, Santa Monica 2001.

Arquilla J., Ronfeldt D., *The Advent of Netwar*, RAND Corporation, Santa Monica 1996.

Arquilla J., Ronfeldt D., *The Advent of Netwar: Analytic Background*, „Studies in Conflict & Terrorism" 1999, nr 22.

Arquilla J., Ronfeldt D., Zanini M., *Networks, Netwar, and Information-Age Terrorism*, [w:] I.O. Lesser, B. Hoffman, J. Arquilla, D. Ronfeldt, M. Zanini, B.M. Jenkins, *Countering the New Terrorism*, RAND Corporation, Santa Monica 1999.

Beam L.R., *Leaderless Resistance*, „The Seditionist" 1992, nr 12.

[24] W roku 1997 operator internetowy Institute for Global Communications, w wyniku długotrwałych ataków na jego konta mailowe, został zmuszony do likwidacji strony wspierającej baskijską ETA.

 DOI: 10.55676/asi.v3i1.20

Blyth T., *Terrorism as Technology: a Discussion of the Theoretical Underpinnings*, [w:] *Technology and Terrorism*, red. D. Clarke, Transaction Publischers, New Brunswick–London 2004.

Cohen F., *Terrorism and Cyberspace*, „Network Security" 2002, nr 5.

Edwards S.J.A., *Swarming and the Future of Warfare*, RAND Corporation, Santa Monica 2005.

Gerlach L.P., Hine V.H., *People, Power, Change: Movements of Social Transformation*, Bobbs-Merrill, Indianapolis 1970.

Hoffman B., *Oblicza terroryzmu*, Bertelsmann Media, Warszawa 2001.

Lia B., *Globalisation and the Future of Terrorism. Patterns and Predictions*, Routledge, London–New York 2005.

Martin G., *Understanding Terrorism. Challenges, Perspectives, and Issues*, Thousand Oaks, London–New Delhi 2003.

Pickerill J., *Cyberprotest. Environmental Activism Online*, Manchester University Press, Manchester–New York 2003.

Zanini M., Edwards S.J.A., *The Networking of Terror in the Information Age*, [w:] *Networks and Netwars: The Future of Terror, Crime, and Militancy*, red. J. Arquilla, D. Ronfeldt, RAND Corporation, Santa Monica 2001.

Źródła internetowe

Arquilla J., Ronfeldt D., *Networks and Netwar*, http://radio-weblogs.com/0107127/stories/2002/09/10/networksAndNetwar.html [dostęp: 19.02.2011].

Arquilla J., Ronfeldt D., *Swarming and the Future of Conflict*, RAND National Defense Research Institute, Santa Monica 2000, http://www.analytictech.com/mb021/swarming%20DB311.pdf [dostęp: 18.02.2011].

Barabàsi A.L., Bonabeau E., *Scale Free Networks*, „Scale Free Networks" may 2003, http://www.scribd.com/doc/6152736/Scale-Free-Networks-and-How-they-impact--everything-by-AlbertLaszlo-Barabasi-and-Eric-Bonabeau [dostęp: 16.12.2009].

Edwards S.J.A., *Swarming on the Battlefield: Past, Present, and Future*, Rand Corporation, 2000, http://www.rand.org/pubs/monograph_reports/MR1100.html [dostęp: 16.02.2011].

Marighella C., *Minimanual of the Urban Guerilla*, Paladin Press, Boulder 1975, http://www.latinamericanstudies.org/marighella.htm; http://www.investigatingtheterror.com/documents/files/Mini-Manual%20of%20the%20Urban%20Guerrilla%20-%20Carlos%20Marighella%20(1969).pdf [dostęp: 18.02.2011].